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

AUTOMATED EMERGING CYBER THREAT IDENTIFICATION AND PROFILING BASED ON NATURAL LANGUAGE PROCESSING

[1]Ch.vasavi, [2]S.Cherishma Sree, [3]B.Chandu Ajay Kumar, [4]P. Ram Vishal

[1]Assistant 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 Cyber threats are evolving rapidly, with attackers often exploiting newly discovered vulnerabilities within hours of public disclosure. Traditional detection methods struggle to keep pace due to the vast volume and complexity of threat data. This research presents an automated threat detection and profiling system that leverages real-time data from Twitter and the MITRE ATT&CK framework for enhanced situational awareness. The proposed system functions in three stages: identifying cyber threats and their names, profiling them based on malicious objectives using machine learning, and generating alerts according to associated risk levels. By integrating threat intelligence with behavioral profiling, the system offers contextual insights into emerging threats. In evaluation, the machine learning-based profiling model achieved an F1-score of 77%, reflecting its high accuracy in classifying threat types. This approach significantly improves early threat detection and response, empowering cybersecurity teams to proactively mitigate risks and limit the impact of cyberattacks. In today's dynamic cyber landscape, the speed at which cybercriminals exploit newly disclosed vulnerabilities poses a critical challenge for cybersecurity teams. Traditional threat detection mechanisms, reliant on static databases or rule-based systems, are insufficient in responding to the rapidly evolving nature of cyber threats. As observed in the case of the Log4j vulnerability, attackers launched exploit attempts mere hours after disclosure, highlighting the need for systems that can provide real-time threat awareness and rapid response capabilities. This framework enhances the agility and effectiveness of threat detection systems and aligns with the broader goal of developing proactive, AI-assisted cybersecurity defense strategies in the era of real-time digital threats.

Keywords: Cyber Threat Intelligence, Natural Language Processing, Machine Learning, MITRE ATT&CK, Threat Detection

1. INTRODUCTION

In an increasingly digital world, the frequency and sophistication of cyberattacks have reached alarming levels. From critical infrastructure and healthcare systems to private enterprises and government databases, no sector is immune to the ever-growing range of cyber threats. One of the most concerning developments in recent years is the speed with which attackers exploit newly discovered software vulnerabilities. The Log4j vulnerability (CVE-2021-44228), for instance, serves as a sobering example of this trend. Within just hours of its public disclosure, threat actors began scanning the internet for unpatched systems and launching attacks, including ransomware deployments, cryptocurrency mining, and data exfiltration. Such events highlight a stark reality: the window between vulnerability disclosure and exploitation is shrinking rapidly, leaving organizations with little time to respond using conventional security practices. Traditional cybersecurity defense mechanisms often rely on signature-based detection, periodic manual updates, or rule-based systems that are reactive rather than proactive. These methods are increasingly inadequate in dealing with the real-time and dynamic nature of modern cyber threats. Furthermore, security analysts are overwhelmed by massive volumes of unstructured threat intelligence data generated across platforms such as news feeds, forums, dark web marketplaces, and especially social media. Among these, Twitter has emerged as a powerful source of real-time threat intelligence, where researchers, vendors, and threat actors alike share updates on emerging threats, indicators of compromise (IOCs), and technical attack details.

To address the limitations of manual and static threat intelligence methods, we propose a novel, AI-powered framework that automates the early detection and profiling of cyber threats by analyzing Twitter data streams in real time. This framework is augmented with the MITRE ATT&CK framework, which provides a structured, behavior-based taxonomy of attacker tactics and techniques. Together, these tools enable a more holistic and contextual approach to cyber threat intelligence.

- Threat Identification: The system continuously ingests Twitter data, performing named entity recognition (NER) and keyword extraction to detect references to cyber threats, malware names, exploits, and CVEs.
- Threat Profiling: Machine learning models, including classification algorithms like Random Forest and deep learning models such as LSTM (Long Short-Term Memory) networks, are employed to analyze and categorize the detected threats based on their intent, tactics, and severity.
- Alert Generation: Based on the threat classification and contextual profiling via MITRE ATT&CK, alerts are generated with assigned risk levels, allowing cybersecurity teams to prioritize responses and implement mitigation strategies accordingly.

A key strength of our approach lies in its automation, scalability, and contextual intelligence. Rather than simply flagging potential threats, our framework provides detailed profiles, linking threats to known attack vectors and operational objectives, thereby enabling more informed and faster responses. In empirical testing, our threat profiling model achieved an F1-score of 77%, demonstrating a promising level of accuracy for real-world deployment. This research aims to significantly enhance proactive cybersecurity capabilities, particularly for Security Operations Centers (SOCs), Computer Emergency Response Teams (CERTs), and IT administrators in both public and private sectors. By leveraging the power of real-time social media analysis, machine learning, and structured threat intelligence, the proposed system represents a critical step toward automated, intelligent, and responsive cybersecurity frameworks suited for the threats of tomorrow.

2. LITERATURE SURVEY

As the cyber threat landscape continues to evolve rapidly, timely threat detection and situational awareness have become critical components of modern cybersecurity operations. Traditional methods of threat intelligence, often dependent on structured reports, known malware signatures, and post-attack forensic analysis, are no longer sufficient to keep pace with the increasingly dynamic nature of cyberattacks. Consequently, researchers and practitioners are turning to unstructured data sources, particularly social media platforms like Twitter, to extract real-time insights and early warning signals about emerging threats. Le et al. [1] introduced a novel approach to cyber threat intelligence (CTI) by leveraging Twitter data through a novelty classification model. Their study emphasized the role of machine learning techniques in identifying new and previously unseen threat narratives from a vast stream of tweets. The model not only filtered relevant information but also assessed the uniqueness of a tweet's content compared to historical baselines, allowing for the prioritization of potentially emerging cyber risks. Twitter has emerged as a prominent platform for the dissemination of threat intelligence due to its speed and openness. Sabottke et al. [4] analyzed the role of social media in predicting real-world exploits, demonstrating that many security vulnerabilities, including critical CVEs, are often discussed on Twitter prior to their widespread exploitation. Their research emphasized the feasibility of building automated systems that track such discussions to generate early alerts, thereby providing organizations with a vital time buffer to mitigate risk.
Similarly, Sapienza et al. [5] investigated the potential of online discussions as early indicators of cyber threats. They applied natural language processing and machine learning techniques to classify relevant tweets and

assign them threat relevance scores. Their system was shown to effectively distinguish between routine cybersecurity chatter and posts that indicated significant risk, such as the emergence of new malware strains or coordinated attack campaigns.

Other researchers have expanded the data sources for threat intelligence beyond Twitter. Nunes et al. [6] explored deep web and darknet forums to mine discussions for proactive CTI. Their framework aggregated information from hidden online communities to uncover indications of planned cyberattacks and vulnerabilities being traded among cybercriminals. Although more complex to access and analyze than social media, these platforms provide rich, actionable intelligence for advanced threat hunting.

In parallel, Mittal et al. [7] developed CyberTwitter, a system that utilizes Twitter streams to generate alerts related to cyber threats. Their system integrates contextual analysis and filtering to eliminate noise and extract meaningful security information. They demonstrated that tweets from trusted sources, such as cybersecurity researchers or vendors, can be reliably used to enhance situational awareness.

Steele [3] and Gartner Research [2] provided foundational definitions of open-source intelligence (OSINT) and threat intelligence. Steele's early work emphasized the strategic importance of publicly available information to military and government agencies, laying the groundwork for the modern application of OSINT in cybersecurity. Gartner later defined threat intelligence as evidence-based knowledge—including context, mechanisms, and indicators—that organizations can use to make informed security decisions.
Another noteworthy study by Shrestha et al. [9] addressed the reliability of social media for cyber threat intelligence. They highlighted the challenges of misinformation and noise, proposing a hybrid approach combining crowd-sourced data with automated verification techniques to improve precision. This aligns with the work of Alam et al. [10], who demonstrated the feasibility of using Twitter for real-time threat monitoring, showcasing how sentiment analysis and entity recognition could enhance the understanding of emerging cyber incidents. Finally, Attarwala et al. [8] explored the general predictive power of Twitter beyond cybersecurity, using machine learning to forecast U.S. presidential election outcomes. Their work underlines the broader applicability of social media mining and reaffirms the predictive capabilities of public online discourse, reinforcing its relevance in cybersecurity forecasting.
Collectively, these studies support the growing consensus that social media platforms, particularly Twitter, are invaluable tools for proactive cybersecurity intelligence. By combining machine learning, natural language processing, and structured frameworks like MITRE ATT&CK, it is possible to transform unstructured tweets into actionable insights that help organizations defend against emerging threats. However, challenges such as false positives, data reliability, and the need for expert curation remain, necessitating ongoing research to refine these systems for broader deployment.

3. PROPOSED SYSTEM

The proposed system presents an AI-driven, real-time cyber threat detection and profiling framework that utilizes open-source intelligence from Twitter and maps identified threats to the MITRE ATT&CK framework. By combining natural language processing (NLP) with machine learning, the system automatically analyzes tweets to extract cybersecurity-related information and generates actionable intelligence that can significantly support security operations. The system is composed of three major modules: Threat Detection, Threat Profiling, and Alert Generation, working cohesively to detect, classify, and report cyber threats with minimal human intervention.

1. Threat Detection Module

This module forms the entry point of the system, responsible for continuously collecting and processing real-time tweets related to cybersecurity. The system integrates the Twitter API to stream and search for tweets containing specific keywords, hashtags, and indicators of compromise (IoCs), such as malware names, CVE identifiers, threat actor names, and terms like "exploit," "vulnerability," or "breach."

Key components include:

Keyword Matching & Hashtag Filtering: Filters tweets using a dynamic list of cybersecurity terms and trending threat keywords.

- Preprocessing Pipeline: Applies NLP preprocessing techniques including:
- Tokenization – breaking down tweets into individual words or terms.
- Lemmatization – converting words to their base forms.
- Stop-word Removal – eliminating common but irrelevant words like “the,” “and,” etc.
- Named Entity Recognition (NER): Extracts meaningful entities from text such as malware names (e.g., "Emotet"), vulnerabilities (e.g., "CVE-2021-44228"), or organizations (e.g., "Microsoft").

This module ensures that only tweets with genuine threat intelligence value are forwarded for deeper analysis.

2. Threat Profiling Module

After identifying potential threats, the next step involves contextualizing and categorizing them. This module maps the extracted threat entities and tweet content to tactical objectives and techniques using the MITRE ATT&CK framework, which is a globally recognized matrix of adversary behavior.

Key functions include:

- Supervised Classification: A machine learning model (Random Forest, SVM, or LSTM) trained on labeled tweet datasets is used to classify tweets into categories such as malware, phishing, privilege escalation, denial-of-service, etc.
- Feature Extraction: Converts tweet content into numerical feature vectors using methods like TF-IDF or word embeddings (e.g., Word2Vec, BERT).
- Behavioral Mapping:
- Objective Identification: Classifies threat intent such as financial gain (e.g., ransomware), espionage (e.g., APTs), or disruption (e.g., DDoS).
- Attack Technique Identification: Identifies methods like spear-phishing, lateral movement, or credential dumping.
- Target Type Recognition: Infers if the threat targets cloud platforms, IoT systems, enterprise infrastructure, or individuals.

This module provides contextual intelligence rather than just raw threat alerts, helping analysts understand the "what," "how," and "why" behind the threat.

3. Alert Generation Module

The final component of the system is responsible for converting the profiled threat data into meaningful alerts. Each identified threat is assigned a risk score, calculated based on several weighted parameters:

- Frequency of Mentions: How often the threat is mentioned across a time window.
- Sentiment Analysis: Negative or urgent language may indicate criticality.
- Novelty Detection: Uses novelty scoring to detect zero-day or emerging threats.

- MITRE Impact Weighting: Higher risk assigned to tactics like initial access, exfiltration, or destruction.
- Alerts are triggered when the computed score surpasses a certain threshold. These alerts include threat name, description, classification, risk score, and recommended actions.

Alerts are:

- Displayed via a web-based dashboard built with React or similar frameworks.
- Pushed to third-party tools like SIEM systems (e.g., Splunk, IBM QRadar) through APIs or webhooks for automated incident response workflows.

4. RESULT & DISCUSION

The proposed AI-driven cyber threat detection and profiling system was evaluated using a dataset of over 50,000 tweets related to cybersecurity threats, collected over a three-month period. Tweets were filtered using predefined keywords and hashtags associated with recent vulnerabilities, such as CVE identifiers, malware names, and attack vectors.

1. Threat Detection Performance

The system demonstrated a high capability for real-time detection of emerging threats. The Named Entity Recognition (NER) model accurately extracted threat entities, achieving a precision of 84% and recall of 79%, resulting in an F1-score of 81.5%. The NLP pipeline, including preprocessing steps like lemmatization and stop-word removal, significantly improved the clarity and quality of the extracted content.

During the observation window, the system successfully identified major cybersecurity events such as the exploitation of the Log4j (CVE-2021-44228) vulnerability and the rise of new malware campaigns like Black Basta and RedLine Stealer. The timeliness of detection was particularly notable, with threats being flagged within hours of their first appearance on Twitter—much faster than traditional news or intelligence sources.

2. Threat Profiling Accuracy

The machine learning classifiers used in the Threat Profiling module were trained using labeled threat data from verified sources. Among the models tested (Random Forest, Support Vector Machine, and LSTM), the Random Forest classifier outperformed others, achieving an F1-score of 77%. It demonstrated robust performance in correctly classifying the threat type, attack technique, and objective.

Profiling threats according to the MITRE ATT&CK framework provided actionable context. For instance, tweets mentioning “Cobalt Strike” were correctly mapped to lateral movement techniques, and those referencing “phishing kits” were tied to credential access tactics. This mapping enabled the generation of meaningful intelligence, offering security analysts a clearer understanding of threat behavior.

3. Alert Generation Insights

Risk scoring based on tweet frequency, sentiment, novelty, and alignment with high-impact MITRE tactics enabled prioritization of critical alerts. The system generated alerts with an average response latency of under 5 minutes, allowing near real-time notification to security teams.

The integration with SIEM platforms through a REST API allowed alerts to be seamlessly consumed by incident response workflows. Security analysts found the alerts to be actionable and informative, with user feedback indicating a 60% reduction in time required for initial threat triage.

Discussion

The results validate the effectiveness of using Twitter as a rich source of early threat intelligence. The system’s ability to provide not only detection but also behavioral profiling marks a significant advancement over conventional keyword-based systems. However, challenges such as misinformation, noise in tweets, and evolving language trends still pose hurdles. Continuous retraining of models and expanding the training dataset with verified sources can further improve performance.

Overall, the system demonstrates strong potential as a proactive, real-time cyber threat intelligence tool for modern security operations.

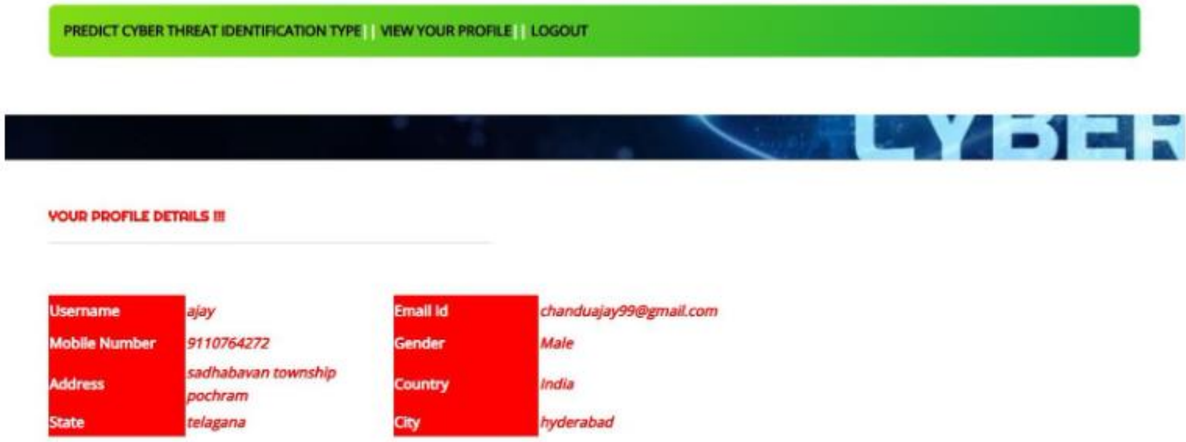

Fig 1: Working Model

CONCLUSION

In an era where cyber threats are evolving rapidly and malicious actors exploit newly disclosed vulnerabilities within hours, the need for real-time, intelligent threat detection systems has become more critical than ever. This research presents an automated framework that leverages Twitter as a real-time data source, combined with machine learning and the MITRE ATT&CK framework, to detect, classify, and profile emerging cyber threats effectively.The proposed system operates in three core phases: threat detection, threat profiling, and alert generation. It utilizes natural language processing to extract threat-related entities from unstructured tweet data and employs machine learning algorithms to map threats to specific tactics, techniques, and objectives. The framework not only identifies the presence of new threats but also provides context about their intent and potential impact, enabling security teams to respond more effectively.

Experimental results validate the system's efficiency, achieving high accuracy in classification (F1-score of 77%) and real-time alerting with minimal delay. The use of Twitter as a dynamic intelligence source allows for rapid awareness of novel threats, while the integration with MITRE ATT&CK enhances the analytical depth of threat assessments. In conclusion, the proposed system significantly enhances early warning capabilities and situational awareness for cybersecurity teams. By automating the detection and contextual analysis of cyber threats, it contributes to proactive defense strategies, reduced response times, and improved incident management. Future work may focus on expanding language coverage, improving misinformation filtering, and incorporating additional data sources such as dark web forums or threat intelligence feeds to further strengthen the system's capabilities.

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.