A Robust Approach for Detecting Malicious Query Access Using GCNN-Attention and BiLSTM with DFA Analysis

K. BABY RAMYA [1], K. PAVANI [2], SHAIK NAZMA[3]

#1 Assistant Professor in the Department of MCA, SRK Institute of Technology, Vijayawada

#2 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.

#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract: In the modern digital ecosystem, language technology resource repositories are increasingly exposed to malicious query access, posing serious risks to data security and intellectual property. This paper proposes a hybrid deep learning framework combining Graph Convolutional Neural Network (GCNN) with Attention mechanism and Bidirectional Long Short-Term Memory (BiLSTM) to effectively detect anomalous query behavior. Textual queries are transformed using TF-IDF feature extraction, enabling efficient representation for classification. To further capture long-range behavioral patterns, Detrended Fluctuation Analysis (DFA) is integrated to distinguish between normal and malicious access trends.

Experimental results demonstrate that the proposed model achieves superior performance with an accuracy of 93.85%, outperforming traditional machine learning approaches such as SVM and Naïve Bayes. The integration of deep learning with long-range correlation analysis provides a robust and scalable solution for securing language technology resources against evolving cyber threats.

Index terms *- — Malicious Query Detection, Language Technology Resources, Deep Learning, Graph Convolutional Neural Network (GCNN), Attention Mechanism, Bidirectional Long Short-Term Memory (BiLSTM), TF-IDF, Detrended Fluctuation Analysis (DFA), Cybersecurity, Access Behavior Analysis*

1. INTRODUCTION

Language technology resources play a vital role in modern digital systems, supporting applications such as information retrieval, text analytics, and intelligent learning platforms. As these repositories become widely accessible across academic, industrial, and public domains, they also face increasing security challenges. In particular, the rise of automated and malicious query access threatens data confidentiality, intellectual property, and overall system reliability.

Traditional security mechanisms rely on machine learning techniques such as Support Vector Machines and Naïve Bayes, which primarily analyze isolated query features. However, these methods fail to capture complex linguistic patterns and long-range behavioral dependencies in user access sequences, making them less effective against sophisticated attacks. The inability to model contextual and

sequential relationships creates a significant gap in accurately identifying malicious query behavior.

To address these limitations, this paper proposes a hybrid deep learning framework that integrates Graph Convolutional Neural Network (GCNN) with an Attention mechanism and Bidirectional Long Short-Term Memory (BiLSTM). This combination enables the system to capture structural, contextual, and temporal features of query data. Additionally, Detrended Fluctuation Analysis (DFA) is incorporated to analyze long-range correlations in user behavior, enhancing detection reliability.

The proposed approach aims to provide a robust, scalable, and intelligent solution for detecting malicious query access in language technology repositories. By improving classification accuracy and understanding user behavior patterns, the system contributes to strengthening cybersecurity and ensuring secure access to valuable linguistic resources.

2. LITERATURE SURVEY

a) AI-Driven Safety and Security for UAVs: From Machine Learning to Large Language Models:

Safety and security risks are growing more complicated as unmanned aerial vehicle (UAV) uses spread beyond emergency response, agriculture, and logistics. It is necessary to keep improving by incorporating conventional artificial intelligence (AI) tools like machine learning (ML) and deep learning (DL), which greatly improve UAV safety and security, in order to address these changing threats, which include physical safety and network security threats. A cutting-edge development in the field of artificial intelligence, large language models (LLMs) are linked to robust learning and adaptability in a variety of contexts. Their appearance is part of a larger trend toward intelligent systems that might ultimately exhibit thinking similar to that of humans. This study covers the development of conventional AI technologies as reported in the literature, highlights the common safety and security risks that influence UAVs, and suggests ways to lessen their effects. It also reviews the state of LLM application in UAV safety and security and draws attention to the shortcomings of conventional AI technology. The difficulties and potential future research paths for enhancing UAV safety and security using LLMs are finally covered in this study. By utilizing their cutting-edge capabilities, LLMs provide potential advantages in crucial fields like emergency response, precision agriculture, and urban air traffic management, promoting revolutionary advancements toward secure, dependable, and adaptable UAV systems that handle contemporary operational challenges.

b) Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering: digital age, network security is essential since sensitive data and critical infrastructure are always at risk. This study aims to enhance network security by integrating deep learning (DL) and machine learning (ML) techniques for instruction detection. Attackers have attempted to compromise security systems by gaining access to networks and collecting private data.One important component of cybersecurity is intrusion detection systems (IDSs), which monitor and analyze data with the

goal of spotting and reporting risky activity to assist stop an attack.The study's vector figures include Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), Long Short-Term Memory (LSTM), and Artificial Neural Network (ANN). To determine the optimum outcomes for identifying and preventing network violations, these models are put through a number of tests. All of the examined models are able to organize data that comes from network traffic, according to the findings that were collected. Thus, models like SVM, KNN, RF, and DT shown successful outcomes in identifying the distinction between normal and invasive behaviors. In network data, deep learning models LSTM and ANN quickly identify intricate and long-term patterns. Because of its excellent precision, accuracy, and memory, it is quite useful for handling complicated incursions.According to our research, SVM and Random Forest are seen to be viable options for practical IDS applications due to their adaptability and explainability. These models may be useful for businesses looking for IDS solutions that are both dependable and easier to understand. Furthermore, LSTM and ANN are appropriate for scenarios with complex, evolving threats due to their capacity to capture consecutive circumstances.

c) Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets:

Botnets are becoming a serious danger to network infrastructure due to the unprecedented cybersecurity vulnerabilities brought about by the proliferation of Internet of Things (IoT) devices. In order to solve these problems, this study integrates Convolutional Neural Network (CNN), Bidirectional Long Short-Term Memory (BiLSTM), Random Forest (RF), and Logistic Regression (LR) using a weighted soft-voting mechanism. It focuses on conventional machine learning and deep learning techniques. Our method provides a multi-layered feature selection technique to improve discriminative power, a hybrid model (ensemble models) for robust detection, an individual deep learning–traditional machine learning performance, and a Quantile Uniform transformation to decrease feature skewness. The system outperforms state-of-the-art models by up to 6.2% on BOT-IOT, CICIOT2023, and IOT23 datasets, achieving 100% accuracy on BOT-IOT, 99.2% on CICIOT2023, and 91.5% on IOT23. By providing scalable, high-performance detection that is flexible to many network conditions and has useful improvements for real-world implementation, these contributions enhance IoT security.

d) Enhancing Multilingual Hate Speech Detection: From Language-Specific Insights to Cross-Linguistic Integration:

Social media allows biased people to promote hate speech against race, gender, religion, and sexual orientation. Constructive interactions in diverse societies can boost self-esteem, while negative comments can hurt social status and mental health.

Detecting and addressing harmful content is essential to reduce its detrimental consequences on communities and people. The increased incidence emphasizes the need for stronger digital platform legislation and strategies to safeguard persons from such harmful behavior. Hate speech is usually intended to degrade or alienate a group based on their identity. hate speech research focuses on resource-aware languages like English, German, and Chinese. However, resource-limited languages like Italian, Spanish, Portuguese, Roman Urdu, Korean, and Indonesian create challenges. Lack of language resources makes information extraction harder. This work aims to detect and enhance multilingual hate speech in 13 languages. We tested traditional machine learning, mainstream deep learning, and transformer-based algorithms to complete our investigation. Hyperparameter tweaking, optimization, and generative setups yielded robust and generalized hate speech detection across dialects. In numerous lesser-studied languages, we improved detection performance by up to 10% in precision and recall. We also improve explainable AI in this environment by providing better insights into model decisions, which is important for regulatory and ethical AI deployment. Through careful comparisons, our study shows significant performance increases across datasets and languages. Our model beat benchmarks with F1-scores of 0.90 in German (GermEval-2018), up from 0.72, and 0.93 in German (GermEval-2021), up from 0.58. It also earned 0.95 in Roman Urdu HS, up from 0.91. For mixed-language datasets like Italian and English (AMI 2018), our accuracy increased from 0.59 to 0.96. Our model's resilience and adaptability set a new benchmark for hate speech detection systems across linguistic contexts.

e) Effective Detection of Malicious Uniform Resource Locator (URLs) Using Deep-Learning Techniques:

Malicious URLs are a widespread cybercrime due to the fast rise in internet use. Due to outmoded feature extraction methods and datasets, traditional detection approaches generally have significant false alarm rates and struggle to keep up with developing threats. We present a deep learning-based methodology for identifying malicious URLs to overcome these constraints. The Char2B model combines BERT and CharBiGRU embedding with a Conv1D layer with a three-kernel kernel and unit-sized stride and padding. After embedding, we compared to the BERT model. The open project directory (DMOZ), PhishTank, and Any.Run provided 87,216 benign and malicious URLs for the study. Models were trained on the training set and tested on the test set using accuracy, precision, recall, and F1-score. Iterative refining maximized model performance and effectiveness. Our model outperformed the baseline BERT model with 98.50% accuracy, 98.27% precision, 98.69% recall, and 98.48% F1-score. Our model had 0.017 false positives, compared to 0.018 for the baseline. The algorithm identified URLs as benign or dangerous by extracting and using useful information, increasing detection. This study shows how our deep learning technique improves cybersecurity by incorporating sophisticated algorithms that improve detection accuracy, defensive mechanisms, and digital safety.

3. METHODOLOGY

i) Proposed Work:

The proposed work introduces a robust and intelligent framework for detecting malicious query

access in language technology resource repositories by integrating machine learning, deep learning, and behavioral analysis techniques. The system begins with collecting query datasets from sources such as Kaggle, followed by preprocessing steps including removal of stopwords, special characters, and normalization to improve data quality. Cleaned textual data is then transformed into numerical form using TF-IDF vectorization, enabling effective feature representation for model training.

To perform classification, the framework employs both traditional and advanced models. Machine learning algorithms such as Support Vector Machine (SVM) and Naïve Bayes are used as baseline models, while a deep learning architecture combining Graph Convolutional Neural Network (GCNN) with an Attention mechanism is utilized to capture complex relationships and feature importance within query data. Further enhancement is achieved by integrating a Bidirectional Long Short-Term Memory (BiLSTM) layer, which captures sequential dependencies in both forward and backward directions, improving the understanding of user behavior patterns.

In addition, the system incorporates Detrended Fluctuation Analysis (DFA) to analyze long-range correlations in query access behavior, enabling differentiation between normal and malicious activities based on behavioral trends. A Flask-based web interface is developed to support real-time query prediction, allowing users to upload data and obtain immediate classification results. This hybrid approach ensures improved detection accuracy, scalability, and practical deployment for securing language technology resources.

ii) System Architecture:

The system architecture follows a structured pipeline for detecting malicious query access in language technology resources. Initially, user queries are provided as input and undergo preprocessing, where noise such as stopwords and special characters is removed. The cleaned data is then converted into numerical feature vectors using TF-IDF, enabling effective representation of textual information. These features are fed into the core detection module, which combines Graph Convolutional Neural Network (GCNN) with an Attention mechanism and a BiLSTM layer. This hybrid model captures structural relationships, important contextual features, and sequential dependencies within query data, ensuring accurate classification of queries.

Following the classification stage, the system performs long-range correlation analysis using Detrended Fluctuation Analysis (DFA) to examine user behavior patterns over time. Based on the learned patterns, the system categorizes outputs into malicious or legitimate queries and provides evaluation metrics for performance assessment. The integration of deep learning and behavioral analysis, as shown in the provided architecture diagram, ensures a robust, scalable, and real-time detection system capable of securing language resource repositories from sophisticated threats.

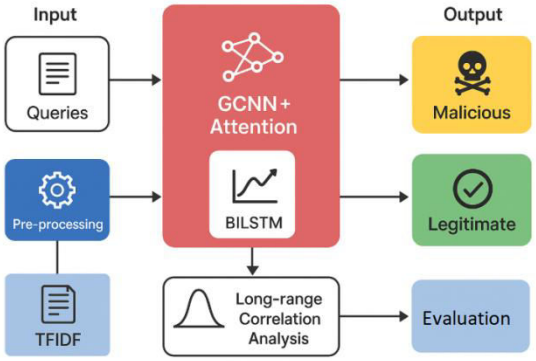

Fig1 proposed architecture

iii) Modules:

1. Importing Packages:

This module initializes the system by loading essential Python libraries required for data processing, visualization, and model development. It ensures a stable environment for executing machine learning and deep learning operations efficiently.

2. Exploring the Dataset:

The dataset is analyzed to understand query distribution, class labels, and data characteristics. This step helps identify imbalance, noise, and patterns, which guide preprocessing and model design decisions.

3. Visualization:

Graphical representations such as charts and plots are used to observe query behavior and class distribution. Visualization improves understanding of data patterns and supports better model tuning.

4. TF-IDF Vectorization:

Textual queries are converted into numerical feature vectors using TF-IDF. This transformation allows machine learning and deep learning models to process linguistic data effectively.

5. Data Splitting (Train & Test):

The dataset is divided into training and testing sets to evaluate model performance on unseen data. This ensures the model generalizes well and avoids overfitting.

6. Model Training:

Different models such as SVM, Naïve Bayes, and the proposed GCNN + Attention + BiLSTM are trained using extracted features. This module enables learning of patterns that distinguish malicious and legitimate queries.

7. Evaluation:

The trained models are evaluated using metrics like accuracy, precision, recall, and F1-score. This helps in comparing performance and selecting the best model.

8. Flask Server:

A web-based interface is developed using Flask to allow real-time interaction. Users can upload queries and receive immediate prediction results.

9. User Login:

Authentication is implemented to ensure only authorized users can access the system. This enhances security and protects sensitive data.

10. Language Query Access Behaviour Detection:

This core module processes input queries through the trained model and DFA analysis to classify them as malicious or legitimate. It provides final predictions along with behavior insights.

11. Logout:

This module securely terminates user sessions, preventing unauthorized access after system usage and maintaining overall system security.

iv) ALGORITHMS:

1. Support Vector Machine (SVM):

Support Vector Machine (SVM) is employed as a baseline supervised learning algorithm to classify queries into malicious or legitimate categories. It works by mapping TF-IDF feature vectors into a high-dimensional space and determining an optimal hyperplane that maximizes the margin between classes. This approach ensures strong generalization capability and robustness against noise in textual

data. Due to its effectiveness in handling sparse data, SVM provides a reliable benchmark for evaluating the performance of advanced deep learning models.

2. Naïve Bayes:

Naïve Bayes is a probabilistic classification algorithm based on Bayes' theorem, assuming independence between features. It calculates the posterior probability of each class by considering the likelihood of feature occurrences in the dataset. This method is computationally efficient and particularly suitable for text classification tasks, as it can handle large vocabularies with minimal complexity. Despite its simplicity, it provides competitive performance and serves as a useful comparison for more complex models.

3. GCNN + Attention:

The Graph Convolutional Neural Network (GCNN) combined with an Attention mechanism enhances feature extraction by capturing both global and local relationships within textual queries. GCNN models the structural dependencies between words, while the Attention mechanism assigns higher weights to the most relevant features, allowing the model to focus on important parts of the input. This combination improves classification accuracy by effectively learning contextual patterns and reducing the impact of irrelevant information in the data.

4. GCNN + Attention + BiLSTM (Proposed Model):

The proposed hybrid model integrates GCNN, Attention, and Bidirectional Long Short-Term Memory (BiLSTM) to achieve superior performance in detecting malicious queries. GCNN extracts structural features, the Attention mechanism highlights significant components, and BiLSTM captures sequential dependencies in both forward and backward directions. This multi-layered architecture enables a deeper understanding of query behavior, improving the detection of subtle and complex malicious patterns while enhancing overall accuracy and reliability.

5. Detrended Fluctuation Analysis (DFA):

Detrended Fluctuation Analysis (DFA) is used to examine long-range correlations in user query access behavior over time. It evaluates fluctuations in query patterns and computes scaling parameters to distinguish between normal and abnormal activities. Values indicating higher correlation typically correspond to malicious behavior, while lower values represent legitimate usage. By integrating DFA with deep learning outputs, the system enhances behavioral analysis and strengthens the overall detection framework.

4. EXPERIMENTAL RESULTS

The proposed system was evaluated using a query dataset consisting of both legitimate and malicious samples. Performance analysis was carried out using standard evaluation metrics such as accuracy, precision, recall, and F1-score. The dataset was divided into training and testing sets to ensure unbiased evaluation. Comparative experiments were conducted between traditional machine learning models (SVM and Naïve Bayes) and the proposed deep learning models (GCNN + Attention and GCNN + Attention + BiLSTM). The results indicate that deep learning approaches significantly outperform traditional methods due to their ability to capture contextual and sequential patterns in query data.

The proposed hybrid model (GCNN + Attention + BiLSTM) achieved the best performance with an accuracy of 93.85%, precision of 93.04%, recall of 94.19%, and F1-score of 93.53%, demonstrating superior detection capability. The integration of BiLSTM improved sequence learning, while DFA enhanced behavioral analysis, leading to better identification of malicious query patterns. Graphical comparisons and performance tables (as shown in the

results section of the document) further confirm that the proposed system provides higher accuracy, reduced false positives, and improved robustness compared to existing approaches.

Accuracy: A test's accuracy is determined by its capacity to distinguish between healthy and ill cases. To gauge the accuracy of the test, find the percentage of examined instances that had true positives and true negatives. According to the computations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: Precision is the number of affirmative cases or the classification's accuracy rate. The following formula is applied to assess accuracy:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: A model's ability to recognise every instance of a pertinent machine learning class is measured by its recall. The ratio of accurately predicted positive observations to the total number of positives indicates how well a model can identify class instances.

$$Recall = \frac{TP}{(FN + TP)}$$

mAP: Mean Average Precision is one ranking quality metric (MAP). It considers the number of relevant recommendations and their position on the list. MAP at K is calculated as the arithmetic mean of the Average Precision (AP) at K for each user or query.

$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: An accurate machine learning model is indicated by a high F1 score. combining precision and recall to increase model correctness. The accuracy statistic quantifies the frequency with which a model correctly predicts a dataset.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

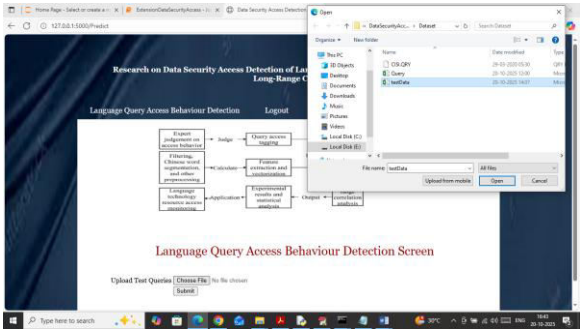

Fig2 upload input

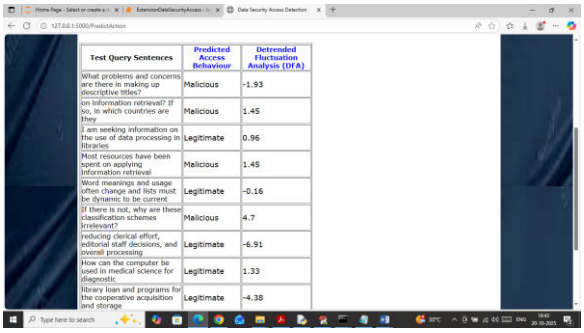

Fig3 results

5. CONCLUSION

This paper presents a robust and intelligent framework for detecting malicious query access in language technology resource repositories using a hybrid deep learning approach. By integrating GCNN, Attention mechanism, and BiLSTM, the

system effectively captures structural, contextual, and sequential patterns in query data, significantly improving detection accuracy. The incorporation of Detrended Fluctuation Analysis (DFA) further enhances the system by analyzing long-range user behavior, enabling reliable differentiation between legitimate and malicious activities.

Experimental results demonstrate that the proposed model outperforms traditional machine learning methods, achieving high accuracy and better overall performance. The combination of deep learning and behavioral analysis provides a scalable, efficient, and practical solution for securing language technology resources. This work contributes to strengthening cybersecurity in digital linguistic platforms by ensuring safe, reliable, and controlled access to sensitive data.

6. FUTURE SCOPE

The proposed system can be further enhanced by integrating advanced transformer-based models such as BERT or GPT to improve contextual understanding of complex query patterns. These models can capture deeper semantic relationships, leading to even higher detection accuracy for sophisticated malicious queries. Additionally, incorporating real-time streaming data analysis can enable continuous monitoring of user behavior and faster detection of evolving threats.

Future work can also focus on deploying the system in cloud and distributed environments to handle large-scale language repositories efficiently. The integration of explainable AI (XAI) techniques can improve transparency by providing interpretable insights into model decisions. Furthermore, extending the framework to support multilingual query detection and adaptive learning mechanisms will enhance its applicability across diverse platforms and dynamic cybersecurity scenarios.

REFERENCES

[1] Yang, Z., Zhang, Y., Zeng, J., Yang, Y., Jia, Y., Song, H., ... & An, J. (2025). AI-Driven safety and security for UAVs: From machine learning to large language models. Drones, 9(6), 392.

[2] Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E. H. M., Shahzad, T., & Khan, M. A. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Scientific Reports, 15(1), 1726.

[3] Ullah, S., Wu, J., Lin, Z., Kamal, M. M., Mostafa, H., Sheraz, M., & Chuah, T. C. (2025). Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets. Scientific Reports, 15(1), 31072.

[4] Hashmi, E., Yayilgan, S. Y., Hameed, I. A., Yamin, M. M., Ullah, M., & Abomhara, M. (2024). Enhancing multilingual hate speech detection: From language-specific insights to cross-linguistic integration. IEEE Access.

[5] Munaye, Y. Y., Workneh, A. B., Chekol, Y. B., & Mekonen, A. M. (2025). Effective Detection of Malicious Uniform Resource Locator (URLs) Using Deep-Learning Techniques. Algorithms, 18(6), 355.

[6] S. B. Naqvi, M. Afzaal, and G. Qiang, “Editorial: Language, corpora, and technology in applied linguistics,” Frontiers Psychol., vol. 14, pp. 1–4, Nov. 2023, doi: 10.3389/fpsyg.2023.1325925.

[7] L. Wiechetek, "Unmasking the myth of effortless big data-making an open source multilingual infrastructure and building language resources from scratch," in Proc. 13th Int. Conf. Lang. Resour. Eval. (LREC), Marseille, France, 2022, pp. 1167–1177.

[8] J. Mariani, "Developing language technologies with the support of language resources and evaluation programs," Lang. Resour. Eval., vol. 39, no. 1, pp. 35–44, Feb. 2005, doi: 10.1007/s10579-005-2694-3.

[9] Z. Peng, F. Liang, and L. Mu, "Big data-based access control system in educational information security assurance," Wireless Commun. Mobile Comput., vol. 2022, pp. 1–7, Jan. 2022, doi: 10.1155/2022/2853821.

[10] R. Asija and R. Nallusamy, "Security and complexity analysis of user and data based access control (UDBAC) model," in Proc. Int. Conf. Current Trends Comput., Electr., Electron. Commun. (CTCEEC), Mysore, India, Sep. 2017, pp. 358–366, doi: 10.1109/CTCEEC.2017.8455187.

[11] S. Alves and M. Fernández, "A graph-based framework for the analysis of access control policies," Theor. Comput. Sci., vol. 685, pp. 3–22, Jul. 2017, doi: 10.1016/j.tcs.2016.10.018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0304397516305965

[12] I. Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," Inf. Sci., vol. 231, pp. 64–82, May 2013.

[13] I. Santos, C. Laorden, and P. G. Bringas, "Collective classification for unknown malware detection," in Proc. Int. Conf. Secur. Cryptogr., Seville, Spain, Jul. 2011, pp. 251–256.

[14] W. Zhang, X. Liang, Y. Zhang, and H. Su, "Sensitive data classification of imbalanced short text based on probability distribution BERT in electric power industry," in Proc. Int. Conf. Pattern Recognit., Mach. Vis. Intell. Algorithms (PRMVIA), Mar. 2023, pp. 169–174, doi: 10.1109/PRMVIA58252.2023.00034.

[15] H. Pei, J. Jia, W. Guo, B. Li, and D. Song, "TextGuard: Provable defense against backdoor attacks on text classification," in Proc. Netw. Distrib. Syst. Secur. Symp., San Diego, CA, USA, 2024, pp. 1–18.

[16] X. Pang, Y. Su, W. Tao, Z. Hu, and H. Chen, "A network security situational awareness system for text classification," J. Phys., Conf. Ser., vol. 2358, no. 1, Oct. 2022, Art. no. 012012, doi: 10.1088/1742-6596/2358/1/012012.

[17] M. Khadhraoui, H. Bellaaj, M. B. Ammar, H. Hamam, and M. Jmaiel, "Survey of BERT-base models for scientific text classification: COVID-19 case study," Appl. Sci., vol. 12, no. 6, p. 2891, Mar. 2022.

[18] I. K. Kusakin, O. V. Fedorets, A. Y. Romanov, "Classification of short scientific texts," Sci. Tech.Inf. Proc., vol. 50, pp. 176–183, 2023, doi: 10.3103/S0147688223030024.

[19] N. Qun, X. Li, X. Qiu, and X. Huang, "End-to-end neural text classification for Tibetan," in Proc. Int. Symp. Natural Lang. Process. Based Naturally Annotated Big Data, 2017, pp. 472–480.

[20] H. Wang, Z. B. Zhao, Y. Y. Li, and X. Q. Zhang, "Construction and application of GCN model for text classification with associated information," Data Anal. Knowl. Discov., vol. 5,

no. 9, pp. 31–41, 2021, doi: 10.11925/infotech.2096-3467.2021.0266.

Author Profiles

Ms. K. Baby Ramya is working as an Assistant Professor in the Department of MCA at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She completed her MCA from Krishna University. She has nearly 3 years of teaching experience at SRK Institute of Technology. Her areas of interest include Machine Learning, Data Science, and Computer Applications.

Mrs. K. Pavani is working as an Assistant and Head of Department of MCA, in SRK Institute of technology in Vijayawada. She completed her MCA and M.Tech in Computer Science. She has 10 years of teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her areas of interest include AI and ML, etc.

Ms. Shaik Nazma is an MCA student in the Department of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She completed her degree in B.Sc.(Computers science) from Andhra loyola College Vijayawada. Her areas of interest are DBMS and Machine Learning.