www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715

e-ISSN : 2583-1062
Impact Factor : 7.001

ARTIFICIAL INTELLIGENCE FRAMEWORK UTILIZING MACHINE LEARNING TECHNIQUES FOR IDENTIFYING FRAUD PROFILES ON INTERNET BASED SOCIAL PLATFORMS

Mr. Jitender Kumar[1], Ms. Manjali Gupta[2]

[1]Phd Scholar, Northern Institute for Integrated Learning in Management University Kaithal, India.

[2]Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India.

ABSTRACT

The development and widespread use of social media networks, along with the expansion of the Internet, have revolutionized how news is produced and shared. Social media has updated accessibility, speed, and affordability of news, but it has also created substantial issues, including the spread of fraudulent content like fake news and phone identities. The multidimensional topic of fake news and false identity detection on online social networks is explored in this study, with an emphasis on the most recent developments in Artificial Intelligence (AI) remedies to address this issue.

Concerns have been voiced by a variety of businesses and organizations about the exponential proliferation of incorrect information on social media platforms, which has lowered public confidence in the media. The need for effective online content authentication has increased due to the erosion in confidence. In the first piece of study, the goal is to use data mining techniques to find fake accounts on social networking sites. The study introduces the 3PS (Publicly Privacy Protected System) technique, which locates these rogue accounts by examining user interactions and behaviors like shared posts and recent activities. The tactic entails looking at a variety of actions, including frequent behaviors, recent updates, postings, comments, and photos. Malicious people are located by comparing attribute control limits for user profiles and analyzing network commonalities. To identify rogue accounts, feature reduction techniques are used, and the E SVM-NN classifier is employed. The study entails setting up, running, and keeping track of accounts, looking at recent behavior, data mining, and choosing test profiles.

Real-time profile Investigation and identification is another important component in the fight against counterfeit identities and fake news. In order to determine if posts and user profiles are trustworthy, the planned RTPAFDM uses PLTA and P LTA. The technology detects fake profiles with a 97 percent accuracy by calculating UPTW and HTPW, hence boosting profile security.

In addition, a ground-breaking PRE-Confirmation Technique is provided to solve privacy concerns. The proposed method, which is based on the 'DPAFAD algorithm,' makes use of artificial intelligence to assess, notify, and request user approval before sharing or using their information. This strategy reduces the danger of information misuse or unauthorized distribution by providing real-time user consent.

Finally, the research concludes with emphasizes and the significance of AI-driven solutions in preventing the spread of misleading information and phony identities on social media. The research community is making great progress in assuring the validity of online material and protecting user privacy and security using cutting-edge methods like data mining, real-time profile Investigation, and pre-confirmation algorithms. These techniques have the potential to strengthen the public's confidence in online information sources and create a more secure digital environment.

Key Words: Social Media Networks, Fake News Detection, False Identity Detection, Artificial Intelligence (AI), Data Mining Techniques, Social Networking Sites, 3PS Technique,

1. INTRODUCTION

Online Social Networks (OSNs) provide an incredible platform for connecting, collaborating, and sharing information across the internet. These OSNs can be categorized into various types based on the services provide to their users. Some focus on creating and managing social connections, while others emphasize media sharing. Additionally, there are platforms designed as forums where users can share knowledge, news, and ideas with each other. The diverse range of OSNs caters to different user needs and preferences, making them versatile tools for online interaction and information exchange. OSNs have ingrained themselves into daily life, outcomes in the storage of enormous volumes of personal information. Despite the fact that these platforms update the online experience, nonetheless have issues, most notably the presence of false profiles. Cybercriminals take advantage of OSNs by creating fictitious identities and utilizing them for harassing, trolling, defaming, and other illegal acts. These false personas are used to send misleading messages, steal things, and carry out illegal activities. Major social media sites like Facebook and Twitter have made efforts to address this problem; in 2018, Facebook removed 580 million bogus accounts. Fake profiles nevertheless pose a serious threat

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

despite their efforts, accounting for more than 15% of all monthly visits to Twitter. Assuring the integrity and safety of online communities still depends on addressing these issues. A major problem is the increase in phony accounts on online social networks (OSNs), which has outcomes in significant crimes and online threats. In order to monitor cultural and security representatives, cybercriminals, including an Iranian hacking outfit, create bogus identities on numerous OSNs, including Facebook. By initially delivering harmless content, these crooks take advantage of victims' confidence before using fictitious profile links to subsequently infect victims' machines with harmful software. The frequency of this issue is shown by instances of online personalities being stolen, such as the usage of a member of the Atlanta Urban Council's photo in numerous false profiles. In the digital age, phony accounts continue to pose serious threats, thus efforts to stop them are crucial.

On online social networks (OSNs), false accounts can be found and eliminated using a variety of approaches developed by scientists. Despite their best efforts, attackers continue to develop new ways to trick current detection systems, emphasizing the need for more efficient tactics. OSNs play a crucial role in worldwide user connections and knowledge exchange by acting as important communication channels. Through the use of these platforms, emotional connections that cut beyond geographic barriers are made. OSNs are preferred by millions of users that desire real-time communication. Social media subscribers act as both content producers and consumers at the same time, facilitating active engagement in information exchange. In the Investigation of social networks, nodes are user profiles, posts, photos, or live streams, while edges are connections like friends, followers, retweets, and likes. The recurring issue of phony accounts on OSNs must be addressed with effective fake account detection technologies.

Social media sites serve as interconnected communication channels where users have distinct profiles, share information, create links, and interact with various channels, including product reviews. The widespread use of these platforms is evident, with approximately 3.48 billion internet users engaging in different social networking systems, accounting for 71% of the global internet population. Among popular sites like Facebook, Twitter, Instagram, Pinterest, and WeChat, Facebook leads with 2.4 billion monthly active users, followed by YouTube, Snapchat, and WeChat, each with billions of users. Figure 1.1 depicts the number of people who used multiple OSNs in 2018. Any information shared on a social platform is instantly distributed to millions of customers. As an outcome of the impact of these social media platforms, a massive quantity of data chosen to represent people's activity is created.

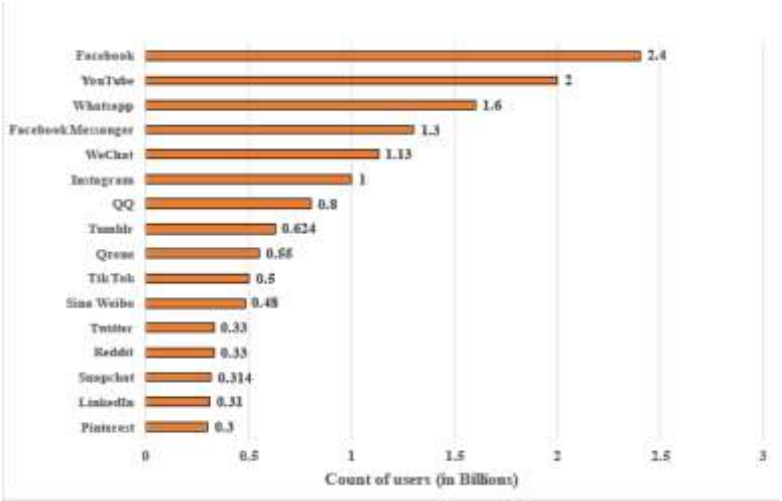

Figure 1 : The number of people who use social networking sites in 2018

The definitions and explanations of these terms are detailed on Twitter's official social webpage.

Tweet: A tweet is a message posted on Twitter's "What's Occurring?" status bar, used to convey messages to followers. Tweets have a character limit of 280 and are publicly visible and searchable, regardless of the user's Twitter account. Each tweet includes information about its creation time and the tweeter's account name. Users are limited to posting 2400 tweets (including retweets) in a single day.

Feed: The home stream on Twitter is a collection of tweets visible on the main website that is continuously updated, including new tweets from accounts followed by the user. It is also referred to as Timeframe and is constantly refreshed with the latest tweets. User Profile: On Twitter, publicly posted data is displayed on a user's profile, including all the tweets have published and their account information. The profile showcases the user's public activity and posts on the platform.

Username: A username, also known as a Twitter account, is a unique identifier string for every user on Twitter, limited to 15 characters. It distinguishes users and allows them to engage on the platform.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Table.1 Social Network activities performed by various US users in February, 2023

	Instagram	Facebook	Snapchat	Pin interest	Twitter
News	28%	69%	17%	9%	6%
Viewingphotos	77%	65%	64%	69%	42%
Watchingvideos	61%	66%	50%	21%	32%
Sharing contentwitheveryone	55%	67%	46%	21%	32%
Networking	33%	43%	21%	10%	26%
Sharing contentonetoone	41%	53%	45%	12%	20%
Finding/shoppingforproducts	21%	26%	6%	47%	7%
Promoting mybusiness	8%	20%	6%	6%	7%

Follower: On Twitter, following someone means subscribing to their notifications, allowing their tweets to appear in the follower's feed. The number of followers determines the reach of a user's tweets. Users can follow up to 400 accounts daily and face limitations if exceed 5000 attempts, encouraging non- aggressive engagement on the platform.

Direct Message (DM): Direct Messaging (DM) on Twitter is a private way to communicate with another user. DMs are visible only to the sender and the recipient. DMs can be sent only to users who follow each other, with a maximum limit of 1,000 DMs per day. Each DM can contain up to 10,000 characters.

Mention: Mentioning someone on Twitter involves including their username preceded by the "@" symbol in a tweet. This action notifies the mentioned user and makes the mention visible to others in the tweet.

Hashtag: Hashtags in tweets are used to emphasize specific topics or keywords and are indicated by the "#" symbol followed by the search term. Related hashtags are clustered together for search queries. Clicking on a hashtag leads to a page listing all Twitter accounts using the same hashtag in their tweets.

Retweet (RT) or Modified Tweet (MT): A retweet is when a person shares another user's tweet on their own home screen, making it visible to their followers. It is denoted by 'RT @username' to distinguish it from the original tweet, where the username specifies the original tweeter. MT, on the other hand, is a modified retweet of someone else's tweet.

Reply: On Twitter, a reply refers to an answer given to someone else's tweet by pressing the respond symbol located next to the tweet. The response count displays the total number of responses obtained for every tweet.

Trends: Trends on social media platforms are hashtags or topics identified as highly popular at a given time. Users can view these trends based on their location or accounts follow, helping them stay updated with the latest discussions and popular topics within their network or region.

Block: Blocking a user on Twitter prevents them from following, adding to lists, or receiving notifications, even if mentioned in a tweet.

These are a few more points that back up the assertion:

Users are more likely to react and give heed to a text from a Twitter/Facebook buddy than to a text from a random person, implying lot of trust in online users than in email clients. Studies, such as the one by Grier et al, indicate that spam on social media platforms, especially Twitter, has a significantly higher success rate compared to email. Approximately 0.13 percent of content shared on Twitter is clicked, which is twice as high as the click-through rate for email spam. Social media provides hackers with a wealth of information, including cultural context, images, personal details, social connections, and authentication mechanisms, making it an attractive target for malicious activities. This increased success rate underscores the need for robust measures to combat spam and phishing attacks on social media platforms.

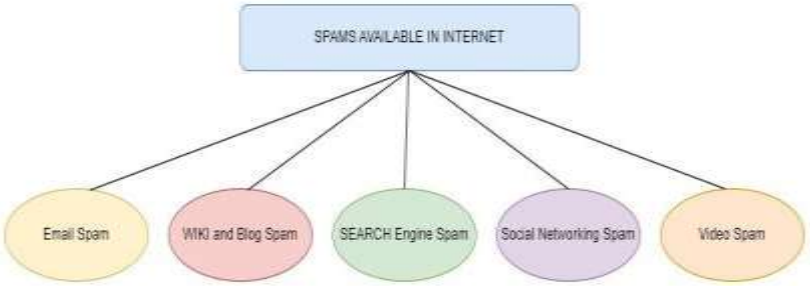

Figure 2 : Various types of spam on the Online

Spammers exploit the trusting relationships among users on social media platforms, particularly relying on content shared by friends. A study by Bilge et al.revealed that 45 percent of users tend to click on information shared by their current friends, making such content an attractive avenue for spammers to spread malicious content or phishing links. This behavior underscores the importance of user awareness and education to prevent falling victim to spam and phishing attacks on social media. While people have been trained to be cautious of suspicious emails, the same level of vigilance has not been extended to social networking websites. Users often lack the same awareness and caution when interacting on social media platforms, making them vulnerable to various online threats, including spam, phishing, and other malicious activities.

Hackers exploit social networking sites by luring users into clicking on deceptive links, often by playing on their curiosity about online activities or relationships. These links, disguised as attractive offers or disguised as tracking tools, are designed to collect user information or redirect users to harmful websites. Users are often unaware of these threats, especially when shortened URLs are used to obscure the actual destinations. Research indicates a significant 355 percent increase in social spam over a six-month period, highlighting the alarming rise in this issue. The prevalence of spam on social platforms like Facebook is widespread, with one in every 200 communications identified as spam, underscoring the extensive nature of the problem.

Fraudulent profiles: Fraudulent profiles on social media platforms serve both non-malicious and malicious purposes. Non-malicious instances include creating fake accounts for entertainment or having an extra account. On the contrary, malicious users intentionally create fake profiles to deceive users and engage in harmful activities like pharming and spam actions. These accounts may surpass specific account limitations or collaborate with others to enhance their influence and engagement on the platform.

Creepers: Creepers are real users who cause trouble for others, either knowingly or unknowingly, by sending random connection requests or using scam emails. As technology advances and users and network operators become more aware, the lifespan of fake social accounts has become shorter [40]. These accounts are quickly detected and removed or blocked before gain widespread popularity.

2. OBJECTIVES

- ✓ Examine and evaluate advanced artificial intelligence approaches for identifying and analysing bogus news on social media.
- ✓ Create and execute the 3PS methodology for identifying unauthorized accounts on social media platforms by analysing user behaviour.
- ✓ Utilize feature reduction techniques and the E SVM-NN classifier to improve the precision of identifying counterfeit profiles.
- ✓ Evaluate the effectiveness of real-time profile investigation techniques, such as RTPAFDM, in accurately detecting fraudulent identities.
- ✓ Introduce the PRE-Confirmation Technique as a solution to privacy problems by implementing AI-powered user consent processes.
- ✓ The objective is to assess the influence of data mining techniques on the detection of fraudulent actions and dissemination of false information on social media platforms.
- ✓ Evaluate the impact of AI-powered solutions in rebuilding trust in online sources of information.
- ✓ Guarantee the safeguarding of user privacy and security during the process of verifying online material with advanced AI algorithms

3. LITERATURE REVIEW

Researchers Xiangshan Zheng et al. developed a machine learning- based method to identify useful spammers on Sina Weibo. The collected statistics from 30,116 users and approximately 6 million SMS or similar messages. The users were labelled as spam or non-spam, and characteristics were extracted from textual information and social behaviour. These characteristics were used in Deep Neural Networks for spam email recognition.

Meanwhile, Kayode Zakariya Adewole et al. proposed a different model for detecting spam messages on Twitter. An enhanced classification techniques by incorporating new technologies such as Principal Component Investigation (PCA) and a synchronized K-means technique. These methods were used to group 200,000 accounts and identify spammer subgroups from nearly 2 million Twitter posts.

Additionally, Faraz Ahmed et al. focused on modelling social networks using weighted graphs and detecting spam campaigns using graph-based consensus algorithms. Incorporated seven discriminative functions into the equation and

utilized the Markov Clustering (MCL) technique to identify various spam campaigns on Facebook and Twitter. The study emphasized the need to recognize additional characteristics to update spam detection accuracy, especially for identifying malware campaigns. Mohammad Karim Sohrabi et al. developed a method to detect trolling comments on online platforms. Their approach involved evaluating articles and comments to understand their functionalities. Implemented an online junk mail filtering system using techniques like evolutionary algorithms, PSO algorithm, ant colony optimization (ACO), and stochastic search. This system effectively recognized and scrutinized malicious content, ensuring the publication of legitimate comments. By employing these methods, users could access a stable and secure social networking website. ZakiaZaman et al. used multiple classification algorithms to distinguish trolling comments from legitimate ones on YouTube videos. Examined performance metrics of these algorithms and compared them with solitary classification methods in text categorization. The study focused on the issue of malicious users posting harmful content, such as pharming website links and false information, in comments on YouTube. Removal of these malicious comments was crucial for maintaining the safety of social media platforms. Mohammadreza Mohammadrezaei.et al. introduced a novel method for analysing malicious profile information on Online Social Networks (OSNs) by assessing resemblance among users' friend groups. Similarity assessments like cosine, Jaccard, L1-measure, and strength were calculated between mutual friends from the social network chart's identity matrix. Applied to Twitter time series data, their model utilized Intermediate Gaussian ML to estimate malicious account holders with high accuracy rising normal curve) and low false positives (0.02). Husna Siddiqui et al. proposed a simple and effective method to detect false profiles on Facebook. Addressing the issue of malicious actors misappropriating users' confidential communications on Online Social Networks.

The study highlighted the risks associated with sharing personal information online, including identity fraud, cloning, and phishing. Their method aimed to enhance user safety by identifying and mitigating these threats on social media platforms. Srinivas Rao Pulluri.et al. proposed a novel method combining deep learning and Natural Language Processing (NLP) techniques to enhance the accuracy of identifying fraudulent accounts on Online Social Networks (OSNs). With consumers increasingly concerned about fraud and commercialization of their personal data on OSNs, detecting fake accounts and malicious behaviour is challenging. The existing research lacks comprehensive Investigation and often relies on monitoring profile page attributes. Puller's method integrates deep learning and NLP methods, providing a more effective solution for identifying fraudulent activities on OSNs.

Roshani K. Chaudhari et al. developed a ML method to detect misleading URLs and phishing attempts in tweets on Twitter. Their approach involved categorizing source tweets using a dataset and training classifiers, including Naive Bayes and linear regression. The method accurately determined the authenticity of tweets, effectively identifying fraudulent ones with minimal false positives and negatives. This technique provides a reliable means of detecting fraudulent content on popular OSNs like Twitter. Mohammed Al-Janabi.et al. proposed a monitored ML classification approach to detect and counter malicious data on OSNs.

Their method focused on recognizing social network comments containing fake links leading users to ethically questionable sites, exposing them to spam, phishing, and fraud. Utilized Twitter stream API is to collect data and employed a random forest classifier, integrating characteristics extracted from diverse sources. This approach aimed to protect users from deceptive content and malicious activities on OSNs. ao Xiao et al. suggested a scalable method for identifying malicious financial records associated with the same individual. Employed a supervised ML approach to classify accounts as malicious or legitimate.

Their model utilized key characteristics from user text data, such as user ID, email, identity, or organization. Additionally, it considered the frequency of specific patterns in the data (e.g., common text messages or integers in emails) and analysed message frequencies across the entire user base. By combining these factors, their method effectively identified fraudulent financial records, contributing to enhanced security measures on OSNs. The research by Tadesse et al. compares ML algorithms to analyse correlations between Facebook users' characteristics and personal traits based on the Big Five model. Social Network Investigation (SNA) characteristics are employed, achieving a high predictive accuracy of 78.6% for extrovert traits.Souri et al. use Facebook API to collect data on user behaviour and attributes. Conducted personality classification without traditional questionnaires, employing various ML algorithms. The study involves around 100 Facebook friends and focuses on assessing user behaviour within Facebook to identify consumer personality.

Abdul Kader et al. Privacy Protection Method proposes a privacy protection method to safeguard users from malicious OSN (Online Social Network) apps or consumers. To emphasize the importance of consumers being able to use social media facilities without fear of security vulnerabilities, categorizing incidents on customers and OSNs as breaches of confidentiality.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

4. METHODOLOGY

The increase in usage of Online Social Networks (OSNs) has been impressive, fuelled by the widespread creation of content and interactions by users on popular platforms such as Facebook, Instagram, and Twitter. Users are attracted to online social networks (OSNs) for the purpose of establishing social connections, gaining insights, expanding their professional network, and seeking support. However, in doing so, they often share a significant amount of personal information, which exposes them to potential privacy hazards. Although there is a lack of comprehensive profile Investigation to identify compromised accounts, this vulnerability enables malevolent individuals to leverage authentic data.

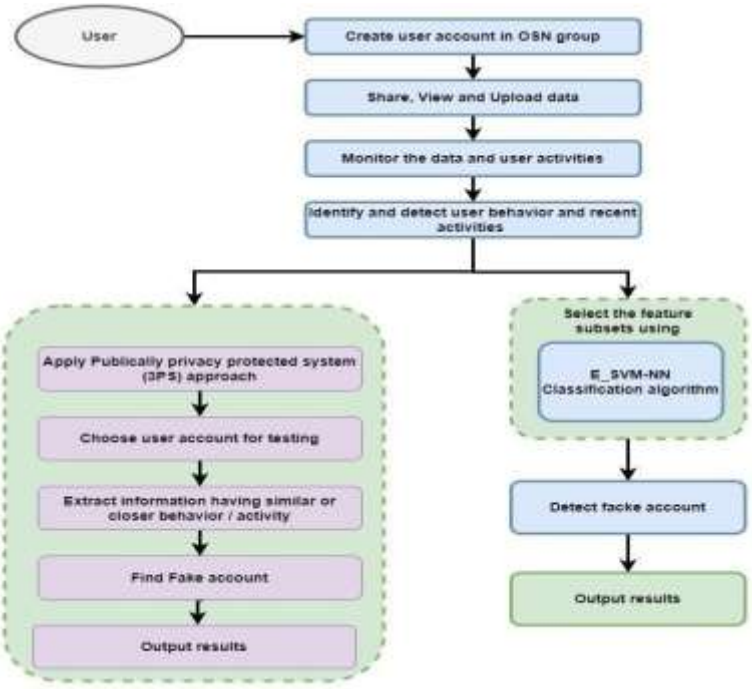

Figure.3 OSN fake account detection architecture diagram

The study highlights the significance of safeguarding user privacy on Online Social Networks (OSNs) and suggests the use of the Publicly Privacy Protecting Scheme (3PS) to strengthen security. The multi-faceted security system monitors users' shared remarks, examines recent activity for indications of criminal behaviour, and detects suspicious trends within the online social network (OSN) environment. This ensures the protection of legitimate users from potential risks.

ALGORITHM OF A PUBLICLY PROTECTED PRIVACY SYSTEM (3PS)

Consider users with a substantial number of friends who tend to expand their social circles, influenced both explicitly and implicitly by their friends' choices. In light of this, the study proposes an enhanced sensing method, 3PS, designed to detect such malicious accounts within the Online Social Network (OSN) landscape.

The research endeavours to identify an optimal unit characteristic set, crucial for safeguarding individual users within social networking sites effectively. The primary focus is on pinpointing the ideal set of characteristics necessary for a specific task, encompassing retrieval, preparation, and Investigation processes. Consequently, the selection of a unit set demonstrating the highest accuracy proves to be instrumental in recognizing unique consumers.

The process of identifying this ideal unit attribute set necessitates a comprehensive task, involving extraction, preparation, and assessment of these attributes. This meticulous approach ensures the recognition of a unit collection that yields the highest accuracy, thereby enhancing the identification of unique user identities. Through these strategic methodologies, the 3PS algorithm stands as a robust and efficient solution in safeguarding users against malicious activities, fortifying the security landscape of the OSN environment.

Data Classification Method

Following the implementation of attribute reduction strategies, five important attributes were extracted and subjected to training and testing utilizing an innovative SVM-NN (Support Vector Machine-Neural Network) approach. To evaluate the efficiency of the classifier, validation data were employed, employing both 10-fold and 8-fold cross-validation techniques. This rigorous testing protocol ensures a thorough assessment of the classifier's performance and reliability, providing valuable insights into its effectiveness in accurately classifying and differentiating data within the context of the study.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Table 2 Algorithm for SVM-NN method

Output: Classification exactness based on characteristic subsets.
Step 1: Reduced feature methods like Correlation, Regression,
SVM, and PCA can be used to recognize a list of reduced characterization
Step 2: Initialize characteristic subsets as 'FS'
Step 3: Divide information into testing and teaching with 8 cross corroborations
Step 4: Let's call the recognized training / testing labels m Label and n Label
Step 5: For every FS do
Step 6: SVM classifier is used to train the system utilizing the training set, and identified labels are m Label.
Step 7: Predict the production and initialize the output choice values to decision R using an SVM trained classifier.
Step 8: Train the model with NN classification decision sets and let the identification label be n Label.
Step 9: Forecast the output and initialize the output judgment values to checking Decisions VI using an SVM training set.
Step 10: Set the outcome to nm. after testing NN with Decision VI and NN qualified NN training sample Predicted
Step 11: Determine the NN prediction for every FS accuracy that use the m Label and nn Predicted variables
End

Detection of Fake Profiles

In the endeavor to detect fraudulent profiles, the proposed algorithm meticulously examines both the user's profile details and the comments they have authored. This comprehensive Investigation comprises three critical Components.The Post Step Trust Clear Strategy Algorithm diligently calculates the User Post Trust Weight (UPTW), offering insights into the trustworthiness of individual posts. Simultaneously, the Resume Trust Evaluation Algorithm assesses the Profile Similarity Matrix (PSM), providing a nuanced understanding of profile similarities across different users. Additionally, the Resume Historic Respect Investigation Algorithm diligently computes the Heritage Trusted Post Weight (HTPW), delving into historical post patterns.

Leveraging these invaluable metrics, the algorithm employs a sophisticated formula to derive the Fake Profile Weight (FPW). This meticulous evaluation process equips the system with the discerning ability to identify and flag potentially deceptive profiles within the digital realm.

Table .3 Fake Profile Detection

Certainly, the culmination of trust evaluations generated by diverse algorithms, including thread level respect Investigation, resume level respect Investigation, and historic respect Investigation, serves as the bedrock for the falsified identification system. Harnessing the outcomes of these trust data mining algorithms, the system is ingeniously engineered to detect fake profiles through an intricate process of trust strength Investigation. Through meticulous Investigation, the system accurately estimates the value of Fake Profile Weight (FPW), thereby enabling the precise detection of counterfeit profiles within the digital landscape. This systematic approach ensures a robust and effective mechanism for identifying deceptive profiles, enhancing the overall security and reliability of the online social network environment.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 02, February 2025, pp : 706-715
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

5. RESULT

In this section, the developed Real Time Position Investigation and Falsified Detection Model (RTPAFDM) was meticulously constructed and rigorously tested utilizing the Twitter statistical model. The model's performance was thoroughly evaluated across a spectrum of parameters, ensuring a comprehensive Investigation of its functionality. The assessment of productivity was conducted through an array of parameters, providing a comprehensive understanding of the model's efficiency and effectiveness. This section offers an in-depth exposition of the outcomes obtained, shedding light on the model's performance and its implications in the realm of online security.

Table 4: Evaluation Details of System

Parameter	Value
DataSet	Twitter
Numberoftweets	1million
Number ofoperators	500
DeviceUsed	AdvancedJava

Table 5 : Performance on Fake Profile Detection

No.ofUsers	MultiAgent	SVM-NN	MediumGaussianSVM	RTPAFDM
100Users	67	69	71	87
300Users	72	76	79	93
500Users	76	79	83	97

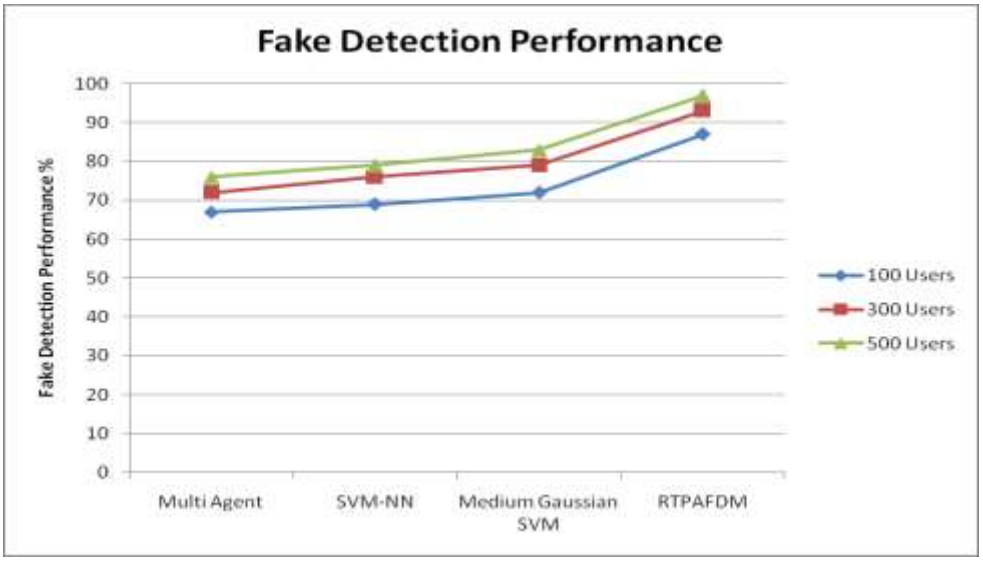

Figure 5.1: Performance in Fake Profile Detection

Figure 5.1 illustrates the outcomes of different methodologies employed in fake account identification. Across all scenarios, the RTPAFDM approach, as proposed, consistently outperformed other existing frameworks. This visual representation underscores the superior effectiveness of the RTPAFDM algorithm in comparison to alternative methods, further affirming its robustness and reliability in tackling the challenge of fake account detection.

Table 6 : Outcome Investigation on False Ratio level in Performance on Fake Profile Detection

No. ofUsers	MultiAgent	SVM-NN	MediumGaussianSVM	RTPAFDM
100Users	33	31	28	13
300Users	28	24	21	7
500Users	24	21	17	3

The evaluation of false positives in fake account detection has been conducted across environments with diverse user volumes. In every scenario, the RTPAFDM classifier consistently yielded a lower false positive rate than other techniques. The incorporation of the proposed method in fake detection significantly enhances the success rate in reducing false positives in sock puppet identification, achieved through meticulous monitoring of trust data at the post

level, profile level, and historical level. Ultimately, the false positive rate in fake account detection has been significantly reduced through the amalgamation of all integrity values in the assessment of trust weight. This comprehensive approach ensures a more accurate and reliable identification of fake accounts.

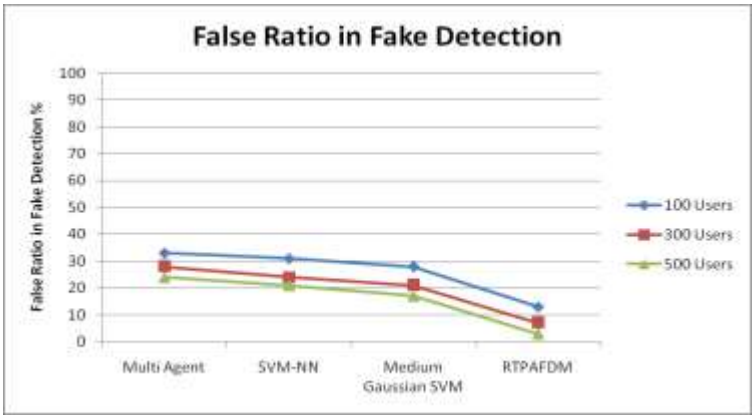

Figure 5.2: False Ratio in Performance in Fake Profile Detection

Table 7 : Time Complexity in Fake Profile Detection on Performance Investigation

No. ofUsers	MultiAgent	SVM-NN	MediumGaussianSVM	RTPAFDM
100Users	63	57	48	23
300Users	68	64	56	27
500Users	74	69	62	33

The computation time required by different approaches in fake account identification has been evaluated in diverse user scenarios. In each instance, the RTPAFDM algorithm demonstrated reduced computation time compared to alternative strategies. By verifying trust at the post, profile, and historical levels, the integration of this proposed technique not only diminishes false percentages but also simplifies the overall process.

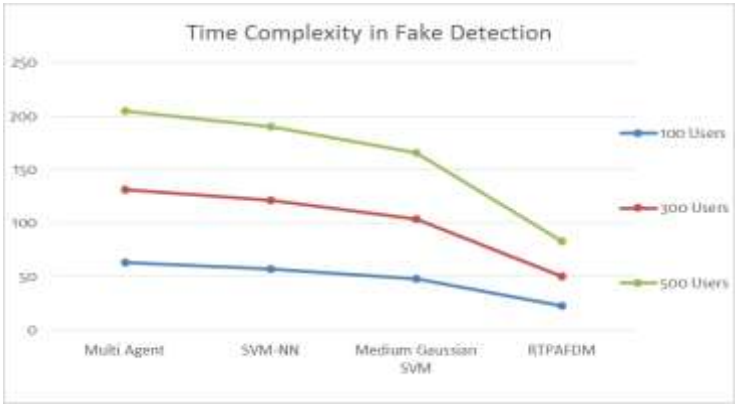

Figure 6 : Fake Profile Detection on Time Complexity Investigation

6. CONCLUSION

The current study presents ML based malicious user detection and unique user protection from across OSN. Its anticipated method considers the customer's shared number of messages, current activities, and behavioral pattern, that is then incorporated into a 3PS (Publicly Privacy Protected System) based technique for detecting malicious activity. Utilizing data mining assessment, malicious customers can be recognized on profile pages by various OSN applications for identifying relevant user trends. The recommended method will be important in protecting the critical use under of the exceptional user's profiles. In addition, an updated SVM-NN classification method predicts fake accounts using subsets of characteristics. In the coming decades, we will add a security utility called 'consumer recommendation choice and preference' to protect the customer's profile details. It has introduced a novel fake user detection on real-time profile Investigation for detecting fake accounts on social networking sites. The system works post-level trust assessment (PLTA), which tracks the comments informed daily and shares the comments internal and external with other customers to claim the trustworthiness of the statement, calculates the worth of Consumer Confidence Weight (CPCW), and completes Profile Threshold Trust Assessment (PTTA). Furthermore, the achievement of fake account identification can be upgraded by adjusting team-level prestige and feedback strategies, which confirms trust based on ability derived

from social connection customer segments and feedback gathered from multiple users. The research presented an efficient method for granting the user complete control over its shared data. The relevant methods of 'Fake profile detection Procedure' have been implemented in this regard, allowing the actual consumer to confer or deny entry to anyone to its data. The algorithmic survey provides a clear picture of all users attempting to obtain its personal details and issues a notification in its contact list. The proposed method is entirely focused on the consumer, and its success demonstrates that it can be greatly expanded.

7. REFERENCES

[1] Andrew Hutchinson, "Facebook Outlines the Number of FakeAccounts on Their Platform in New Report," 2018. [Online]https://www.socialmediatoday.com/news/Facebook-outlines-the- number-of-fake- accounts-on-their-platform-in-new-repo/523614/. [Accessed: 14-Jan- 2022].

[2] Nicholas Fandos K. R, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts - The New York Times," The New York Times, 2018, [Online]. Available: https: www.nytimes. com/ 2018/07/31/ us/politics/facebook-political-campaign-idterms.html. [Accessed: 18- Jan-2022].

[3] Vergeer M., Hermans L, and Sams, S, "Online social networks and micro- blogging in political," Party Polit., Vol. 19, No. 3, pp. 477–501, May 2013.

[4] Aichner, Thomas and Frank Jacob, "Measuring the degree of corporate social media use," International Journal of Market Research, Vol. 57, No. 2, pp. 257-276, 2015.

[5] Kharaji M. Y, Riza F. S, and Khayyambashi M. R, "A New Approach for Finding Cloned Profiles in Online Social Networks," Vol. 6, pp. 25–37, 2014.

[6] Zeifman I, "Bot traffic is up to 61.5% of all website traffic," 2013, [Online]. Available: https://www.incapsula.com/blog/bot-traffic-report- 2013.html. [Accessed: 24-Jul-2016].

[7] Egele, Manuel, GianlucaStringhini, Christopher Kruegel and Giovanni Vigna, "Compa: Detecting compromised accounts on social networks," In NDSS, Vol. 13, pp. 83-91. 2013.

[8] Y. Zhao, "Detecting and characterizing social spam campaigns," 10th ACM SIGCOMM conference on Internet measurement, pp. 35-47, 2010.

[9] Stein, Tao, Erdong Chen and Karan Mangla, "Facebook immune system," 4th Workshop on Social Network Systems, pp. 1-8, 2011.

[10] Kumar S., Cheng J., Leskovec J, and Subrahmanyan V. S, "An Army of Me: sock puppets in Online Discussion Communities," 26th Int. Conf. World Wide Web, pp. 857–866, 2015.

[11] Gao P., Gong N. Z., Kulkarni S., Thomas K, and Mittal P, "Sybil Frame: A Defense-in-Depth Framework for Structure-Based Sybil Detection," Computer. Res. Repos., p. 17, 2015.

[12] Yu H and Kaminsky, M, "Sybil Guard: Defending against Sybil Attack via Social Networks," IEEE/CM Trans-actions Newt., Vol. 16, No. 3, pp. 576–589, 2008.

[13] Adikari S., Pacis K. D and undefined, "Identifying Fake Profiles in LinkedIn," aisel.aisnet.org., 2014.

[14] Wang A.H, "Detecting Spam Bots in Online Social Networking Sites: A ML Approach," Data Appl. Secure. Priv. XXIV, Lect. Notes Computer. Sci., Vol. 6166, pp. 335–342, 2010.

[15] Subrahmanyan, V.S et al. "The DARPA Twitter Bot Challenge," Jan. 2016.

[16] Khafaji M. Y and Rizvi F. S, "An IAC Approach for Detecting Profile Cloning in Online Social Networks," Vol. 6, No. 1, pp. 75–90, 2014.

[17] Solorio T., Hasan R, and Mizan M, "A Case Study of Sockpuppet Detection in Wikipedia," Proc. Work. Lang. Anal. Soc. Media, No. Lams, pp. 59–68, 2013.

[18] Fire M., Goldschmidt R, and Elovici Y, "Online Social Networks: Threats and Solutions Survey," IEEE Common. Surv. TUTORIALS Online, Vol. 16, No. 4, pp. 1–20, 2013.