JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Implementation of Fraud Detection on Social Media Networking Websites using Machine Learning

[1] Sai Sindhu V, [2]Tejovathi S, [3]Lokapavani S, [4] Ravi Paavana, [5] Pavan kumar U

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor
[1] Department of Electronics and Communication Engineering (ECE),
[1]Narayana Engineering College, Nellore, India

Abstract : The main objective behind developing this project is to detect the frauds on social media Networks. This days, social media has a significant impact on everyone's life. Most people frequently utilize social media platforms such as Facebook, Twitter, Instagram. To determine who poses threats on these platforms, it is necessary to distinguish between the real and fake social media profiles. In this study identifying fake accounts utilizing data types is improved in this proposed work employing high gradient boosting algorithms and Natural Language Processing. In order to investigate the relationship between various machine learning methods and multi-features in time series, in this study a variety of Python and the necessary libraries, such as SK learn, Numpy, and Pandas are used and XG Boost is the best machine learning technique for finding fake profiles.

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. 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. You must make use of automatic bot prevention technology. By making the LSTM, XG boost, random forest, and multi-layered neural network models, made a contribution to technology. These methods are some instances of machine learning with supervision.

II. EASE OF USE

A.Machine Learning

Machine learning is a subfield of AI that focuses on developing algorithms and models that give computers the ability to learn from data, identify patterns from within the data, and make decisions based on their learnings.

Different types of machine learning

1. supervised learning
2. unsupervised learning
3. Reinforcement learning

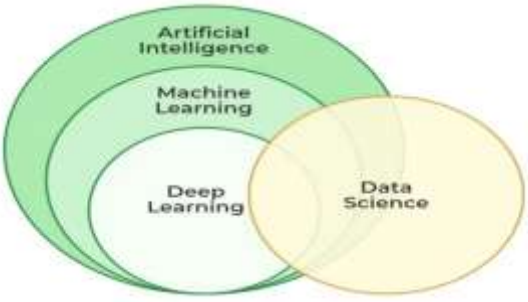

FIG 1. MACHINE LEARNING

Fraud Prevention and Detection

Increasingly, machine learning is being used in fraud prevention and detection due to its ability to analyse large quantities of data, identify patterns, and adapt to new information. Some common applications of machine learning in fraud prevention include :

1. Anomaly Detection
2. Risk Scoring
3. Network Analysis
4. Identity Analysis
5. Adaptive Analysis
6. Test Analysis

B Challenges and limitations of Machine Learning

The primary challenge of machine learning is the lack of data or the diversity in the dataset. A machine cannot learn if there is no data available. Besides, a dataset with a lack of diversity gives the machine a hard time. A machine needs to have heterogeneity to learn meaningful insight. It is rare that an algorithm can extract information when there are no or few variations. It is recommended to have at least 20 observations per group to help the machine learn. This constraint leads to poor evaluation and prediction.

III. PROPOSED METHODOLOGY

We employed XG Boost, a random forest [19] method, and observable features from a profile-focused multi-layered neural network in this model. The model can easily read the extracted characteristics that were saved in a CSV file. Finally, whether a profile is genuine or not is finally determined by the training, testing, and analysis of the model. Because Google provides free GPU utilization, researchers choose Google Colab to build models. The 12-gigabyte (GB) Google Colab NVIDIA Tesla K80 GPU can run continuously for 12 hours. This technique is quite good at identifying fake profiles. After being trained, this model's accuracy might be greater than in earlier comparable research. This design also emphasizes a visually pleasing framework. A representation of the system architecture is shown in Figure below.

I.

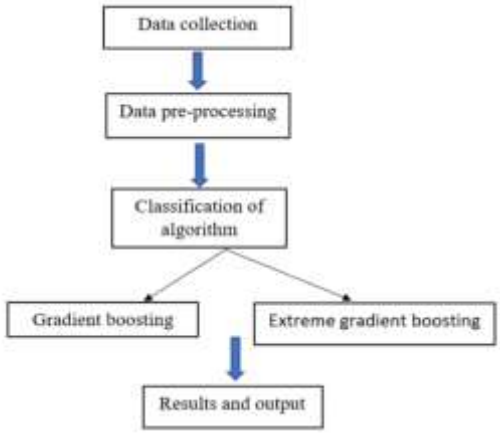

Fig 2. System Architecture

A .Data Collection and Preprocessing

The first step in implementing our fake account detection system is data collection. We gather a comprehensive dataset comprising user activities, including spam commenting, interaction rates, and indicators of artificial behavior. This data is sourced from various social media platforms, ensuring it includes a mix of genuine and fake accounts for robust analysis. Once collected, the data undergoes preprocessing to clean and transform it into a suitable format for analysis. Missing values are handled appropriately, and categorical variables are encoded. Feature engineering is also performed to extract and create new features that may enhance the model's performance.

B. Feature Selection and Engineering

With the pre-processed data ready, we move to feature selection and engineering. This involves identifying the most relevant features that contribute to distinguishing fake accounts from genuine ones. Techniques such as correlation analysis and principal component analysis (PCA) are employed to reduce dimensionality and select key features. Additionally, we engineer new features that capture the nuances of user behaviour, such as the frequency of posts, average interaction rates, and patterns in comment activity. These engineered features are crucial as they provide additional predictive power to the gradient boosting model.

C. Model Training With Gradient Boosting Algorithm

The core of our implementation is the gradient boosting algorithm, specifically XGBoost and GBM (Gradient Boosting Machine). We train these models using the prepared dataset. Gradient boosting involves building an ensemble of decision trees, where each tree corrects the errors of the previous ones. This iterative process continues until the model achieves optimal performance. We use various performance metrics such as accuracy, precision, recall, and F1 score to evaluate the model during training. Hyperparameter tuning is conducted to optimize the model further, although even default hyperparameter values yield impressive results.

D. Model Evaluation and Deployment

After training and fine-tuning the model, we evaluate its performance on a separate test dataset to ensure its effectiveness in identifying fake accounts. The model's predictions are compared with actual labels to assess its accuracy and reliability. Once validated, the model is deployed into a real-time environment. We integrate the gradient boosting model with a backend system that monitors user activities continuously. The system flags suspicious accounts based on the model's predictions, enabling proactive measures to be taken against fake accounts. Continuous monitoring and periodic retraining are implemented to keep the model updated with the latest trends and behaviors in fake account activities.

E. Handling Missing Data and Robustness

One of the strengths of our chosen gradient boosting algorithm is its ability to handle missing data. Unlike some other models that require complete datasets, gradient boosting can manage missing values gracefully, imputing them during the training process. This feature is particularly beneficial as it ensures the robustness of our system in real-world scenarios where data might be incomplete. The model's robustness is further enhanced by using cross-validation techniques, ensuring that it generalizes well to unseen data and maintains high accuracy across different subsets of the dataset

F. Dataset Collection

The MIB dataset was used .3474 actual profiles and 3351 false profiles made up the data set. The data set utilized E13 and TFP for legitimate accounts and TWT, INT, and FSF for fraudulent ones. For machine extraction, the data is stored in CSV format. In Figure, each indicator x-axis displays the characteristics that were utilized to recognize the fake profile. During the preprocessing, these were chosen. The number of entries for each feature that is present in the dataset is shown on the y-aixs.

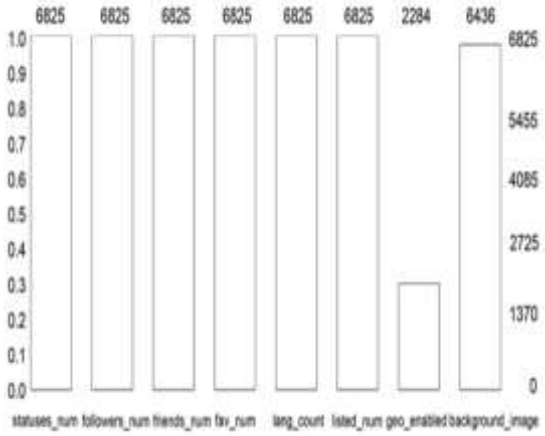

Fig 3. Dataset of fraud detection

G. Model Development

In this section, we presented the proposed solution to the challenge of detecting phony accounts by focusing on the features of such a situation. To begin with, a calculation was done to get the social network's graph's adjacency matrix. After that, a calculation was made to determine the degrees to which nodes (social network users) are similarly based on their network friends. Following that, the similarity matrices for each of the stated metrics were constructed, including the similarity based on common friends, the similarity based on Jaccard, the similarity based on cosine, and any other relevant measures. At this point, several matrices were shown to show how similar the nodes were to each other.

All of the data was tagged as normal because the data in these circumstances is unbalanced and 98 - 99 percent of it relates to the exact majority class (normal users), making it difficult to understand the clarification of both the minority class (fake subscribers) and the overall accuracy of classifications. The SMOTE was used to get the statistics to reach equilibrium in order to tackle this problem.

H. Artificial Neural Network

Deep learning neural network systems behave similarly to the similar neuron networks largely seen in the human brain [22]. Each layer of the neural network contains neurons (nodes). we made use of Keras' sequential. Three hidden layers, an output layer, and an input layer are all parts of the model's construction (Figure 3). Each has activation capabilities aside from the output layer. As a function for activating the output layer, sigmoid is used. The model was built using the Adam optimizer and the binary merge loss function. This model makes use of ANN with the aforementioned architecture. Lastly, the sigmoid function gives out a number between 0 and 1 that shows whether it thinks a given profile is fake or real based on its prediction.

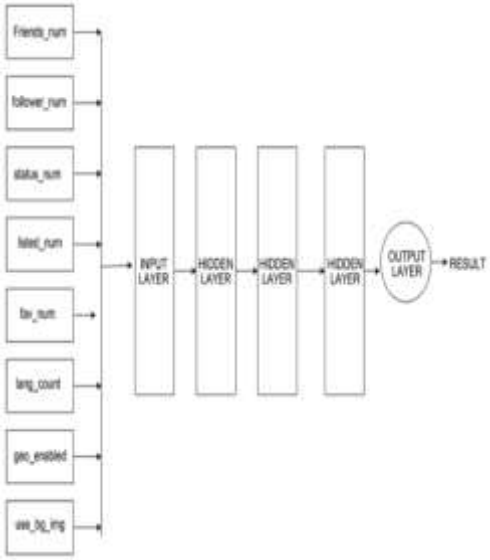

Fig 4. ANN Architecture

I.Random Forest

The ensemble learning approach known as random forest (or random-decision forest) is one example of this kind of method. Machine learning employs this technique because it is simple to apply both to classification and regression issues. Like in Figure 4, rather than depending on a single decision tree, the random forest uses predictions from each tree and predicts the result based on the votes of the majority of predictions. Random-forest, however, creates many more decision trees than the decision tree method does, and the final result seems to be the sum of nearly all of decision trees that have been created. For profile detection, we employed the random forest method. The model takes in data and outputs relevant results. f=1B∑Bb=1fb(x′).The bootstrap aggregating procedure is used to fit the trees (fb) to the sample for the given set of X=x1,x2,⋯,xn and Y=y1,y2,⋯,yn answers. A random sample is selected at regular intervals (B times). After being trained, the following procedure is used to determine the results for a given sample(x').

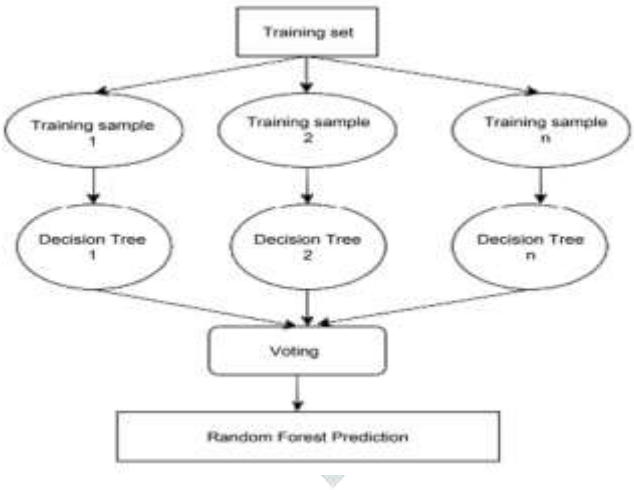

Fig 5.Random Forest Architecture

J . Extreme Gradient Boost

Another ensemble learning technique for regression is XG Boost. Subsampling of different parameters of Stochastic Gradient boosting this algorithm is implemented.

The disadvantage of random forest is that it works best when all the inputs are present, or when there are no missing values. we employs a gradient boosting approach to get around this.

K . Random Forest and Other Approaches

Several model's accuracy, such as decision trees, xgboost, random forests, and ada boosts, is shown in the comparison plot below (Figure 7). The XG boost, which is equal to 0.996, produces the highest level of precision. Additionally, decision trees and random forests both have an accuracy of about 0.99. The author now gets an ADA boost, at last.

The accuracy comparison and ROC curve graphics are shown below.

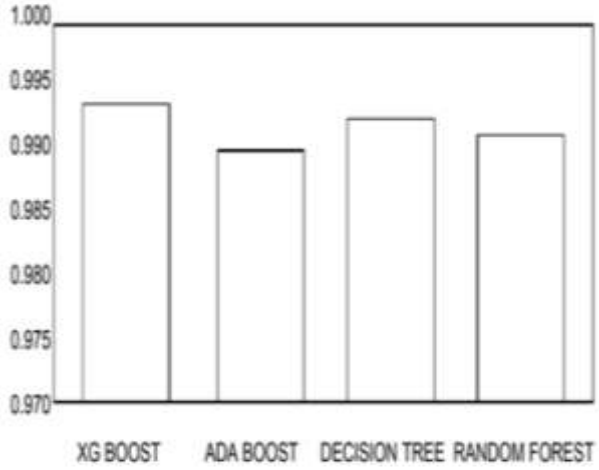

Fig 6.Different Model Accuracy

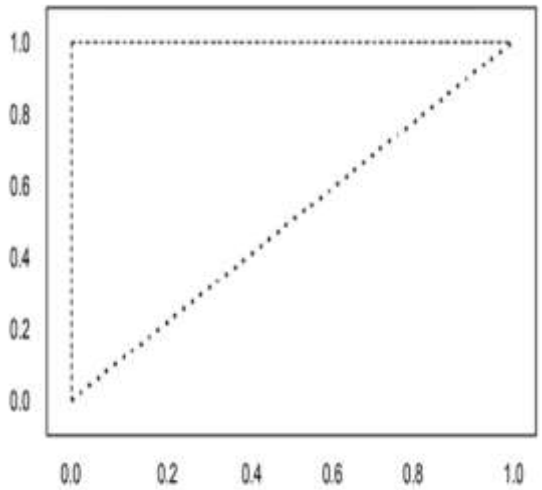

Fig 7.XG Boost ROC Curve

L . Software Description

Visual Studio

Visual Studio is an integrated development environment (IDE) developed by Microsoft for building a variety of software applications, including desktop, web, mobile, cloud, and game development projects. It provides a comprehensive set of tools, features, and extensions to streamline the development process and enhance productivity for individual developers and teams.

IV. RESULTS AND DISCUSSION

Fake accounts on Twitter have the ability to change concepts like influence and popularity, which could have an effect on the economy, the political system, and society. They are dangerous for social media networks. This work uses a variety of algorithms to recognize false profiles, as the authors claimed in the introduction, so that makes sure that users won't be alarmed or damaged by malicious people. The authors of one of the previous research developed a blacklist that effectively distinguishes the fake features from the fake accounts. Various algorithms for machine learning are compared in this study to show which ones produce the best results (XG Boost 99.6%), even though those results are higher (94.9%) than those of the previous spam word list-based method (91.1%). In a study that used dynamic CNN, Deep Profile was introduced as a method that employs a supervised learning algorithm to foresee phony accounts. Another intriguing technique to determine sybil features based mostly on registration time was employed by another study [23]. Because they had similar IP phone numbers and addresses to the sybil, many legitimate individuals were incorrectly labeled as false positives, according to the investigation's authors. In different-sized towns, they had rates of false positives of 7%, 3%, and 21%. The study's authors had a 95% accuracy rate, which was a stunning result. In a study [24] that used feature extraction using phony profiles, the SVM-NN classification system had the highest performance of 98.3% in predicting sybil profiles .

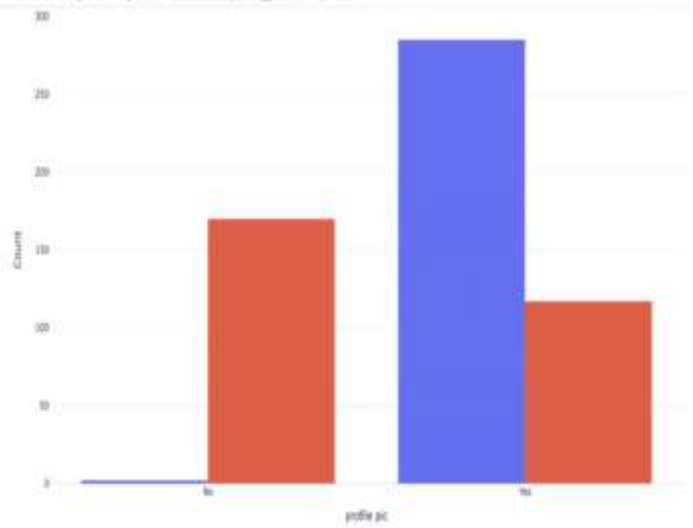

Fig 8. Result

Fig 9. user interface

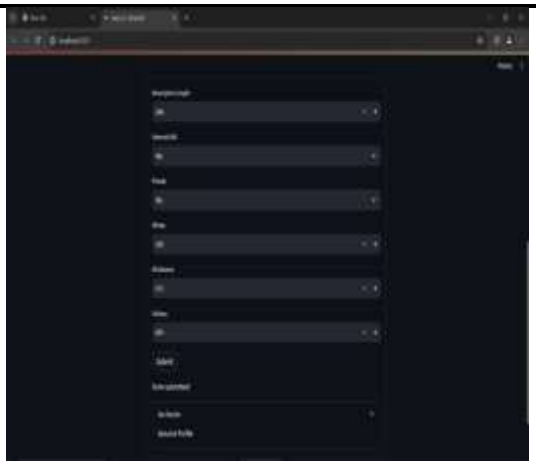

Fig 10.Fraud Detection of Real Account

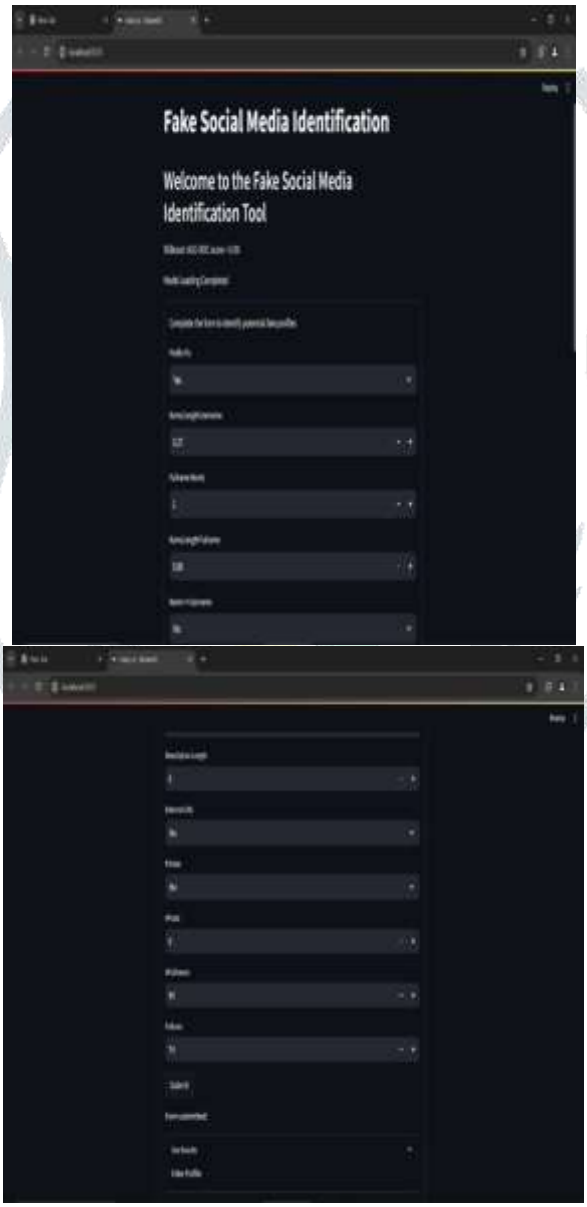

Fig 11.Fraud Detection of Fake Account

V . CONCLUSION

In summary, the project on detecting fake accounts through the application of the gradient boosting algorithm and innovative methodologies has yielded promising outcomes. By leveraging advanced machine learning techniques and feature engineering approaches, the system demonstrates enhanced accuracy and robustness in identifying fraudulent activities on social media platforms. Through rigorous experimentation and performance evaluation, the project outperforms previous methods, showcasing its efficacy in distinguishing between genuine and fake accounts.

Looking ahead, the success of this project underscores its potential for broader applications and future advancements in fraud detection and cybersecurity. Further research and development efforts could focus on refining the algorithm, exploring additional data sources, and enhancing collaboration across interdisciplinary domains to address emerging challenges in online security and trustworthiness.Ultimately, the project contributes to the ongoing efforts to create a safer and more secure digital environment for users worldwide.

REFERENCES

[1] Van Der Walt, E. and Eloff, J. (2018) Using Machine Learning to Detect Fake Identities: Bots vs Humans. IEEE Access, 6, 6540-6549.

[2] Kudugunta, S. and Ferrara, E. (2018) Deep Neural Networks for Bot Detection. Information Sciences, 467, 312-322.

[3] Ramalingam, D. and Chinnaiah, V. (2018) Fake Profile Detection Techniques in Large-Scale Online Social Networks: A Comprehensive Review. Computers & Electrical Engineering, 65, 165-177.

[4] Hajdu, G., Minoso, Y., Lopez, R., Acosta, M. and Elleithy, A. (2019) Use of Artificial Neural Networks to Identify Fake Profiles. 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, 3 May 2019, 1-4.

[5] Swe, M.M. and Myo, N.N. (2018) Fake Accounts Detection on Twitter Using Blacklist. 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 6-8 June 2018, 562-566.

[6] Wanda, P. and Jie, H.J. (2020) DeepProfile: Finding Fake Profile in Online Social Network Using Dynamic CNN. Journal of Information Security and Applications, 52, Article ID: 102465.

[7] Kodati, S., Reddy, K.P., Mekala, S., Murthy, P.S. and Reddy, P.C.S. (2021) Detection of Fake Profiles on Twitter Using Hybrid SVM Algorithm. E3S Web of Conferences, 309, Article No. 01046.

[8] Meshram, E.P., Bhambulkar, R., Pokale, P., Kharbikar, K. and Awachat, A. (2021) Automatic Detection of Fake Profile Using Machine Learning on Instagram. International Journal of Scientific Research in Science and Technology, 8, 117-127.

[9] Chakraborty, P., Muzammel, C.S., Khatun, M., Islam, S.F. and Rahman, S. (2020) Automatic Student Attendance System Using Face Recognition. International Journal of Engineering and Advanced Technology (IJEAT), 9, 93-99.

[10] Sayeed, S., Sultana, F., Chakraborty, P. and Yousuf, M.A. (2021) Assessment of Eyeball Movement and Head Movement Detection Based on Reading. In: Bhattacharyya, S., Mršić, L., Brkljačić, M., Kureethara, J.V. and Koeppen, M., Eds., Recent Trends in Signal and Image Processing, Springer, Singapore, 95-103.

[11] Chakraborty, P., Yousuf, M.A. and Rahman, S. (2021) Predicting Level of Visual Focus of Human's Attention Using Machine Learning Approaches. In: Shamim Kaiser, M., Bandyopadhyay, A., Mahmud, M. and Raym K., Eds., Proceedings of International Conference on Trends in Computational and Cognitive Engineering, Springer, Singapore, 683-694.

[12] Muzammel, C.S., Chakraborty, P., Akram, M.N., Ahammad, K. and Mohibullah, M. (2020) Zero-Shot Learning to Detect Object Instances from Unknown Image Sources. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9, 988-991.

[13] Sultana, M., Ahmed, T., Chakraborty, P., Khatun, M., Hasan, M.R. and Uddin, M.S. (2020) Object Detection Using Template and Hog Feature Matching. International Journal of Advanced Computer Science and Applications, 11, 233-238.

[14] Faruque, M.A., Rahman, S., Chakraborty, P., Choudhury, T., Um, J.S. and Singh, T.P. (2021) Ascertaining Polarity of Public Opinions on Bangladesh Cricket Using Machine Learning Techniques. Spatial Information Research, 30, 1-8.

[15] Sarker, A., Chakraborty, P., Sha, S.S., Khatun, M., Hasan, M.R. and Banerjee, K. (2020) Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data. Journal of Computer and Communications, 8, 50-62.

[16] Ahammad, K., Shawon, J.A.B., Chakraborty, P., Islam, M.J. and Islam, S. (2021) Recognizing Bengali Sign Language Gestures for Digits in Real Time using Convolutional Neural Network. International Journal of Computer Science and Information Security (IJCSIS), 19, 11-19.

[17] Sultana, M., Chakraborty, P. and Choudhury, T. (2022) Bengali Abstractive News Summarization Using Seq2Seq Learning with Attention. In: Tavares, J.M.R.S., Dutta, P., Dutta, S. and Samanta, D., Eds., Cyber Intelligence and Information Retrieval, Springer, Singapore, 279-289.

[18] Ahmed, M., hakraborty, P. and Choudhury, T. (2022) Bangla Document Categorization Using Deep RNN Model with Attention Mechanism. In: Tavares, J.M.R.S., Dutta, P., Dutta, S. and Samanta, D., Eds., Cyber Intelligence and Information Retrieval, Springer, Singapore, 137-147.

[19] Reddy, S.D.P. (2019) Fake Profile Identification Using Machine Learning. International Research Journal of Engineering and Technology (IRJET), 6, 1145-1150.

[20] Khaled, S., El-Tazi, N. and Mokhtar, H.M. (2018) Detecting Fake Accounts on Social Media. 2018 IEEE International Conference on Big Data (Big Data), Seattle, 10-13 December 2018, 3672-3681.

[21] Elyusufi, Y. and Elyusufi, Z. (2019) Social Networks Fake Profiles Detection Using Machine Learning Algorithms. In: Ahmed, M.B., Boudhir, A.A., Santos, D., El Aroussi, M. and Karas, İ.R., Eds., Innovations in Smart Cities Applications Edition 3, Springer, Cham, 30-40.

[22] Joshi, U.D., Singh, A.P., Pahuja, T.R., Naval, S. and Singal, G. (2021) Fake Social Media Profile Detection. In: Srinivas, M., Sucharitha, G., Matta, A. and Chatterjee, P., Eds., Machine Learning Algorithms and Applications, Scrivener Publishing LLC, Beverly, MA, 193-209.

[23] Yuan, D., Miao, Y., Gong, N. Z., Yang, Z., Li, Q., Song, D., Wang, D. and Liang, X. (2019) Detecting Fake Accounts in Online Social Networks at the Time of Registrations. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, 11-15 November 2019, 1423-1438.

[24] Roy, P.K. and Chahar, S. (2020) Fake Profile Detection on Social Networking Websites: A Comprehensive Review. IEEE Transactions on Artificial Intelligence, 1, 271-285.