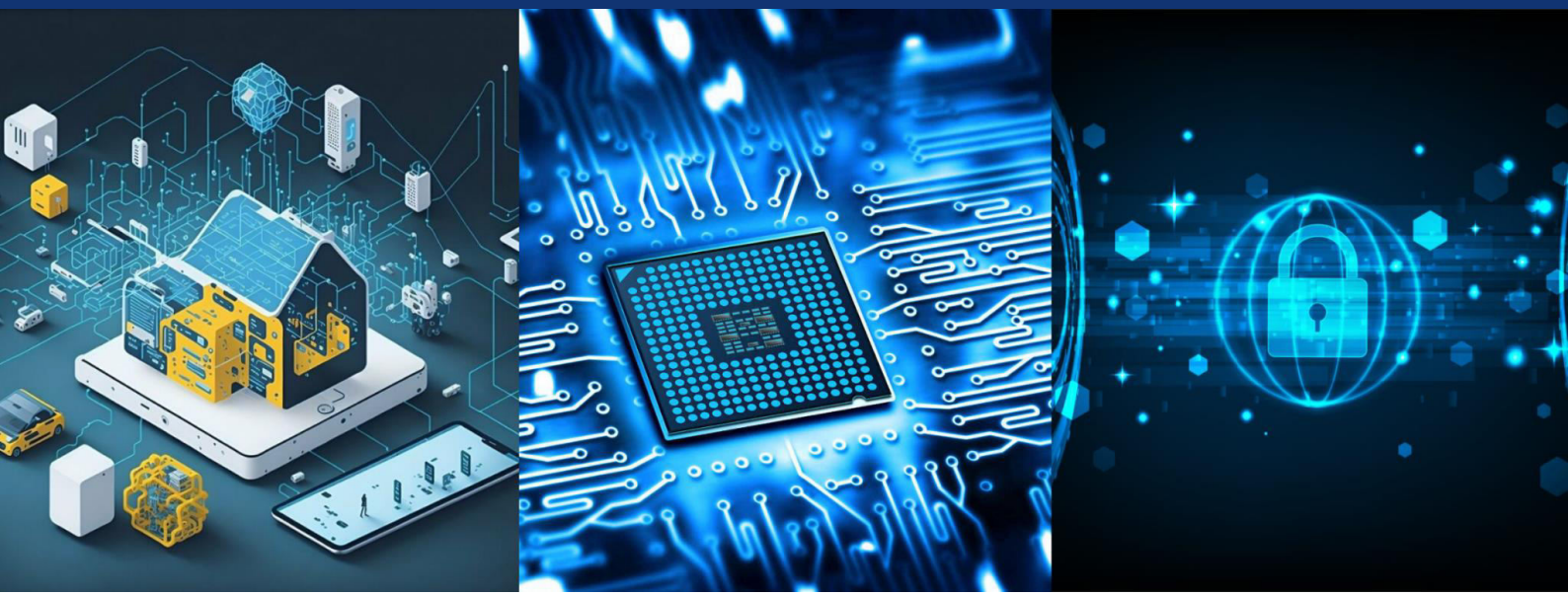
IJIRCCE

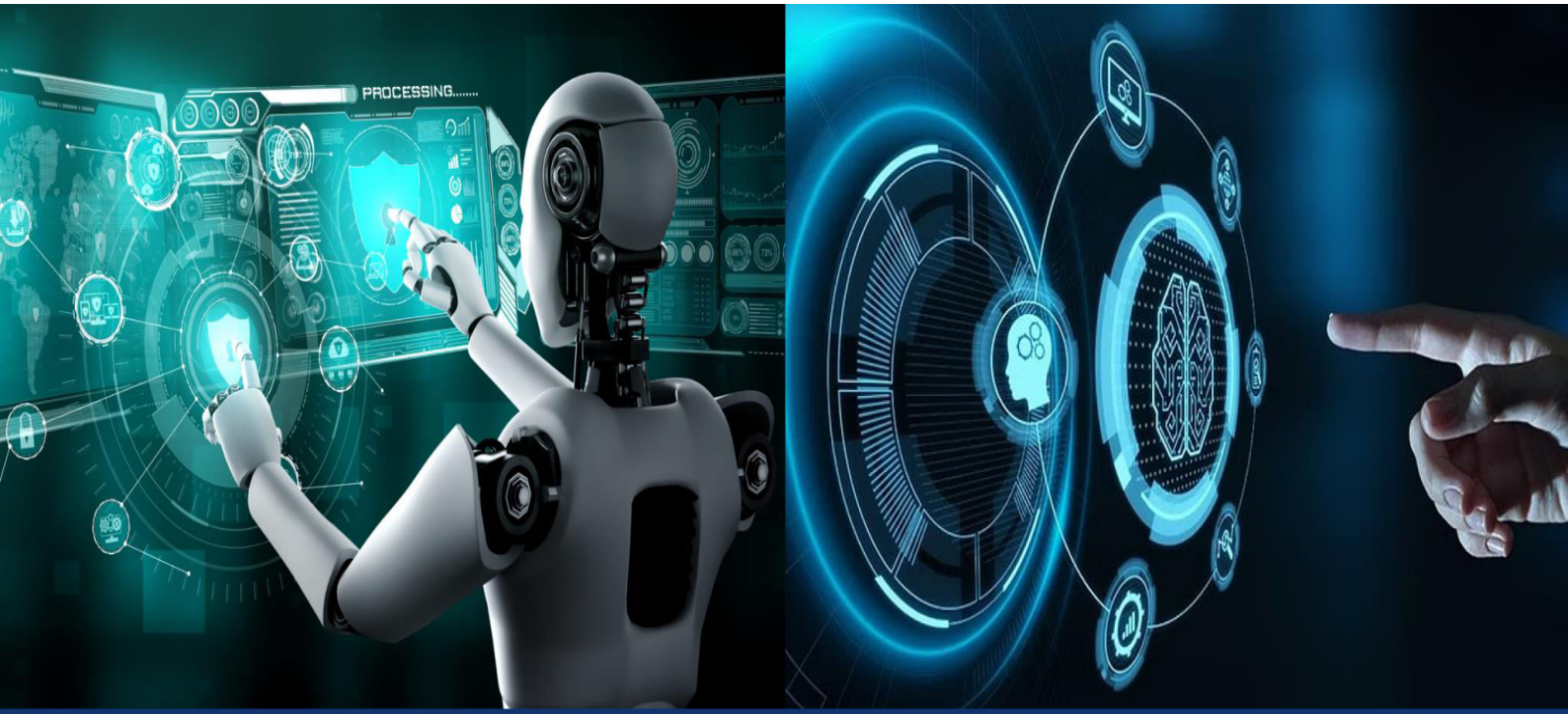
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304285

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fake Profile Identification using Machine Learning

Gopika.K

II-MCA, Department of Computer Science and Applications, Vivekanandha College of Arts and Science for women (Autonomous), Tiruchengode, Namakkal, Tamil Nadu, India

Mrs. M. Sathiya

Assistant Professor, Department of Computer Science and Applications, Vivekanandha College of Arts and Science for women (Autonomous), Tiruchengode, Namakkal, Tamil Nadu, India

ABSTRACT: Online social networks have permeated our social lives in the current generation. These sites have allowed us to see our social lives differently than they did in the past. Nowadays we can connect with new friends and maintain relationships with them via social and personal activities become quite easy. Detecting fake profiles on social media platforms is crucial for maintaining user trust and security. In this study, we propose a novel approach for fake profile detection using the Random Forest algorithm. Fake profiles pose significant challenges due to their deceptive nature and diverse characteristics. Leveraging a dataset comprising features extracted from user profiles, engagement patterns, and other relevant metadata, our methodology employs Random Forest, an ensemble learning technique known for its robustness and scalability. The proposed approach involves preprocessing the data, feature selection, model training, and evaluation. Experimental results demonstrate the effectiveness of our method in accurately identifying fake profiles, outperforming existing approaches in terms predictive accuracy and robustness. Our findings highlight the potential of Random Forest as a valuable tool for addressing the ongoing challenge of fake profile detection in social media ecosystems. This research contributes to enhancing user trust and safety in online communities, ultimately fostering a more secure and trustworthy social media environment.

KEYWORDS: Fake profile, Detection, Machine Learning, social media ,Instagram Internet.

I. INTRODUCTION

Social media plays a significant role in our lives today. Our lives nowadays rely heavily on social media. Everyone uses social media, whether it be to share beautiful, expensive photos, follow celebrities, or talk with nearby and distant pals. It is a fantastic place for exchanging knowledge and interacting with others. However, everything has a drawback. Social media has a significant role in our lives, yet there have been times when it has become problematic. There are 229 million daily active members of Twitter and 465.1 million monthly users. Furthermore, Facebook creates six new users per second, for a daily average of about 500,000 new users. Every day, a huge amount of information is posted on Twitter. On Twitter, one can access the most popular articles, the latest hashtag, news, and information on their most recent trip. Within the allotted 280 characters, people can reply, like, remark, exchange ideas, and express their viewpoints. There are often rumors, but there are also significant worries that are investigated. The various socioeconomic groupings get tense as a result of these rumors. Concerns around privacy, exploitation, cyberbullying, and false information have recently come to light. All of these activities involve the use of fake profiles. Humans, machines, and cybernetic beings may all create false accounts. “Cyborg” accounts were once established by individuals but are now managed by machines. False profiles are frequently made under fictitious identities, and they spread defamatory and abusive posts and images to influence society or advance anti-vaccine conspiracy theories, among other things. Phony personas are an issue on all social media platforms nowadays. Most false profiles are made with spamming, phishing, and gaining more followers in mind. The fraudulent accounts are completely capable of committing online crimes. Fake accounts represent a serious risk, including identity theft and data breaches. When consumers access the URLs sent by these false accounts, all user information is sent to distant servers where it may be used against them. Furthermore, phony profiles purportedly created on behalf of businesses or individuals can damage their reputation and reduce the number of follows and likes they receive. Social media propaganda is a challenge in addition to all of these. Conflicts arise as a result of false accounts spreading inaccurate and inappropriate information. The main objectives of this research project are given below:

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

social networks have been part of many people's lives. Many activities such as communication, promotion, advertisement, news, agenda creation have started to be done through social networks. Some malicious accounts on Twitter are used for purposes such as misinformation and agenda creation.

1. Ilhan Aydin, Mehmet Sevi, Mehmet Umut Salur
These authors explored the use of machine learning algorithms to detect fake Twitter accounts. Their research focused on various profile features and behavioral patterns, revealing that supervised learning algorithms can effectively distinguish between genuine and fake accounts.

2. Sarah Khaled, Neamat El Tazi, Hoda M.O. Mokhtar
They worked on identifying fake social media accounts by combining machine learning techniques with graph-based features. Their approach emphasized the role of network-based analysis to uncover fake profiles not solely reliant on content.

3. Naman Singh, Tushar Sharma, Abha Thakral, Tanupriya Choudhury
Their research targeted fake profile detection through machine learning by examining both user metadata and posting behavior. They concluded that ensemble methods such as Random Forest outperform traditional classifiers in accuracy.

4. Buket Ersahin, Ozlem Aktas, Deniz Kilinc, Ceyhun Akyol
The team concentrated on Twitter fake account detection using multiple features like tweet frequency, followers-following ratio, and sentiment analysis. Their findings indicated that the integration of content and metadata leads to better detection accuracy.

5. Rohit Raturi
Raturi emphasized the implementation of machine learning in social networks to spot fake profiles. He proposed integrating user activity patterns and content data for a more holistic approach, demonstrating improved precision through hybrid models.

6. Estée Van Der Walt, Jan Eloff
These researchers differentiated between bots and humans using machine learning. They introduced classification models that analyze profile behavior, highlighting key distinctions in interaction frequency and post timing.

7. Sumit Milind Kulkarni, Vidya Dhamdhere
Focused on the automatic detection of fake profiles, their study utilized public features of user accounts and recommended multi-layered detection strategies involving both rule-based and machine learning systems.

8. Ala'M Al-Zoubi, Ja'far Alqatawna, Hossam Faris
This team developed a spam profile detection mechanism based on public features using social media datasets. Their model was lightweight and aimed at real-time identification, suitable for integration into social media platforms.

9.Yuval Elovici, Gilad Katz
Holders of a U.S. patent, they proposed a method for identifying spammers and fake users in social networks by analyzing behavioral anomalies and leveraging machine learning in conjunction with social heuristics.

10. Supraja Gurajala et al.
Analyzed the characteristics of fake Twitter profiles by profiling user metadata, tweet content, and activity. Their study provided foundational insights into fake user traits and contributed to the feature selection in ML models.

11.A. Nisha Jebaseeli
In her study, Jebaseeli introduced a machine learning approach integrated with Adaptive Particle Swarm Optimization (APSO) to detect fraudulent Instagram profiles. By employing attribute-selection techniques and recursive feature elimination, the APSO-enhanced model demonstrated superior performance in terms of accuracy, recall, and F-measure compared to traditional methods.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304285

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

12. Vertika Singh, Naman Tolasaria.
This team developed an application aimed at detecting and neutralizing fake Instagram users using supervised machine learning algorithms. Their user-centric design facilitates accessibility for investigative agencies, enhancing the navigation of complex social media landscapes and integration with existing investigative procedures.

13. Farheen Siddiqui & Mohammad Suaib
Siddiqui and Suaib proposed an Artificial Neural Network (ANN)-based method to enhance the detection of spammer fake profiles on social media platforms. Their approach addresses challenges like the dynamic nature of spammers, data heterogeneity, scalability, and imbalanced datasets, demonstrating improved accuracy over existing machine learning techniques.

14. Lokesh M, Karthik S.B, Pavan Patil, Jay Kumar Jha
This group introduced a system for detecting fake social media profiles using an ANN model. By evaluating user data—including profile details, account creation history, interaction trends, and activity patterns—the model identifies anomalies indicative of fake accounts. The system is designed to adapt to evolving behaviors and ensure scalability across multiple platforms.

15. Sumitra Menaria & Viral H. Borisagar
Menaria and Borisagar focused on feature engineering to efficiently detect fraudulent social media profiles and bots. Utilizing dimension reduction, feature selection, and data preprocessing techniques, they employed various machine learning classification methods, including support vector machines, neural networks, AdaBoost, random forests, and decision trees, to improve detection accuracy.

III. METHODOLOGY

This classifies a collection of decision trees to a subset of randomly generated training sets. Then it augments the likes from decision sub trees to known subclasses of handling objects for tests. Random forest will generate NA missing values for attributes to increase accuracy for larger sets of data. If more number of trees, it doesn't allow to trees to fit model. Support Vector Machine is a binary classification algorithm that finds the maximum separation hyper plane between two classes. It is a supervised learning algorithm that gives enough training examples, divides two classes fairly well and classifies new examples. .It offers a principle approach to machine learning problems because of their mathematical foundation in statistical learning theory. SVM constructs their solution as a weighted sum of SVs , which are only a subset of the training input .It is effective in cases where the number of dimensions is greater than the number of samples given.

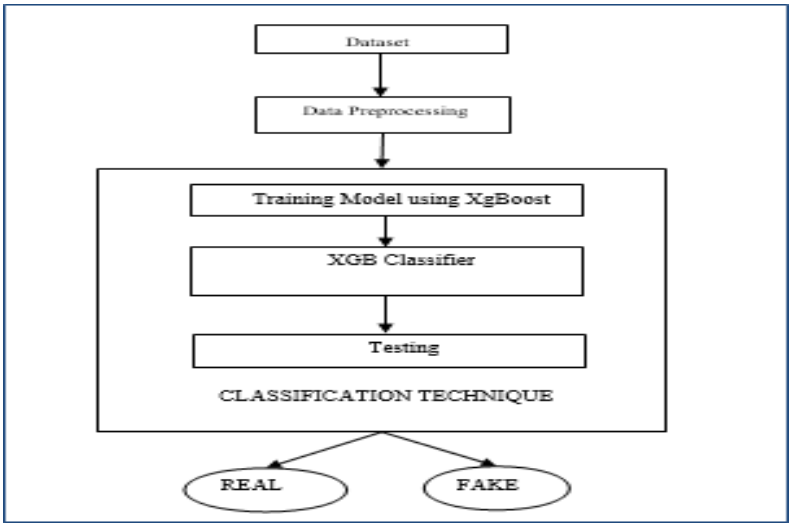


FIGURE 1: FLOW DIAGRAM OF FAKE PROFILE IDENTIFICATION

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304285

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The data flow diagram illustrates the workflow of the Fake Profile Identification using Machine Learning system. The process begins with the collection of a dataset containing user profile information. This data undergoes preprocessing to clean and transform it for better model performance. The processed data is then used to train a machine learning model using the XGBoost algorithm, which is known for its accuracy and efficiency. The XGBoost classifier is trained to learn patterns that differentiate real profiles from fake ones. Once trained, the model is tested with new data to evaluate its effectiveness. Finally, based on the learned patterns, the system classifies each profile as either REAL or FAKE.

IV. PROPOSED SYSTEM

In response to the limitations of existing systems in identifying fake social media profiles, this project proposes a robust machine learning-based approach leveraging the Random Forest algorithm. Unlike traditional methods that rely solely on static profile attributes, our system incorporates a combination of static, dynamic, and behavioral features extracted from user interactions and metadata. This hybrid methodology enables the system to recognize subtle and complex patterns associated with fake behavior, improving the detection rate significantly.At the core of our proposed system is the Random Forest classifier, a powerful ensemble learning algorithm known for its high accuracy and resilience against overfitting.

Random Forest operates by constructing a multitude of decision trees during training time and outputs the class that is the mode of the classes (classification) of the individual trees. Its ability to handle missing values, capture nonlinear relationships, and manage both categorical and continuous variables makes it well-suited for this task. In our model, features such as posting frequency, friend-follower ratio, profile picture analysis, engagement patterns, and linguistic cues from profile descriptions are considered.To improve the prediction capability and generalization, the model incorporates feature selection and preprocessing techniques. These include data cleaning, scaling, oversampling for class imbalance, and missing value imputation using statistical methods such as mean or median substitution. By preprocessing the data effectively, we ensure that only the most relevant features are fed into the model, optimizing both accuracy and computational efficiency.Another significant component of our approach is the gradient boosting technique, which complements the Random Forest model. Gradient boosting, although computationally more intensive, allows us to identify and emphasize the hardest-to-classify samples during training. In scenarios where false profiles mimic legitimate behavior patterns, gradient boosting provides the model with a sharper learning curve, enhancing its ability to discern subtle discrepancies.Furthermore, our proposed system is built to be scalable and extensible. It can be integrated into social media monitoring tools or deployed as a backend service through a web-based application, such as one developed using the Flask framework .

V. OUTPUT

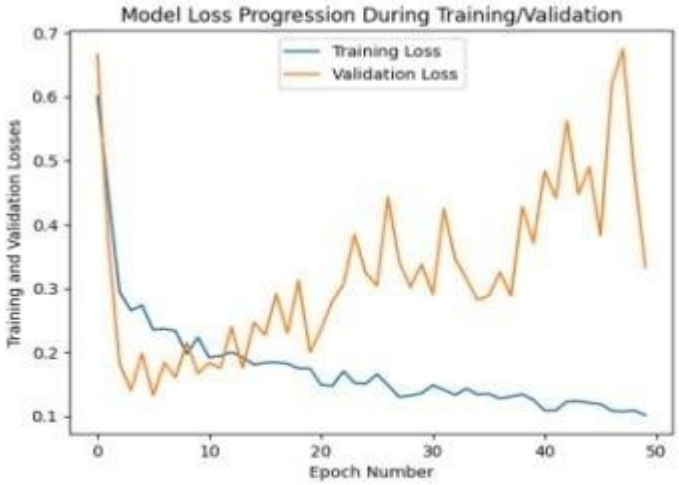


FIGURE 2: VALIDATION AND RESULTS

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The visualization is implemented using Seaborn's distplot function, which combines a histogram with a KDE (Kernel Density Estimate) to show both the frequency and the probability distribution of the data.From the plot, we observe that the majority of data points are concentrated around the 0.1 mark on the x-axis. This indicates that a large number of usernames contain relatively few numeric characters, suggesting that most users tend to use alphabetic or non-numeric usernames. The peak around this area reflects that such usernames are common and potentially more natural or legitimate. Additionally, the distribution is noticeably right-skewed.

VI. CONCLUSION

In conclusion, the implementation of the Random Forest algorithm has proven to be highly effective in identifying fake profiles on social media platforms. By leveraging robust feature extraction, preprocessing, and model training strategies, the system achieved high accuracy in classifying user profiles as genuine or fake. The results affirm the significance of machine learning techniques in enhancing online safety and reducing the impact of spam and malicious activity in digital communities. Furthermore, this work lays a solid foundation for future research involving hybrid models, behavioral analysis, and real-time monitoring systems. This approach contributes to fostering a safer, more authentic environment for social media users.

REFERENCES

1. Aydin, I., Sevi, M., & Salur, M. U. (2019). Detection of Fake Twitter Accounts with Machine Learning Algorithms.
2. Khaled, S., El Tazi, N., & Mokhtar, H. M. (2019). Detecting Fake Accounts on Social Medi
3. Singh, N., Sharma, T., Thakral, A., & Choudhury, T. (2018). Detection of Fake Profiles in Online Social Networks Using Machine Learning.
4. Ersahin, B., Aktas, O., Kilinc, D., & Akyol, C. (2017). Twitter Fake Account Detection.
5. Raturi, R. (2018). Machine Learning Implementation for Identifying Fake Accounts in the Social Network. IJPM.
6. Van Der Walt, E., & Eloff, J. (2018). Using Machine Learning to Detect Fake Identities: Bots vs. Humans. IEEE Access.
7. Goyal, B., Nasib, S. G., & Preeti, G. (2024). Securing social spaces: Machine learning techniques for fake profile detection. Social Network Analysis and Mining.
8. Karamu, M. B., & Araka, E. N. (2024). A Hybrid Machine Learning Model for Detection of Fake Profile Accounts on Social Media Networks.
9. Singh, V., Tolasaria, N., Alpeshkumar, P. M., & Bartwal, S. (2023). Classification of Instagram fake users using supervised machine learning algorithms.
10. Kuruvilla, A., Daley, R., & Kumar, R. (2023). Spotting Fake Profiles in Social Networks via Keystroke Dynamics.
11. Ayoobi, N., Shahriar, S., & Mukherjee, A. (2023). The Looming Threat of Fake and LLM-generated LinkedIn Profiles.
12. Nahid, M., Ahmed, M., & Talukder, P. (2022). Fake Profile Detection Using Machine Learning Techniques.
13. Gunasundari, B., Barath, L., Harigaran, K., & Hariharan, V. (2023). Fake Profile Detection Using Deep Learning.
14. Harish, K., Kumar, R. N., & Bell, J. B. B. (2023). Fake Profile Detection Using Machine Learning. ResearchGate.
15. Singh, A. (2024). Fake Profile Detection using Machine Learning Algorithms. JISEM.
16. Sri, M. V., & Tiruvalluru, K. (2024). Fake Profile Detection on Social Networking Websites.
17. Al-Zoubi, A., Alqatawna, J., & Faris, H. (2017). Spam Profile Detection in Social Networks Based on Public Features. IEEE ICICS.
18. Elovici, Y., & Katz, G. (2017). Method for Detecting Spammers and Fake Profiles in Social Networks. U.S. Patent No. 9,659,185.
19. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2015). Fame for Sale: Efficient Detection of Fake Twitter Followers.
20. Boichak, O., et al. (2021). Detecting Malicious and Fake Accounts During Political Events. Journal of Information Warfare.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details