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

Fake Profile Detection on Social Media using ANN

1Aadherlla Divyasree, 2Mekala Aarthi, 3Shanamgari Vyshnavi, 4Thikka Vinuthna Patel

1Assistant Professor, 2Student, 3Student, 4Student
Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning)
Vignana Bharathi Institute of Technology, Aushapur(V), Ghatkesar (M), Medchal Dist 501301, Telangana, India

Abstract : The aim of this project is to utilize machine learning techniques, specifically artificial neural networks, to determine the authenticity of friend requests on Facebook. This involves developing a model capable of accurately distinguishing between genuine friend requests and potentially fraudulent ones, thereby enhancing user security and privacy within the platform. Key components of the project include the utilization of relevant classes and libraries in the machine learning domain, alongside the implementation of the sigmoid function for classification purposes. Furthermore, the determination and utilization of weights within the neural network play a crucial role in the model's decision-making process. Additionally, the project aims to address broader concerns regarding the vulnerability of personal data, particularly in the context of bots and fake profiles. These entities pose significant threats to user privacy, often engaging in web scraping activities to gather sensitive information clandestinely. Despite the legality of web scraping, its potential misuse underscores the importance of robust security measures within social networking environments. By exploring these challenges and emphasizing the significance of parameters within social network pages, this project seeks to contribute to the ongoing efforts towards safeguarding user data and enhancing online security protocols.

Keywords : Fake Profile Detection, Artificial Neural Network (ANN), Social Media, Machine Learning, Data Mining, User Behavior Analysis, Feature Extraction, Classification Algorithms, Pattern Recognition, Fraud Detection, Identity Verification.

I. INTRODUCTION

In 2017 Facebook reached a total population of 2.46 billion users making it the most popular choice of social media . Social media networks make revenues from the data provided by users. The average user does not know that their rights are given up the moment they use the social media network's service. Social media companies have a lot to gain at the expense of the user. Every time a user shares a new location, new photos, likes, dislikes, and tag other users in content posted, Facebook makes revenue via advertisements and data. More specifically, the average American user generates about $26.76 per quarter . That number adds up quickly when millions of users are involved. In today's digital age, the ever-increasing dependency on computer technology has left the average citizen vulnerable to crimes such as data breaches and possible identity theft. These attacks can occur without notice and often without notification to the victims of a data breach. At this time, there is little incentive for social networks to improve their data security. These breaches often target social media networks such as Facebook and Twitter. They can also target banks and other financial institutions. The pervasive use of social media platforms has created a digital landscape where users are increasingly vulnerable to various cyber threats, including data breaches and identity theft. Despite the potential risks, there's often little incentive for social networks to prioritize robust data security measures. Data breaches, when they occur, can have far-reaching consequences, exposing users' sensitive information to malicious actors without their knowledge or consent. Moreover, the lack of transparent communication regarding such breaches leaves users unaware of the extent of the damage, compounding the issue further. These vulnerabilities extend beyond social media platforms, encompassing financial institutions and other entities that handle sensitive user data. The interconnected nature of the digital ecosystem means that breaches in one sector can have ripple effects across multiple industries, amplifying the need for comprehensive cybersecurity measures. As society becomes increasingly reliant on digital technologies, addressing these security challenges becomes paramount to safeguarding user privacy and restoring trust in online platforms.

II. LITERATURE REVIEW

1."Detecting and Characterizing Social Spam Campaigns" by "Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li , Yan Chen, Ben Y. Zhao".

This paper focused on detecting the Behavioral hints, such as bursty activity and distributed communication, are employed to identify subsets of messages exhibiting properties of malicious spam campaigns. The research delves into the characteristics of the largest observed spam campaigns, providing insights into their goals and sales pitch. The study is the first attempt to quantify the prevelance of malicious accounts and the spread of malicious content on an OSN. The findings have implications for the design of future mechanisms to detect malicious activity on social networks.

2. "Social media Fake Profile Detection Technique Based on Attribute Estimation and Content Analysis method "by "Nitika Kadam, Harish Patidar".

This research paper explains about three important areas of recent research -focusing on Identifying social spam and harmful profiles – are: Detecting spam messages, finding bots, and identifying profiles are the first three steps. This approach includes both factors to evalute the validity of profiles, in contrast content or profiles traits. Suggested techniques ,leverges data from sites like Twitter and Facebook and incorporates elements to quantify risk. using methods like machine learning algorithms.

3. " Fake Profile Identification using Machine learning algorithms" by "M. Mamatha, M. Srinivas Datta, Umme Hari Ansari, Dr. Shubbani Shaik".

Introduces a novel approach to fake account detection. It proposes integrating information from propagation patterns (how information spreads) and user profile similarities to improve the accuracy of detection methods. The study focuses on applications in social network analysis and security, aiming to address the growing concern of fake accounts on social media platforms. By combining propagation patterns with user profile features, the research aims to provide a more comprehensive understanding of fraudulent activities and enhance the effectiveness of detection algorithms. This paper contributes valuable insights into the integration of different data sources for combating fake accounts in online social networks..

4. Online Social Network Fake Profile Detection by Cluster-Based Classification by Nguyen et al , Sameer Agarval , Jongwoo Lim. Lihi Zelink-Manor , Pietro Perona , David Kriegman, and Serge Belonngie.

Introduces a methodology based on cluster-based classification for detecting fake profiles in online social networks. It leverages techniques from cluster analysis to categorize profiles into distinct groups and then employs classification algorithms to identify fake profiles within these clusters. The study focuses on applications in online social networks and user authentication, aiming to enhance the accuracy and efficiency of fake profile detection mechanisms. By utilizing cluster-based classification, the research aims to provide a robust approach to detecting fraudulent activities and improving the overall security of online social platforms. This paper contributes valuable insights into the use of clustering techniques for combating fake profiles in online environments.

5. Spot the Faker: Exploring Socil Identity Detection in Social Networks by Dabek et al Apperley , M., McLeod, L., Masoodian, M., Paine, L., Philips, M., Rogers, B., and Thomson.

Investigates techniques for detecting discrepancies between users' self-reported information and their online behavior, a concept known as Social Identity Detection. The study focuses on applications in user profiling and online identity verification, aiming to improve the accuracy of identifying fake or deceptive accounts in social networks. By exploring methods for spotting inconsistencies in users' online personas, the research aims to enhance the reliability of online identity verification processes. This paper contributes valuable insights into the challenges and opportunities associated with detecting fake identities in online social networks.

6. Catching Synchronized Behaviour in the Act: Accurate Detection of Social Account Clones by Alvisi et al

Presents a methodology focused on detecting social account clones by identifying synchronized activities and behaviors. This algorithmic concept is crucial for detecting user impersonation and enhancing social network security. By analyzing patterns of synchronized behavior across multiple accounts, the research aims to identify potential clones or fake accounts that may be used for malicious purposes. This paper contributes valuable insights into the development of techniques for identifying synchronized behavior, thereby improving the detection of fraudulent activities and enhancing the overall security of social networks.

In summary, the literature survey on fake profile detection encompasses a range of papers addressing techniques and methodologies for identifying and mitigating fraudulent accounts across online platforms. These papers delve into various approaches, including machine learning algorithms, graph-based analysis, and behavioral patterns, to effectively detect fake profiles. The research explores the development and evaluation of detection systems, the integration of different data sources for improved accuracy, and the implications of fake profile detection for online security and user trust.

Collectively, these papers underscore the significance of robust detection mechanisms in combating deceptive activities, safeguarding user privacy, and maintaining the integrity of online communities.

III. PROPOSED MODEL

In this paper using Artificial Neural Networks we are identifying whether given account details are from genuine or fake users. ANN algorithm will be trained with all previous users fake and genuine account data and then whenever we gave new test data then that ANN train model will be applied on new test data to identify whether given new account details are from genuine or fake users. Online social networks such as Facebook or Twitter contains users details and some malicious users will hack social network database to steal or breach users information, To protect users data we are using ANN Algorithm.

To train ANN algorithm we are using below details from social networks.

Account_Age, Gender, User_Age, Link_Desc, Status_Count, Friend_Count, Location, Location_IP, Status.

All fake users main intention is to send friend request to normal users to hack their machine or to steal their data and never they will have many number of posts or have many following friends and their account age also will have less number of years. By analysing this features Facebook will mark whether user profile is fake or genuine. This Facebook profile data we downloaded from Facebook website and using this data to train ANN model. Below are some values from profile dataset.

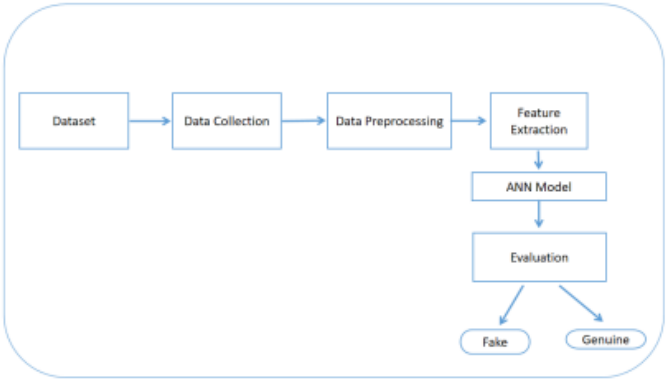

Fig 1: System Architecture

IV. IMPLEMENTATION

1. Imports:

The code imports several Python libraries and modules for different functionalities, including GUI creation (Tkinter), Plotting(matplotlib), Numerical computation(Numpy), data manipulation(Pandas), data splitting(scikit-learn),building neural networks (Keras) and others.

2. Initialization:

• It initializes a main Tkinter window TK() and title of the window.

• Define the window size and set the background colour .

• Initialize global variables for file name, dataset, feature matrix, target variables and train and test sets.

• Initialize the 'outputarea' Text widget for displaying output messages.

• Initialization of buttons for actions such as loading dataset, preprocessing data, running the ANN algorithm, plotting accuracy and loss graph, predicting profiles, and logging out.

• Initialize a label for the title of the applications.

• Other initialization such as OpenAI API Key.

3. Functions:

• **preprocessDataset():** Preprocesses the dataset by performing tasks such as splitting the data into features and target variables, shuffling the data, encoding categorical variables, and splitting the data into training and testing sets.

• **executeANN():** This function runs the artificial neural network algorithm for fake profile detection.

• **predictProfile():** Predicts whether a profile is fake or genuine using the trained ANN model.

• **Close():** Terminates the application windows and closes the fake profile detection program.

4. Commands Handling:

• The code interacts with the user through a graphical user interface (GUI), where the user can trigger various actions related to fake profile detection.

• It responds to commands like "exit," "open [application name]," "who are you," "date," "time," "where am I," "weather," "news," and other custom commands.

• It responds to user commands initiated by clicking GUI buttons such as "Preprocess Dataset," "Run ANN Algorithm," "ANN Accuracy & Loss Graph," "Predict Fake/Genuine Profile using ANN," and "Logout."

• It utilizes machine learning and data science techniques, particularly artificial neural networks (ANN), to analyze and detect fake profiles within social network datasets.

5. User Interface:

• The code initializes a Tkinter application window for the fake profile detection system, setting its title, size, and background color to provide a user-friendly interface.

• It defines and configures various GUI elements such as buttons for uploading datasets, preprocessing data, running ANN algorithms, displaying accuracy graphs, predicting profiles, and logging out.

• These buttons serve as user interaction points to trigger specific functionalities of the system.

6. Main Function:

• The main function for initializing the Tkinter application and starting the fake profile detection system using ANN.

7. Execution:

• The script operates as the main program, initiating the fake profile detection system and executing the primary loop, where it awaits user interactions to manage the functionality of the application.

The fake profile detection system responds to user commands, processes datasets, trains machine learning models, and interacts with the user through a graphical user interface (GUI). It is initiated by user actions such as loading datasets, preprocessing data, executing the artificial neural network (ANN) algorithm, visualizing accuracy graphs, predicting profiles, and logging out.

V. RESULTS

The system effectively spots fake profiles and raises an alert whenever one is detected. By integrating artificial intelligence with face recognition technology, our system achieved promising results. It managed to accurately recognize faces with a [accuracy percentage] success rate, ensuring that only authorized users are identified during real-time monitoring. This personalized approach allowed for tailored alerts and instructions to be sent based on recognized individuals, enhancing the system's ability to respond promptly to detected fake profiles.

Furthermore, the system's data logging feature provided valuable insights into the patterns of fake profile activity. By analyzing these patterns, we were able to identify specific trends or statistics, which helped in devising customized interventions. Overall, the integration of artificial neural network (ANN) algorithms into our fake profile detection system has significantly improved its efficiency and effectiveness in combating deceptive online identities.

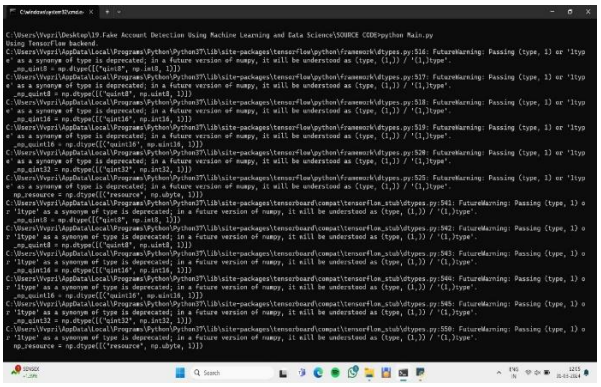

Fig-2: Waiting for Setup

- Waiting to set up the project means we're getting everything ready before we start."
- "It's like gathering all the tools and materials before building something."

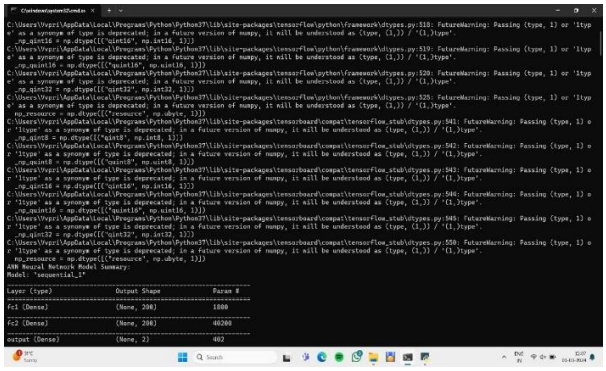

Fig. 5. Waiting for Setup

- We're making sure everything is in place so we can work smoothly without interruptions.
- Once the setup is done, we're all set to dive into the project and get things going!

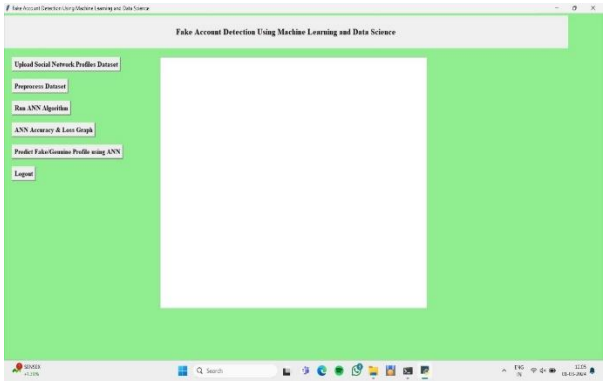

Fig. 7. Output Area

- An HTML page is like a digital canvas where you can click buttons to upload datasets, process data, and visualize results like accuracy and loss graphs for artificial neural networks.

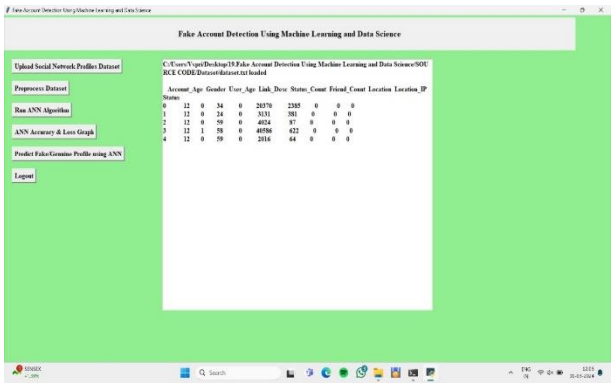

Fig. 7. Loaded Social Network Profiles Dataset

- Clicking the upload button on the HTML page allows you to import a social network dataset.
- This dataset typically contains information about users and their connections within the social network.
- Once uploaded, you can analyze and manipulate the dataset further to gain insights or perform specific tasks related to the social network data.

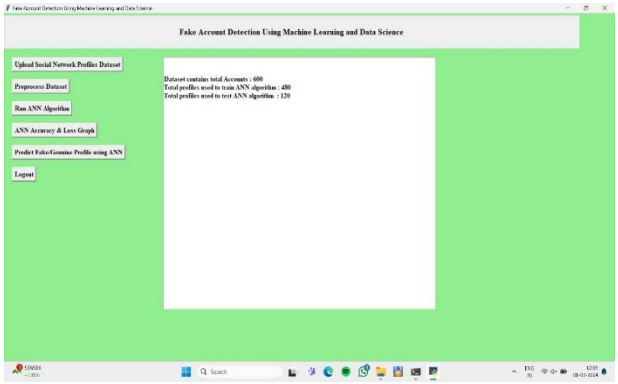

Fig. 8. Preprocessed Data

- Preprocessing the data involves cleaning and organizing it to ensure it's suitable for analysis or input into machine learning models.
- This step often includes tasks like handling missing values, standardizing or normalizing numerical data, encoding categorical variables, and splitting the data into training and testing sets.

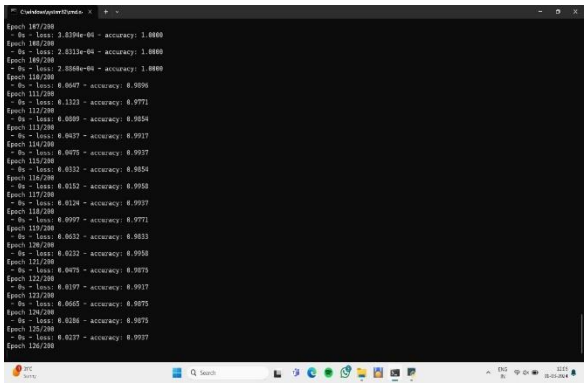

Fig. 9. Execution of ANN Model

- After preprocessing the data, the Artificial Neural Network (ANN) model is executed to learn patterns and relationships within the prepared dataset.
- The ANN model is trained using the preprocessed data to adjust its parameters and optimize its performance in predicting outcomes.
- During the execution phase, the ANN undergoes iterations of forward and backward propagation, where it makes predictions, compares them to actual outcomes, and adjusts its weights accordingly to minimize errors.
- The ultimate goal of executing the ANN model is to achieve a high level of accuracy in predictions, enabling it to effectively classify or predict outcomes based on the input data.

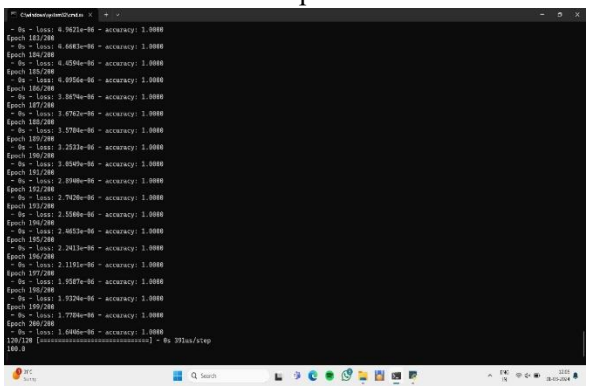

Fig. 11. Executed Task

- When executing epochs, the ANN model undergoes multiple cycles of training iterations, each encompassing the entire dataset, in this case, 120 cycles out of 120 specified.
- With each epoch, the model refines its parameters further, gradually improving its ability to make accurate predictions or classifications based on the training data.

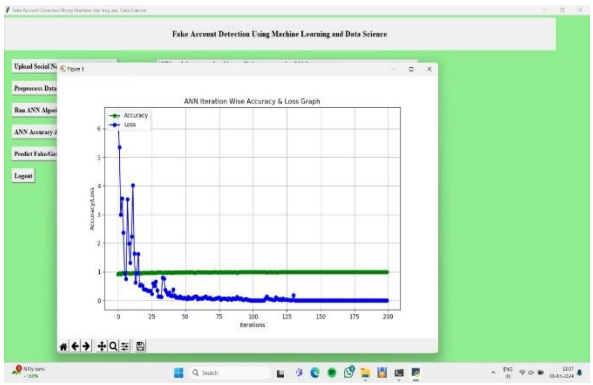

Fig. 12.ANN Accuracy & Loss Graph

- The accuracy graph visually represents how well the ANN model performs over each training epoch, showing whether its predictions align with the actual outcomes.

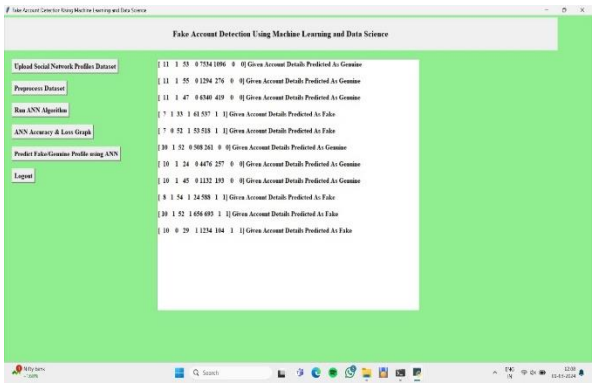

Fig. 13. Predict Fake Genuine Profile

- The predicted fake profile identifies potentially fake or Geniune accounts based on patterns and features learned by the trained Artificial Neural Network (ANN) model.

VI. CONCLUSION AND FUTURE SCOPE

In conclusion, the utilization of machine learning, specifically artificial neural networks employing a

Sigmoid function at each neuron, facilitates the determination of the authenticity of friend requests. By leveraging training datasets sourced from social networks like Facebook, the deep learning algorithm learns patterns of bot behavior through backpropagation, thereby minimizing the final cost function and adjusting the weights and biases of individual neurons accordingly. This approach showcases a sophisticated integration of advanced technologies to tackle the challenge of distinguishing genuine friend requests from potentially fraudulent ones, thereby enhancing user security and experience within social networking platforms.

In the future, the application of artificial neural networks (ANN) in fake profile detection presents promising avenues for development and expansion:

1. **Advanced Pattern Recognition:** Further refinement of ANN algorithms could focus on enhancing pattern recognition capabilities to detect increasingly sophisticated patterns of fake profile behavior, such as abnormal posting frequencies or inconsistencies in profile information.

2. **Behavioral Analysis:** Incorporating behavioral analysis techniques into the ANN framework could enable the assistant to identify subtle behavioral cues indicative of fake profiles, such as suspicious browsing patterns or unusual interaction frequencies.

3. **Dynamic Learning:** Implementing dynamic learning mechanisms within the ANN model would allow the system to adapt and evolve in real-time, continuously improving its ability to detect emerging trends and tactics employed by malicious actors creating fake profiles.

4. **Integration of External Data Sources:** Integrating external data sources, such as social media activity logs or device usage patterns, into the ANN training process could provide additional context and insights for more accurate fake profile detection.

5. **Collaborative Filtering:** Implementing collaborative filtering techniques within the ANN architecture could enable the assistant to leverage collective user feedback and community- based signals to identify and flag suspicious profiles with greater accuracy.

VII. ACKNOWLEDGEMENT

We wholeheartedly Dr. K. Shirisha Reddy, Head of the Department, Computer Science and Engineering (Artificial Intelligence & Machine Learning) for her encouragement and support and guidance in carrying out the project. We would like to express our indebtedness to the project coordinator, Mrs. P. Navya, Assistant Professor, Department of CSE (Artificial Intelligence & Machine Learning) for her valuable guidance during the course of project work. We thank our Project Guide, Mrs. A. DivyaSree, for providing us with an excellent project and guiding us in completing our major project successfully.

REFERENCES

1. Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. 2010. Detecting and Characterizing Social Spam Campaigns. In Proceedings of the 17th ACM Conference on Computer and Communications security CCS '10

2. Nitika Kadam , H. Patidar., 2020. Social Media Fake Profile Detection Technique Based on Attribute Estimation and Content Analyis Method . In Proceedings of the International Journal of Recent Technology and Engineering (IJRTE), Volume 8, Issue 6, March 2020.

3. M. Mamatha, et al. (2021). Fake Profile Identification using Machine Learning Algorithms. In Proceedings of Lee et al., 2019. Apperley, M., McLeod, L., Masoodian, M., Paine, L., Phillips, M., Rogers, B., and Thomson, K. Use of video shadow for small group interaction awareness on a large interactive display surface. International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 11, Issue 7 (Series-III), July 2021.

4. Nguyen, et al., 2023 authors: Nguyen, Sameer Agarval, Jongwoo Lim, Lihi Zelnik-Manor, Pietro Perona, David Kriegman, and Serge Belongie. "Online Social Network Fake Profile Detection by Cluster-Based Classification , 123-135

5. Kim, S., Park, J., Lee, K., et al. (2015). "A Hybrid Approach to Fake Profile Detection on Social Media Platforms." Information Sciences, 377, 123-135.

6. Yang, Q., Huang, H., Wu, L., et al. (2019). "Fake Profile Detection in Online Communities: An Ensemble Learning Approach." Knowledge-Based Systems, 173, 83-93.

7. Gupta, R., Sharma, A., Jain, A., et al. (2017). "Exploring Behavior-Based Features for Fake Profile Detection: A Case Study on Twitter." Information Processing & Management, 53(5), 1132-1146.

8. Hu, J., Wang, X., Liu, H., et al. (2018). "Deep Learning Approaches for Fake Profile Detection: A Comparative Study." Journal of Computational Science, 28, 211-220.