

# Enhancing authenticity and trust in social media: an automated approach for detecting fake profiles

Manu Vasudevan Unni, Jeevananda S., Jacob Joseph Kalapurackal, Saba Fatma

School of Business and Management, CHRIST (Deemed to be University), Bengaluru, India

---

## Article Info

### Article history:

Received Jan 21, 2024

Revised Feb 24, 2024

Accepted Mar 16, 2024

---

### Keywords:

Coyote optimization algorithm

Deep belief network

Deep learning

Fake profile detection

Social network

---

## ABSTRACT

Fake profile detection on social media is a critical task intended for detecting and alleviating the existence of deceptive or fraudulent user profiles. These fake profiles, frequently generated with malicious intent, could engage in different forms of spreading disinformation, online fraud, or spamming. A range of techniques is employed to solve these problems such as natural language processing (NLP), machine learning (ML), and behavioural analysis, to examine engagement patterns, user-generated content, and profile characteristics. This paper proposes an automated fake profile detection using the coyote optimization algorithm with deep learning (FPD-COADL) method on social media. This multifaceted approach scrutinizes user-generated content, engagement patterns, and profile attributes to differentiate genuine user accounts from deceptive ones, ultimately reinforcing the authenticity and trustworthiness of social networking platforms. The presented FPD-COADL method uses robust data pre-processing methods to enhance the uniformness and quality of data. Besides, the FPD-COADL method applies deep belief network (DBN) for the recognition and classification of fake accounts. Extensive experiments and evaluations on own collected social media datasets underscore the effectiveness of the approach, showcasing its potential to identify fake profiles with high scalability and precision.

*This is an open access article under the [CC BY-SA](#) license.*



---

## Corresponding Author:

Manu Vasudevan Unni

School of Business and Management, CHRIST (Deemed to be University)

Bengaluru, Karnataka, India

Email: manuvasudevanunni@gmail.com

---

## 1. INTRODUCTION

Massive amounts of internet data are generated by social media platforms. In order to obtain "Likes," "Clicks," and "Views" on their content, cybercriminals use online platforms to build fictitious profiles. Once they reach their goals, they alter the profile to something else in order to disseminate their scams. The majority of firms are aware of the false identities that criminals have made to mimic their content, but their only real option is to denounce these accounts to the social media sites' policy authorities. In present scenario, social networking is a well-known restoration inside the web. Whereas it attracts more than thousands of users and spends a lot of time on such services [1]. Online social network (OSN) is one of the common services that diverse from social interface-based platforms that are comparable to MySpace or Twitter, to accept distribution-centric stages suggestive of Twitter or Google Buzz, to social contact typically brought to current networks like Flickr [2]. On the other side, improving safety anxieties and defending the OSN's privateness still suggest a most significant holdup and observed mission. Men and women can able to share any one amount of their private understanding when using social networks (SNs). In the present scenario, it is very important part of everyone's daily lives [3]. It becomes an effective application to connect populace the world for sharing several data such as photos, messages and videos. Moreover, an abnormal problem like fake accounts causes

major anxiety in OSN security [4]. Many researchers developed several models in order to enhance OSN security differently. For example, research develops an effective network technique for improving the protection of OSN [5]. Generally, all devices have a safety tool to solve and access the device like PIN, keyboard patterns and password. However, the conventional technique sets user data in danger it is because there is extra safety to check the activities of users and act after login to the app [6]. Illegal persons may be capable of cracking the easy PIN or passwords of devices like mobile phones or wearable gadgets. By covering social media, opponents seek to violate other clients' privacy and exploit their identities and IDs by creating bogus accounts [7]. Automated false profile identification can boost social media security. It identifies and removes cyberbullies, harassers, and other harmful users. Social media services must recognize opponents and create phony profiles to remove them [8]. Social media sites invest much on manual content filtering and profile verification. Management can optimize resource allocation by shifting human moderators to more difficult or high-impact jobs with automation. Cost reductions and operational efficiency may ensue. Social media phony accounts inflict greater damage than other cybercrimes. Experts are focusing more on removing bogus accounts [9]. Numerous studies have identified fake social media profiles. Social media networks store massive quantities of data. Data integrity is protected by automatic false profile detection. Platform administrators need accurate and trustworthy user data for analytics, advertising, and other data-driven operations to generate income and make decisions. Different methods have been used to discover fake accounts, including buddy system comparisons [10], feature resemblances, and profile assessments over time using IP addresses. We ask digital ecosystem managers, policymakers, and stakeholders to understand the need of strong fake profile identification as a vital element of effective social media management as we discuss our approach's technical components. Existing methods cannot distinguish phony user accounts from genuine ones based on user-generated content, interaction patterns, and profile features. This research proposes fake profile detection utilizing the coyote optimization algorithm with deep learning (FPD-COADL) to address this issue.

This study presents an automated fake profile detection using FPD-COADL technique on social media. The study gathers questionnaires from management professionals, enriching the fake profile detection process with valuable insights from experts in the field. The presented FPD-COADL technique uses robust data pre-processing techniques to improve the quality and uniformness of data. Besides, the FPD-COADL technique applies the deep belief network (DBN) model for the identification and classification of fake accounts. To optimize the performance of the DBN model, the COA is utilized for hyperparameter tuning, enhancing detection accuracy and efficiency. Extensive experiments and evaluations on real-world social media datasets underscore the effectiveness of the approach, showcasing its potential to identify fake profiles with high scalability, accuracy in predicting the fake profiles and precision.

## 2. RELATED WORKS

Shalini *et al.* [11], a recurrent neural network (RNN) is developed. The study employs machine learning (ML) for detection. The features are removed from the dataset depending on the time frequency. The network offers extreme accurateness for the fake recognition as well as real personalities on the dataset of social media. It gains good correctness with RNN employing dissimilar beginning works. This research is very useful for detecting mischievous accounts from an excessive dataset. Harris *et al.* [12], the programmed recognition of fake profiles has been developed. When users trust that a social media platform is actively working to combat fake profiles and fraudulent activities, they are more likely to engage with genuine users and share personal information. This trust is essential for the growth and long-term sustainability of the platform. The forecast of false Instagram outlines is simplified by utilizing supervised learning machine models. Based on the detection, false profile identifications are kept in a data dictionary for additional assistance for the worried experts to capture essential activities besides fake profiles on social media. Research has been completed to equate the classification approaches employed to verify the dataset.

Soumya *et al.* [13] goal of this research is to verify as well as identify trustworthy and false profiles generated in OSN via ML-based models. Using employing models like radial function (RF), deep neural networks (DNN) and support vector machine (SVM) to overcome procedures like giving absent value, documentation of variables, cleaning and authentication of information will be finished on entire datasets. Kadam and Sharma [14], an advanced-based ML technique was proposed for categorizing the false as well as real profiles. Five ML models are used such as SVM, artificial neural network (ANN), Naïve Bayes (NB), K-nearest neighbor (KNN) and C4.5 decision tree to authenticate the technique. Lastly, upgrading the back propagation neural network (BPNN) and then scoring the model for a false profile detection method is designed. The presence of fake profiles can lead to a poor user experience, such as encountering spam, scams, or fake content. By effectively detecting and removing such profiles, the user experience is improved. Users are more likely to stay engaged, return to the platform, and recommend it to others.

Kodati *et al.* [15], recognition of fake accounts on the Twitter platform employing a hybrid SVM technique is projected. The ML-based hybrid SVM method was utilized in this paper for the detection of false

and real accounts in the Twitter platform as well as used the method of feature selection, dimension reduction, and bots. Few features are employed in the developed hybrid SVM model and the profiles are properly categorized by suggested model. Shreya *et al.* [16], DNN and ML algorithms such as RF, ANN, and SVM techniques are employed in order to evaluate the probability that Facebook account data is precise or not. The dataset utilized in this work is captured from GitHub which is a Facebook profile dataset for recognizing false and honest profiles. Additionally, the study has labeled the connected classes and libraries.

### 3. THE PROPOSED MODEL

In this study, a novel presented an automated FPD-COADL technique on social media. The goal of FPD-COADL technique contains three main processes such as data pre-processing, DBN-based detection, and COA-based parameter tuning. Figure 1 depicts the entire process of FPD-COADL algorithm. The Figure 1 depicts the overall process of FPD-COADL algorithm. The proposed work collects the data from various sources of social media and is fed as the training data to the proposed model. The processed data is treated for the fake account identification and classification process using deep belief network model.

#### 3.1. Data preprocessing

Platform-authorized APIs can acquire social media data. APIs regulate data access, assuring platform terms of service and data usage compliance. Web scraping may be done legally and respectfully, respecting the platform's robots.txt file and without overloading its servers. Informed permission is required for gathering profile data. Data collection, purpose, and usage should be disclosed to users. Consent can be requested by cookie alerts, opt-ins, or privacy settings. Data should be stored securely according to industry standards and data protection laws. Protect data at rest and in transit with robust encryption.

Social media fake profile detection relies on pre-processing to be successful and accurate. The first pre-processing processes often structure and sanitize raw data. Eliminating duplicate entries, cleansing text data, and addressing missing values are examples. Text normalisation uses stemming, lemmatization, lowercase, and punctuation removal to standardise word format. Tokenization breaks text into phrases or words for analysis. Stop words, such as "and" and "the," are often removed to decrease textual noise. Material-specific variables (post frequency, sentiment analysis scores) and user profile attributes (username, bio, follower count) are often extracted from user-generated material.

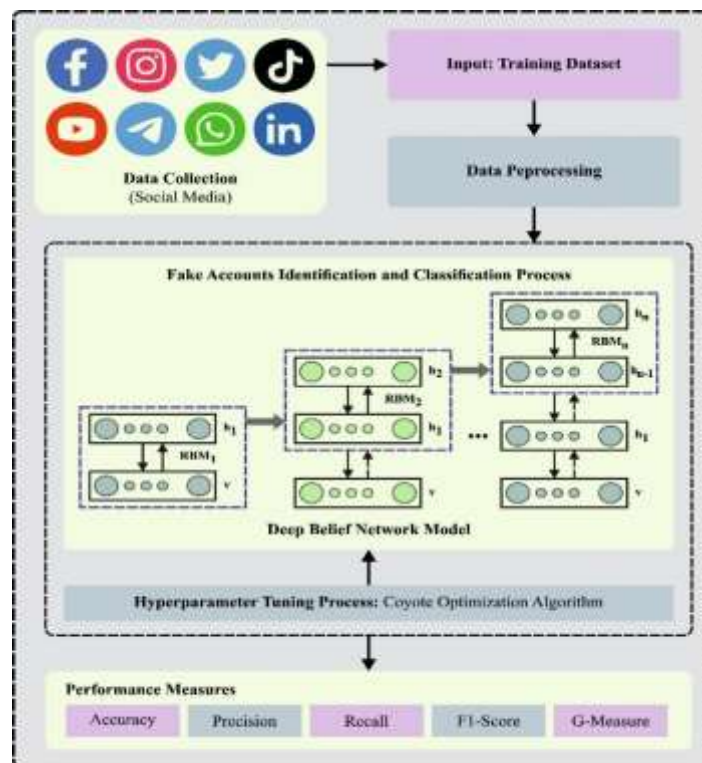


Figure 1. Overall process of FPD-COADL algorithm

### 3.2. DBN-based detection model

The architecture of DBN comprises BPNN and restricted Boltzmann machine (RBM). RBM is a type of stochastic, generative neural network that consists of visible and hidden units. It is used for unsupervised learning, particularly in the domain of feature learning, dimensionality reduction, and collaborative filtering. A Boltzmann perceptron neural network is another name for a Feedforward neural network. This type of network architecture is composed of layers of interconnected neurons, but it does not have the same layers of stochastic units and learning characteristics found in RBMs. BPNNs are used for various tasks, including supervised learning, classification, and regression.

The output, hidden, and visible layers are the three layers of DBN [17]. While learning, the feature goes through multiple hidden layers before getting the input or visible layers. Finally, the labelling classes are correctly allotted to the resultant layer. Also, RBM has input and concealed layers with bi-directional connections between them. Where  $h = h_1, h_2, \dots, h_n$ , and  $v = v_1, v_2, \dots, v_m$ ,  $m$  and  $n$  are the number of input and hidden units. The subsequent formula defines the energy function of RBM.

$$E(v, h; \theta) = -\sum_{i=1}^m \sum_{j=1}^n w_{ij} v_i h_j - \sum_{i=1}^m a_i v_i - \sum_{j=1}^n b_j h_j \tag{1}$$

In (1), parameter  $\theta$  includes the bias input layer  $a_i$ , the bias-concealed layer  $b_i$ , and the weight connection  $w_{ij}$  between the nodes. The joint distribution can be given in the (2) and (3).

$$p(v, h) = \frac{1}{R(\theta)} e^{-E(v,h)} \tag{2}$$

$$R(\theta) = \sum_{v,h} e^{-E(v,h)} \tag{3}$$

Where the factor  $R(\theta)$  is utilized as a normalization. The probability distribution of the input layer is (4).

$$p(v) = \sum_n p(v, h) = \frac{1}{R(\theta)} \sum_h e^{-E(v,h)} \tag{4}$$

Assume that the node in all the corresponding layers is not linked, the likelihood dissemination of each layer can be given as (5) and (6).

$$p(h_j = 1|v; \theta) = \sigma(\sum_{i=1}^m w_{ij} v_i + b_j) \tag{5}$$

$$p(v_i = 1|h; \theta) = \sigma(\sum_{j=1}^n w_{ij} h_j + a_i) \tag{6}$$

Whereas  $\sigma(x) = 1/(1 + \exp(x))$  is sigmoid function. Using adjustment to bias  $a_i$ ,  $b_j$ , and weight  $w_{ij}$ , RBM aims at maximizing the probability  $p(v)$ . With the maximum probability estimate, the RBM parameter set  $\theta = \{a_i, b_i, w_{ij}\}$  is attained from the training dataset. The CD algorithm can identify the parameter set  $\theta$ .

$$w_{ij}^{(t+\Delta t)} = w_{ij}^{(t)} + \frac{\alpha}{\beta} (\langle v_i h_j \rangle_{data} - \langle v_i h_j \rangle_{model}) \tag{7}$$

$$a_i^{(t+\Delta t)} = a_i^{(t)} + \frac{\alpha}{\beta} (\langle v_i \rangle_{data} - \langle v_i \rangle_{model}) \tag{8}$$

$$b_j^{(t+\Delta t)} = b_j^{(t)} + \frac{\alpha}{\beta} (\langle h_j \rangle_{data} - \langle h_j \rangle_{model}) \tag{9}$$

Where the learning rate and the batch size are  $\alpha$  and  $\beta$  respectively. The existing hidden layer was exposed as the next visible layer of RBM once the training was complete. The resultant deep feature was classified after the RBM training was accomplished. COA is stimulated by the representation of social lives of coyotes inherent in North America. The population is separated into smaller pack or group [18]. Every individual group is generally comprised of male and female coyotes. Furthermore, coyote lives in group, sometimes they leave the member to join other groups. When users perceive a platform as a safe and trustworthy environment, they are more likely to engage with confidence. Automated fake profile detection demonstrates the platform's commitment to user safety and integrity. By proactively addressing fake profiles, the platform fosters trust among its users, promoting a positive user experience and encouraging user retention and growth. Online platforms rely on accurate and authentic user data for various purposes, including user engagement, content recommendations, and targeted advertising. Fake profiles can compromise the integrity of user data and skew analytics.

#### 4. EXPERIMENTAL VALIDATION

One of the foremost ethical considerations is the prevention of bias and discrimination in ML models. It is the ethical responsibility of management to ensure that class imbalance management does not favor one class over the other, as this can lead to unfair, biased, and potentially harmful predictions. By emphasizing fairness, equity, transparency, and accountability in the ML process, management can contribute to the responsible and ethical use of artificial intelligent (AI) technologies, such as fake profile detection, while avoiding harmful bias or discrimination. The Table 1 provide the details of the normal and fake profile from the total samples considered for the testing and training of the proposed work.

Table 1. Details of dataset

Class	No. of samples
Normal profile	1,000
Fake profile	1,000
Total samples	2,000

##### 4.1. Data collection

In this work, we have collected our own fake profile dataset using a set of five questions that can be included in a questionnaire for gathering insights and data relevant to fake profile detection. A set of 2,000 persons are involved in the data collection process. The list of questions are given as follows.

Q1: Have you encountered or suspected the presence of fake profiles on social media platforms in your professional experience? If so, please describe the characteristics or behaviors that led to your suspicions.

Q2: In your opinion, what are the most common motivations for creating fake profiles on social media within the management or business context? (e.g., Competitor sabotage, and reputation manipulation)

Q3: How do you believe fake profiles could potentially impact individuals or organizations in the management field? Please provide examples if applicable.

Q4: What specific characteristics or patterns do you think are indicative of a fake profile in a professional or management-related context? (e.g., unusual posting frequency, unverified credentials)

Q5: Are there any tools, strategies, or best practices you recommend for detecting and mitigating fake profiles in the realm of management or business-related social media? Please share your insights on effective detection methods or preventive measures.

Q6: How often do you encounter profiles on social media that you suspect may be fake or deceptive, and what are the common characteristics or behaviors that raise your suspicion?

Q7: What specific information or patterns in user-generated content, such as posts, comments, or messages, do you believe are indicative of a fake profile?

Q8: In your opinion, what are the primary motives for creating deceptive profiles on social media, and what types of content or activities are these profiles typically involved in?

Q9: Are there any particular strategies or techniques you use to differentiate between genuine and fake profiles when assessing social media accounts?

##### 4.2. Results analysis

Figure 2 illustrates the classifier analysis of the FPD-COADL method on test dataset. Figures 2(a) and (b) shows the confusion matrices given by the FPD-COADL model on 70:30 of training (TR) phase/testing (TS) phase. The outcome indicated that the FPD-COADL method has appropriately recognized and classified two classes. Additionally, Figure 2(c) exhibits the precision-recall (PR) investigation of the FPD-COADL technique. The figure shown that the FPD-COADL model is gained higher PR performance with every classes. Besides, Figure 2(d) represents the receiver operating characteristic curve (ROC) analysis of the FPD-COADL method. This outcome indicated that the FPD-COADL system leads to proficient outcomes with greater ROC values with various classes.

The fake profile detection outcomes of the FPD-COADL method are inspected in Table 2 and Figure 3. The results pointed out that the FPD-COADL technique attains normal and fake profiles effectually. With 70% of TR Phase, the FPD-COADL technique offers average  $accu_y$  of 96.27%,  $prec_n$  of 96.30%,  $reca_l$  of 96.27%,  $F1_{score}$  of 96.28%, and  $G_{measure}$  of 96.28%, respectively. Also, based on 30% of TS Phase, the FPD-COADL system provides average  $accu_y$  of 95.65%,  $prec_n$  of 95.50%,  $reca_l$  of 95.65%,  $F1_{score}$  of 95.50%, and  $G_{measure}$  of 95.53%, correspondingly.

To determine the effectiveness of the FPD-COADL model, we have produced accuracy curves for both the TR and TS phases, as shown in Figure 4. These curves give valuable insights into the model's proficiency and learning process to generalize. As we improve the count of epochs, an obvious expansion in

both TR and TS  $accu_y$  curves become marked. This improvement implies the model's capacity to higher recognize patterns within both the TR and TS databases.

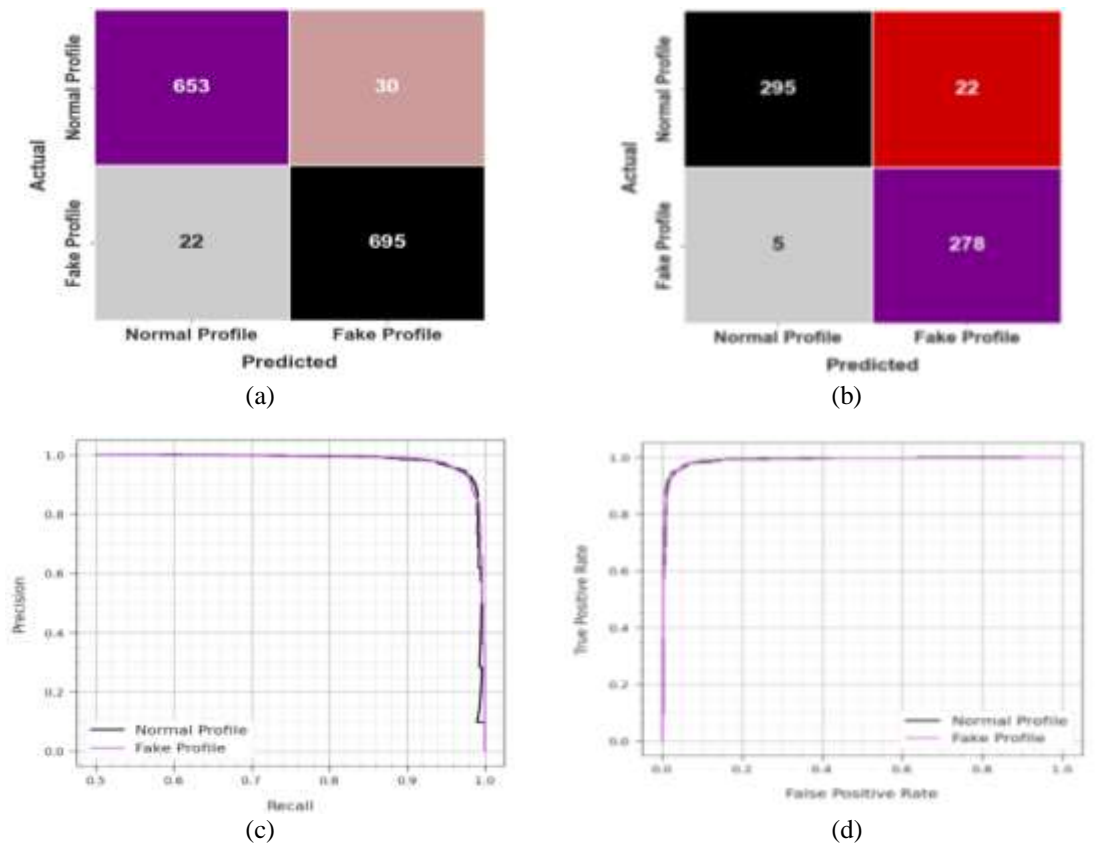


Figure 2. Classifier outcome of: (a) TR phase (70%) confusion matrices, (b) TS phase (30%) confusion matrices, (c) PR curve, and (d) ROC curve

Table 2. Fake profile detection outcome of FPD-COADL technique on 70:30 of TR phase/TS phase

Class	$Accu_y$	$Prec_n$	$Recal_t$	$F1_{score}$	$G-Measure$
TR phase (70%)					
Normal profile	95.61	96.74	95.61	96.17	96.17
Fake profile	96.93	95.86	96.93	96.39	96.40
Average	96.27	96.30	96.27	96.28	96.28
Ts phase (30%)					
Normal profile	93.06	98.33	93.06	95.62	95.66
Fake profile	98.23	92.67	98.23	95.37	95.41
Average	95.65	95.50	95.65	95.50	95.53

Figure 5 also provides an overview of the model's loss values across the training process. The reducing trend in TR loss over epochs shows that the model persistently improves its weights to diminish predicted errors on both TR and TS data. This loss curve considers how better the model fits the training datasets. Remarkably, the TR and TS loss reliably minimize, representing the model's efficient learning of patterns existing in both databases. Also, it exhibits the model's adaptation in decreasing differences between predictive and the actual training labels. In Figure 6 and Table 3, the comparison performance of the FPD-COADL method is examined [19].

The results portrayed that the FPD-COADL technique [20] offers improved results. Based on  $accu_y$ , the FPD-COADL technique gains increasing  $accu_y$  of 96.27% while the NB, GB, LR, SVM, and SBO-FCCUAV models obtain decreasing  $accu_y$  values of 93.89%, 90.78%, 90.38%, 90.62%, and 95.63% respectively. Also, with  $prec_n$ , the FPD-COADL method achieves raising  $prec_n$  of 96.30% whereas the NB, GB, LR, SVM, and SBO-FCCUAV techniques get reduced  $prec_n$  values of 86.90%, 90.66%, 95.49%, 90.04%,

and 94%. Meanwhile, on  $reca_l$ , the FPD-COADL method achieves raising  $reca_l$  of 96.27% whereas the NB [21], GB [22], LR [23], SVM [24], and SBO-FCCUAV techniques [25] get reduced  $reca_l$  values of 86.94%, 90.69%, 87.34%, 93.21%, and 96.27%. At last, on  $F1_{score}$ , the FPD-COADL method achieves raising  $F1_{score}$  of 96.28% whereas the NB, GB, LR, SVM, and SBO-FCCUAV techniques [26] get reduced  $F1_{score}$  values of 87%, 91%, 90.60%, 93.42%, and 96.28%. Therefore, the FPD-COADL technique can be used for accurate fake profile detection. This research work performed the detection of fake profiles in the social media and the performance shall further be enhanced by detecting the behavior of the profile, its post and the type of data traffic which could be processed using the any advanced neural network technologies.

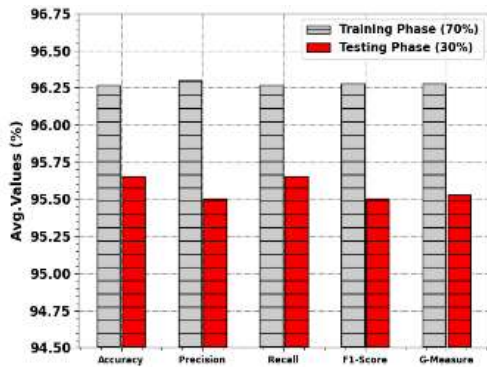


Figure 3. Average analysis of FPD-COADL model 70:30 of TR phase/TS phase



Figure 4.  $Accu_y$  curve of the FPD-COADL model



Figure 5. Loss curve of FPD-COADL model

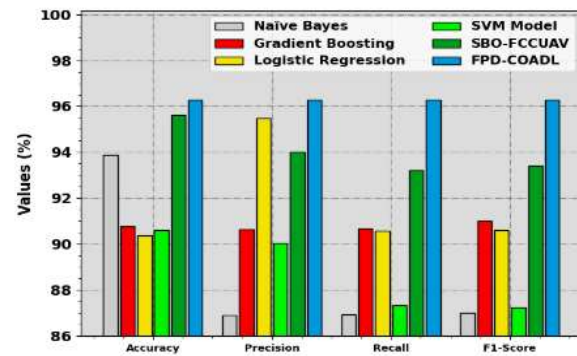


Figure 6. Comparative outcome of FPD-COADL algorithm with recent methods

Table 3. Comparative outcome of FPD-COADL approach with existing techniques

Classification model	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
Naive Bayes	93.89	86.90	86.94	87.00
Gradient boosting	90.78	90.66	90.69	91.00
Logistic regression	90.38	95.49	90.59	90.60
SVM model	90.62	90.04	87.34	87.24
SBO-FCCUAV	95.63	94.00	93.21	93.42
FPD-COADL	96.27	96.30	96.27	96.28

### 5. CONCLUSION

The study introduces the automated FPD-COADL technique on social media. The presented FPD-COADL technique uses robust data pre-processing techniques to improve the quality and uniformness of data. Besides, the FPD-COADL technique applies the DBN model for the identification and classification of fake accounts. The COA is utilized for hyperparameter tuning, enhancing detection accuracy and efficiency to optimize the performance of DBN model. Extensive experiments and evaluations on real-world social media





datasets underscore the effectiveness of the approach, showcasing its potential to identify fake profiles with high scalability and precision. The proposed work outperforms well in terms of detecting the fake profiles in the social media with 96.27%, precision with 96.3%, recall with 96.27%, and F1 score with 96.28%. This research contributes to bolstering the trustworthiness and security of online social networking platforms, preserving the integrity of digital communities and protecting users from deceptive profiles. The performance of the proposed work in detecting the fake profiles in the social media, could further be enhanced by introducing non-supervised learning models or ANNs in detecting the anomaly traffic pattern or behavior among the social media users.

## REFERENCES





- [1] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman, and M. S. Hossain, "Sybil defense techniques in online social networks: A survey," *IEEE Access*, vol. 5, pp. 1200–1219, 2017, doi: 10.1109/ACCESS.2017.2656635.
- [2] P. V. Bindu and P. S. Thilagam, "Mining social networks for anomalies: methods and challenges," *Journal of Network and Computer Applications*, vol. 68, pp. 213–229, Jun. 2016, doi: 10.1016/j.jnca.2016.02.021.
- [3] M. Mohammadrezaei, M. E. Shiri, and A. M. Rahmani, "Identifying fake accounts on social networks based on graph analysis and classification algorithms," *Security and Communication Networks*, vol. 2018, pp. 1–8, Aug. 2018, doi: 10.1155/2018/5923156.
- [4] Y. Qin, R. Jia, J. Zhang, W. Wu, and X. Wang, "Impact of social relation and group size in multicast ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 4, pp. 1989–2004, Aug. 2016, doi: 10.1109/TNET.2015.2437955.
- [5] N. Kokciyan and P. Yolum, "PriGuard: a semantic approach to detect privacy violations in online social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 10, pp. 2724–2737, Oct. 2016, doi: 10.1109/TKDE.2016.2583425.
- [6] P. Wanda, Selo, and B. S. Hantono, "Model of secure P2P mobile instant messaging based on virtual network," in *2014 International Conference on Information Technology Systems and Innovation (ICITSI)*, Nov. 2014, pp. 81–85. doi: 10.1109/ICITSI.2014.7048242.
- [7] E. Van Der Walt and J. Eloff, "Using machine learning to detect fake identities: bots vs humans," *IEEE Access*, vol. 6, pp. 6540–6549, 2018, doi: 10.1109/ACCESS.2018.2796018.
- [8] J. R. C. Nurse, A. Erola, M. Goldsmith, and S. Creese, "Investigating the leakage of sensitive personal and organisational information in email headers," *Journal of Internet Services and Information Security (JISIS)*, vol. 5, no. 1, pp. 70–84, 2015.
- [9] M. Li, Y. Xiang, B. Zhang, F. Wei, and Q. Song, "A novel organizing scheme of single topic user group based on trust chain model in social network," *International Journal of Communication Systems*, vol. 31, no. 1, Jan. 2018, doi: 10.1002/dac.3387.
- [10] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," *Digital Investigation*, vol. 23, pp. 31–49, Dec. 2017, doi: 10.1016/j.diin.2017.09.002.
- [11] A. K. Shalini, S. Saxena, and B. S. Kumar, "Designing a model for fake news detection in social media using machine learning techniques," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2S, 2023.
- [12] P. Harris, J. Gojal, R. Chitra, and S. Anithra, "Fake Instagram profile identification and classification using machine learning," in *2021 2nd Global Conference for Advancement in Technology (GCAT)*, Oct. 2021, pp. 1–5. doi: 10.1109/GCAT52182.2021.9587858.
- [13] T. R. Soumya, S. S. Manohar, N. B. S. Ganapathy, L. Nelson, A. Mohan, and M. T. Pandian, "Profile similarity recognition in online social network using machine learning approach," in *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Sep. 2022, pp. 805–809. doi: 10.1109/ICIRCA54612.2022.9985683.
- [14] N. Kadam and S. K. Sharma, "Social media fake profile classification: a new machine learning approach," in *Advances in Data-Driven Computing and Intelligent Systems*, 2023, pp. 823–839. doi: 10.1007/978-981-99-0981-0\_62.
- [15] S. Kodati, K. P. Reddy, S. Mekala, P. S. Murthy, and P. C. S. Reddy, "Detection of fake profiles on twitter using hybrid SVM algorithm," *E3S Web of Conferences*, vol. 309, Oct. 2021, doi: 10.1051/e3sconf/202130901046.
- [16] K. Shreya, A. Kothapelly, D. V., and H. Shanmugasundaram, "Identification of fake accounts in social media using machine learning," in *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Dec. 2022, pp. 1–4. doi: 10.1109/ICERECT56837.2022.10060194.
- [17] H. Myriam *et al.*, "Advanced meta-heuristic algorithm based on particle swarm and Al-Biruni Earth radius optimization methods for oral cancer detection," *IEEE Access*, vol. 11, pp. 23681–23700, 2023, doi: 10.1109/ACCESS.2023.3253430.
- [18] E. S. Ali, S. M. A. Elazim, and A. S. Balobaid, "Implementation of coyote optimization algorithm for solving unit commitment problem in power systems," *Energy*, vol. 263, Jan. 2023, doi: 10.1016/j.energy.2022.125697.
- [19] P. Wanda and H. J. Jie, "DeepProfile: finding fake profile in online social network using dynamic CNN," *Journal of Information Security and Applications*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102465.
- [20] G. Sansonetti, F. Gasparetti, G. D'aniello, and A. Micarelli, "Unreliable users detection in social media: deep learning techniques for automatic detection," *IEEE Access*, vol. 8, pp. 213154–213167, 2020, doi: 10.1109/ACCESS.2020.3040604.
- [21] B. L. V. S. Aditya and S. N. Mohanty, "Heterogenous social media analysis for efficient deep learning fake-profile identification," *IEEE Access*, vol. 11, pp. 99339–99351, 2023, doi: 10.1109/ACCESS.2023.3313169.
- [22] P. K. Roy and S. Chahar, "Fake profile detection on social networking websites: a comprehensive review," *IEEE Transactions on Artificial Intelligence*, vol. 1, no. 3, pp. 271–285, Dec. 2020, doi: 10.1109/TAI.2021.3064901.
- [23] A. M. Meligy, H. M. Ibrahim, and M. F. Torky, "Identity verification mechanism for detecting fake profiles in online social networks," *Int. J. Comput. Netw. Inf. Secur. (IJCNIS)*, vol. 9, no. 1, pp. 31–39, 2017.
- [24] P. Durairaj and S. Ramachandran, "A survey on security issues and solutions in virtual private network," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 14, pp. 1183–1192, 2018.
- [25] F. Masood *et al.*, "Spammer detection and fake user identification on social networks," *IEEE Access*, vol. 7, pp. 68140–68152, 2019, doi: 10.1109/ACCESS.2019.2918196.
- [26] D. Nevado-Catalán, S. Pastrana, N. Vallina-Rodriguez, and J. Tapiador, "An analysis of fake social media engagement services," *Computers & Security*, vol. 124, Jan. 2023, doi: 10.1016/j.cose.2022.103013.







**BIOGRAPHIES OF AUTHORS**

**Mr. Manu Vasudevan Unni**     holds triple Master's degrees from institutions in France and India, demonstrating a strong academic background coupled with industrial experience. His research interests encompass a broad spectrum, including consumer behavior, privacy concerns, brand loyalty, strategic marketing, international business, and marketing. Presently, he is pursuing a Ph.D. at Christ University, Bangalore, while also serving as an Assistant Professor at St. Claret College, Bangalore, India. He can be contacted at email: manuvasudevanunni@gmail.com.







**Dr. Jeevananda S.**     an esteemed academician, holds degrees including MBA, MFT, MPhil, and a Ph.D. As a Professor and Associate Dean at the School of Business and Management, Christ University, he boasts over two decades of extensive experience. He has authored numerous articles listed in Scopus, Web of Science, ABDC, and UGC, and has chaired multiple conferences. His expertise lies primarily in the domain of marketing. He can be contacted at email: Jeevananda.s@christuniversity.in.



**Dr. Jacob Joseph Kalapurackal**     is an Associate Professor in the School of Business and Management at Christ University, Bengaluru. With an impressive academic background encompassing an MA, MBA, and Ph.D., He brings a wealth of knowledge and expertise to his role. His scholarly contributions are notable, with a total of 15 journal articles published between 2013 and 2020. His research focuses on advancing understanding in the realms of management studies, making him a valuable asset to both his institution and the academic community at large. He can be contacted at email: Jacob.joseph.k@christuniversity.in.



**Dr. Saba Fatma**     MBA, Ph.D., is an Associate Professor at the School of Business and Management, affiliated with Christ University. With a diverse research portfolio, her interests span customer experience, pricing strategies, retail dynamics, and educational paradigms. Renowned for her scholarly contributions, she has numerous publications featured in prestigious journals including Scopus, Web of Science, and other eminent academic platforms. She can be contacted at email: saba.fatma@christuniversity.in.