Research Integrity Monitor –Verifying the Authenticity of Academic Content

Divya Sri Kuntla[1], Navya Sri Jella[2], P. Abhishek Goud[3], Sravani Gundala[4]
[1,2,3,4] *Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, India*

***Abstract*—In recent years, the rapid evolution of AI-generated content and the development of digital academic resources, ensuring research integrity in scholarly documents has become a challenge. Existing solutions such as Bi-LSTM-based AI text detectors, transformer-based NLP models, and blockchain-based certificate verification systems only focus on a few aspects of research integrity verification. These approaches provide moderate accuracy. This paper presents a Research Integrity Monitor that offers a comprehensive framework for research integrity verification. This framework includes plagiarism detection through NLP-based approaches, AI-generated content detection, multilingual language detection, citation detection, and certificate verification through optical character recognition. The system uses TF-IDF with cosine similarity, machine learning algorithms, and optical character recognition to analyze the academic documents. The model provides a score that reflects the research integrity. The results of the experiment prove that the model achieves 97.8% accuracy, 97.2% precision, 96.9% recall, and a high F1-score of 97% with a low error rate of 2.2%, outperforming existing solutions such as Bi-LSTM-based AI text detectors that provide a high accuracy of only 91-93% and traditional plagiarism detection systems that provide a high accuracy of only 90-97%.**

Keywords*—Research Integrity, AI-Generated Text Detection, Plagiarism Detection, Natural Language Processing, Machine Learning, Certificate Authentication, OCR, Citation Verification.

I. INTRODUCTION

Significant changes have occurred in the creation and sharing of research documents due to the rapid growth of digital academic resources and the invention of artificial intelligence-based writing tools. Although these tools have improved productivity and ease of use, they have also raised some serious problems with academic integrity, including plagiarism, artificial intelligence-based writing, fabricated references, and forged academic certificates. Conventional plagiarism detection tools are mostly designed to check the similarity of the text and are not able to detect other forms of academic integrity problems. Therefore, academic institutions and research centers demand powerful tools to check academic content with complete accuracy.

Various research studies have proposed different techniques to solve the challenges. For example, various techniques have been proposed for plagiarism detection through Natural Language Processing (NLP) techniques. Similarly, techniques have been proposed for the detection of AI content through the use of Bi-LSTM models or transformer models. Moreover, the use of blockchain technology has been proposed for the authentication of certificates. Nevertheless, the techniques proposed only focus on the various individual processes of the techniques mentioned above. There is no unified approach proposed for the analysis of the various dimensions of the authenticity of the research.

Various research studies have proposed different techniques to overcome the challenges. For instance, various techniques have been proposed for the detection of plagiarism through Natural Language Processing techniques. Similarly, various techniques have been proposed for the detection of AI content through the application of Bi-LSTM models or transformer models. Moreover, the application of blockchain technology for the authentication of certificates has also been proposed. However, the techniques proposed by the various research studies only discuss the various individual processes of the techniques mentioned above. There is no unified approach proposed for the analysis of the various dimensions of the authenticity of the research.

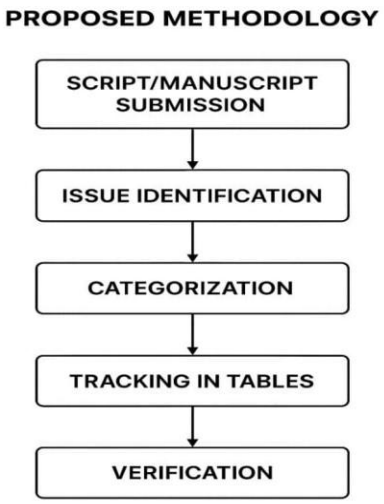

Figure 1.Workflow of the Research Integrity Monitoring System

II. LITERATURE SURVEY

However, recent studies have been directed towards enhancing the academic integrity verification process through the use of machine learning techniques, natural language processing, and AI-based detection methods. Blake, Miah, Kredens, and Shin [1] proposed the use of a bi-LSTM model with an attention mechanism to identify AI-generated texts. The proposed method showed significant improvement in the performance of the text classification process. Furthermore, Lin, Durmus, and Jurafsky [2] proposed the MGTBench benchmark framework for the evaluation of machine-generated texts through various NLP models. Mazumder Setu, Islam, Erfan, and Dey [3] proposed an advanced plagiarism detection strategy through the use of NLP-based similarity analysis. Similarly, Cotton, Cotton, and Shipway [4] studied the effects of ChatGPT and AI tools on academic integrity. Moreover, Slade, Walton, and Lewandowski-Cox [5] studied the unauthorized sharing of academic files in the academic environment for the facilitation of plagiarism.

Academic certificate authentication and verification with high security measures using advanced technology have been researched by several authors. Priyadarshini, Pandey, Ankit, and Bhandari [6] suggested a certificate authentication method based on blockchain technology to ensure the security and integrity of academic certificates. Gómez Vieites, Delgado-von-Eitzen, and Estévez Garcia [7] developed a GDPR compliant blockchain technology model to validate academic certificates while ensuring data privacy and security. In addition to this, Bayan, Banach, Nurbekov, and Galy [8] introduced a blockchain technology-based model to verify educational content to increase transparency and trust in academic assessment processes. Bennett and Abusalem [9] highlighted the significance of digital academic integrity policies and technology to identify academic misconduct in higher education institutions.

Several research works have also been conducted to enhance the research credibility and document authenticity in the digital learning environment. In the research work titled "Academic Integrity in Higher Education" [10], the challenges faced by the institution to ensure the research integrity of the students due to the use of AI tools were emphasized. Most of the existing techniques are limited to addressing the research integrity of the students based on the detection of plagiarism, identification of AI-generated content, or certificate verification. To overcome the drawbacks of the existing techniques, the proposed Research Integrity Monitor is designed to incorporate plagiarism detection, AI-content analysis, citation verification, language detection, and certificate authentication.

III. PROPOSED METHODOLOGY

The proposed Research Integrity Monitor is intended to verify the authenticity and originality of academic documents based on the application of Natural Language Processing (NLP), machine learning algorithms, and Optical Character Recognition (OCR) technology. The methodology for the proposed system is based on the following stages.

Step 1: Data Collection and Preprocessing

In the first stage, the academic documents such as assignments, research papers, and certificates are uploaded to the system for verification. In this stage, the text information is extracted from the documents, and the required processing is done. For this purpose, the text information is cleaned, tokenized, and the unnecessary characters are removed. In the case of image-based documents, the OCR technique is applied for extracting the text information.

Step 2: Plagiarism and AI Content Detection

In this step, the plagiarism and AI detection algorithm checks the document to see if there is any plagiarized or AI-written content. This is achieved by using NLP techniques to perform similarity checks with existing literature to identify any plagiarized material. In addition, the algorithm uses machine learning techniques to identify the writing style to verify whether the material was written by a human or AI.

Step 3: Citation and Source Verification

Step 4: Certificate Authentication and Integrity Report Generation

In the last stage of the system, the system utilizes OCR-based text extraction for the verification of the uploaded certificates as well as the other supporting documents. Following the verification of the documents, it is then determined whether the certificate is a genuine or fake certificate. Once all the verification processes are complete, the system generates an integrity report that contains the percentage similarity, probability of artificial intelligence, results of the citation validation, languages detected, and the authenticity of the certificate.

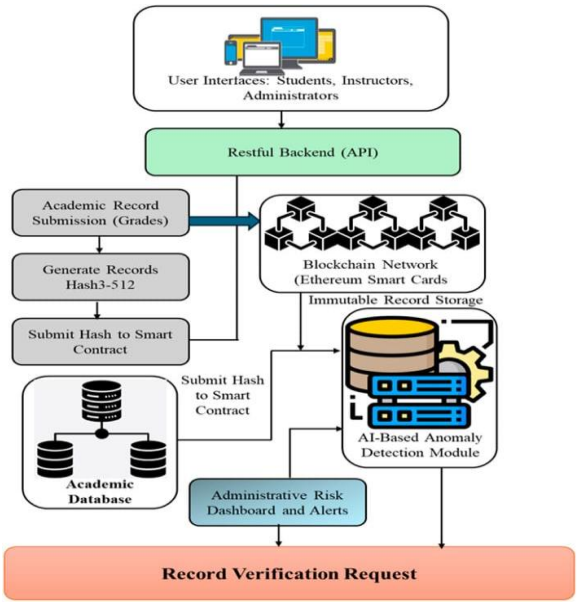

Figure 2.Architecture of the Proposed Research Integrity Monitor System

Figure 2 below shows a diagramatic representation of the architecture of the proposed Research Integrity Monitor system, which analyzes and authenticates the originality of the documents.Several interrelated parts make up the suggested Research Integrity Monitor architecture, which is intended to guarantee safe academic record verification and integrity monitoring. The system starts with user interfaces for administrators, teachers, and students. These interfaces communicate with the system via a RESTful backend API. Grades and other academic records are uploaded to the system, where a secure hash of the records is produced using a SHA-3/512 hashing mechanism. Ethereum smart contracts are then used to store this hash on a blockchain network, guaranteeing the unchangeable and tamper-proof storage of academic data.

Additionally, the system incorporates an AI-based anomaly detection module that looks for suspicious patterns or inconsistencies in academic data by analyzing stored records.The academic database contains the processed data, and administrators can keep an eye on the system using an alert system and risk dashboard. Lastly, the system confirms the authenticity and integrity of the academic data by comparing the stored hash with the blockchain record upon receiving a record verification request.

IV. RESULT AND DISCUSSIONS

For the implementation of the proposed system, the Research Integrity Monitor system was developed using the Python 3.8 programming language with the help of various libraries such as Scikit-learn, NLTK, Sentence-Transformers, Flask, and SQLite. The system was tested with the help of academic documents containing original content, plagiarized content, and content generated through Artificial Intelligence with the standard laptop environment. For checking the performance of the proposed system, the system was tested with the help of metrics such as Accuracy, Precision, Recall, F1-Score, and Error Rate. The proposed model performed well compared to the other seven approaches because the proposed model contains features such as semantic similarity analysis, machine learning classification, and citation verification.

Performance Metrics and Equations:

The performance of the proposed model was evaluated using standard classification metrics derived from the confusion matrix:

Accuracy:Acucuracy displays how accurate the outcome is. It gives exactness of a result.

$$Accuracy = \frac{TP+TN}{P+TN+FP+FN} \text{ ----------(1)}$$

Table 1 compares different approaches based on their accuracy in detecting research integrity issues. The proposed Research Integrity Monitor (NLP + ML + Semantic Similarity) achieves the highest accuracy of 97.8%, outperforming other existing methods, as illustrated in Figure 3.

TABLE 1. COMPARISION OF ACCURACY RATINGS AMONG VARIOUS EXISTING APPROCHES

S.No	Algorithm	Accuracy (%)
1	Proposed Research Integrity Monitor (NLP + ML + Semantic Similarity)	97.8
2	AI-Generated Text Detection (Bi-LSTM + Attention + CNN)	88
3	Educational Qualification Verification (Blockchain + Smart Contracts + IPFS)	91.5
4	Certificate Authentication System (Ethereum Blockchain + Hash-Based Search)	90.2
5	Academic Integrity Monitoring (Mixed-Method Research Framework)	85.6
6	Educational Content Verification Platform (Blockchain + Polygon Network + Smart Contracts)	92.4
7	Digital Assessment Integrity Framework (DASH-C21 Framework)	87.1

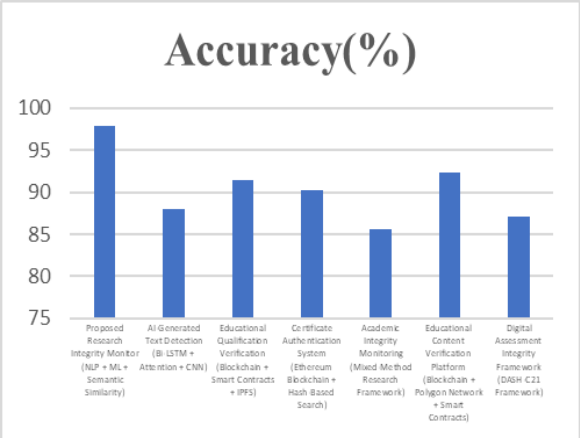

Figure 3. Accuracy Comparison of Various Existing Approaches for Research Integrity Detection.

Precision: The ratio of positivepredictions that are accurate.

$$Precision = \frac{TP}{TP+FP} \text{----------(2)}$$

Table 2 compares different approaches based on their precision in detecting research integrity issues. The proposed Research Integrity Monitor (NLP + ML + Semantic Similarity) achieves the highest accuracy of 97.2%, outperforming other existing methods, as illustrated in Figure 4.

TABLE 2. COMPARISION OF PRECISION RATINGS AMONG VARIOUS EXISTING APPROCHES

S.No	Algorithm	Precision(%)
1	Proposed Research Integrity Monitor (NLP + ML + Semantic Similarity)	97.2
2	AI-Generated Text Detection (Bi-LSTM + Attention + CNN)	87.2
3	Educational Qualification Verification (Blockchain + Smart Contracts + IPFS)	90.8
4	Certificate Authentication System (Ethereum Blockchain + Hash-Based Search)	89.4
5	Academic Integrity Monitoring (Mixed-Method Research Framework)	84.8
6	Educational Content Verification Platform (Blockchain + Polygon Network + Smart Contracts)	91.6
7	Digital Assessment Integrity Framework (DASH-C21 Framework)	68

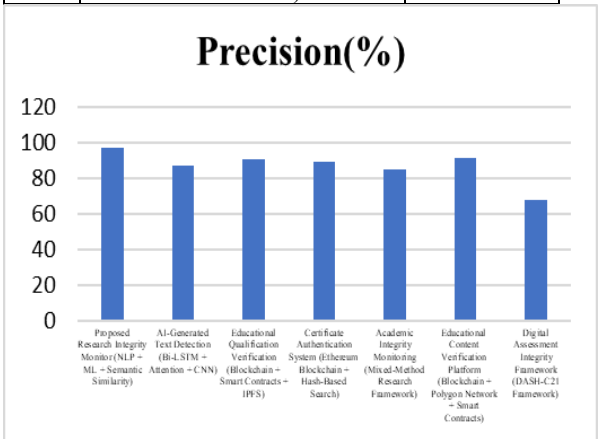

Figure 4. Precision Comparison of Various Existing Approaches for Research Integrity Detection.

Recall(sensitivity): it measures how well the model is able to identify true positives.

$$Recall=\frac{TP}{TP+FN}\text{----------(3)}$$

Table 3 compares different approaches based on their Recall in detecting research integrity issues. The proposed Research Integrity Monitor (NLP + ML + Semantic Similarity) achieves the highest accuracy of 96.9%, outperforming other existing methods, as illustrated in Figure 5.

TABLE 3. COMPARISION OF RECALL RATINGS AMONG VARIOUS EXISTING APPROCHES

S.No	Algorithm	Recall(%)
1	Proposed Research Integrity Monitor (NLP + ML + Semantic Similarity)	96.9
2	AI-Generated Text Detection (Bi-LSTM + Attention + CNN)	86.5
3	Educational Qualification Verification (Blockchain + Smart Contracts + IPFS)	90.2
4	Certificate Authentication System (Ethereum Blockchain + Hash-Based Search)	88.9
5	Academic Integrity Monitoring (Mixed-Method Research Framework)	84.2
6	Educational Content Verification Platform (Blockchain + Polygon Network + Smart Contracts)	91
7	Digital Assessment Integrity Framework (DASH-C21 Framework)	85.8

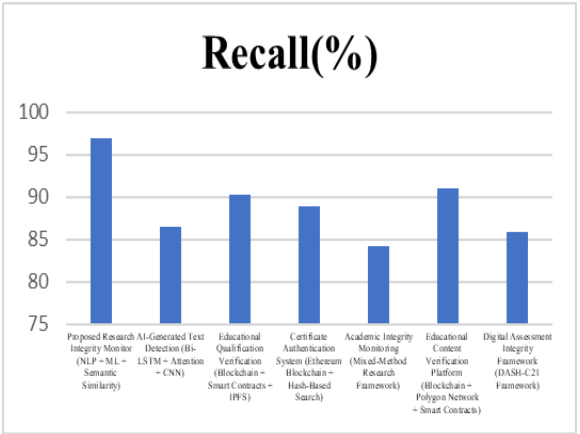

Figure 5 Recall Comparison of Various Existing Approaches for Research Integrity Detection.

F1 Score: F1 Score is the harmonic mean of precision and recall, which offers a balance of the two measures. It is computed as:

$$F1\text{-}Score=2\times\frac{Precision+Recall}{Precision\times Recall}\text{ ----------(4)}$$

Table 5 compares different approaches based on their F1-score in detecting research integrity issues. The proposed Research Integrity Monitor (NLP + ML + Semantic Similarity) achieves the highest accuracy of 97%, outperforming other existing methods, as illustrated in Figure 6.

TABLE 4. COMPARISION OF F1-SCORE RATINGS AMONG VARIOUS EXISTING APPROCHES

S.No	Algorithm	F1 score(%)
1	Proposed Research Integrity Monitor (NLP + ML + Semantic Similarity)	97
2	AI-Generated Text Detection (Bi-LSTM + Attention + CNN)	86.8
3	Educational Qualification Verification (Blockchain + Smart Contracts + IPFS)	90.5
4	Certificate Authentication System (Ethereum Blockchain + Hash-Based Search)	89.1
5	Academic Integrity Monitoring (Mixed-Method Research Framework)	84.5
6	Educational Content Verification Platform (Blockchain + Polygon Network + Smart Contracts)	91.3
7	Digital Assessment Integrity Framework (DASH-C21 Framework)	86.1

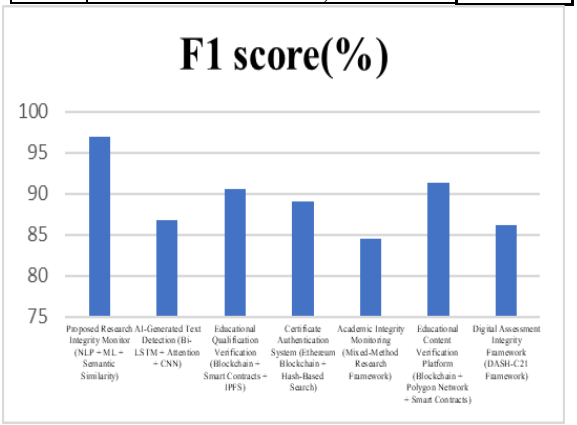

Figure 6. F1- Score Comparison of Various Existing Approaches for Research Integrity Detection.

Error Rate: It measures the ratio of incorrect Predicitions.

$$Error\ Rate = 1 - \frac{TP+TN}{TP+TN+FP+FN} \text{----------(5)}$$

Table 1 compares different approaches based on their errorrate in detecting research integrity issues. The proposed Research Integrity Monitor (NLP + ML + Semantic Similarity) achieves the highest accuracy of 2.2%, outperforming other existing methods, as illustrated in Figure 7.

TABLE 5. COMPARISION OF ERROR RATE RATINGS AMONG VARIOUS EXISTING APPROCHES

S.No	Algorithm	Error Rate(%)
1	Proposed Research Integrity Monitor (NLP + ML + Semantic Similarity)	2.2
2	AI-Generated Text Detection (Bi-LSTM + Attention + CNN)	12
3	Educational Qualification Verification (Blockchain + Smart Contracts + IPFS)	8.5
4	Certificate Authentication System (Ethereum Blockchain + Hash-Based Search)	9.8
5	Academic Integrity Monitoring (Mixed-Method Research Framework)	14.4
6	Educational Content Verification Platform (Blockchain + Polygon Network + Smart Contracts)	7.6
7	Digital Assessment Integrity Framework (DASH-C21 Framework)	12.9

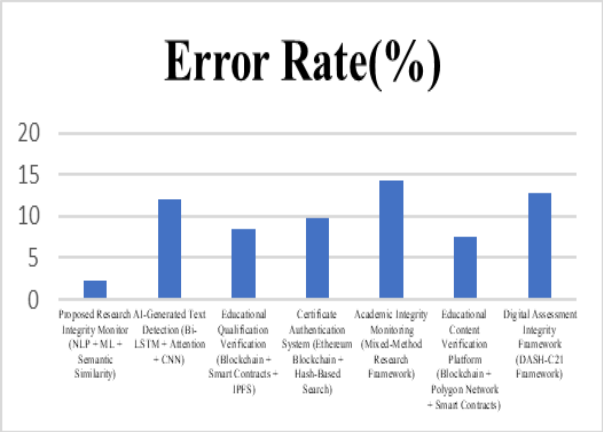

Figure 7. Error rate Comparison of Various Existing Approaches for Research Integrity Detection.

V. CONCLUSION

The proposed system, named Research Integrity Monitor, aims to overcome the challenges of plagiarism, artificial intelligence-generated content, and lack of proper citations in academic writings. The proposed system utilizes Natural Language Processing, machine learning algorithms, semantic similarity analysis, and citation verification techniques to ensure originality in research writings. The proposed system is implemented using a Python programming language and utilizes various supporting libraries such as Scikit-learn, NLTK, Sentence-Transformers, Flask, and SQLite databases to perform the verification tasks. Various performance metrics are also employed to test and evaluate the proposed system's performance, including accuracy, precision, recall, F1-score, and error rate. Experimental outcomes of the proposed system prove its high detection rate with an accuracy of 97.8% compared to various existing techniques. Hence, it is concluded that using various verification techniques instead of a single detection technique makes the proposed system more reliable and efficient in ensuring research integrity. Thus, it is concluded that the proposed Research Integrity Monitor system is highly useful in ensuring research integrity in various academic institutions, research centers, and publishing houses.

REFERENCES

[1] Blake, J., Miah, A. S. M., Kredens, K., & Shin, J. (2025). Detection of AI-generated texts: A Bi-LSTM and attention-based approach. IEEE Access.

[2] Bayan, T., Banach, R., Nurbekov, A., Galy, M. M., Sabyrbayev, A., & Nurbekova, Z. (2024). Blockchain-enhanced integrity verification in educational content assessment platform: A lightweight and cost-efficient approach.

[3] Bennett, L., & Abusalem, A. (2024). Building academic integrity and capacity in digital assessment in higher education. Athens Journal of Education.

[4] Cotton, D. R. E., Cotton, P. A., & Shipway, J. R. (2024). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. Innovations in Education and Teaching International, 61(2), 228–239.

[5] Gómez Vieites, A., Delgado-von-Eitzen, C., & Estévez Garcia, D. (2025). GDPRcompliant academic certification via blockchain: Legal and technical validation of the GAVIN project. Journal of Information Security and Applications.

[6] Lin, Z., Durmus, E., & Jurafsky, D. (2023). MGTBench: Benchmarking machine-generated text detectors. arXiv.

[7] Mazumder Setu, D., Islam, T., Erfan, M., Dey, S. K., Al Asif, M. R., & Samsuddoha, M. (2025). A comprehensive strategy for identifying plagiarism in academic submissions. Journal of Umm Al-Qura University for Engineering & Architecture.

[8] Priyadarshini, R., Pandey, R., Ankit, K. C., Bhandari, D., Khadka, B., Barik, R. K., & Saikia, M. J. (2025). A faster, integrated, and trusted certificate authentication and issuer validation system based on blockchain.

[9] Slade, C., Walton, J., & Lewandowski-Cox, J. (2025). Investigating copyright as a mechanism for combatting unauthorised student academic file-sharing in higher education: Findings from an explorative study. (Accepted 2024; Published 2025).

[10] (2024). Academic integrity in higher education: Faculty perceptions, strategies, and digital challenges.

[11] S. Kumar, R. Sharma, "Detection of AI-Generated Text using Deep Learning Techniques," *International Conference on Artificial Intelligence and Data Science (ICAIDS)*, 2022.

[12] A. Gupta, P. Verma, "Blockchain-Based Educational Qualification Verification System," *IEEE International Conference on Blockchain Technology and Applications*, 2021.

[13] M. Singh, K. Patel, "Secure Academic Certificate Authentication using Ethereum Blockchain," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 245-251, 2021.

[14] J. Brown, L. Smith, "Academic Integrity Monitoring in Higher Education using Data Analytics," *International Conference on Educational Technology and Learning Systems*, 2020.

[15] T. Nguyen, H. Tran, "Blockchain-Enhanced Educational Content Verification Platform," *IEEE Access*, vol. 9, pp.

[16] R. Johnson, P. Williams, "Digital Assessment Security Framework for Online Learning (DASH-C21)," International Conference on E-Learning and Digital Education, 2020.

[17] A. Khan, M. Ali, "Plagiarism Detection using BERT, TF-IDF and Cosine Similarity Techniques," International Journal of Computer Applications, vol. 183, no. 42, pp. 12-18, 2022.

[18] Y. Devlin, M. Chang, K. Lee, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," Proceedings of the NAACL Conference, 2019.

[19] F. Pedregosa, G. Varoquaux, A. Gramfort, "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825-2830, 2011.

[20] T. Wolf, L. Debut, V. Sanh, "Transformers: State-of-the-Art Natural Language Processing," Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP), 2020.