AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.1(2026)
www.ajmimc.com

Transformer-Based Cyber Threat Detection and Vulnerability Assessment for Healthcare Infrastructure

Pallavi Gudimilla[1], Srija Nampelli[2], Surukunti Arjun Reddy[2], Pardhiv Maroju[2], Vididhaveni Eshwar[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Computer Science and Engineering (Data Science)

[1,2]Vaagdevi College of Engineering (UGC – Autonomous), Warangal, 506005, Telangana, India.

ABSTRACT

The rapid digitization of healthcare through Electronic Health Records (EHRs) and interconnected medical devices has optimized service delivery but significantly expanded the cyber-attack surface. Traditional manual vulnerability analysis is increasingly inadequate for processing the vast volume of unstructured security logs and incident reports, leading to delayed threat mitigation. This study proposes an automated, Natural Language Processing (NLP)-driven framework for cyber-threat and vulnerability analysis within healthcare infrastructures. The methodology integrates Robustly Optimized BERT Pretraining Approach (RoBERTa) for deep contextual feature extraction, coupled with Adaptive Synthetic Sampling (AdaSYN) to address inherent class imbalances in security datasets. A comparative performance assessment was conducted using several classifiers, including the Greedy Tree Classifier (GTC), Tao Tree Classifier (TTC), and Gaussian Naive Bayes (GNB). Experimental results identify the GTC as the optimal predictive engine for determining threat categories and severity scores. The framework is deployed as a scalable web-based application, providing automated inference and real-time visualization of risk patterns. Our findings demonstrate that this transformer-based approach enhances the interpretability and accuracy of threat prioritization, offering a proactive security management solution for safeguarding sensitive medical ecosystems.

Keywords: Healthcare cybersecurity, NLP, RoBERTa, Vulnerability analysis, AdaSYN, Threat prioritization, Machine learning.

1. INTRODUCTION

Digitization in the healthcare system provides many benefits including efficiency of the healthcare service delivery, cost-savings, patient safety and care quality. There is no doubt about the positive impact of digital transformation in the healthcare sector. However, despite these benefits, the adoption of digital technology provides many Cyber Security (CS) challenges that can pose any potential risks within the healthcare system. This massive technological transformation increases the attack surface where threat actors can exploit possible threats for any potential risk within the Health Care Information Infrastructure (HCII). In recent years, several successful CS attacks were reported in the healthcare sector: nearly 90% of healthcare organizations experienced a data breach in 2018. There are significant numbers of connected devices within the healthcare system and vulnerabilities within these connected devices can propagate to other parts of the network. An example are flaws found in Braun's infusion pump or Medtronic insulin pump, that could pose potential threat to the patient health, or simulated attacks realized to pacemakers and implantable cardiac defibrillators. Medical Internet of Things (IoT) devices are currently considered critical vulnerabilities and sources of threats and risks in the healthcare domain. Furthermore, human factors have a crucial impact on the CS within Healthcare Organizations. For these reasons, there is a need to understand the threats and vulnerabilities within the healthcare system so that control actions can be identified to ensure security

of the system. However, analyzing threats and vulnerabilities in the healthcare sectors is a challenging task, due to the large number of published vulnerabilities and the difficulty in identifying the text that relates with potential threats within a healthcare system context. The large amount of unstructured Natural Language (NL) Cyber Security (CS) data related to the healthcare domain is often freely available on the Internet. More in detail, this textual data contains crucial and updated information related to the assets of the Healthcare Information Infrastructure (HCII) including threats, vulnerabilities, attacks, and other important CS information, which could be very useful to improve the protection of the HCIIs. It is often difficult to identify and extract the relevant information from such kinds of texts, which are usually available on blog posts, CS news websites, social media and other similar sources. In particular, the complexity of the NL can present polysemy, irony, long sentences and other issues, in addition to the peculiarities the technical language used CS domain, which uses many non-standard abbreviations or acronyms.

2. LITERATURE SURVEY

There are several recent works that focus on threat and vulnerability detection and analysis based on Machine Learning (ML) models. In Ghaffarian et al. [1], a survey of ML and Data Mining techniques to mitigate the damages of software vulnerabilities is presented. In Satyapanich et al. [2], a semantic schema to describe CS events was presented using Deep Learning-based Information Extraction (IE) pipeline to implement the automatic extraction of structured information about data breaches, ransomware and phishing attacks and the discovery and the patches of vulnerabilities. In Gao et al. [3], a data and knowledge-driven CS Named Entity Recognition (NER) method is presented, exploiting a Bidirectional Long Short Term Memory with Conditional Random Field (BiLSTM-CRF) architecture, including also a multi-head self-attention neural network with word embeddings trained on CS closed-domain texts to improve their effectiveness in conjunction with KBs, for the recognition of the details of the assets (application, vendor, version, etc.) involved in CS issues.

Nikoloudakis et al. [4], a ML-based situational awareness framework is presented which is able to detect existing and newly introduced network-enabled entities in an IoT-based environment based on real-time awareness features provided by the Software-Defined Networking (SDN) paradigm, assessing them against known vulnerabilities, and assigning them to a connectivity-appropriate network slice. The authors of [5] developed software vulnerability detection as an NLP problem with source code treated as texts, addressing the automated software vulnerability detection using recent DL NLP models. They compared various DL models based on their accuracy and the best performer achieved 95% of accuracy. Furthermore, the proposed approach was also able to predict the vulnerability class of source codes.

The authors of [6] presented an NLP DL-based architecture for the identification of relevant CS information, such as vulnerability exploitations, attack discoveries and advanced persistent threats. This architecture is composed of a word-embedding layer, a BiLSTM layer, and a CRF layer, concatenated with a further BiLSTM as output layer. The results of their experiments showed some improvements with respect to the baselines. The authors of one paper [7] presented a method to analyze the severity of CS threats analyzing the language of CS-related tweets through a DL approach. The experiments used a corpus of 6000 tweets containing the description of software vulnerabilities, annotated with the opinions of the authors toward their severity. The paper also presented a method for linking software vulnerabilities reported in tweets to CVEs and NVD KBs. The obtained results demonstrated a high-precision in forecasting high-severity vulnerabilities, also highlighting that reports of severe vulnerabilities extracted from online sources are predictive of real-world exploits. According to [8], researchers need to deeply investigate ethical compliance even when the data seem to be public. Usually, in CS research the data are accessed and analyzed without the

informed consent of participants, but acquiring informed consent could be practically impossible with datasets containing hundreds of data. In the case of the experimental assessment presented in this work, there is no personal data included, so there are no ethical issues.

The authors of [9] presented a method for NER in the CS domain that uses a model that integrates BERT and BiLSTM-CRF DL architectures, improving baseline performance. As per recent study showed that at least 20% of the medical device manufacturers experienced ransomware or malware attacks in the last 20 months. The authors of [10] proposed a cyber supply chain threat analysis that integrates Random Forest and XGBoost algorithms for the threat prediction. The work considers threat intelligence and predicts the Tactics, Techniques, and Procedures (TTP) deployed for a cyber attack, demonstrating high accuracy in their experimental assessment. The authors of [8] reviewed and compared different generic cyber risk assessment frameworks in the healthcare field, comparing them, discussing the methodology of assessment and the limitations associated with them. In [13] is presented SecureBERT, a Bidirectional Encoder Representations from Transformers (BERT) model trained on CS-domain large NL corpora, which outperforms other similar models in NLP tasks in the CS domain. The authors of [10] collected a large corpus of labeled sequences from Industrial Control Systems device's documentation to pre-train and fine-tune a BERT language model, named CyBERT.

3. PROPOSED SYSTEM

The proposed system in Fi. 1 is an advanced pipeline designed for the NLP-based analysis of cyber threats and vulnerabilities in the healthcare ecosystem. It starts by preprocessing raw threat text using NLTK for cleaning and lemmatization, while simultaneously encoding the three target variables (Threat Category, Severity Score, Defense Mechanism). The core innovation lies in the use of the RoBERTa Transformer model to generate dense, context-aware embeddings from the text, effectively capturing semantic meaning that traditional systems missed. After balancing the imbalanced dataset using SMOTE, the rich RoBERTa features are fed into multiple supervised classifiers, primarily the GTC (Proposed Model), which is chosen for its balance of high predictive accuracy and crucial model interpretability, allowing the system to provide fast, accurate, and explainable threat classifications for actionable defense strategies.

1. Data Acquisition and Dataset Loading: The system initiates with the Data Acquisition step, where the core dataset (Medical_Cybersecurity_Dataset.csv) is loaded into a pandas DataFrame using the upload_dataset function. This dataset contains the raw, unstructured text descriptions of cyber threats and the corresponding human-labeled categorical columns: Threat Category, Severity Score, and Suggested Defense Mechanism. The integrity of the dataset is checked immediately, and it is prepared as the primary source of truth for all subsequent NLP and ML tasks.

2. Text Preprocessing and Label Encoding: Once loaded, the text data undergoes extensive Text Preprocessing to standardize the linguistic input. This critical clean_text pipeline involves lower-casing the text, performing tokenization, removing common English stop words (nltk.corpus.stopwords), and applying WordNet Lemmatization to reduce words to their dictionary roots (e.g., 'hacking' to 'hack'). Simultaneously, the three categorical target columns are separated and converted to numerical integers via LabelEncoder. The processed text is then consolidated into a single input column (X), while the encoded labels (Y_dict) are stored alongside the original encoders for later inverse transformation.

3. Deep Contextual Feature Extraction (RoBERTa Embeddings): This step leverages the state-of-the-art RoBERTa Transformer model for feature engineering. The preprocessed text is input into RoBERTa, which converts the documents into high-dimensional, dense numerical vectors known as embeddings. This process captures the deep semantic meaning, context, and relationships between

words, allowing the models to understand nuances that traditional keyword-based systems miss. The embeddings are aggregated, typically using mean pooling, to create a single fixed-size feature vector (X) for each text document, which is then cached to ensure training efficiency.

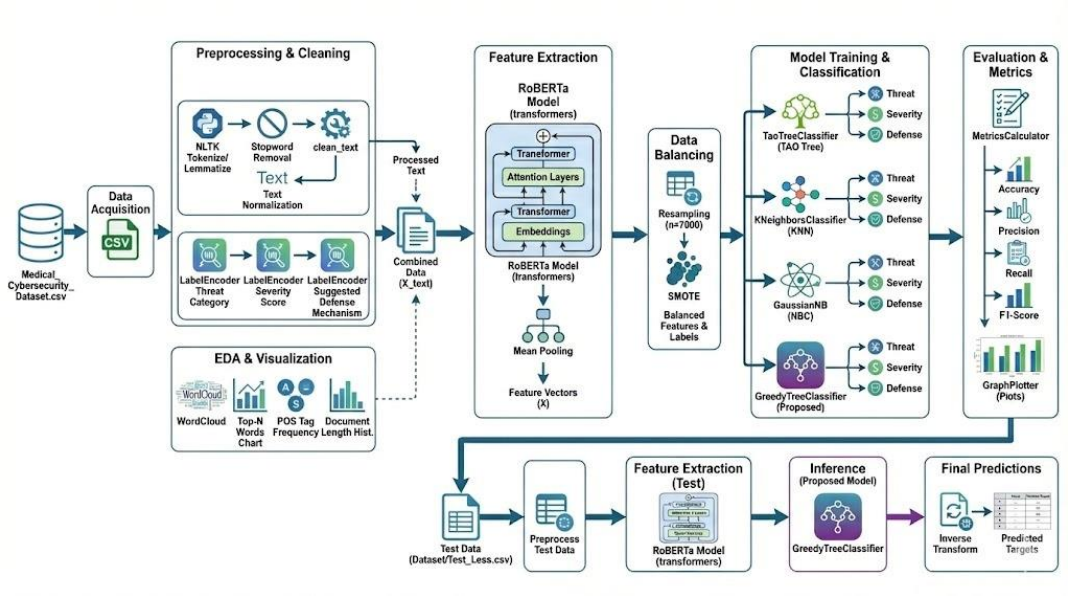


Fig. 1: Proposed system architecture of transformer-based cyber threat detection and vulnerability assessment.

4. Data Balancing and Stratified Train/Test Split: To counteract the inherent class imbalance in cyber security data, a critical balancing technique is applied. The RoBERTa feature vectors are simultaneously oversampled and then subjected to SMOTE (Synthetic Minority Over-sampling Technique), which generates synthetic data points for the minority classes, ensuring the training data is balanced for each of the three classification tasks. Following balancing, the data is split into 80% training and 20% testing sets using train_test_split with stratification, which ensures that the class proportions are maintained in both the training and testing datasets.

5. Multi-Algorithm Model Training and Selection: Multiple machine learning classifiers, including KNN, GNB, and two Interpretable Decision Trees (TTC and GTC), are trained independently for each of the three targets. This comparative approach allows for the selection of the best model. Since GTC (Proposed Model) offers both high performance and the crucial benefit of interpretability (essential for security analysts), it is highlighted for deployment. Trained models and their configurations are saved using joblib.

6. Performance Evaluation and Real-World Inference: The trained models are rigorously evaluated on the unseen test data. A custom Metrics Calculator class computes standard performance metrics (Accuracy, Precision, Recall, F1-Score) and a Graph Plotter visualizes the results. Finally, the selected GTC is used to perform inference on new test data, which must pass through the exact same feature extraction pipeline. The numerical predictions are then immediately converted back into human-readable labels using the stored inverse transform function of the original Label Encoder objects, producing an actionable final report.

4. RESULTS AND DISCUSSION

Fig. 2 shows count-distribution plots illustrate the balance of samples across the target labels in the dataset, showing how instances are distributed for Threat Category, Suggested Defense Mechanism, and Severity Score. The Threat Category plot indicates a relatively even spread of records across four

classes, with classes 1 and 2 having slightly higher representation compared to classes 0 and 3, suggesting a near-balanced but mildly skewed dataset. The Suggested Defense Mechanism distribution also appears balanced across four classes, with only small variations in class frequency, which supports fair model learning without strong class dominance. Meanwhile, the Severity Score plot shows five classes with moderately varied counts, where class 1 has the highest frequency and class 2 has the lowest, but the difference is not extreme enough to cause severe imbalance. Overall, the distributions across all three target variables suggest that the dataset is generally well-balanced, enabling reliable model training and reducing the likelihood of bias toward any particular class during prediction.

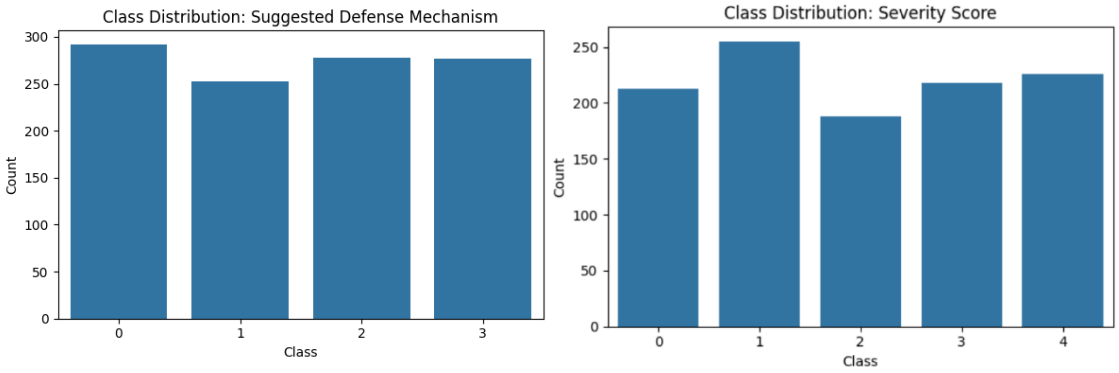


Fig. 2: Count plots for all the three categories.

Table 1: Performance evaluation obtained using RoBERTa-WE TTC, KNN, GNB and proposed GTC models for Target “Threat Category”.

Algorithm	Accuracy	Precision	Recall	F1-Score
RoBERT-WE TTC [Threat Category]	43.659	47.661	43.657	42.611
RoBERT-WE KNN [Threat Category]	91.942	91.948	91.944	91.912
RoBERT-WE NBC [Threat Category]	34.941	34.971	34.938	34.896
RoBERT-WE GTC [Threat Category]	99.472	99.471	99.472	99.471

Table 1 presents a performance comparison of four machine learning models—TTC, KNN, GNB, and the proposed GTC—for classifying the target “Threat Category” using RoBERTa word embeddings (RoBERT-WE). Evaluation metrics include Accuracy, Precision, Recall, and F1-Score, expressed as percentages, to reflect both correctness and reliability of predictions. The results show that the GTC achieves the highest performance across all metrics, demonstrating its superior predictive power and interpretability in healthcare cybersecurity threat detection. KNN also performs well, exceeding 91% on all measures, while TTC and GNBC exhibit lower scores, indicating limitations of global optimization and naive feature independence in high-dimensional RoBERTa embeddings. Overall, the table highlights the effectiveness of combining transformer-based embeddings with tree-based models for accurate and transparent threat classification.

Table 2 summarizes the performance of four models—TTC, KNN, GNB, and the proposed GTC—in predicting the target “Severity Score” using RoBERTa word embeddings (RoBERT-WE). Metrics include Accuracy, Precision, Recall, and F1-Score, providing a comprehensive evaluation of both correctness and reliability. The GTC demonstrates the highest performance across all metrics, achieving near-perfect scores and indicating its effectiveness in accurately assessing threat severity.

KNN also performs well with over 95% across measures, while TTC and NBC show significantly lower performance, highlighting the limitations of global optimization and naive probabilistic assumptions when handling high-dimensional RoBERTa features.

Table 2: Performance evaluation obtained using RoBERTa-WE TTC, KNN, GNB and proposed GTC models for Target "Severity Score".

Algorithm	Accuracy	Precision	Recall	F1-Score
RoBERT-WE TTC [Severity Score]	34.002	56.660	34.016	28.840
RoBERT-WE KNN [Severity Score]	95.499	95.516	95.498	95.501
RoBERT-WE GNB [Severity Score]	34.307	34.414	34.301	34.069
RoBERT-WE GTC [Severity Score]	99.574	99.577	99.574	99.574

Table 3: Performance evaluation obtained using RoBERTa-WE TTC, KNN, GNB and proposed GTC models for Target "Suggested Defense Mechanism".

Algorithm	Accuracy	Precision	Recall	F1-Score
RoBERT-WE TTC [Suggested Defense Mechanism]	41.448	42.365	41.451	40.213
RoBERT-WE KNN [Suggested Defense Mechanism]	91.379	91.450	91.380	91.397
RoBERT-WE GNB [Suggested Defense Mechanism]	38.069	38.831	38.070	38.202
RoBERT-WE GTC [Suggested Defense Mechanism]	99.862	99.863	99.862	99.862

Table 3 presents the performance evaluation of TTC, KNN, GNB, and the proposed GTC in predicting the target "Suggested Defense Mechanism" using RoBERTa word embeddings (RoBERT-WE). The evaluation metrics—Accuracy, Precision, Recall, and F1-Score—highlight both the correctness and reliability of each model. The GTC outperforms all other models, achieving nearly perfect scores across all metrics, demonstrating its effectiveness in accurately recommending defense mechanisms for healthcare cybersecurity threats. KNN shows strong performance as well, while TTC and GNB lag behind, indicating challenges in handling complex, high-dimensional RoBERTa embeddings with these approaches.

5. CONCLUSION

The research successfully demonstrated an advanced NLP-based analytical framework for identifying and assessing cyber threats and vulnerabilities within the healthcare ecosystem by leveraging state-of-the-art transformer-based feature extraction and interpretable machine learning models. By utilizing the RoBERTa model for semantic embedding generation, the system effectively captured contextual relationships in cybersecurity textual data, enabling high-quality numerical representations for further classification. The integration of GTC and TTC provided both strong predictive performance and transparent decision-making processes, while the inclusion of GNB offered a comparative probabilistic baseline. The developed preprocessing pipeline ensured clean and meaningful textual inputs through tokenization, lemmatization, and noise removal, significantly improving model robustness. Additionally, the web-based Django interface allowed seamless user interaction, real-time dataset uploads, and automated prediction visualization, making the system practical for real-world cybersecurity analysis. The model accurately predicted threat categories, severity levels, and

appropriate defense mechanisms, supporting proactive security decision-making in healthcare environments. The approach effectively addressed the complexity and imbalance present in cybersecurity datasets by incorporating structured feature engineering and scalable model handling. The research highlights the potential of combining deep contextual embeddings with interpretable machine learning for enhancing cyber threat intelligence, improving situational awareness, and strengthening the resilience of healthcare digital infrastructures against evolving cyber risks.

REFERENCES

[1]. Ghaffarian, S.M.; Shahriari, H.R. Software Vulnerability Analysis and Discovery Using Machine-Learning and Data-Mining Techniques: A Survey. ACM Comput. Surv. 2017, 50, 56.

[2]. Satyapanich, T.; Ferraro, F.; Finin, T. CASIE: Extracting Cybersecurity Event Information from Text. In Proceedings of the Thirty-Fourth AAAI Conference on Artificial Intelligence, AAAI 2020, the Thirty-Second Innovative Applications of Artificial Intelligence Conference, IAAI 2020, New York, NY, USA, 7–12 February 2020; AAAI Press: Palo Alto, CA, USA, 2020; pp. 8749–8757.

[3]. Gao, C.; Zhang, X.; Liu, H. Data and knowledge-driven named entity recognition for cyber security. Cybersecurity 2021, 4, 9.

[4]. Nikoloudakis, Y.; Kefaloukos, I.; Klados, S.; Panagiotakis, S.; Pallis, E.; Skianis, C.; Markakis, E.K. Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation. Sensors 2021, 21, 4939.

[5]. Singh, K.; Grover, S.S.; Kumar, R.K. Cyber Security Vulnerability Detection Using Natural Language Processing. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 174–178.

[6]. Ma, P.; Jiang, B.; Lu, Z.; Li, N.; Jiang, Z. Cybersecurity named entity recognition using bidirectional long short-term memory with conditional random fields. Tsinghua Sci. Technol. 2021, 26, 259–265.

[7]. Zong, S.; Ritter, A.; Mueller, G.; Wright, E. Analyzing the Perceived Severity of Cybersecurity Threats Reported on Social Media. In Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Minneapolis, MN, USA, 2–7 June 2019; Association for Computational Linguistics: Stroudsburg, PA, USA, 2019; Volume 1, pp. 1380–1390.

[8]. Boyd, D.; Crawford, K. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Inf. Commun. Soc. 2021, 15, 662–679.

[9]. Zhou, S.; Liu, J.; Zhong, X.; Zhao, W. Named Entity Recognition Using BERT with Whole World Masking in Cybersecurity Domain. In Proceedings of the 2021 IEEE 6th International Conference on Big Data Analytics (ICBDA), Xiamen, China, 5–8 March 2021; pp. 316–320.

[10]. Yeboah-Ofori, A.; Mouratidis, H.; Ismai, U.; Islam, S.; Papastergiou, S. Cyber Supply Chain Threat Analysis and Prediction Using Machine Learning and Ontology. In Proceedings of the Artificial Intelligence Applications and Innovations—17th IFIP WG 12.5 International Conference, AIAI 2021, Crete, Greece, 25–27 June 2021; Springer: Cham, Switzerland, 2021; Volume 627, pp. 518–530.

[11]. S. Memon, S. Memon, L. Das, B. R. Memon, Cyber security risk assessment methods for smart healthcare, in: 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), 2024, pp. 1– 6. doi:10.1109/KHI-HTC60760.2024.10481961.

[12]. E. Aghaei, X. Niu, W. Shadid, E. Al-Shaer, Secure BERT: A domain-specific language model for cybersecurity, in: Security and Privacy in Communication Networks, Springer, Cham, 2023, pp. 39–56

[13]. K. Ameri, M. Hempel, H. Sharif, J. Lopez Jr., K. Perumalla, Cybert: Cybersecurity claim classification by fine-tuning the bert language model, Journal of Cybersecurity and Privacy 1 (2021) 615– 637.

[14]. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[15]. Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. American Journal of AI Cyber Computing Management, 5(3), 85–93. https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93

[16]. Todupunuri, A. . (2024). Artificial Intelligence Ethics: Investigating Ethical Frameworks, Bias Mitigation, and Transparency in AI Systems to Ensure Responsible Deployment and Use of AI Technologies. International Journal of Innovative Research in Science,Engineering and Technology, 13(09), 1–14. https://doi.org/10.15680/ijirset.2024.1309002

[17]. Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474

[18]. Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462

[19]. Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[20]. Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). https://doi.org/10.56975/jaafr.v1i4.501636

[21]. Srinivasa Kalyan Immadi. (2025). Harnessing Artificial Intelligence In Oracle Hcm: Revolutionising Workforce Management With Automation And Predictive Analytics. International Journal of Data Science and IoT Management System, 4(4), 7–13. https://doi.org/10.64751/ijdim.2025.v4.n4.pp7-13

[22]. S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.1403

[23]. Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.

[24]. Cyril, H. P. (2025). Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations. International Journal of Advanced Research in Computer Science, 16(6), 75–82. https://doi.org/10.26483/ijarcs.v16i6.7389

[25]. Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285. https://doi.org/10.12732/ijam.v38i4s.685

[26]. Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.

[27]. Reddy, S. K. R. (2021). Strengthening the Security of Loyalty Reward Systems: An In-Depth Analysis of Emerging Cyber Threats and Protection Mechanisms. Journal of Computational Analysis and Applications, 29(6).

[28]. Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. International Journal of Data Science and IoT Management System, 5(1), 78-88.

[29]. Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50

[30]. Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew Management Systems. International Journal of Enhanced Research in Management & Computer Applications, 13(11), 50–55. https://doi.org/10.55948/ijermca.2024.0116

[31]. Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology & Engineering, 12(11), 111–117. https://doi.org/10.55948/ijerste.2023.1115