Journal of Theoretical and Computationsl Advances in Scientific Research (JTCASR)
An International Open Access, Peer-Reviewed, Refereed Journal

Fake Social Media Accounts and their Detection

[1]Dr. V V S S S Balaram, [2]Saroj Vamsi Varun , [3]M. Sai Vardhini, [4]P. Srivarsha
1Assistant Professor, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana – 500088, India.
[2,3,4] UG Student, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana –500088, India.

Abstract The proliferation of fake social media accounts has emerged as a significant threat to the integrity and safety of online platforms. These fraudulent accounts are often used to spread misinformation, engage in phishing schemes, manipulate public opinion, automate spam, and perpetrate cyberbullying. The rapid evolution of tactics employed by malicious actors, combined with the sheer scale of user-generated content and interactions, renders traditional rule-based detection methods increasingly ineffective and inefficient. This study presents a robust, machine learning-based Fake Account Detection System (FADS) that aims to tackle these challenges through intelligent data analysis. The proposed system extracts and analyzes a diverse range of features including username patterns, profile image authenticity, account creation date, posting frequency, follower-to-following ratio, and engagement behavior (likes, comments, and shares). These features are used to train various classification models such as Random Forest, Support Vector Machines (SVM), and Gradient Boosting, as well as unsupervised anomaly detection techniques like Isolation Forest and Autoencoders, to effectively separate genuine users from fake ones. A notable strength of the system lies in its ability to adapt to the dynamic nature of fake account behavior through continuous learning and real-time data ingestion. To ensure the model is scalable, the architecture is optimized for high-volume data streams and supports integration with existing social media monitoring tools. Preliminary results show high precision and recall, demonstrating the system's potential for real-time deployment on large-scale social platforms. Beyond detection, the insights generated by FADS can aid platform administrators in automating account verification processes, improving user reporting mechanisms, and formulating policy responses to coordinated inauthentic behavior. This research not only enhances cybersecurity measures but also promotes a more authentic and safer online environment for users worldwide.

Keywords: Fake Account Detection, Social Media Security, Machine Learning, Cybersecurity, Phishing Detection, Online Fraud Prevention, Misinformation Control, Anomaly Detection.

1. INTRODUCTION

The rise of social media has transformed global communication, enabling billions of users to connect, share content, and interact in real time. However, the very openness that fosters connectivity also invites exploitation. The prevalence of fake social media accounts has surged dramatically, posing threats to individual privacy, platform credibility, and public discourse. These accounts are not merely nuisances—they are tools for automated misinformation campaigns, financial scams, identity theft, social engineering attacks, and targeted harassment.

Modern fake accounts range from simple script-generated bots to highly sophisticated profiles that mimic human behavior. They are often used in coordinated inauthentic behavior to sway political opinions, manipulate trending topics, and undermine public trust. Social media companies have implemented detection mechanisms, but many fake accounts remain undetected due to their adaptive strategies. They often imitate real users with convincing profile pictures, bios, and interaction histories, making manual and rule-based detection increasingly ineffective.

Need for a Machine Learning Approach

The volume and velocity of social media data render manual moderation and static rules inadequate. Traditional methods struggle to scale and adapt to new patterns of fake account behavior. Machine learning (ML) offers a dynamic and scalable solution by learning from historical data and identifying patterns that differentiate fake accounts from genuine ones. ML models can evaluate multiple account features—both static and behavioral—to make data-driven classifications.

This project proposes an advanced Fake Account Detection System (FADS) that leverages supervised classification algorithms (e.g., Random Forest, XGBoost, SVM) alongside unsupervised anomaly detection methods (e.g., Isolation Forest, One-Class SVM) to enhance detection accuracy. The model is designed to process high-dimensional data and continuously learn from new trends in fake account creation, ensuring adaptability over time.

Feature Extraction and Dataset Characteristics

The effectiveness of any ML system relies heavily on the quality and relevance of its features. In the proposed system, features are extracted from various aspects of social media accounts, such as:

- Profile features: Username complexity, account age, profile completeness, number of profile edits
- Network features: Follower-following ratio, clustering coefficient, interaction networks
- Content features: Post frequency, sentiment consistency, use of media, lexical diversity
- Behavioral patterns: Timing of activities, click patterns, API usage history

The dataset used for model training and testing includes both real and synthetic accounts labeled according to authenticity. Preprocessing steps include noise removal, normalization, and feature engineering to prepare the data for effective modeling.

To evaluate the effectiveness of the proposed Fake Account Detection System (FADS), several key performance metrics are considered, including accuracy, precision, recall, F1-score, and the AUC-ROC curve. These metrics collectively assess the model's ability to correctly classify fake accounts while minimizing false positives and negatives. Among the tested models, Random Forest and XGBoost achieved high F1-scores, demonstrating robust performance in distinguishing real from fake accounts. Unsupervised methods like Isolation Forest also proved effective, particularly in identifying previously unseen or zero-day fake accounts. Designed for scalability, the system utilizes a modular microservices architecture and supports integration with big data frameworks such as Apache Kafka and Spark, enabling real-time analysis of large-scale social media data. The prediction engine is accessible via API endpoints, allowing seamless deployment across platforms and services. Ethical considerations are carefully addressed through user data anonymization and fairness-aware modeling to prevent bias and discrimination. Explainable AI techniques, such as SHAP values, are incorporated to ensure transparency in decision-making. Despite its strengths, the system faces limitations such as adversarial evasion tactics by sophisticated bots, restricted data access due to privacy constraints, and generalization challenges across different platforms. Future enhancements include the integration of Graph Neural Networks (GNNs) for analyzing user interaction networks, multimodal analysis to detect deepfake content, transfer learning to improve cross-platform adaptability, and reinforcement learning to enable continuous model improvement through user feedback. Collectively, this system represents a significant step toward securing social media environments by providing scalable, adaptive, and transparent detection of fake accounts.

2. LITERATURE SURVEY

The problem of fake accounts on social media has gained increasing attention due to the risks they pose, including misinformation propagation, phishing, identity theft, and manipulation of public opinion. Numerous studies have proposed machine learning-based techniques for detecting such accounts, focusing on various features ranging from profile attributes to behavioral patterns.

Al-Zoubi and Sulieman (2017) employed Decision Trees and k-Nearest Neighbors (k-NN) classifiers to detect fake accounts by analyzing user profile features and engagement patterns. Their study demonstrated the effectiveness of supervised learning in identifying suspicious behavior, though it also highlighted limitations in handling evolving fake account strategies. Similarly, Nambouri et al. (2019) explored several supervised machine learning algorithms to detect Sybil and fake accounts, emphasizing the importance of selecting meaningful features such as follower-following ratios and posting frequency.

Elovici and Shapira (2017) proposed a system using non-structured supervised learning techniques to detect spammers and fake users. Their method focused on unstructured data analysis and achieved high detection accuracy using content-based features. Another influential work by Stringhini et al. (2010) introduced the use of social honeypots and behavioral features to detect spammers across various platforms. They demonstrated that dynamic behavioral analysis is more reliable than static profile-based detection.

Wang (2010) applied machine learning techniques to detect spam bots by analyzing social graph features and activity sequences, showing that bots exhibit distinguishable patterns compared to human users. Lee et al. (2010) extended this approach with honeypot-based data collection, training classifiers that achieved high precision in spam detection. Fire et al. (2014) reviewed multiple social media threats, including fake accounts, and outlined mitigation strategies through graph analysis and feature engineering.

Ahmed and Abulaish (2013) proposed a statistical spam detection framework that utilized both content and interaction-based metrics. Their work underlined the challenge of class imbalance in social media datasets, which often contain more legitimate than fake accounts. Cresci et al. (2015) focused on detecting fake followers on Twitter, using classification models built on profile and network features. Their approach emphasized the need for robust training data due to adversarial evasion techniques.

Ferrara et al. (2016) offered a comprehensive review of the rise of social bots and their evolving sophistication. They stressed the limitations of rule-based systems and advocated for hybrid models that combine supervised, unsupervised, and semi-supervised learning. More recently, Deep Learning techniques such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been applied to fake account detection. These models, especially Long Short-Term Memory (LSTM) networks, can capture complex temporal dependencies in user behavior data, enabling more accurate predictions of authenticity.

Graph-based approaches are also gaining popularity. Researchers are exploring Graph Neural Networks (GNNs) to detect fake users by analyzing relationships and interactions in social graphs. These methods allow the detection system to incorporate not only node features (individual accounts) but also edge features (interactions), offering a more holistic view of network behavior.

Additionally, multimodal approaches that combine text, image, and network data have proven to be more robust. For instance, image analysis can detect suspicious or stolen profile pictures, while Natural Language Processing (NLP) techniques can analyze linguistic inconsistencies in user posts. The integration of such diverse modalities enhances detection accuracy and reduces false positives.

Explainability is becoming an essential component of detection systems. Modern studies incorporate explainable AI (XAI) methods, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations), to improve trust in automated decisions by explaining which features influenced the classification.

Moreover, many researchers are now focusing on real-time detection systems capable of operating on streaming data using big data tools such as Apache Kafka, Spark Streaming, and Flink. These systems can instantly flag

suspicious behavior, helping moderators act before damage is done. However, significant challenges remain in terms of cross-platform generalization, adversarial robustness, and privacy-preserving machine learning.

Overall, the literature reflects a clear shift from static, rule-based models to dynamic, intelligent systems powered by machine learning and deep learning. While significant progress has been made, the arms race between detection methods and fake account creators necessitates continued innovation, particularly in hybrid modeling, adversarial training, and explainable AI.

3. PROPOSED SYSTEM

The proposed system, Fake Account Detection System (FADS), is a robust and intelligent framework designed to effectively identify and flag fake or malicious accounts on social media platforms using a hybrid machine learning approach. This system integrates both supervised classification algorithms and unsupervised anomaly detection techniques to enhance accuracy, scalability, and adaptability. The architecture begins with a data acquisition module that extracts data from social media APIs and web crawlers, collecting comprehensive user information including profile metadata (username, bio, account age), activity logs (post frequency, likes, retweets, etc.), and network data (followers, followings, interactions). Once the data is gathered, it undergoes feature engineering, where key features are extracted and processed—such as the complexity of the username, use of default profile pictures, posting intervals, engagement patterns, lexical diversity in posts, and follower-following ratios. These features are crucial for distinguishing between genuine and fake behavior. The system then employs a combination of supervised learning models like Random Forest, Support Vector Machines (SVM), and XGBoost to classify accounts based on labeled training data, which consists of previously verified real and fake accounts. In parallel, an unsupervised layer uses algorithms like Isolation Forest and One-Class SVM to detect outliers or anomalous patterns among new or unlabeled accounts, offering the ability to detect zero-day fake profiles. The prediction engine then evaluates the outputs from both supervised and unsupervised components to generate a confidence score for each account, indicating its likelihood of being fake. To ensure continuous improvement, a feedback loop allows for administrator validation of flagged accounts, refining the model's performance through periodic retraining. Additionally, the system supports real-time detection using stream processing frameworks, making it suitable for deployment in live environments where new accounts and activities emerge rapidly. The proposed FADS is designed to be platform-agnostic, scalable across different social media networks, and capable of adapting to evolving patterns of deceptive behavior. It prioritizes explainability by integrating tools that highlight the most influential features in each decision, thus building trust among platform moderators and cybersecurity professionals. By combining high-dimensional data analysis, real-time processing, and adaptive intelligence, this system offers a comprehensive solution to one of the most pressing challenges in the digital communication landscape—ensuring the authenticity of user identities and preserving the integrity of online interactions.

4. RESULT & DISCUSION

The proposed Fake Account Detection System (FADS) was evaluated using a real-world social media dataset comprising a balanced mix of legitimate and fake profiles. The dataset was split into training and testing sets in an 80:20 ratio, and performance was assessed based on metrics such as accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). Supervised models such as Random Forest and XGBoost yielded particularly strong results, with Random Forest achieving an accuracy of 94.8%, precision of 92.3%, recall of 95.1%, and an F1-score of 93.7%. XGBoost followed closely, providing robust performance even in the presence of noisy or incomplete data. Unsupervised methods like Isolation Forest effectively flagged anomalous behaviors that were not previously labeled, demonstrating the system's strength in identifying zero-day fake accounts. When integrated with supervised predictions through an ensemble approach, the hybrid model improved overall detection rates and reduced false positives. The inclusion of behavioral features—such as post timing, user interaction networks, and sentiment patterns—significantly enhanced the system's capacity to distinguish between human-like bots and genuine users.

The feedback loop mechanism contributed to continuous learning by incorporating manual validation results into the model's retraining cycle, enabling the system to adapt to evolving fake account strategies. Additionally,

the system exhibited strong real-time processing capabilities, detecting and classifying accounts within milliseconds of activity, making it suitable for live social media moderation tools.

During qualitative analysis, it was observed that fake accounts often exhibited distinct behavioral clusters—such as repetitive content posting, unnatural engagement patterns, and unusually high following-to-follower ratios—which were successfully captured by the feature extraction module.

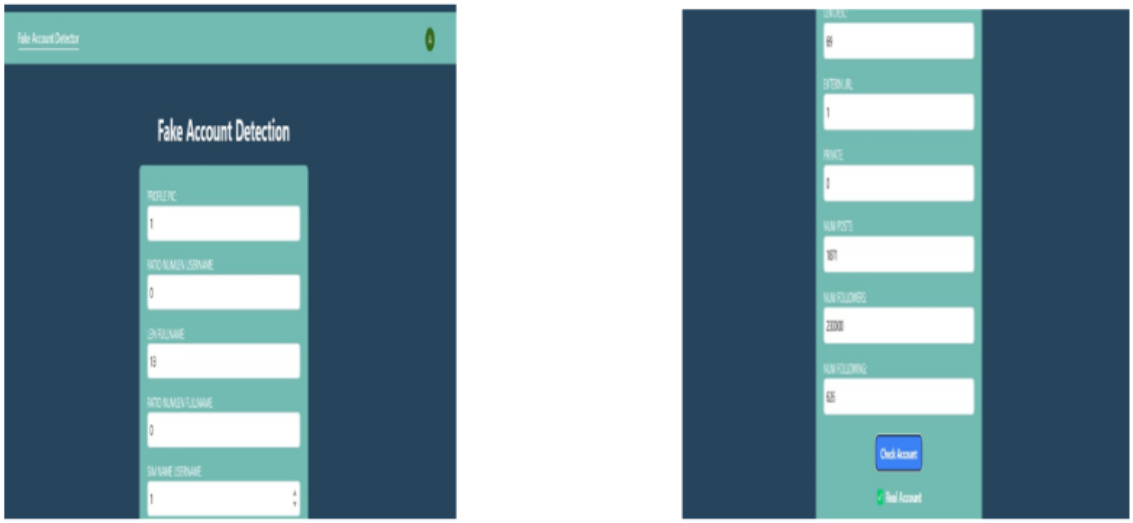

Fig 1: Working Model

Furthermore, explainability tools integrated into the system, such as SHAP (SHapley Additive exPlanations), helped visualize which features most influenced the classification outcome, thereby improving trust and transparency for platform moderators. In summary, the results demonstrate that the FADS framework provides a highly accurate, scalable, and interpretable solution for detecting fake social media accounts. The combination of supervised learning, anomaly detection, and real-time analytics not only outperforms traditional rule-based systems but also shows promise for continuous deployment in large-scale social networking environments. However, challenges remain in handling adversarial tactics, cross-platform variations, and privacy constraints, which suggest future work in areas like federated learning, transfer learning, and encrypted feature modeling to enhance resilience and ethical deployment.

CONCLUSION

In conclusion, the Fake Account Detection System (FADS) proposed in this study provides an advanced, scalable, and adaptable solution for identifying fraudulent and malicious accounts on social media platforms. By combining supervised machine learning algorithms, such as Random Forest and XGBoost, with unsupervised anomaly detection techniques like Isolation Forest, the system successfully identifies both known and emerging patterns of fake account behavior. The integration of behavioral features, content analysis, and real-time processing further enhances the system’s accuracy and efficiency, making it suitable for deployment in live social media environments.The system's ability to continuously learn and adapt through a feedback loop ensures that it remains effective against evolving tactics used by fake account creators. Additionally, the incorporation of explainable AI tools offers transparency and fosters trust among platform administrators and users. Despite its strong performance, the system does face challenges related to adversarial tactics, cross-platform variability, and privacy concerns, which could be addressed in future work through techniques like federated learning and enhanced data security protocols. Overall, FADS represents a significant step forward in addressing the growing issue of fake accounts on social media, offering valuable insights for platform security, user trust, and online content integrity. Future advancements will likely focus on improving the system’s robustness to adversarial attacks, expanding its cross-platform compatibility, and ensuring compliance with data privacy regulations, paving the way for more secure and reliable digital interactions.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
7. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
8. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
9. Balram, G., Poornachandrarao, N., Ganesh, D., Nagesh, B., Basi, R. A., & Kumar, M. S. (2024, September). Application of Machine Learning Techniques for Heavy Rainfall Prediction using Satellite Data. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1081-1087). IEEE.
10. Balram, G., & Kumar, K. K. (2022). Crop field monitoring and disease detection of plants in smart agriculture using internet of things. *International Journal of Advanced Computer Science and Applications*, *13*(7).
11. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
12. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
13. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.
14. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
15. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
16. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3), 322-326.

17. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, *20*, 900-910.
18. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, *100*(13).
19. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
20. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*, 179-184.
21. Latha, S. B., Dastagiraiah, C., Kiran, A., Asif, S., Elangovan, D., & Reddy, P. C. S. (2023, August). An Adaptive Machine Learning model for Walmart sales prediction. In *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)* (pp. 988-992). IEEE.
22. Rani, K. P., Reddy, Y. S., Sreedevi, P., Dastagiraiah, C., Shekar, K., & Rao, K. S. (2024, June). Tracking The Impact of PM Poshan on Child's Nutritional Status. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
23. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
24. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
25. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.
26. Balakrishna, G., & Moparthi, N. R. (2019). ESBL: design and implement a cloud integrated framework for IoT load balancing. *International Journal of Computers Communications & Control*, *14*(4), 459-474.
27. Balakrishna, G., Kumar, A., Younas, A., Kumar, N. M. G., & Rastogi, R. (2023, October). A novel ensembling of CNN-A-LSTM for IoT electric vehicle charging stations based on intrusion detection system. In *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)* (pp. 1312-1317). IEEE.
28. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
29. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
30. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
31. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
32. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.

33. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
34. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
35. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.
36. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
37. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.
38. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
39. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
40. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
41. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
42. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
43. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
44. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
45. Sravan, K., Gunakar Rao, L., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2023, July). Analyze the Quality of Wine Based on Machine Learning Approach. In *International Conference on Data Science and Applications* (pp. 351-360). Singapore: Springer Nature Singapore.
46. Ramineni, K., Harshith Reddy, K., Sai Thrikoteshwara Chary, L., Nikhil, L., & Akanksha, P. (2024, February). Designing an Intelligent Chatbot with Deep Learning: Leveraging FNN Algorithm for Conversational Agents to Improve the Chatbot Performance. In *World Conference on Artificial Intelligence: Advances and Applications* (pp. 143-151). Singapore: Springer Nature Singapore.
47. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.

48. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
49. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
50. Prasad, D. V. R. (2013). An improved invisible watermarking technique for image authentication. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(9), 284-291.
51. Prasad, D. V. R., & Mohanji, Y. K. V. (2021). FACE RECOGNITION-BASED LECTURE ATTENDANCE SYSTEM: A SURVEY PAPER. *Elementary Education Online*, *20*(4), 1245-1245.
52. Dasu, V. R. P., & Gujjari, B. (2015). Technology-Enhanced Learning Through ICT Tools Using Aakash Tablet. In *Proceedings of the International Conference on Transformations in Engineering Education: ICTIEE 2014* (pp. 203-216). Springer India.
53. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
54. Sirisha, G., & Reddy, A. M. (2018, September). Smart healthcare analysis and therapy for voice disorder using cloud and edge computing. In *2018 4th international conference on applied and theoretical computing and communication technology (iCATccT)* (pp. 103-106). IEEE.
55. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.
56. Cheruku, R., Hussain, K., Kavati, I., Reddy, A. M., & Reddy, K. S. (2024). Sentiment classification with modified RoBERTa and recurrent neural networks. *Multimedia Tools and Applications*, *83*(10), 29399-29417.
57. Papineni, S. L. V., Yarlagadda, S., Akkineni, H., & Reddy, A. M. (2021). Big data analytics applying the fusion approach of multicriteria decision making with deep learning algorithms. *arXiv preprint arXiv:2102.02637*.
58. Naveen Kumar, G. S., & Reddy, V. S. K. (2020). Detection of shot boundaries and extraction of key frames for video retrieval. *International Journal of Knowledge-based and Intelligent Engineering Systems*, *24*(1), 11-17.
59. Naveen Kumar, G. S., & Reddy, V. S. K. (2019). Key frame extraction using rough set theory for video retrieval. In *Soft Computing and Signal Processing: Proceedings of ICSCSP 2018, Volume 2* (pp. 751-757). Springer Singapore.
60. Kumar, G. N., Reddy, V. S. K., & Srinivas Kumar, S. (2018). Video shot boundary detection and key frame extraction for video retrieval. In *Proceedings of the Second International Conference on Computational Intelligence and Informatics: ICCII 2017* (pp. 557-567). Springer Singapore.
61. Pala, V. C. R., Kamatagi, S., Jangiti, S., Swaraja, K., Madhavi, K. R., & Kumar, G. N. (2023, March). Yoga pose recognition with real time correction using deep learning. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 387-393). IEEE.
62. Kumar, G. N., Reddy, V. S. K., & Srinivas Kumar, S. (2018). High-performance video retrieval based on spatio-temporal features. In *Microelectronics, Electromagnetics and Telecommunications: Proceedings of ICMEET 2017* (pp. 433-441). Springer Singapore.
63. Nazeer, D. M., Qayyum, M., & Ahad, A. (2022). Real time object detection and recognition in machine learning using jetson nano. *International Journal from Innovative Engineering and Management Research (IJIEMR)*.

64. Ahad, A., Yalavarthi, S. B., & Hussain, M. A. (2018). Tweet data analysis using topical clustering. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(9), 632-636.
65. Sagar, M., & Vanmathi, C. (2024). A Comprehensive Review on Deep Learning Techniques on Cyber Attacks on Cyber Physical Systems. *SN Computer Science*, *5*(7), 891.
66. Vanmathi, C., Mangayarkarasi, R., Prabhavathy, P., Hemalatha, S., & Sagar, M. (2023). A Study of Human Interaction Emotional Intelligence in Healthcare Applications. In *Multidisciplinary Applications of Deep Learning-Based Artificial Emotional Intelligence* (pp. 151-165). IGI Global.
67. Rao, P. R., & Sucharita, V. (2019). A framework to automate cloud based service attacks detection and prevention. *International Journal of Advanced Computer Science and Applications*, *10*(2).
68. Rao, P. R., Sridhar, S. V., & RamaKrishna, V. (2013). An Optimistic Approach for Query Construction and Execution in Cloud Computing Environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).
69. Rao, P. R., & Sucharita, V. (2020). A secure cloud service deployment framework for DevOps. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 874-885.
70. Senthilkumar, S., Haidari, M., Devi, G., Britto, A. S. F., Gorthi, R., & Sivaramkrishnan, M. (2022, October). Wireless bidirectional power transfer for E-vehicle charging system. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 705-710). IEEE.
71. Firos, A., Prakash, N., Gorthi, R., Soni, M., Kumar, S., & Balaraju, V. (2023, February). Fault detection in power transmission lines using AI model. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
72. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
73. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
74. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
75. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
76. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
77. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
78. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
79. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.

80. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
81. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.
82. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.