SMS SPAM DETECTION USING MACHINE LEARNING

G.Nikhil[1], Ch.Sravan[2], S.Srijan[3], Dr. A. Jyothi[4]

[1,2,3,4]*Department of Computer Science and Engineering, Anurag University, India.*

*Corresponding author's email: *nikhilgoli0504@gmail.com*
sravanchoudari9989@gmail.com
srijanreddysandi1234@gmail.com

Abstract. An efficient SMS spam detection system is developed using the Multinomial Naive Bayes (MNB) algorithm. It employs a labeled dataset and extracts features with the term frequency-inverse document frequency (TF- IDF) method. The MNB algorithm classifies messages by modeling term probability distributions. Parameter tuning and pre-processing techniques like text normalization and stop-word removal enhance feature quality. Experimental results show high accuracy, precision, recall, and F1-score, making MNB suitable for real-time applications. The system provides a practical solution for SMS spam detection and enhances mobile communication security.

Keywords. SMS, Multinomial Naïve Bayes, Mobile Communication Security.

1. INTRODUCTION

This project addresses the increasing issue of spam SMS, which poses risks like phishing, fraud, and data theft. Scammers frequently adapt their methods, making traditional spam detection techniques ineffective. The project proposes developing an advanced machine learning model to classify and detect spam messages accurately, providing better protection to users. The model leverages algorithms such as Naïve Bayes and TF-IDF vectorizer for initial detection but plans to enhance accuracy by incorporating Random Forest and Support Vector Machine (SVM). The aim is to improve performance by using larger datasets and more robust preprocessing techniques. Additionally, this solution could be integrated into an app, offering users real-time spam detection. The ultimate goal is to provide a safer digital environment by reducing exposure to harmful messages.

2. LITERATURE SURVEY

2.1 Sefat E Rahman and Shofi Ullah (2020)

In this model, I tackle the issue by addressing email spam detection by combining sentiment analysis, Word Embeddings, and a Bidirectional LSTM network to analyze both sentiment and sequence in email body text. A Convolutional Neural Network enhances training and feature extraction. Tested on datasets like lingspam, the model achieves 98-99% accuracy, outperforming traditional classifiers and state-of-the-art methods, demonstrating its efficiency in combating spam challenges.

2.2 Haiying Shen and Ze Li (2013)

In this model, I tackle the challenge of rising unsolicited emails by introducing a new spam filter approach. I point out the limitations of traditional static filters and emphasize the adaptability of Bayesian filters, which continuously learn from new spam. However, Bayesian filters face challenges like susceptibility to clever spammers and slow adaptation. Recognizing the underutilization of social networks in current filters, I propose the Social network Aided Personalized and effective spam filter (SOAP). SOAP uses a distributed overlay through social network links, with each node autonomously checking spam, departing from traditional centralized methods. SOAP focuses on social relationships and interests for adaptive spam detection, introducing four key components: social closeness-based filtering, interest-based filtering, adaptive trust management, and friend notification. Through performance evaluations, SOAP shows significant improvement in Bayesian spam filter accuracy, attack-resilience, and efficiency, setting a new standard in spam detection.

2.3 A Machine Learning based spam detection mechanism(2020)

In this model, I address the common issue of receiving spam emails in today's internet-centric data environment, where such emails are often commercial or may even contain phishing links with malware. Recognizing the importance of detecting and identifying these spam emails to save system time and memory space, I propose a prudent mechanism. Our presented algorithm focuses on filtering both spam and non-spam emails by generating a dictionary and features, which are then trained through machine learning for effective results. This approach aims to enhance email security and optimize system resources efficiently.

2.4 Analysis of Optimized Machine Learning and Deep Learning Techniques for Spam Detection (2021)

In this model, I address the common issue of email spam detection using DBSCAN, Isolation Forest, and feature selection techniques like Heatmap and Chi-Square. Combining machine learning and deep learning, it incorporates ensemble methods like Multinomial Naïve Bayes, Random Forest, KNN, Gradient Boosting, RNN, and ANN. Comparative analysis shows outstanding performance, with 100% accuracy and 0 errors in machine learning, and 99% accuracy with a loss of 0.0165 in deep learning, based on a UCI dataset, demonstrating its effectiveness in identifying spam emails.

3. SYSTEM DESIGN

The SMS spam detection system leverages a Multinomial Naive Bayes (MNB) classifier, focusing on classifying SMS messages into spam or non-spam. The process involves data collection, preprocessing (cleaning, tokenization, normalization), and feature extraction through term frequency-inverse document frequency (TF-IDF). The MNB model is trained and evaluated on labeled datasets to improve accuracy, achieving high performance in real-time applications.

3.1 Backend Architecture

The backend is developed using Python for data preprocessing, TF-IDF feature extraction, and training a

Multinomial Naive Bayes model for spam detection. The backend is responsible for managing all core functionalities, including:

Data Processing: Collects SMS messages from datasets, cleans, tokenizes, and applies TF-IDF for feature extraction.

Model Training: Utilizes Multinomial Naive Bayes, calculating probabilities for spam classification based on word frequencies.

Evaluation and Deployment: Evaluates using metrics like accuracy and precision; integrates the model into a production environment for live spam detection.

3.2 Frontend Architecture

The frontend of the platform is built with Streamlit to create a web interface, enabling users to input messages and view spam detection results in real-time.key features include:

User Interface: A web-based interface built using Streamlit, allowing users to input messages for spam prediction.

Display and Interaction: Upon message input, displays classification results (spam or not spam), offering a user-friendly experience for real-time spam detection.

3.3 Security

Protection of User Privacy: The model protects privacy by filtering messages locally, reducing data exposure risk.

Adaptability to Evolving Spam Techniques: The model adapts to evolving spam patterns, keeping security measures up to date.

Prevention of Unwanted Communication: The system blocks spam, preventing phishing and malware for a safer messaging experience.

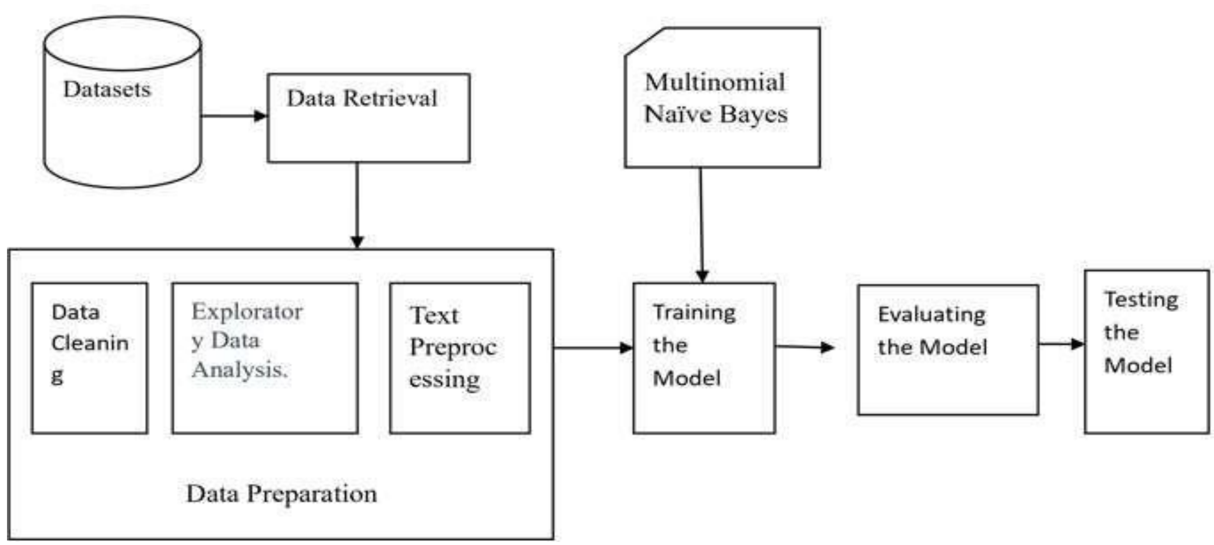
4. METHODOLOGY

4.1 Data Collection

The dataset from UCI includes labeled SMS messages, categorized as spam or non-spam. Data preprocessing involves cleaning and standardizing text data for efficient machine learning. Various statistical methods ensure comprehensive, high-quality input for accurate model training.

4.2 System Architecture

The architecture begins with data collection and cleaning, followed by exploratory data analysis (EDA) and preprocessing to enhance text quality. A Multinomial Naive Bayes classifier is trained on the processed dataset to detect spam. Finally, the model undergoes validation and testing, providing real-time spam classification on user messages.



5. RESULTS AND DISCUSSION

5.1 Performance

The model achieved an accuracy of 97% and a precision score of 1.0, showing strong predictive reliability. Evaluation metrics confirm robust classification of spam vs. non-spam messages. The system's lightweight design allows for efficient, real-time spam detection. Additionally, its accuracy minimizes false positives, enhancing user trust and satisfaction.

5.2 User Experience

The web interface allows users to easily check messages for spam, enhancing accessibility. Minimal processing time ensures a seamless, responsive user experience.

5.3 Security

The spam detection model improves SMS security by identifying and blocking potential threats. It minimizes exposure to phishing and malware, offering enhanced protection.

6. CONCLUSION

The Multinomial Naive Bayes algorithm proves effective in SMS spam detection, achieving high accuracy and precision. Its simplicity, combined with robust performance, makes it suitable for real-time applications. The model's adaptability to new spam patterns highlights its potential as a reliable spam filter. The project contributes to mobile communication security by providing users with a practical solution to filter unwanted messages. As SMS spam evolves, continuous model optimization will be crucial.

7. FUTURE SCOPE

Future developments for the SMS Spam Detection using Machine Learning include:

Incorporation of Ensemble Methods: Future work can use ensemble techniques to boost accuracy and robustness against spam.

Real-Time Adaptability: Real-time learning from new spam patterns can make the model more adaptive to evolving tactics.

User Feedback Integration: User feedback can refine the model, personalizing spam detection and improving precision.

REFERENCES

1. Kumar, T. V. (2018). Project Risk Management System Development Based on Industry 4.0 Technology and its Practical Implications.
2. Tambi, V. K., & Singh, N. (2015). Potential Evaluation of REST Web Service Descriptions for Graph-Based Service Discovery with a Hypermedia Focus.
3. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.
4. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
5. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
6. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural NetworkBased Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
7. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
8. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
9. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
10. Arora, P., & Bhardwaj, S. Mitigating the Security Issues and Challenges in the Internet of Things (IOT) Framework for Enhanced Security.
11. Sakshi, S. (2024). A Large-Scale Empirical Study Identifying Practitioners' Perspectives on Challenges in Docker Development: Analysis using Stack Overflow.

12. Sakshi, S. (2023). Advancements and Applications of Generative Artificial Intelligence and show the Experimental Evidence on the Productivity Effects using Generative Artificial Intelligence.
13. Sakshi, S. (2023). Assessment of Web Services based on SOAP and REST Principles using Different Metrics for Mobile Environment and Multimedia Conference.
14. Sakshi, S. (2022). Design and Implementation of a Pattern-based J2EE Application Development Environment.
15. Sharma, S., & Dutta, N. (2018). Development of New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation. Development, 7(11).
16. Sharma, S., & Dutta, N. (2017). Development of Attractive Protection through Cyberattack Moderation and Traffic Impact Analysis for Connected Automated Vehicles. Development, 4(2).
17. Sharma, S., & Dutta, N. (2015). Evaluation of REST Web Service Descriptions for Graph-based Service Discovery with a Hypermedia Focus. Evaluation, 2(5).
18. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
19. Sharma, S., & Dutta, N. (2015). Cybersecurity Vulnerability Management using Novel Artificial Intelligence and Machine Learning Techniques. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
20. Sharma, S., & Dutta, N. (2017). Classification and Feature Extraction in Artificial Intelligence-based Threat Detection using Analysing Methods.
21. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
22. Sharma, S., & Dutta, N. (2015). Distributed DNN-based Middleware for Cyberattack Detection in the Smart IOT Ecosystem: A Novel Framework and Performance Evaluation Technique.
23. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. Technology, 2(2).
24. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
25. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
26. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
27. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
28. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
29. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
30. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.
31. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
32. Archana, B., & Sreedaran, S. (2023). Synthesis, characterization, DNA binding and cleavage studies, in-vitro antimicrobial, cytotoxicity assay of new manganese (III) complexes of N-functionalized macrocyclic cyclam based Schiff base ligands. Polyhedron, 231, 116269.
33. Archana, B., & Sreedaran, S. (2022). New cyclam based Zn (II) complexes: effect of flexibility and para substitution on DNA binding, in vitro cytotoxic studies and antimicrobial activities. Journal of Chemical Sciences, 134(4), 102.
34. Archana, B., & Sreedaran, S. (2021). POTENTIALLY ACTIVE TRANSITION METAL COMPLEXES SYNTHESIZED AS SELECTIVE DNA BINDING AND ANTIMICROBIAL AGENTS. European Journal of Molecular and Clinical Medicine, 8(1), 1962-1971.
35. Rasappan, A. S., Palanisamy, R., Thangamuthu, V., Dharmalingam, V. P., Natarajan, M., Archana, B., ... & Kim, J. (2024). Battery-type WS2 decorated WO3 nanorods for high-performance supercapacitors. Materials Letters, 357, 135640.
36. Arora, P., & Bhardwaj, S. (2017). Investigation and Evaluation of Strategic Approaches Critically before Approving Cloud Computing Service Frameworks.
37. Arora, P., & Bhardwaj, S. (2017). Enhancing Security using Knowledge Discovery and Data Mining Methods in Cloud Computing.
38. Arora, P., & Bhardwaj, S. (2017). Combining Internet of Things and Wireless Sensor Networks: A Security-based and Hierarchical Approach.
39. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. machine learning, 8(7).
40. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
41. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
42. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.

43. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. Methods, 8(2).
44. Onyema, E. M., Gude, V., Bhatt, A., Aggarwal, A., Kumar, S., Benson-Emenike, M. E., & Nwobodo, L. O. (2023). Smart Job Scheduling Model for Cloud Computing Network Application. *SN Computer Science*, *5*(1), 39.
45. Hasnain, M., Gude, V., Edeh, M. O., Masood, F., Khan, W. U., Imad, M., & Fidelia, N. O. (2024). Cloud-Enhanced Machine Learning for Handwritten Character Recognition in Dementia Patients. In *Driving Transformative Technology Trends With Cloud Computing* (pp. 328-341). IGI Global.
46. Kumar, M. A., Onyema, E. M., Sundaravadivazhagan, B., Gupta, M., Shankar, A., Gude, V., & Yamsani, N. (2024). Detection and mitigation of few control plane attacks in software defined network environments using deep learning algorithm. *Concurrency and Computation: Practice and Experience*, *36*(26), e8256.
47. Gude, V., Lavanya, D., Hameeda, S., Rao, G. S., & Nidhya, M. S. (2023, December). Activation of Sleep and Active Node in Wireless Sensor Networks using Fuzzy Logic Routing Table. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1358-1360). IEEE.
48. Gorantla, V. A. K., Sriramulugari, S. K., Gorantla, B., Yuvaraj, N., & Singh, K. (2024, March). Optimizing performance of cloud computing management algorithm for high-traffic networks. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 482-487). IEEE.
49. Sriramulugari, S. K., & Gorantla, V. A. K. (2023). Deep learning based convolutional geometric group network for alzheimer disease prediction. *International Journal of Biotech Trends and Technology*, *13*(3).
50. Sriramulugari, S. K., & Gorantla, V. A. K. Cyber Security using Cryptographic Algorithms.
51. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Jiwani, N., & Kiruthiga, T. (2023, December). The slicing based spreading analysis for melanoma prediction using reinforcement learning model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
52. Sriramulugari, S. K., Gorantla, V. A. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The opinion based analysis for stressed adults using sentimental mining model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-6). IEEE.
53. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The smart computation of multi-organ spreading analysis of COVID-19 using fuzzy based logical controller. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
54. Gude, Venkataramaiah (2023). Machine Learning for Characterization and Analysis of Microstructure and Spectral Data of Materials. *International Journal of Intelligent Systems and Applications in Engineering* 12 (21):820 - 826.
55. 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.
56. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
57. Thangamani, M., Satheesh, S., Lingisetty, R., Rajendran, S., & Shivahare, B. D. (2025). Mathematical Model for Swarm Optimization in Multimodal Biomedical Images. In *Swarm Optimization for Biomedical Applications* (pp. 86-107). CRC Press.
58. Chithrakumar, T., Mathivanan, S. K., Thangamani, M., Balusamy, B., Gite, S., & Deshpande, N. (2024, August). Revolutionizing Agriculture through Cyber Physical Systems: The Role of Robotics in Smart Farming. In *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)* (Vol. 1, pp. 1-6). IEEE.
59. Tiwari, V., Ananthakumaran, S., Shree, M. R., Thangamani, M., Pushpavalli, M., & Patil, S. B. (2024). RETRACTED ARTICLE: Data analysis algorithm for internet of things based on federated learning with optical technology. *Optical and Quantum Electronics*, *56*(4), 572.
60. Sakthivel, M., SivaSubramanian, S., Prasad, G. N. R., & Thangamani, M. (2023). Automated detection of cardiac arrest in human beings using auto encoders. Measurement: Sensors, 27, 100792.
61. CHITHRAKUMAR, T., THANGAMANI, M., KSHIRSAGAR, R. P., & JAGANNADHAM, D. (2023). MICROCLIMATE PREDICTION USING INTERNET OF THINGS (IOT) BASED ENSEMBLE MODEL. *Journal of Environmental Protection and Ecology*, *24*(2), 622-631.
62. Vasista, T. G. K. (2017). Towards innovative methods of construction cost management and control. *Civ Eng Urban Plan: Int J*, *4*, 15-24.
63. Hsu, H. Y., Hwang, M. H., & Chiu, Y. S. P. (2021). Development of a strategic framework for sustainable supply chain management. *AIMS Environmental Science*, (6).
64. Venkateswarlu, M., & Vasista, T. G. (2023). Extraction, Transformation and Loading Process in the Cloud computing scenario. *International Journal of Engineering Applied Sciences and Technology*, *8*, 232-236.
65. Sagar, M., & Vanmathi, C. (2022, August). Network Cluster Reliability with Enhanced Security and Privacy of IoT Data for Anomaly Detection Using a Deep Learning Model. In *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)* (pp. 1670-1677). IEEE.

66. 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.
67. Sagar, M., & Vanmathi, C. (2024). Hybrid intelligent technique for intrusion detection in cyber physical systems with improved feature set. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-17.
68. 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.
69. Kumar, N. A., & Kumar, J. (2009). *A Study on Measurement and Classification of TwitterAccounts*.
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. Gorthi, R. S., Babu, K. G., & Prasad, D. S. S. (2014). Simulink model for cost-effective analysis of hybrid system. *International Journal of Modern Engineering Research (IJMER)*, *4*(2).
73. Rao, P. R., & Sucharita, D. V. (2019). A framework to automate cloud based service attacks detection and prevention. *International Journal of Advanced Computer Science and Applications*, *10*(2), 241-250.
74. 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).
75. 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.
76. Selvan, M. A., & Amali, S. M. J. (2024). RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE.