IJIREEICE

ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13340

A Machine Learning-based System for Fake Profile Identification

S. DHARSHAN[1], S. SAKTHI VEL[2], S.S. KISHORE[3], DR.K. THENMOZHI[4]

Student, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore,
Tamil Nadu, India[1-3]

Professor, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore,
Tamil Nadu, India[4]

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. Online Social Networks (OSN) are contributed in all areas such as Research in all domains, Job-related areas, Technology oriented areas, Health care, and business-oriented areas, Information gathering and data collection, and so on. One of the biggest problems on these social media platforms is fake profiles. Impersonating to be someone else and causing harm and defamation to the real person or advertising or popularizing removed propaganda on someone’s name to get more benefit is the motto of such profile creators. There have been many studies regarding these fake accounts and how can they be mitigated. Many approaches such as graph-level activities or feature analysis have been taken into consideration to identify fake profiles. These methods are outdated when compared to arising issues of these days. In this paper, we proposed a technique using machine learning for fake profile detection which is efficient.

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

I. INTRODUCTION

Online social networking sites (OSNs) have had a profound impact on how people communicate and sustain connections in today's digital environment. Because they make networking, socialising, and communicating easy, these platforms have become indispensable parts of our everyday life. In contrast to the past, whenever social contacts could only take place in person or over the phone, OSNs give users the opportunity to virtually engage with individuals all over the world. Access to real-time information, improved global communication, and enhanced cooperation are the outcomes of this shift. OSNs are now essential resources for both professional and personal development because of their impact in a variety of fields, such as education, work, business, and healthcare. However, a number of safety and privacy concerns are also brought about by these platforms' continued growth.

Millions of people worldwide are impacted by the spread of phoney profiles on social networking platforms, which has become a serious issue. These bogus accounts are frequently made for nefarious reasons, such as money fraud, identity theft, cyberbullying, and the spread of false information. Because OSNs are utilised for a variety of purposes, including networking, entertainment, and job hunting, the existence of phoney accounts compromises the legitimacy and integrity of user interactions. In addition to misleading real users, fake profiles encourage unethical behaviour including disseminating misleading information, conniving gullible people, and launching social engineering assaults. In order to guarantee a more secure and dependable online environment, investigators and platform administrators are now making it a top priority to address this dilemma.

Fake accounts may affect important domains like politics, finance, and the general population, therefore their effects go beyond mere inconveniences. Several instances have shown how fake accounts have been used to propagate misinformation, sway public opinion, and start phoney trends.

Fake accounts are commonly used in the business world for misleading marketing strategies, increasing follower counts, and creating phoney online reviews to deceive customers. Furthermore, impersonating respectable people and institutions has resulted in credibility loss and harm to one's reputation. It is crucial to create sophisticated methods to recognise and lessen the hazards posed by phoney profiles as fraudsters' tactics to get beyond conventional security measures are always changing along with OSNs.

DOI: 10.17148/IJIREEICE.2025.13340

Current techniques for identifying phoney accounts usually involve examining user behaviour, profile information, and interaction trends. Although these methods have occasionally worked well, they frequently don't keep up with the increasingly complex strategies used by dishonest users. The constantly changing characteristics of OSNs makes it difficult for conventional methods like rule-based filtering and graph- based detection to keep up. Since scammers are always changing their tactics, it can be difficult to tell the difference between real and fraudulent accounts. In order to improve detection accuracy and guarantee preventative actions against fraudulent activities, researchers have been investigating more effective approaches. This calls for the incorporation of intelligent technologies that can detect and eliminate fraudulent profiles with little assistance from humans.

The use of machine learning algorithms has demonstrated encouraging outcomes in recent years when it comes to identifying fraudulent internet activity. Machine learning algorithms can examine enormous volumes of user data, spot questionable activity, and flag accounts that could be fraudulent by utilising data-driven insights. Machine learning-based strategies are more flexible than traditional ones, enabling them to change in tandem with new threats. These models can become more accurate predictors and better at differentiating between real and fraudulent profiles by learning from past data. The way social media companies handle the rising issue of phoney profiles might be completely changed by this move towards intelligent automation.

An effective false profile detection system may greatly improve platform integrity and user security. Social networks may provide a more reliable atmosphere for users to communicate and participate by reducing the number of fake accounts. Strong detection systems can also guarantee adherence to data privacy laws, shield consumers from online dangers, and slow the spread of misleading material. Such systems work well because they may strike a compromise between efficiency and precision, minimising false positives and increasing the identification of real threats.

Research and innovation must continue as the battle against phoney profiles heats up in order to keep up with new threats to internet security.

In the end, combating the problem of fraudulent accounts necessitates a multifaceted strategy that includes user awareness, policy enforcement, and technology developments. Collaboration between social media businesses, cybersecurity specialists, and regulatory agencies is just as vital as machine learning algorithms in identifying bogus accounts. OSNs may build a more secure and genuine online environment by enforcing strict verification procedures and encouraging a culture of digital responsibility. The continuous initiatives in this field demonstrate the shared dedication to protecting social media platforms' integrity and guaranteeing that users may communicate in a safe and meaningful way.

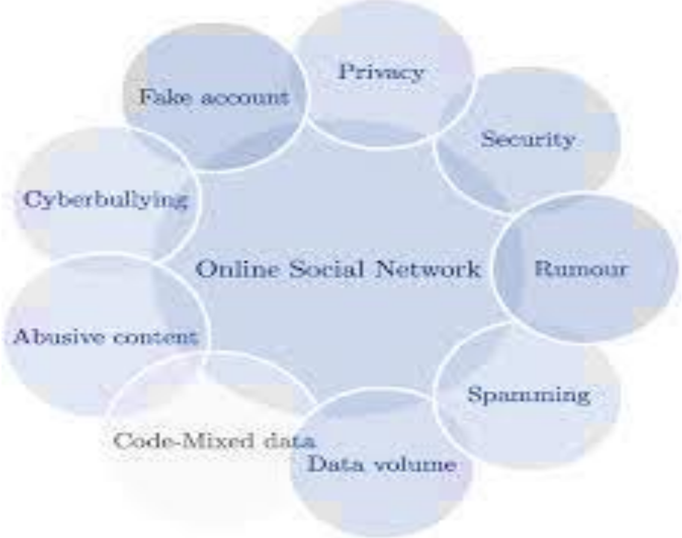


Figure-1: Various Challenges Associated with Online Social Networks

MOTIVATION OF MACHINE LEARNING

Online social networks, or OSNs, have revolutionised how individuals interact, exchange information, and connect. Knowledge sharing, professional networking, and interpersonal interactions have all been transformed by these platforms. Users now have the option to join in debates, collaborate on research, and locate career possibilities with only a few clicks. But since OSNs have grown quickly, a number of issues have surfaced, such as disinformation, cyberthreats, and privacy issues.

Among these, the spread of phoney profiles is a serious problem that jeopardises platform integrity and user confidence. Malicious activities including identity theft, disseminating misleading information, and influencing public opinion are common uses for fake accounts. Conventional techniques for identifying fraudulent accounts depend on laborious and ineffective rule-based systems or manual verification.

Prior methods for identifying fraudulent profiles mostly relied on heuristic-based detection methods, rule-based filtering, or user-reported complaints. These techniques depended on pre-established patterns including content verification, buddy network analysis, and the frequency of questionable activity. Traditional approaches are no longer viable, though, as hackers have adjusted by creating increasingly complex ways to avoid detection. Additionally, because OSNs have so many users, manual review procedures are not scalable. Human-defined rule- based automated detection techniques are prone to mistakes and frequently miss the changing strategies employed by those who create false profiles. A more clever and flexible strategy is needed to stay up with new dangers as fraudulent operations become more sophisticated.

A potent weapon in the fight against online dangers, such as the identification of fraudulent profiles, is machine learning (ML). Because machine learning models learn from past data and get better over time, they are more resilient to emerging threats than rule-based systems. By examining characteristics including user behaviour, connections to networks, and content trends, machine learning algorithms are able to reliably differentiate between authentic and fraudulent accounts. For example, supervised learning models may be trained to anticipate new accounts using labelled datasets that contain both real and false profiles. By spotting irregularities in user behaviour, unsupervised learning approaches can point up possible phoney profiles that deviate from normal activity patterns. OSNs can preserve platform integrity with a scalable solution because to ML's dynamic nature, which guarantees ongoing progress.

Comparing machine learning techniques to conventional detection methods reveals a number of benefits. They reduce the time needed for manual verification by enabling real-time identification of phoney profiles. Secondly, ML models are ideal for massive social media with millions of members since they are very scalable. Machine learning systems can also effectively handle large volumes of data, revealing intricate linkages and patterns that rule-based systems would miss. To improve detection accuracy, ML-driven techniques may also integrate data from other sources, including content analysis, interaction patterns, and user metadata. These models get better over time as a result of constantly learning from fresh data, guaranteeing their continued efficacy against changing fraudulent activity. These advantages demonstrate the need to use machine learning (ML) techniques to address the rising issue of fraudulent accounts.

To successfully identify phoney profiles, a variety of machine learning approaches have been investigated. In classification tasks, supervised learning algorithms like Random Forest, Decision Trees, Support Vector Machines (SVM), and Neural Networks have shown excellent accuracy. Datasets with labelled examples of real and fraudulent accounts are used to train these models. Without previous labelling, unsupervised methods such as anomaly detection and clustering can reveal questionable patterns of behaviour. Furthermore, text material, user-generated media, and behavioural patterns are being analysed using deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). The dependability of false profile detection systems is further reinforced by ensemble learning techniques, which integrate several models to improve forecast accuracy.

OVERVIEW OF THE PROJECT

Greetings Modern civilisation has been profoundly impacted by Online Social Networks (OSNs), which have altered the way people connect, communicate, and sustain relationships. These platforms provide smooth professional and social networking in a number of domains, such as technology, business, healthcare, and research. OSNs must contend with issues including false information, privacy problems, cyberthreats, and most notablyphony profiles as they grow. Due of their involvement in fraud, defamation, impersonation, and propaganda dissemination, fake accounts seriously endanger users. For platform integrity and user security to be maintained, such risks must be recognised and mitigated. When it comes to dealing with contemporary dangers, conventional techniques like feature-based detection and graph analysis have proven inadequate. In order to successfully identify and remove phoney profiles from OSNs, a sophisticated method utilising machine learning methods is suggested.

Social media fake personas are becoming a bigger problem for people, companies, and organisations. These accounts are made by malicious people in order to propagate false information, conduct fraud, influence public opinion, or impersonate others.

Conventional detection techniques are no longer effective due to the growing complexity of these profiles. Many phoney accounts imitate actual users by using automated interactions, manufactured personal information, and falsely created photos.

DOI: 10.17148/IJIREEICE.2025.13340

Such phoney accounts have an influence on financial fraud, political propaganda, and disinformation efforts in addition to violating personal privacy. Strong detection systems that can recognise and eliminate these fraudulent accounts instantly are needed to address this problem. Current solutions depend on network-based and behavioural aspects, but because fraudulent accounts are constantly changing, a sophisticated machine learning-driven strategy is required to successfully counter these threats.

Architecture and Implementation of the System Preprocessing, feature extraction, model training, classification, and data gathering are some of the phases that make up the system architecture. First, information is collected from both real and phoney profiles on different social networking sites. Data quality is improved by preprocessing methods such feature selection, text normalisation, and noise reduction. Using historical information, machine learning models are taught to categorise profiles according to recognised structural and behavioural characteristics. The technology uses real- time monitoring to dynamically identify new fraudulent activity. By using recently discovered phoney profiles to retrain models, a feedback loop is incorporated to increase accuracy. In order to give decision-making transparency and enable administrators and users to comprehend the reasoning behind categorisation judgements, explainable AI approaches are also integrated.

MACHINE LEARNING IN FAKE PROFILE DETECTION

A vital component of contemporary life, online communal networks (OSNs) enable users to interact, communicate, and exchange information on a worldwide scale. Many domains, such as research, job social media, healthcare, business, and technology, benefit greatly from these platforms. However, in addition to their benefits, OSNs come with a number of concerns, the most significant of which is the spread of fraudulent profiles. The creation of fake accounts is done for nefarious purposes such disseminating false information, posing as somebody, and committing fraud. People, companies, and even national stability are seriously threatened by the existence of these accounts. Although there are a lot of conventional ways to identify and counteract these fraudulent submissions, they are becoming antiquated because of the changes in hostile actors' tactics.

Fake accounts provide a serious cybersecurity risk as they may be used for cyberbullying, identity theft, scams, and political manipulation. Attackers use OSNs to advocate unlawful activity, disseminate propaganda, and disparage people or groups. Because Facebook, Instagram, Twitter, and other social media sites have so many users, it is almost difficult to manually detect such false accounts. Furthermore, standard rule-based detection algorithms are unsuccessful since phoney accounts are frequently made to look authentic. Cybercriminals circumvent security measures by employing complex tactics including automated engagement and bot-driven exchanges. Furthermore, because they mimic human behaviour, fake profiles can easily pass for real ones, making it difficult for standard procedures of verification to identify them.

To identify fraudulent profiles, a number of traditional approaches have been used, such as human verification procedures, keyword filtering, and graph-based analysis. These methods' efficiency and scalability are constrained by their reliance on human interaction and predetermined rules. High false positive and false negative rates result from traditional approaches' inability to keep up with attackers' developing social media strategies. Machine learning-based methods, on the other hand, provide a more flexible and dynamic solution. Large datasets and sophisticated algorithms are used to help machine learning models identify trends and more precisely identify fraudulent activity. By examining user behaviour, profile attributes, and social interactions, methods including supervised learning, unsupervised learning, and deep learning aid in automating the detection process. These models are ideal for identifying and reducing fraudulent profiles since they keep getting better over time.

Numerous machine learning methods, each with their own advantages, have been used to identify phoney profiles on OSNs. Models for supervised learning, including Random Forest, Decision Trees, and the use of support vector machines (SVM), categorise profiles using labelled datasets that include samples of both authentic and fraudulent accounts. Unsupervised learning techniques, such as anomaly detection and clustering, can detect odd behaviour without the need for labelled data. Deep learning models that analyse text, images, and user interactions, like Convolutional neural network networks (CNN) and Recurrent Neural Networks (RNN), also improve detection accuracy. Features such as the age of the account, the number of friends, the frequency of posts, and the engagement patterns are examined by feature extraction techniques. By utilising the advantages of various algorithms, ensemble learning—a combination of several machine learning approaches—further increases detection efficiency.

In online social networks, machine learning has shown itself to be an effective technique for identifying phony profiles. These models outperform conventional techniques in detecting fraudulent activity by utilizing sophisticated algorithms and data-driven insights.

DOI: 10.17148/IJIREEICE.2025.13340

However, machine learning models need to change in tandem with attackers' more complex tactics. Enhancing explainability, lowering bias in detection models, and incorporating real-time fraud protection methods should be the main goals of future research. Furthermore, to provide all-encompassing solutions, researchers, social media businesses, and cybersecurity specialists must work together. Scaling the deployment of AI-powered false profile detection systems would improve online safety, safeguard user identities, and lessen online dangers. As technology develops, further machine learning innovation will be essential to guaranteeing a more secure and reliable online social networking environment.

II. LITERATURE REVIEW

Probing the behavioral patterns usually involves checking the posting frequency, follower growth, and some interaction anomalies that help indicate the presence of fraud in profiles.
Machine Learning Models: All these actions fall under unsupervised learning techniques such as clustering and supervised learning methods like SVM and decision trees.
Natural Language Applications : NLP techniques may also be beneficial in detection of unnatural and repetitive speeches in forge profiles.
Network Tracing: By investigating relations between accounts, group coordinated faked profiles or botnets can be established.of security breaches brought on by fraudulent accounts have been the subject of several studies. Effective detection tactics require an understanding of the nature of these networks.

Online relationships have been severely affected by the existence of phony personas on social media sites. Fraudulent accounts are frequently made for nefarious reasons, such as fraud, disseminating false information, and impersonation. Fake accounts can participate in cybercrime, disseminate propaganda, and influence public opinion, according to studies. Kumar et al.'s (2020) research emphasizes the role that phony accounts play in online fraud and defamation. These accounts use social engineering techniques to trick real users, which frequently results in damage to their finances or reputation. Furthermore, automated bots that mimic human behavior make it much harder to identify bogus accounts. Traditional detection approaches are losing their effectiveness due to the sophistication of these dishonest methods, which calls for the creation of more sophisticated identification procedures.

Numerous techniques have been used to identify phony profiles on OSNs. Heuristic-based techniques like activity tracking and buddy network analysis were the main focus of early research. According to Cao et al. (2019), graph-based techniques examine user connectivity patterns to spot irregularities. Feature analysis is another popular method that looks at characteristics like profile age, activity frequency, and engagement rates. Although these methods offer a certain degree of accuracy, they frequently fall behind the constantly changing fraudulent strategies. The efficiency of traditional detection techniques has been further reduced by the emergence of deepfake technology and automated bot interactions. According to recent studies, combining machine learning and artificial intelligence may greatly improve the precision and effectiveness of false profile identification systems.

A viable method for identifying phony social media accounts is machine learning. In order to categorize fraudulent profiles, several research have investigated supervised and unsupervised learning approaches. To differentiate between real and fraudulent profiles, supervised learning models like decision trees and support vector machines (SVMs) use labeled datasets. To find questionable patterns without pre-established classifications, unsupervised techniques like clustering and anomaly detection have also been used. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two deep learning approaches, have shown impressive effectiveness in detecting fraudulent accounts. The ability to identify misleading text linked to fake profiles has been considerably enhanced by recent developments in Natural Language Processing (NLP). The use of ensemble learning to combine many machine learning algorithms has demonstrated encouraging outcomes in terms of improving detection accuracy.

Even with major improvements, there are still a number of obstacles to overcome in order to identify fraudulent profiles. The fact that fraudulent strategies are always changing and that bad actors are constantly adapting to avoid detection systems is one of the main challenges. Additionally, detection techniques have scaling challenges due to the massive volume of data created on social media networks. Additionally, privacy issues limit the usefulness of some approaches by impeding the acquisition and analysis of user data. The identification method is made much more difficult by the existence of hybrid profiles, or accounts that display both human and bot-like activities. To overcome these obstacles, detection models must be updated often, feature selection methods must be enhanced, and ethical concerns must be incorporated into data processing procedures.
The necessity of adaptable algorithms that can react quickly to new threats is emphasized by researchers.
Novel approaches have been put forth in recent research to improve the identification of fraudulent profiles.

Model training and robustness have increased with the use of generative adversarial networks (GANs) for data augmentation. Additionally, blockchain technology has been investigated as a way to prevent fraudulent account creation and validate user identities. In order to improve the interpretability of machine learning models and help researchers comprehend decision-making processes, explainable AI (XAI) approaches have been created. The creation of hybrid models, which integrate many detection methods for increased accuracy, is one area of future study. Security measures against fake accounts may be further strengthened by cooperation between researchers, social media companies, and regulatory agencies. Reducing the frequency of phony profiles also requires increasing user awareness and putting stronger verification procedures in place.

1.RELATED WORK

Researchers throughout the world are becoming increasingly concerned about the problem of phony profiles on Online Social Networks (OSNs). Numerous research have tried to address this problem in various ways. Rule-based screening techniques were the main emphasis of early efforts, which detected questionable activity including excessive friend requests, unusual communication patterns, or incomplete profiles. But frequently, these methods were unable to keep up with the changing strategies employed by scammers. After that, researchers used heuristic-based methods to distinguish between authentic and fraudulent profiles by examining information and behavioral patterns. These techniques have drawbacks when it came to effectively managing large-scale networks, notwithstanding their occasional success. Furthermore, they were unable to generalize effectively across other social media sites.

Graph-based techniques have become a crucial part of the false profile detection process. Taking into account the structural characteristics of the social network, researchers examined the social relationships among users. Fake profiles frequently display unique connection patterns, such creating close-knit groups with other fake identities or engaging with actual individuals far less frequently. To improve the identification of bogus profiles, strategies such as clustering algorithms, anomaly detection in network topologies, and PageRank-based trust models were used. Although these techniques showed promise, they frequently had trouble with dynamic and changing phony profiles and demanded a significant amount of processing power. Some of these problems were resolved with the advent of deep learning techniques, which made it possible for models to more successfully discover complex patterns within the graph topologies.

The detection of fraudulent accounts has also been greatly aided by feature-based categorization methods. To create categorization models, researchers retrieved a variety of user attributes, such as friend count, activity levels, profile completeness, and engagement metrics. To determine if an account is authentic or false, supervised learning algorithms like Random Forests, Decision Trees, and Support Vector Machines (SVM) have been employed extensively. In order to increase the precision of classification models, some research has looked at ensemble learning strategies. However, a major obstacle was that the quality and availability of labeled datasets were crucial to the efficacy of these techniques. Additionally, feature engineering was sometimes a laborious and manual procedure, which limited these methods' capacity to respond to emerging threats.

In addition to technological methods, scholars have looked at the sociological and psychological facets of creating false profiles. The reasons why people impersonate, the psychological effects of false profiles on victims, and the function of false information propagated by fraudulent accounts have all been examined in studies. Designing more efficient detection and mitigation techniques has required an understanding of these aspects. Some studies have also highlighted the role that policy laws have in preventing fraudulent behaviors on social media platforms, as well as the significance of user education and awareness in lessening the effect of phony profiles.

In the final analysis, identifying fraudulent accounts on social networks has shown to be a complex problem that combines aspects of social sciences, machine learning, network analysis, deep learning, and adversarial learning. Even though there has been a lot of improvement, fraudsters are always coming up with new strategies, therefore this field needs constant study and innovation. By utilizing machine learning to improve the effectiveness and precision of fake profile identification, the suggested method in this research expands on these established techniques, overcoming their drawbacks and adjusting to the latest social network security issues.

2. EXISTING SYSTEM APPROACH

The existing systems use very fewer factors to decide whether an account is Fake or not. The factors largely affect the way decision making occurs. When the number of factors is low, the accuracy of the decision making is reduced significantly. There is an exceptional improvement in fake account creation, which is unmatched by the software or application used to detect the fake account.

Due to the advancement in creation of fake account, existing methods have turned obsolete. The most common

DOI: 10.17148/IJIREEICE.2025.13340

algorithm used by fake account detection Applications is the Random forest algorithm.

The algorithm has few downsides such as inefficiency to handle the categorical variables which has different number of levels. Also, when there is an increase in the number of trees, the algorithm's time efficiency takes a hit.
The majority of false profile detection systems now in use use a small number of indicators to identify if an account is authentic or fraudulent. Usually, these algorithms merely look at simple characteristics like the frequency of posts, account age, and the presence of a profile picture. Modern phony accounts, however, are designed to seem like real users, making it difficult for conventional algorithms to tell them apart. These models frequently produce significant false positive and false negative rates because of the limited number of parameters taken into account. Improving detection accuracy requires a more complete feature set that includes language patterns, network linkages, and behavioral analysis. The efficacy of current detection techniques is still below ideal if a variety of parameters are not taken into account.

Conventional machine learning methods like Random Forest, Support Vector Machines (SVM), and Naïve Bayes are used by the majority of false profile detection systems now in use. Although these algorithms function well on organized datasets, they are unable to efficiently handle complicated data from social networks. These models' main flaw is their dependence on preset patterns, which are rendered outdated when attackers modify their strategies. These models also suffer with real-time processing and lack flexibility, which results in slower detection and reaction times. Modern methods like deep learning and graph-based models are needed to overcome this constraint in order to improve pattern identification and adaptability.

Many of the current detection techniques are no longer effective due to the quick growth of fraudulent accounts. When it comes to clever attackers that are always changing their tactics, rule-based detection systems that rely on preset heuristics are especially unsuccessful. Attackers also take advantage of flaws in social media algorithms, which makes it challenging for traditional models to correctly identify suspicious activity. Traditional systems' inability to self-improve in response to new threats is made worse by their absence of automatic learning. Fake profile detection systems must use adaptive learning strategies like Generative Adversarial Networks (GANs) and Reinforcement Learning to overcome these obstacles.

3.PROPOSED SYSTEM

The proposed framework, the sequence of processes that need to be followed for continues detection of fake profiles with active learning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by social networking companies. The detection process starts with the selection of the profile that needs to be tested. After the selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented. This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake.

Selecting and developing appropriate characteristics for categorization comes next after preprocessing. The system separates authentic profiles from fraudulent ones by extracting behavioral, network-based, and user-based characteristics. Account age, the completeness of the bio, and the frequency of posts are examples of user-based features. Clustering coefficients, reciprocal interactions, and buddy connections are all examined via network- based characteristics. Behavioral capabilities include sentiment analysis of posts, activity surges, and login trends. To make sure that only the most pertinent characteristics are taken into account for classification, the dataset is refined using sophisticated feature selection techniques like Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE).

The classification model is used to classify the profile as authentic, dubious, or fraudulent when the characteristics are completed. The suggested architecture combines deep learning methods like Recurrent Neural Networks (RNNs) and Graph Neural Networks (GNNs) with a variety of machine learning models, such as Random Forest and Support Vector Machines (SVM). By combining the advantages of many models, a hybrid ensemble technique increases accuracy. Because the categorization process is iterative, the model improves its ability to make decisions with each new piece of data. By giving each classification a confidence level, probabilistic scoring systems lower the number of false positives and negatives.

This framework's capacity for active learning makes it special. Feedback is gathered from system administrators and user reports as profiles are categorized. Over time, the model can adjust and get better thanks to this feedback loop. The training dataset is updated with the new labels once mislabeled profiles are manually reviewed.
The model's weighting for various features may be dynamically adjusted with the use of reinforcement learning

DOI: 10.17148/IJIREEICE.2025.13340

techniques. The system's ability to differentiate between real and fraudulent profiles improves with the amount of data it analyzes, strengthening its resistance to changing fraudulent strategies.

In order to sustain high detection accuracy, the framework is constantly trained using fresh data. In order to incorporate freshly labeled data into the training set without necessitating a whole retraining session, the system employs incremental learning. The scalability of cloud-based deployment makes it possible to identify millions of profiles in real time across several OSN platforms. APIs make it easier to integrate with current security procedures for social networking. In order to facilitate prompt actions like verification requests, content filtering, or account termination, automated notifications advise administrators about high-risk profiles. The responsiveness of the detecting system is further improved by real-time monitoring.

III. METHODOLOGY

Machine learning methods are used in the suggested approach for online social network (OSN) fraudulent profile identification in order to improve efficiency and accuracy. Data is first gathered by using web scraping, APIs, or publicly accessible datasets to extract user information from OSNs. User variables including buddy networks, posting frequency, textual content, interaction patterns, and completeness of profiles are all included in the dataset. Preprocessing is essential for managing missing values, getting rid of duplicate information, and cleaning and standardizing data. Furthermore, the quality of textual data is enhanced by normalization methods like tokenization and stemming. In order to minimize biases in model training, data augmentation techniques are used to balance the dataset. The revised dataset is organized for feature extraction when preprocessing is finished, guaranteeing that classification models employ only significant features.

By examining a variety of user and network attributes, feature extraction is essential in spotting fraudulent profiles. Activity logs, post linguistic trends, profile age, and verification status are examples of user-based functionality. Network-based characteristics evaluate user connections, clustering patterns, and the frequency of interactions with other users. Behavioral characteristics assess abnormalities in engagement, time-zone discrepancies, and login behaviors. Text post sentiment analysis aids in identifying hostile, deceptive, or artificial intelligence-generated content. Only the most pertinent qualities are kept by using sophisticated feature selection techniques like Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE). The methodology guarantees a thorough approach to separating phony accounts from real ones by integrating statistical, network, and behavioral factors.

The suggested approach includes feedback systems and active learning to increase flexibility. Fake profiles that are found are reported, and the categorization algorithm is improved with input from administrators or users. By modifying weights and updating decision thresholds, reinforcement learning approaches enable ongoing model development. For smooth detection, the framework is implemented as a scalable cloud-based API that interfaces with OSN platforms. For suspect profiles, automated warnings and intervention tools are used, such as asking for identification verification.

SIMULATION WORKFLOW

A organized workflow for managing account creation and financial data processing is depicted by the block diagram. Before creating an account, pertinent user data is gathered in the "Assemble Data" part of the procedure. This stage guarantees that all information required for verification is gathered. The "Create Account" section starts the account setup procedure when the data is collected. The algorithm makes sure that the necessary fields—like financial and personal information are filled out. Because it lays the groundwork for the validation procedure and ensuing financial transactions, this phase is essential.

The "Validate Data" phase is carried out after account creation to confirm the veracity and correctness of the information supplied. Prior to further processing, data validation makes ensuring that mistakes, inconsistencies, or fraudulent inputs are found. The system advances to the "And Financial Data" step when the validation is successful, at which point pertinent financial records are connected to the newly established account. This stage guarantees that the user's profile has accurate financial data, which is required for transactions or account features.

Following financial data integration, all validated financial information is consolidated in the "Financial Accounts" block, guaranteeing that the user's financial profile is appropriately organized. In the last stage, "Check Out the Results," users or system administrators can examine the data that has been processed. At this point, individuals may view the completed outcomes of their financial setup and any differences can be resolved. A dependable financial processing system is ensured by the

DOI: 10.17148/IJIREEICE.2025.13340

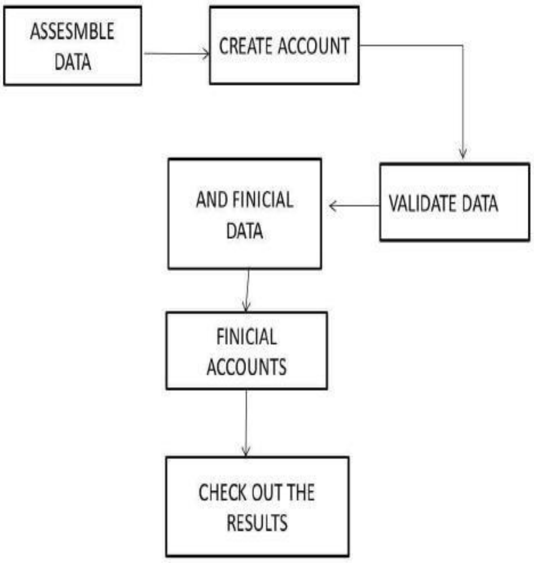
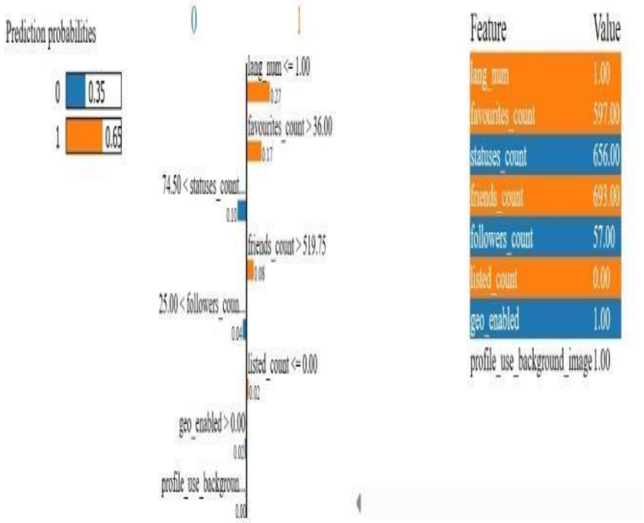


Figure-2: Simulation workflow, which places a strong emphasis on data correctness, validation, and safe account formation. However, a few spelling mistakes in the graphic, such using "FINICIAL" instead of "FINANCIAL," should be fixed for clarity.

IV. RESULT AND DISCUSSION

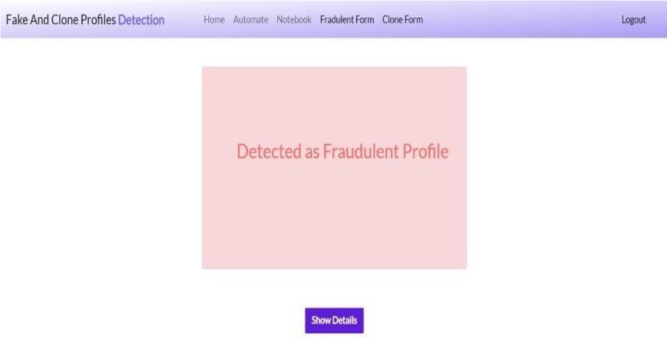
The first image displays a "Prediction Form" where a user inputs various Twitter profile-related numerical features such as "Statuses Count," "Followers Count," "Friends Count," "Favourites Count," and "Listed Count." Additionally, it includes checkboxes for "Geo Enabled" and "User's Profile Background Image" along with a dropdown for language selection. The form has a "Predict" button, suggesting it is part of a machine learning or classification system.



Feature	Value
lang_num	1.00
favourites_count	597.00
statuses_count	656.00
friends_count	693.00
followers_count	57.00
listed_count	0.00
geo_enabled	1.00
profile_use_background_image	1.00

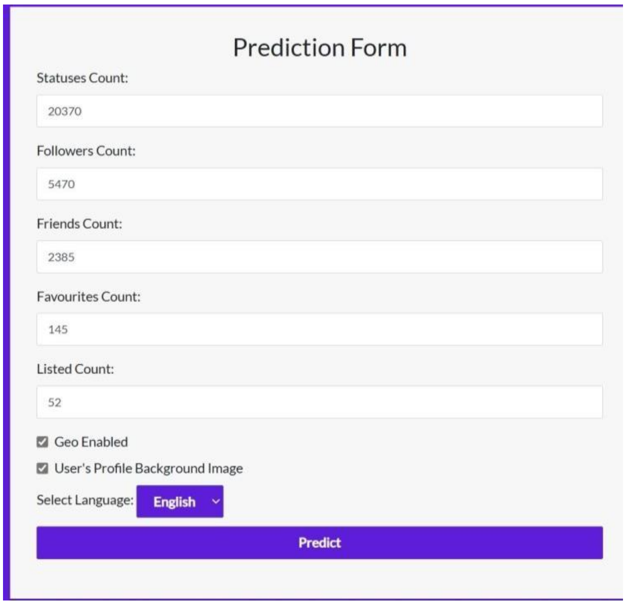
The second image shows the prediction results. The output indicates prediction probabilities, with a high probability (0.89) assigned to class "0" and a lower robability (0.11) for class "1." A feature importance visualization highlights the most influential features in the classification, with attributes such as "Followers Count," "Statuses Count," "Favourites Count," and "Friends Count" contributing significantly. The feature- value table presents the exact input values used in the prediction.

This setup appears to be a Twitter profile classification model, possibly used for detecting bots or categorizing users based on their activity and profile characteristics.



Detected as Fraudulent Profile

Figure-2: Prediction Probabilities1



Prediction Form

Statuses Count: 20370

Followers Count: 5470

Friends Count: 2385

Favourites Count: 145

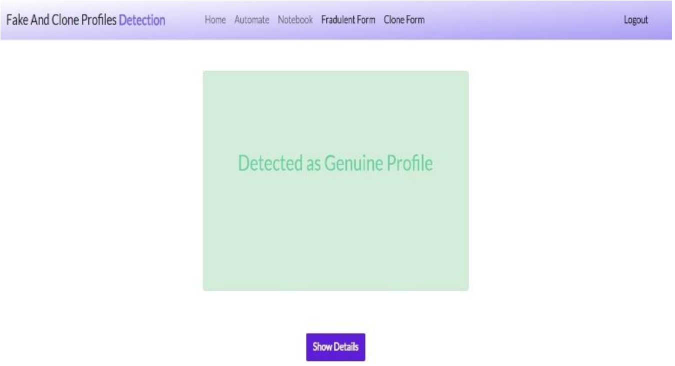
Listed Count: 52

☑ Geo Enabled

☑ User's Profile Background Image

Select Language: English

Figure-3: Prediction Form



Detected as Genuine Profile

Figure-4: Show the Prediction

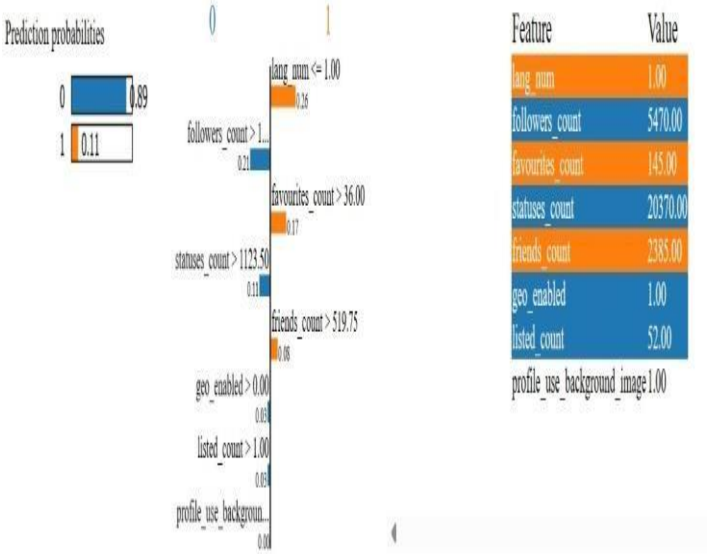


Figure-5: Prediction Probabilities 2

VI.CONCLUSION

Through utilization of different kinds of Machine Learning Algorithms, this paper is aimed to exploit different aspects of dataset which has not been deeply considered in literature and to find a good way of detection of the fake and automated accounts. In this paper we have presented a Machine Learning pipeline for detecting fake accounts in online social networks. Rather than making a prediction using one single algorithm, our system uses three different classification algorithms to determine whether or not an account in the provided dataset is a fake account or not. Our evaluation using Support Vector Machine, Random Forest and Neural Networks showed strong performance, and the comparison of the accuracy of prediction seemed to be higher using Support Vector Machine for the given dataset. The Accuracy of detecting fake accounts is found to be higher using Random Forest Algorithm followed by Neural Networks Algorithm for a given dataset.

Additionally, utilizing deep learning architectures like Graph Neural Networks (GNNs) or Transformer-based models could improve the detection of sophisticated fake accounts that mimic real user behavior; incorporating real-time monitoring and adaptive learning mechanisms will also allow the system to evolve with emerging patterns of fraudulent activities, ensuring continuous improvement in fake account detection across various online social networks; and combining multiple models through techniques like stacking or boosting can help mitigate weaknesses in individual algorithms and enhance overall performance. Future improvements to this approach could involve integrating ensemble learning techniques to further improve classification accuracy and robustness.

REFERENCES

[1] Giglietto, N. Righetti, L. Rossi, and G. Marino, ''It takes a village to manipulate the media: Coordinated link sharing behavior during 2018 and 2019 Italian elections,'' Inf., Commun. Soc., vol. 23, no. 6, pp. 867– 891, May 2020.
[2] M. Mazza, M. Avvenuti, S. Cresci, and M. Tesconi, ''Investigating the difference between trolls, social bots, and humans on Twitter,'' Comput. Commun., vol. 196,pp. 23–36, Dec. 2022.
[3] K. Thomas, C. Grier, D. Song, and V. Paxson, ''Suspended accounts in retrospect: An analysis of Twitter spam,'' in Proc. ACM SIGCOMM Conf. Internet Meas. Conf., New York, NY, USA, Nov. 2011, pp. 243– 258.
[4] Yang, R. C. Harkreader, and G. Gu, ''Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers,'' in Recent Advances in Intrusion Detection, R. Sommer, D. Balzarotti, and G. Maier, Eds. Berlin, Germany: Springer, 2011, pp. 318– 337.
[5] M. Mateen, M. A. Iqbal, M. Aleem, and M. A. Islam, ''A hybrid approach for spam detection for Twitter,'' in Proc. 14th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST), Jan. 2017, pp. 466–471.
[6] B. Erçahin, Ö. Aktaş, D. Kilinç, and C. Akyol, ''Twitter fake account detection,'' in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388–392.
[7] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ''Twitter spam detection: Survey of new approaches and comparative study,'' Comput. Secur., vol. 76, pp. 265– 284, Jul. 2018.