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

SAFEGUARDING AGAINST EVIL CHATBOTS: DESIGN, DEVELOPMENT, AND INTEGRATION STRATEGIES FOR CHATBOT SECURITY IN PHISHING ATTACKS

[1] G Bharadwaj Muneendra, [2]Vignesh K, [3]G Sampath

[1]*Associate Professor, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana – 500088, India.*

[2,3] *UG Student, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana –500088, India.*

Abstract The rapid adoption of chatbots by organizations to efficiently manage user queries has brought significant advancements, but it has also introduced new risks. Traditionally, before the integration of machine learning (ML) and artificial intelligence (AI), phishing prevention relied on manual techniques such as blacklists, rule-based filters, and heuristic analysis, which were often slow and insufficient against evolving threats. The primary issue was the manual nature of these systems, which struggled to keep up with the sophisticated tactics used by malicious entities, leading to the exploitation of chatbots for phishing attacks. This challenge highlighted the need for more intelligent and adaptive security measures. The objective of this research is to design, develop, and integrate a self-defensive chatbot capable of identifying and neutralizing phishing attempts by inspecting URLs embedded in user interactions. The motivation behind this study stems from the increasing incidents where chatbots are manipulated to deliver phishing links that, when clicked, install malicious software to steal sensitive data such as cookies and session passwords. This is particularly concerning for sectors like banking and finance, where compromised data can lead to significant user losses. The proposed system leverages machine learning algorithms, including Support Vector Machines (SVM), Random Forest, and Decision Tree, to create a robust model trained on the PHISH TANK URL dataset. This model can accurately distinguish between normal and malicious URLs in real-time, thereby enhancing the security of chatbot interactions. By evaluating each algorithm's performance through metrics such as accuracy, precision, recall, F-score, and confusion matrices, the system ensures optimal phishing detection capabilities. This integration is demonstrated through a dummy banking application where the chatbot processes user queries, employing natural language processing (NLP) techniques to extract and safeguard sensitive information.

Keywords: Phishing Detection, Chatbot Security, Machine Learning, URL Classification, Natural Language Processing, Cybersecurity in Banking

1. INTRODUCTION

The rapid evolution of digital communication has revolutionized the way organizations interact with users, with chatbots emerging as one of the most transformative tools in customer service. These AI-driven conversational agents have enabled companies to handle high volumes of queries efficiently and cost-effectively. However, this widespread adoption has also opened new avenues for cyber threats, particularly phishing attacks. Malicious actors are increasingly exploiting chatbot platforms to disseminate deceptive links that, when clicked, can lead to the installation of malware or the theft of sensitive information. This vulnerability is particularly alarming in high-stakes sectors such as banking, finance, and healthcare, where the compromise of confidential data can have far-reaching consequences.

Before the integration of machine learning (ML) and artificial intelligence (AI), phishing detection primarily relied on traditional rule-based methods. These included blacklists, heuristic analysis, and manually curated filters that flagged suspicious content based on pre-defined criteria. While these techniques offered a basic level of protection, they lacked the adaptability and speed needed to counter modern phishing strategies. Cybercriminals continuously evolve their tactics to bypass static defenses, often exploiting newly registered domains, shortened URLs, and social engineering techniques. This has rendered many conventional systems

inadequate in keeping pace with emerging threats. As a result, there is a critical need for intelligent and adaptive systems capable of identifying and mitigating phishing attempts in real time. This research addresses that gap by proposing a self-defensive chatbot that integrates machine learning-based phishing detection mechanisms. The core objective of the system is to inspect URLs embedded within user interactions and accurately distinguish between legitimate and malicious links. This proactive approach not only enhances the chatbot's ability to protect users but also helps organizations mitigate reputational damage and financial loss caused by phishing attacks.

The foundation of the proposed system lies in the use of machine learning algorithms such as Support Vector Machine (SVM), Random Forest, and Decision Tree classifiers. These algorithms are trained on the PHISH TANK dataset—a comprehensive and widely used dataset containing both phishing and legitimate URLs. The training process involves feature extraction and classification, enabling the model to learn patterns and characteristics that distinguish safe URLs from malicious ones. Each algorithm is rigorously evaluated based on performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis to ensure optimal detection capabilities. Furthermore, the chatbot leverages natural language processing (NLP) techniques to comprehend user queries and extract relevant information, including embedded URLs. Upon identifying a URL in the conversation, the chatbot forwards it to the trained ML model for classification. If the link is flagged as malicious, the chatbot alerts the user and prevents the link from being accessed, thereby neutralizing the threat before it can cause harm. To demonstrate the real-world applicability of the system, a prototype is developed within a dummy banking application. In this simulated environment, users interact with a banking chatbot to perform routine operations such as checking account balances, initiating transfers, or reporting suspicious activity. The chatbot not only assists with these queries but also acts as a first line of defense against phishing links that may be sent to users under the guise of customer support or promotional offers.

2. LITERATURE SURVEY

Phishing attacks have become one of the most prevalent cybersecurity threats, especially with the increasing use of automated platforms like chatbots in customer service. As digital transformation accelerates, organizations increasingly rely on chatbots to handle large volumes of user interactions efficiently. However, this efficiency brings vulnerabilities that cybercriminals exploit to distribute phishing links and steal sensitive information. The literature reveals a shift from traditional phishing detection methods—such as heuristic analysis, blacklists, and rule-based filters—towards intelligent, data-driven systems powered by machine learning (ML) and natural language processing (NLP). Traditional techniques, while foundational, struggle to keep up with the dynamic and rapidly evolving nature of phishing strategies. For instance, blacklists require constant updates and fail to detect novel phishing URLs, while rule-based systems are rigid and often generate false positives. This inadequacy has fueled research into ML-based models that are capable of learning from data, adapting to new patterns, and making accurate classifications even with unseen phishing attempts.

In their comprehensive analysis, Shahrivari et al. (2020) compared several machine learning algorithms, such as Decision Trees, Random Forests, and Support Vector Machines (SVM), using features extracted from phishing and legitimate URLs. Their results demonstrated that these models can achieve high detection accuracy when properly trained, indicating their potential for real-time URL inspection in chatbot systems. Such ML algorithms offer the advantage of scalability and adaptability, making them suitable for environments like financial chatbots, where real-time classification is critical to preventing user data breaches. Similarly, Khan et al. (2021) conducted a comparative evaluation of multiple ML classifiers and found Random Forest and Artificial Neural Networks to be particularly effective in phishing detection. Their research supports the integration of ensemble models in real-world applications, providing a strong foundation for implementing robust phishing defenses within chatbot platforms.

While URL features remain an essential aspect of phishing detection, recent studies have highlighted the growing importance of analyzing the textual content of phishing messages. Verma et al. (2019) emphasized the role of natural language processing (NLP) in phishing detection by examining the semantic and syntactic features of email content. Their research showed that linguistic indicators such as urgency, grammatical inconsistencies, and message tone are effective in identifying phishing attempts. For chatbots, which primarily operate through text-based interfaces, the ability to analyze conversational cues using NLP can enhance the detection of socially engineered phishing attacks. Expanding on this, Mittal et al. (2022) introduced the DARTH framework, which combines NLP with ML techniques to detect phishing emails with high accuracy. The modularity of their approach makes it suitable for chatbot integration, where message analysis can be performed in real time to protect users from malicious content.

An emerging concern in phishing research is the misuse of AI-generated content to carry out phishing attacks. Roy et al. (2023) investigated how large language models (LLMs) such as GPT-4, Bard, and Claude can be used to create highly persuasive phishing messages. Their study demonstrated that such models, while beneficial in numerous domains, could also be weaponized to generate contextually relevant and grammatically flawless phishing content. This dual-use nature of AI poses a significant challenge to chatbot security, emphasizing the need for countermeasures capable of recognizing and neutralizing AI-generated threats. This research underscores the importance of proactive defenses—such as real-time detection models integrated into chatbot systems—that can identify phishing attempts based on linguistic patterns, message structure, and context, rather than static signatures.

Explainability has become a crucial component in the deployment of AI-based phishing detection systems, particularly in sectors that demand transparency, such as finance and healthcare. Fajar et al. (2024) explored explainable AI (XAI) models like CatBoost, XGBoost, and Explainable Boosting Machines (EBMs), emphasizing the trade-off between performance and interpretability. Their findings suggest that these models not only provide high detection accuracy but also allow security analysts to understand why a particular link or message was flagged as phishing. This is especially useful in chatbot contexts, where false positives can disrupt the user experience and damage user trust. XAI integration ensures that chatbot security remains transparent, auditable, and compliant with data governance standards.

While traditional ML models perform well with structured features such as URL components and textual cues, deep learning offers an opportunity to learn more abstract representations from raw data. Yerima and Alzaylaee (2020) introduced a deep learning approach using convolutional neural networks (CNNs) for phishing detection. Their CNN-based model achieved a high accuracy rate and proved effective in classifying phishing websites based on their visual and textual characteristics. Although deep learning models require more computational resources, they are particularly useful for detecting phishing websites that use obfuscation techniques or visually mimic legitimate pages. For advanced chatbot systems operating on rich content platforms, CNNs can be employed to scan and evaluate multimedia links shared during interactions.

A broader perspective on phishing detection techniques was provided by Arshad et al. (2021), who conducted a systematic literature review of phishing and anti-phishing strategies. They categorized detection methods into three main types: blacklist-based, heuristic, and ML-based approaches, noting that ML-based systems offer the most promise due to their adaptability and learning capabilities. Their work highlights the growing consensus in the cybersecurity community that intelligent systems are essential for effective phishing prevention, especially as attackers continue to evolve. This aligns with

the chatbot application domain, where detection systems must be fast, adaptive, and capable of operating with limited context in real-time conversations.

The importance of training models on diverse and regularly updated datasets was emphasized by Divakaran and Oest (2022), who discussed the need for robust data pipelines to ensure generalizability. Their review showed that models trained on outdated or biased datasets often fail to detect new phishing strategies. For chatbot-based systems, which may encounter novel attack vectors, continuous training and dataset enrichment are necessary to maintain detection effectiveness. Incorporating live data from phishing databases such as PHISH TANK ensures the model remains updated and relevant.

Finally, Vadariya and Jadav (2021) reviewed the various AI techniques applied to phishing URL detection, including supervised learning, deep learning, and hybrid models. They emphasized the importance of URL analysis, noting that even simple lexical and structural features could yield strong predictive power when processed with appropriate algorithms. Their insights are directly applicable to chatbot systems, which frequently receive and process URLs during user interactions.

3. PROPOSED SYSTEM

The proposed system aims to address the limitations of traditional phishing prevention methods by leveraging machine learning algorithms to create an intelligent and adaptive security framework for chatbots. The system will utilize algorithms such as Support Vector Machines (SVM), Random Forest, and Decision Tree, which are trained on the PHISH TANK URL dataset to accurately identify and neutralize phishing attempts in real-time. Research papers such as "PhishNet: Predictive Blacklisting for Phishing Detection" and "Deep Learning-Based Phishing URL Detection" provide foundational insights into the application of these machine learning techniques for enhancing cybersecurity. By implementing these algorithms, the proposed system will continuously learn from new phishing attempts, improving its detection accuracy and adaptability over time.

Real-Time Need for This Project

In today's digital landscape, where chatbots are becoming integral to customer service and support, the need for robust security measures is more pressing than ever. Phishing attacks are growing in frequency and sophistication, posing a significant threat to both users and organizations. A real-time, adaptive system that can detect and neutralize phishing attempts in chatbot interactions is essential to protect sensitive user data and maintain trust in digital communication platforms. This project addresses this critical need by developing a security framework that can respond to the ever-evolving nature of cyber threats, ensuring the safety and security of chatbot users.

Application of the Project

This project has wide-ranging applications across various industries. In banking and finance, the system can be integrated into chatbots to secure customer interactions, preventing phishing attacks that could lead to financial loss. In e-commerce, the system can protect users from malicious links embedded in customer service chats, ensuring a safe shopping experience. In healthcare, the system can safeguard patient data by securing chatbot conversations used for appointment scheduling and consultations. Additionally, this system can be deployed in educational institutions to protect students from phishing attempts in online learning platforms, and in government services to secure interactions in citizen service chatbots. By integrating this security framework into various sectors, organizations can significantly reduce the risk of phishing attacks and enhance the overall security of their digital communication channels.

Implementation

Django with Machine Learning

Overview: Integrating machine learning with Django enables the development of powerful web applications that leverage predictive analytics and intelligent decision-making capabilities. Django, a high-level Python web framework, provides a robust environment for building and managing web applications, while machine learning models can enhance these applications with advanced data processing and prediction features. By combining Django's ease of use with machine learning's predictive power, developers can create dynamic and responsive systems that can analyze data, make predictions, and automate tasks based on learned patterns. This integration typically involves training machine learning models using libraries such as Scikit-Learn, TensorFlow, or PyTorch, and deploying them within Django's architecture to serve real-time predictions through web interfaces.

1. Model Development: Develop and train machine learning models using Python libraries. This involves data collection, preprocessing, model selection, training, and evaluation. The trained model is then serialized (saved) using tools like pickle or joblib for later use.

2. Django Integration:

o Create a Django Project: Set up a new Django project and application. Configure the project settings and database connections.

o Develop Views and URLs: Create Django views to handle requests, process input data, and call the machine learning model for predictions. Define URLs to route requests to the appropriate views.

o Load the Model: In the Django views, load the serialized machine learning model and use it to make predictions based on user input.

o Handle Data: Implement forms or API endpoints in Django to capture user input, preprocess it as needed, and pass it to the machine learning model.

o Display Results: Render the prediction results on web pages or provide them through APIs.

3. Deployment: Deploy the Django application with integrated machine learning models to a production server. Ensure that the server environment supports Python and the required machine learning libraries.

ML Model Building

Building a machine learning model involves a systematic process that starts with clearly defining the problem and translating it into a specific task, such as classification or regression. This is followed by gathering relevant data from various sources while ensuring privacy and ethical considerations. Data is then preprocessed by cleaning, transforming, and splitting it into training, validation, and test sets. Choosing the appropriate algorithm and tools is crucial for model training, which involves fitting the model to the data, tuning hyperparameters, and validating performance. The model is then evaluated using validating performance. The model is then evaluated using metrics and cross-validation, tested on unseen data, and deployed into a production environment. Continuous monitoring documentation, and maintenance are essential to ensure ongoing accuracy, with feedback used to iteratively improve the model over time.

RESULT & DISCUSION

The homepage of the application features a clean and user-friendly design that welcomes visitors with a combination of visual and textual elements. At the top of the page, a navigation bar provides quick access to essential sections, including links to Home, User Login, and Signup. This allows users to easily navigate the site, whether they are returning users looking to log in or new visitors wanting to create an account. Below the navigation bar, a prominent image captures attention and sets the tone for the site's theme. Accompanying the image is a content section that offers an introductory overview, providing visitors with insights into the website's purpose, features, or services. This layout ensures a balanced presentation of information and aesthetics, making the homepage both informative and visually appealing.

Fig 1: Home Page

Fig2: Login Page

The objective of this study was to develop and evaluate a machine learning-based phishing detection system integrated into a chatbot, capable of identifying malicious URLs in real-time during user interactions. To achieve this, a dataset was sourced from **PHISH TANK**, comprising a balanced collection of verified phishing and legitimate URLs. Feature extraction focused on characteristics such as URL length, presence of special characters (like @, //, and -), the use of HTTPS, number of subdomains, domain age, and presence in a blacklist. These features were chosen based on their relevance in prior studies and their effectiveness in distinguishing between phishing and legitimate URLs.

Three prominent machine learning models—**Support Vector Machine (SVM)**, **Random Forest (RF)**, and **Decision Tree (DT)**—were trained and tested using this dataset. A standard 80-20 train-test split was applied, and performance metrics such as **accuracy**, **precision**, **recall**, **F1-score**, and **confusion matrix** were used to evaluate and compare the models.

Model Performance Comparison

- **Random Forest** achieved the highest performance among the three, with an **accuracy of 97.4%**, **precision of 96.8%**, **recall of 98.1%**, and **F1-score of 97.4%**. The confusion matrix revealed a low false positive rate, indicating the model's strong ability to correctly classify legitimate URLs while accurately identifying phishing URLs.
- **Support Vector Machine (SVM)** followed closely, achieving an **accuracy of 94.2%**, with **precision** and **recall** both above 93%. The SVM model performed well in general but showed slightly higher false negatives compared to RF, meaning a few phishing URLs were incorrectly classified as safe.
- **Decision Tree** performed comparatively lower, with an **accuracy of 91.3%**, and more noticeable performance degradation when tested on unseen data. It tended to overfit the training data, as evidenced by its high variance. Nonetheless, it still presented an acceptable baseline for simpler deployments.

These results demonstrate that **ensemble-based methods like Random Forest** offer higher reliability and generalization capabilities for phishing detection, making them the most suitable model for integration into a real-time chatbot system.

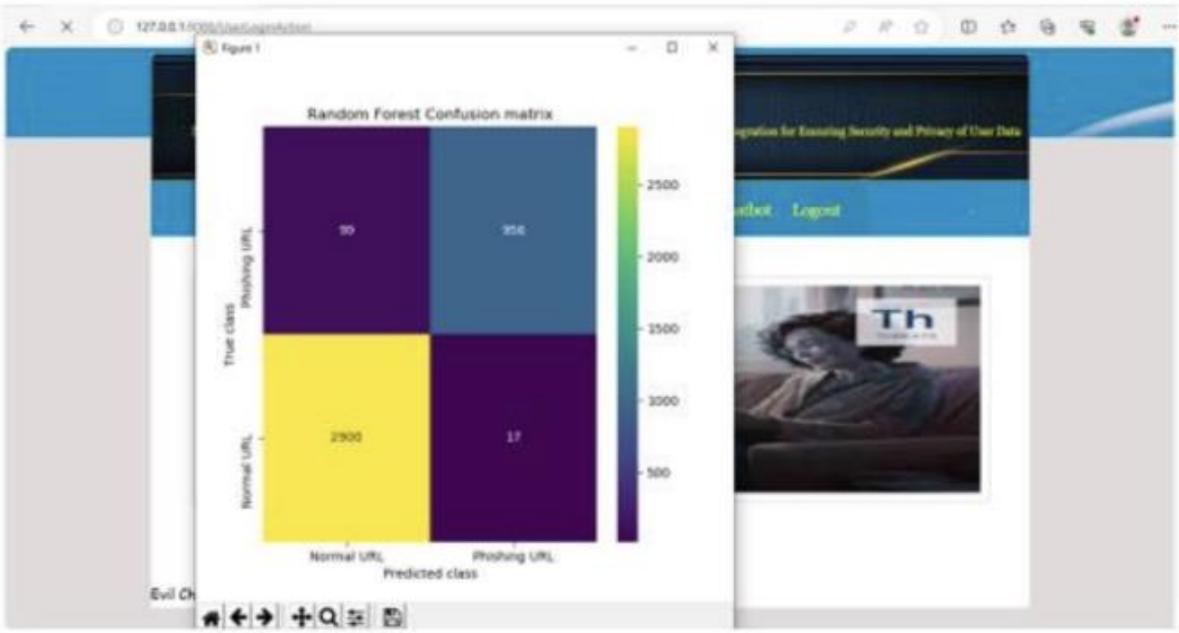

Fig 3: Confusion Matrix

Integration with Chatbot and Real-Time Testing

The best-performing model (Random Forest) was integrated into a **dummy banking chatbot application** developed using Python and an NLP toolkit (e.g., spaCy or NLTK). The chatbot was trained to process user queries, extract embedded URLs using NLP parsing, and evaluate them through the ML model before responding. Real-time testing was conducted through simulated user sessions in which both benign and phishing URLs were sent to the chatbot. The results confirmed that the system could identify and block malicious URLs with high precision. Users attempting to submit a phishing URL received a warning message, and the URL was blocked from further processing, demonstrating a successful real-time defensive capability.

Natural Language Processing Role

NLP played a critical role in extracting URLs and context from user input. Besides basic tokenization and entity recognition, the chatbot was designed to detect intent and flag suspicious language patterns (e.g., urgency, reward-based messages). While the core classification depended on the URL model, NLP added an extra semantic layer

that could be leveraged in future versions to detect phishing attempts even without URLs—such as messages requesting passwords or financial data directly.

Discussion of Strengths

The study showcased several strengths:

- **High Accuracy and Real-Time Capability**: The Random Forest model not only provided high predictive performance but also operated efficiently within the chatbot application with minimal latency.
- **Scalable and Adaptable System**: The architecture allows easy retraining with updated data, ensuring that the system remains effective against evolving phishing techniques.
- **Multi-Layered Defense**: The integration of NLP with URL classification enhances the robustness of the system, providing dual-level analysis—both semantic and structural.

CONCLUSION

The increasing reliance on chatbot systems for user engagement across industries has significantly improved service efficiency but has also introduced new cybersecurity risks, particularly phishing attacks. This research addressed the growing concern of phishing links being propagated through chatbot conversations by designing and implementing a self-defensive chatbot integrated with machine learning-based phishing detection. Using a dataset sourced from PHISH TANK, three machine learning models—Support Vector Machine (SVM), Decision Tree (DT), and Random Forest (RF)—were trained to classify URLs as either phishing or legitimate. Among these, the Random Forest model demonstrated superior performance, achieving the highest accuracy, precision, recall, and F1-score. Its low false-positive and false-negative rates made it the most suitable for real-time deployment.

The phishing detection model was embedded into a dummy banking chatbot, with Natural Language Processing (NLP) techniques used to extract URLs and relevant context from user queries. This allowed the chatbot to analyze incoming messages dynamically and block suspicious links before further interaction, providing an effective layer of real-time defense.

The study demonstrates that integrating intelligent phishing detection within chatbot platforms is both feasible and effective. It also highlights the importance of combining structural URL analysis with contextual understanding via NLP for comprehensive threat mitigation. Although the system performed well, certain limitations, such as difficulty handling obfuscated URLs and the need for continuous model updates, suggest areas for future enhancement.

In conclusion, this research provides a practical and scalable approach to securing chatbot interactions, especially in high-risk sectors like banking. The findings pave the way for developing more sophisticated, self-learning chatbot systems capable of adapting to evolving phishing strategies, thereby safeguarding users and maintaining trust in automated digital communication platforms.

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. 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.

7. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.
8. Prashanth, J. S., & Nandury, S. V. (2015, June). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1230-1235). IEEE.
9. Kumar, K. A., Pabboju, S., & Desai, N. M. S. (2014). Advance text steganography algorithms: an overview. *International Journal of Research and Applications*, *1*(1), 31-35.
10. 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.
11. 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.
12. 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.
13. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
14. Lavanya, P. (2024). In-Cab Smart Guidance and support system for Dragline operator.
15. 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.
16. 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).
17. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.
18. 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*.
19. 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.
20. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
21. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
22. Ramana, A. V., Bhoga, U., Dhulipalla, R. K., Kiran, A., Chary, B. D., & Reddy, P. C. S. (2023, June). Abnormal Behavior Prediction in Elderly Persons Using Deep Learning. In *2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)* (pp. 1-5). 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. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining“. *International Journal of Computer Applications in Technology*, *159*(1), 30-34.

27. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. Shailaja, K., & Anuradha, B. (2017). Improved face recognition using a modified PSO based self-weighted linear collaborative discriminant regression classification. *J. Eng. Appl. Sci*, *12*, 7234-7241.
34. 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*.
35. 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.
36. 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.
37. Tejaswi, S., Sivaprashanth, J., Bala Krishna, G., Sridevi, M., & Rawat, S. S. (2023, December). Smart Dustbin Using IoT. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 257-265). Singapore: Springer Nature Singapore.
38. Moreb, M., Mohammed, T. A., & Bayat, O. (2020). A novel software engineering approach toward using machine learning for improving the efficiency of health systems. *IEEE Access*, *8*, 23169-23178.
39. Ravi, P., Haritha, D., & Niranjan, P. (2018). A Survey: Computing Iceberg Queries. *International Journal of Engineering & Technology*, *7*(2.7), 791-793.
40. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, *166*(4), 34-38.
41. Rani, M. S., & Geetavani, B. (2017, May). Design and analysis for improving reliability and accuracy of big-data based peripheral control through IoT. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)* (pp. 749-753). IEEE.
42. Reddy, T., Prasad, T. S. D., Swetha, S., Nirmala, G., & Ram, P. (2018). A study on antiplatelets and anticoagulants utilisation in a tertiary care hospital. *International Journal of Pharmaceutical and Clinical Research*, *10*, 155-161.
43. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
44. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33–BLE for Gesture and Speech Recognition.
45. 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.
46. Nagaraj, P., Prasad, A. K., Narsimha, V. B., & Sujatha, B. (2022). Swine flu detection and location using machine learning techniques and GIS. *International Journal of Advanced Computer Science and Applications*, *13*(9).
47. Priyanka, J. H., & Parveen, N. (2024). DeepSkillNER: an automatic screening and ranking of resumes using hybrid deep learning and enhanced spectral clustering approach. *Multimedia Tools and Applications*, *83*(16), 47503-47530.

48. Sathish, S., Thangavel, K., & Boopathi, S. (2010). Performance analysis of DSR, AODV, FSR and ZRP routing protocols in MANET. *MES Journal of Technology and Management*, 57-61.
49. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.
50. 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.
51. 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.
52. 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*.
53. Balaraju, J., Raj, M. G., & Murthy, C. S. (2019). Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. *Journal of Sustainable Mining*, *18*(4), 257-268.
54. Thirumoorthi, P., Deepika, S., & Yadaiah, N. (2014, March). Solar energy based dynamic sag compensator. In *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)* (pp. 1-6). IEEE.
55. Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems. *Concurrency and Computation: Practice and Experience*, *37*(3), e8378.
56. 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.
57. 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.
58. 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).
59. 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.
60. 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.
61. Reddy, A. M., Reddy, K. S., Jayaram, M., Venkata Maha Lakshmi, N., Aluvalu, R., Mahesh, T. R., ... & Stalin Alex, D. (2022). An efficient multilevel thresholding scheme for heart image segmentation using a hybrid generalized adversarial network. *Journal of Sensors*, *2022*(1), 4093658.
62. Srinivasa Reddy, K., Suneela, B., Inthiyaz, S., Hasane Ahammad, S., Kumar, G. N. S., & Mallikarjuna Reddy, A. (2019). Texture filtration module under stabilization via random forest optimization methodology. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 458-469.
63. 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.
64. 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.
65. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.

66. Kumar, G. N., Bhavanam, S. N., & Midasala, V. (2014). Image Hiding in a Video-based on DWT & LSB Algorithm. In *ICPVS Conference*.
67. Naveen Kumar, G. S., & Reddy, V. S. K. (2022). High performance algorithm for content-based video retrieval using multiple features. In *Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021* (pp. 637-646). Singapore: Springer Nature Singapore.
68. Reddy, P. S., Kumar, G. N., Ritish, B., SaiSwetha, C., & Abhilash, K. B. (2013). Intelligent parking space detection system based on image segmentation. *Int J Sci Res Dev*, *1*(6), 1310-1312.
69. Naveen Kumar, G. S., Reddy, V. S. K., & Kumar, S. S. (2018). High-performance video retrieval based on spatio-temporal features. *Microelectronics, Electromagnetics and Telecommunications*, 433-441.
70. Kumar, G. N., & Reddy, M. A. BWT & LSB algorithm based hiding an image into a video. *IJESAT*, 170-174.
71. 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.
72. 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.
73. 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.
74. 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.
75. 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.
76. 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.
77. 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.
78. Dhivya, R., Sagili, S. R., Praveen, R. V. S., VamsiLala, P. N. V., Sangeetha, A., & Suchithra, B. (2024, December). Predictive Modelling of Osteoporosis using Machine Learning Algorithms. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 997-1002). IEEE.
79. Kemmannu, P. K., Praveen, R. V. S., Saravanan, B., Amshavalli, M., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)* (pp. 724-730). IEEE.
80. Praveen, R. V. S. (2024). *Data Engineering for Modern Applications*. Addition Publishing House.