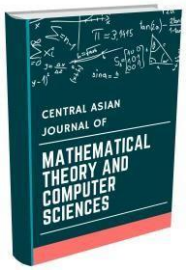

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 05 | November 2024 ISSN: 2660-5309

Article

Application of the Catboost Classifier for the Detection of Android Ransomware

S. Suman Rajest[1*], R. Regin[2]

1. Professor, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
2. Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, India.

* Correspondence: sumanrajest414@gmail.com

Abstract: Android ransomware attacks are becoming more common, threatening user data and privacy. Conventional antivirus systems struggle to identify these assaults, especially new or undiscovered types, stressing the need for more advanced IDS. Our study uses machine learning to create an Android IDS that can identify ransomware and other threats. The proposed IDS improves Android device security by detecting advanced threats. By using machine learning methods like the CatBoostClassifier, the IDS can adapt to changing ransomware threats and scan network data for malicious patterns. To prevent developing ransomware assaults and secure user data and privacy, this proactive strategy is essential. The method requires gathering and pre-processing Android device network traffic data, selecting ransomware detection features, and training the machine learning model. To ensure ransomware detection, the IDS is assessed using accuracy and false positive rate. This IDS significantly improves Android device security and ransomware protection. The IDS can protect Android user data and privacy by improving ransomware detection and mitigation.

Keywords: Conventional Antivirus, Sophisticated Intrusion Detection Systems (IDS), Leveraging Machine Learning, Ransomware Attacks, Employers Accessing

Citation: Rajest, S, S. Application of the Catboost Classifier for the Detection of Android Ransomware. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(5), 476-486.

Received: 10th Aug 2024
Revised: 11th Sept 2024
Accepted: 24th Oct 2024
Published: 21th Nov 2024

1. Introduction

Technology has changed communication, education, business, and healthcare. People can gain new skills and make informed judgments because to the internet's global connectivity. Businesses can now reach worldwide customers and operate 24/7 thanks to e-commerce. Remote employment allows people to work from anywhere and companies to access a global talent pool [1]. Technology also raises security, privacy, and digital divide problems. Laws and programs promoting online safety and addressing the digital gap address these challenges. No one is safe from cybercriminals' increasing techniques. They utilize harmful software to steal private data and misuse or demand a ransom. Statista estimates that 72% of organizations worldwide were affected by ransomware in 2023. It was the biggest number ever recorded, growing over five years. Since 2018, almost 50% of poll respondents said ransomware has harmed their companies [2-7]. Ransomware is malicious software that locks you out of your computer or files until you pay a large amount. It works by encrypting files on a victim's computer or network,

making them unreadable, and requesting payment for the decryption key. A powerful encryption method is used by ransomware to encrypt files on a computer, rendering them unreadable without the decryption key [8-12].

The ransomware notifies the victim of the attack and provides instructions on how to pay the ransom when the encryption procedure is finished. Ransomware attacks can be very bad for both people and businesses. Victims may have to pay a ransom and face financial losses, data loss, downtime, and reputational harm [13-19]. Attacks utilising ransomware may have more general effects, such as upsetting vital infrastructure or significant financial losses. Ransomware comes in various forms, such as file-encrypting and locker ransomware, which prevents the victim from accessing their device. In addition, several ransomware variations use doxing, threatening to release private data until the ransom is paid [20-23]. Ransomware attacks are a big problem that is getting worse for people, companies, and governments worldwide. Through preventive measures against ransomware and efficient countermeasures during attacks, people and institutions can lessen their vulnerability to this nasty virus. These include using secure passwords, backing up key files regularly, updating software, and exercising caution when opening email attachments or clicking links. Strong cybersecurity defences, such as intrusion detection systems, firewalls, and antivirus software, must also be in place [24-29]. To protect against ransomware attacks, it is essential to take several precautions.

To protect against ransomware attacks, preventive measures include using secure passwords, backing up key files regularly, updating software, and exercising caution when opening attachments. Strong cybersecurity defences, such as intrusion detection systems, firewalls, and antivirus software, must also be in place. Machine learning is crucial in identifying ransomware threats by analysing file access patterns, network traffic, and user activity. This paper proposes an android ransomware classification model using machine learning and the CatBoost Classifier model. The model's robustness and generalizability are enhanced by its built-in regularisation strategies [30-35].

The goal of developing the model is to detect and classify the ransomware. This includes collecting and pre-processing data, selecting the necessary features, training, and evaluating the performance. The paper aims to build a robust model to detect ransomware attacks accurately. This will help with network security and reduce ransomware attacks. Implementing this model in Android devices will enable real-time detection of ransomware attacks and thus protect against incoming ransomware attacks [36-41]. Ransomware attacks on Android devices have escalated into a significant cybersecurity concern, jeopardising user data and privacy. The existing antivirus solutions often fall short of effectively identifying and mitigating these attacks due to the ever-changing nature of ransomware and the intricate Android ecosystem. Consequently, an urgent need is to create an advanced Intrusion Detection System (IDS) capable of accurately distinguishing network traffic from Android devices as either ransomware or benign. This IDS must detect and respond to ransomware threats in real-time, thereby fortifying network security and safeguarding Android users against the severe consequences of ransomware attacks. To address this challenge, the paper aims to leverage machine learning techniques, specifically the CatBoostClassifier [42-49]. This approach is intended to develop a robust and efficient IDS tailored for detecting ransomware on Android devices. The paper aspires to contribute meaningfully to the cybersecurity landscape by creating such a system. It seeks to offer a proactive solution to effectively combat the rising ransomware threats targeting Android devices. This initiative aligns with the broader goal of enhancing cybersecurity and protecting users' digital assets from malicious attacks [50-55].

Literature Review

This survey paper investigates the potential of data-driven techniques for identifying malware threats in 6G networks, which represent the next generation of high-speed, connected infrastructure. By examining recent research trends in network-based

intrusion detection systems, the review emphasizes the role of data analysis in recognizing network vulnerabilities. The paper assesses the strengths of various detection approaches and highlights areas for improvement within current methodologies. Ultimately, this exploration contributes to the understanding of how emerging data-driven technologies can bolster the security framework of advanced 6G network architectures, offering a foundation for continued research in secure 6G environments [56].

A recent study explores the use of the Social Leopard Algorithm to create a specialized intrusion detection honeypot designed for identifying IoT ransomware attacks. By tailoring the honeypot to detect malicious activity within IoT devices, the research aims to reinforce cybersecurity within IoT environments [57]. This approach demonstrates how bio-inspired algorithms can enhance threat detection by mirroring natural predator-prey dynamics. This novel approach promises to improve response to IoT ransomware, a growing concern as IoT devices become more integrated into both personal and industrial settings, demanding stronger protective measures to maintain data integrity [58].

In another study, researchers implement transfer learning using the optimal ECOC-SVM configuration to achieve vision-based malware detection. This methodology leverages pre-existing knowledge within transfer learning to enhance detection accuracy for vision-based malware, where visual signatures indicate potential threats [59]. The study suggests that incorporating native instructions into this process could further boost efficiency, particularly in detecting mobile ransomware. By improving detection speed and accuracy, this approach provides a viable solution for the growing need to secure mobile devices against ransomware and similar malicious threats through advanced machine learning techniques [60].

An innovative neural network-based approach has been proposed to detect cryptographic functions within malware, addressing the complexity of modern encryption tactics used by malicious software. This methodology focuses on identifying specific encryption patterns, enabling the detection of concealed or sophisticated malware [61]. By refining the accuracy of malware classification, this research illustrates the potential of neural networks to evolve with the increasing complexity of cryptographic threats. The study's findings suggest that neural networks could play a key role in future malware detection frameworks by recognizing advanced encryption methods [62].

In the field of document security, a study has examined the detection of unknown malicious Microsoft Office documents through active learning methods that utilize structural feature extraction. This innovative approach seeks to improve the identification of potentially dangerous Office file formats by targeting specific structural markers indicative of malicious activity [63]. By employing active learning, the system adapts to new threats and unknown malware signatures, enhancing the protection of document-based workflows. The approach addresses a critical vulnerability and showcases the effectiveness of adapting structural feature analysis for heightened malware detection [64].

To combat botnet attacks in IoT environments, a hybrid machine learning model has been developed, offering a robust approach to detecting threats unique to interconnected devices. The model combines multiple machine learning techniques to address the multifaceted nature of botnet behavior [65]. By efficiently analyzing IoT network traffic, this hybrid model mitigates the impact of botnets, which can compromise security across numerous devices. The research highlights the importance of specialized machine learning strategies for IoT, where traditional methods may struggle with the dynamic and varied nature of connected devices [66].

This comprehensive review provides a detailed analysis of multiple malware detection methods, focusing on their advantages, limitations, and evolving trends in cybersecurity. By examining different approaches, the review offers valuable insights into

which techniques hold the most promise for future developments [67]. The review suggests that a balanced approach, incorporating strengths from various methods, may yield the most resilient defense against evolving malware threats. These insights contribute to a deeper understanding of malware detection strategies and inspire further research into innovative solutions for more secure digital ecosystems [68].

Paper description

The Extra Trees Classifier assumes the role of the primary algorithm for predictive modelling tasks. Operating within ensemble learning, this classifier, also called Extremely Randomised Trees, emerges as a pivotal member of the decision tree classifier family. Its modus operandi involves the creation of a multitude of decision trees during the training phase, culminating in determining the class that predominates amongst the individual tree predictions. One of the most notable characteristics of the Extra Trees Classifier lies in its penchant for randomness [69].

Unlike conventional decision trees that meticulously seek out the optimal split at each node based on predetermined criteria like Gini impurity or information gain, Extra Trees diverge by opting for a randomised approach to feature subset selection and split point determination. This deliberate randomness is a bulwark against variance and overfitting, rendering the model less susceptible to the harmful effects of noisy data and outliers [70]. Moreover, the computational efficiency of the Extra Trees Classifier is a testament to its prowess. Thanks to its innate parallelisation capabilities, the model can construct multiple trees concurrently and independently. This parallel processing prowess allows it to harness the computational might of multi-core processors and distributed computing environments, thereby delivering expedited training times compared to its ensemble counterparts [71].

However, despite its commendable attributes, the Extra Trees Classifier may exhibit suboptimal performance under certain circumstances, particularly when faced with intricate datasets characterised by high-dimensional feature spaces or skewed class distributions. More advanced algorithms like CatBoost may emerge as preferred alternatives in such scenarios, offering superior accuracy and resilience [72]. In summary, while the Extra Trees Classifier holds its ground as a dependable and interpretable baseline model for predictive analytics endeavours, its efficacy may be outshone by sophisticated techniques such as CatBoost, which leverages intricate algorithms and optimisation methodologies to attain heightened accuracy and predictive prowess [73].

The ExtraTrees Classifier may face limitations in effectively prioritizing critical features for ransomware detection, which can lead to suboptimal performance. Its ability to discern the most impactful features could be constrained, affecting the model's accuracy and reliability in identifying ransomware [74]. Additionally, the model is susceptible to overfitting, particularly when working with high-dimensional data. Overfitting can restrict its generalization capability, meaning it may perform well on training data but fail to maintain similar accuracy when tested on new, unseen data. This issue can hinder the classifier's effectiveness in real-world applications [75].

Another challenge lies in the model's scalability, particularly concerning its capacity to handle large volumes of network traffic data from Android devices. Limited scalability could reduce its ability to function in real-time, which is essential for prompt ransomware detection. Furthermore, the problem of data imbalance is common in ransomware detection, where benign samples often vastly outnumber ransomware samples. This imbalance can impede the model's learning process, causing it to favor benign predictions and potentially overlook ransomware instances [76].

Performance trade-offs also emerge as a critical consideration, especially when balancing metrics such as accuracy, precision, recall, and F1-score. Each metric offers unique insights into the model's efficacy, yet focusing too heavily on one may detract from another. Therefore, careful evaluation and balance of these metrics are essential, ensuring

the ransomware detection system meets specific operational requirements effectively [77-83].

2. Materials and Methods

This study aims to develop an Intrusion Detection System (IDS) for Android devices using the CatBoost Classifier to detect ransomware. The methodology includes data collection, pre-processing, feature selection, model training, and performance evaluation.

1. *Data Collection:* Network traffic data was collected from Android devices to serve as the input dataset. This data included benign and ransomware traffic patterns to train and test the model effectively.
2. *Data Pre-processing:* The raw data underwent cleaning to remove noise and inconsistencies, enhancing data quality for accurate model training. Missing values were handled through imputation, and outliers were addressed. Feature scaling and normalization ensured consistency across data points.
3. *Feature Selection:* Key features that signify ransomware activity were selected from the dataset. This step is crucial to improve model efficiency by focusing on indicators of ransomware behavior.
4. *Model Selection and Training:* The CatBoost Classifier was chosen due to its efficiency in handling categorical data and managing imbalanced datasets. The model was trained on the pre-processed data, using cross-validation to optimize hyperparameters and prevent overfitting. The model training process involved iterating on parameters to maximize the model's ransomware detection accuracy.
5. *Performance Evaluation:* The trained model was evaluated using metrics such as accuracy, precision, recall, F1-score, and specificity. Additionally, the Receiver Operating Characteristic (ROC) curve was used to analyze the model's performance comprehensively. The model achieved a high accuracy rate, with scores in metrics such as precision, recall, and F1-score, affirming its robustness.
6. *Deployment and Real-time Testing:* The model was deployed in a simulated environment for real-time testing. This environment allowed for continuous network monitoring, where the model classified incoming network traffic as either benign or ransomware.

3. Results and Discussion

The proposed methodology commences with precisely defining the problem statement and objectives, ensuring harmony with paper goals and stakeholders' expectations. Data pre-processing emerges as a pivotal facet, encompassing a spectrum of techniques to ensure dataset quality and suitability for modelling. This encompasses addressing missing values via imputation or deletion, identifying and remedying outliers that may distort model performance, and standardising or normalising features for uniformity and comparability across diverse scales.

Furthermore, techniques such as data transformation, like log transformations or feature scaling, are wielded to refine feature distributions and bolster model interpretability. After meticulous data pre-processing, the methodology unfolds with a robust data collection strategy to procure pertinent datasets for analysis and model development [84-89]. This involves delineating suitable data sources, procuring the data, and executing preliminary pre-processing steps to rectify missing values, outliers, and data inconsistencies. Additionally, exploratory data analysis (EDA) techniques may be leveraged to glean insights into the dataset's attributes and underlying trends. Following data pre-processing, feature engineering takes centre stage, wherein meaningful features are crafted or chosen to amplify the model's predictive prowess [90].

Drawing upon domain expertise, this step may entail techniques like dimensionality reduction, categorical variable encoding, and novel feature creation grounded in domain-specific insights. Armed with the prepared dataset, the subsequent phase entails selecting

an apt machine learning algorithm or ensemble tailored to the specific problem domain [91-92]. Model selection factors include dataset size, complexity, and desired performance metrics. The chosen algorithm is then trained on the pre-processed data, employing techniques like cross-validation to fine-tune hyperparameters and curb overfitting. Finally, the trained model undergoes evaluation using appropriate performance metrics, with its resilience and generalisation capabilities scrutinised via rigorous testing on unseen data. The proposed methodology underscores a systematic and iterative approach, wherein insights from each phase inform subsequent decisions, culminating in development of effective and dependable predictive models aligned with the paper's objectives.

Implementing the intrusion detection system (IDS) for Android devices using machine learning involves several essential steps. First, data collection is necessary to gather network traffic data from Android devices, which will serve as input for training the machine learning model. After collection, the data undergoes pre-processing to clean and remove any noise or inconsistencies, ensuring high-quality data for model training. The next step is feature selection, where the most relevant features that indicate ransomware activity are chosen from the pre-processed data. This step enhances the model's efficiency and effectiveness. Following this, model selection is critical, with the CatBoostClassifier being a suitable option for this task, given its ability to handle categorical features and effectively address data imbalance issues common in security datasets. After selecting the model, model training takes place, feeding the pre-processed data into the model and adjusting parameters to optimize performance. Once trained, model evaluation is conducted using performance metrics like accuracy, precision, recall, and F1-score to assess the model's capability in detecting ransomware effectively.

The trained model is then deployed to Android devices for real-time detection. Integrated into the device's security framework, the model continuously monitors network traffic, identifying potential ransomware threats. Finally, testing and validation in a real-world setting confirms the IDS's reliability and effectiveness, ensuring it provides consistent protection against ransomware on Android devices. The dataset is used to train the proposed CatBoost Classifier model. The model is tested dataset and validated. The proposed model detects and classifies ransomware using the paper provided. The model is evaluated using Accuracy, Average Precision, Average Recall, Average F1 score, Specificity, and Error rate. The model is also evaluated using the ROC Curve. The parameter values are Accuracy 97.79%, Average Precision 97.49%, Average Recall 97.68% and Average F1-score 97.57. A Learning Curve is used to show a comparison between training accuracy and validation accuracy.

Table 1, Catboost-Extra Tree Classifier Classification Report

Model	Metrics			
	Accuracy	Average Precision	Average Recall	Average F1-score
ExtraTrees Classifier	92.32 %	92.53%	91.79%	92.05%
CatBoost Classifier	97.66	97.35%	97.41%	97.42%

Table 1 illustrates the difference in metrics for the ExtraTrees Classifier and the CatBoost Classifier. The same dataset was trained, but there is a difference between the metrics, which clearly shows that the CatBoost Classifier is best suited and makes accurate predictions for the loaded dataset.

4. Conclusion

In conclusion, the research proposes utilizing machine learning to categorize Android device network traffic as ransomware or benign. The paper uses the CatBoost

Classifier, which excels in categorical network traffic data characteristics. Collection and pre-processing network monitoring records and model training allow the IDS to detect and respond to cyber attacks in real time. The CatBoost Classifier classifies network traffic well, separating ransomware from benign activity. Cybersecurity applications benefit from its capacity to manage unbalanced data and produce interpretable results. The study emphasizes machine learning's role in network security and cyberdefense. The proposed IDS can boost cybersecurity and protect against ransomware attacks in manufacturing sites and other environments. Monitoring and maintaining the model will guarantee it detects new threats and secures networks. The intrusion detection system (IDS) for identifying Android device network traffic as ransomware or benign could be improved in the future. The CatBoost Classifier works, but other algorithms, such as CNNs or RNNs, might be tested. Future IDS improvements could focus on sophisticated machine learning, adding features, optimizing pre-processing pipelines, and improving deployment methodologies. These improvements may help the IDS detect and respond to Android ransomware threats.

REFERENCES

1. I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization,” International Journal of Computer Applications, vol. 80, no. 13, pp. 18–23, 2013.
2. I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization for Kidney Transplantation,” International Journal of Computer Applications, vol. 92, no. 6, pp. 25–29, 2014.
3. M. M. Abbassy and A. Abo-Alnadr, “Rule-based emotion AI in Arabic Customer Review,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 9, p.12, 2019.
4. M. M. Abbassy and W. M. Ead, “Intelligent Greenhouse Management System,” 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020.
5. M. M. Abbassy, “Opinion mining for Arabic customer feedback using machine learning,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP3, pp. 209–217, 2020.
6. H. AbdulKader, E. ElAbd, and W. Ead, "Protecting Online Social Networks Profiles by Hiding Sensitive Data Attributes," Procedia Computer Science, vol. 82, pp. 20–27, 2016.
7. I. E. Fattoh, F. Kamal Alsheref, W. M. Ead, and A. M. Youssef, "Semantic Sentiment Classification for COVID-19 Tweets Using Universal Sentence Encoder," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–8, 2022.
8. W. M. Ead, W. F. Abdel-Wahed, and H. Abdul-Kader, "Adaptive Fuzzy Classification-Rule Algorithm in Detection Malicious Web Sites from Suspicious URLs," International Arab Journal of e-Technology, vol. 3, pp. 1–9, 2013.
9. M. A. Abdelazim, M. M. Nasr, and W. M. Ead, "A Survey on Classification Analysis for Cancer Genomics: Limitations and Novel Opportunity in the Era of Cancer Classification and Target Therapies," Annals of Tropical Medicine and Public Health, vol. 23, no. 24, 2020.
10. F. K. Alsheref, I. E. Fattoh, and W. M. Ead, "Automated Prediction of Employee Attrition Using Ensemble Model Based on Machine Learning Algorithms," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–9, 2022.
11. M. M. Abbassy, “The human brain signal detection of Health Information System IN EDSAC: A novel cipher text attribute based encryption with EDSAC distributed storage access control,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP7, pp. 858–868, 2020.
12. M. M. and S. Mesbah, “Effective e-government and citizens adoption in Egypt,” International Journal of Computer Applications, vol. 133, no. 7, pp. 7–13, 2016.
13. M.M.Abbassy, A.A. Mohamed “Mobile Expert System to Detect Liver Disease Kind”, International Journal of Computer Applications, vol. 14, no. 5, pp. 320–324, 2016.
14. R. A. Sadek, D. M. Abd-alazeem, and M. M. Abbassy, “A new energy-efficient multi-hop routing protocol for heterogeneous wireless sensor networks,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 11, 2021.
15. S. Derindere Köseoğlu, W. M. Ead, and M. M. Abbassy, “Basics of Financial Data Analytics,” Financial Data Analytics, pp. 23–57, 2022.

16. W. Ead and M. Abbassy, “Intelligent Systems of Machine Learning Approaches for developing E-services portals,” EAI Endorsed Transactions on Energy Web, p. 167292, 2018.
17. W. M. Ead and M. M. Abbassy, “A general cyber hygiene approach for financial analytical environment,” Financial Data Analytics, pp. 369–384, 2022.
18. R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, “Malware detection on highly imbalanced data through sequence modeling,” in Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security - AISec’19, 2019.
19. J. Cruz Ángeles, The legal-community obligations of the large digital service provider platforms in the metaverse era, Cuad. transnational law , vol. 14, no. 2, p. 294-318, 2022.
20. J. Cruz Ángeles, The guardians of access to the metaverse. (Re)thinking the Competition Law of the European Union, Cuad. transnational law , vol. 15, no. 1, p. 275-296, 2023.
21. W. M. Ead and M. M. Abbassy, “IoT based on plant diseases detection and classification,” 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
22. W. M. Ead, M. M. Abbassy, and E. El-Abd, “A general framework information loss of utility-based anonymization in Data Publishing,” Turkish Journal of Computer and Mathematics Education, vol. 12, no. 5, pp. 1450–1456, 2021.
23. A. M. El-Kady, M. M. Abbassy, H. H. Ali, and M. F. Ali, “Advancing Diabetic Foot Ulcer Detection Based On Resnet And Gan Integration,” Journal of Theoretical and Applied Information Technology, vol. 102, no. 6, pp. 2258–2268, 2024.
24. M. M. Abbassy and W. M. Ead, “Fog computing-based public e-service application in service-oriented architecture,” International Journal of Cloud Computing, vol. 12, no. 2–4, pp. 163–177, 2023.
25. E. Vashishtha and H. Kapoor, "Enhancing patient experience by automating and transforming free text into actionable consumer insights: a natural language processing (NLP) approach," International Journal of Health Sciences and Research, vol. 13, no. 10, pp. 275-288, Oct. 2023.
26. K. Shukla, E. Vashishtha, M. Sandhu, and R. Choubey, "Natural Language Processing: Unlocking the Power of Text and Speech Data," Xoffencer International Book Publication House, 2023, p. 251.
27. B. Naeem, B. Senapati, M. S. Islam Sudman, K. Bashir, and A. E. M. Ahmed, "Intelligent road management system for autonomous, non-autonomous, and VIP vehicles," World Electric Veh. J., vol. 14, no. 9, 2023.
28. M. Soomro et al., "Constructor development: Predicting object communication errors," in 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), 2023.
29. M. Soomro et al., "In MANET: An improved hybrid routing approach for disaster management," in 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology, 2023.
30. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Lecture Notes in Computer Science, Singapore: Springer Nature Singapore, 2023, pp. 22–39.
31. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Big Data Intelligence and Computing. DataCom 2022, Lecture Notes in Computer Science, vol. 13864, C. H. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds., Singapore: Springer, 2023, pp. 22–39.
32. D. K. Sharma and R. Tripathi, “4 Intuitionistic fuzzy trigonometric distance and similarity measure and their properties,” in Soft Computing, De Gruyter, 2020, pp. 53–66.
33. D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. Kalyan Chakravarthi, “Applications of two separate methods to deal with a small dataset and a high risk of generalization,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
34. D. K. Sharma, B. Singh, M. Anam, K. O. Villalba-Condori, A. K. Gupta, and G. K. Ali, “Slotting learning rate in deep neural networks to build stronger models,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
35. K. Kaliyaperumal, A. Rahim, D. K. Sharma, R. Regin, S. Vashisht, and K. Phasinam, “Rainfall prediction using deep mining strategy for detection,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
36. I. Nallathambi, R. Ramar, D. A. Pustokhin, I. V. Pustokhina, D. K. Sharma, and S. Sengan, “Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach,” Environ. Pollut., vol. 304, no. 119182, p. 119182, 2022.

37. H. Sharma and D. K. Sharma, "A Study of Trend Growth Rate of Confirmed Cases, Death Cases and Recovery Cases of Covid-19 in Union Territories of India," Turkish Journal of Computer and Mathematics Education, vol. 13, no. 2, pp. 569–582, 2022.
38. A. L. Karn et al., "Designing a Deep Learning-based financial decision support system for fintech to support corporate customer's credit extension," Malays. J. Comput. Sci., pp. 116–131, 2022.
39. A. L. Karn et al., "B-lstm-Nb based composite sequence Learning model for detecting fraudulent financial activities," Malays. J. Comput. Sci., pp. 30–49, 2022.
40. P. P. Dwivedi and D. K. Sharma, "Application of Shannon entropy and CoCoSo methods in selection of the most appropriate engineering sustainability components," Cleaner Materials, vol. 5, no. 100118, p. 100118, 2022.
41. A. Kumar, S. Singh, K. Srivastava, A. Sharma, and D. K. Sharma, "Performance and stability enhancement of mixed dimensional bilayer inverted perovskite (BA2PbI4/MAPbI3) solar cell using drift-diffusion model," Sustain. Chem. Pharm., vol. 29, no. 100807, p. 100807, 2022.
42. A. Kumar, S. Singh, M. K. A. Mohammed, and D. K. Sharma, "Accelerated innovation in developing high-performance metal halide perovskite solar cell using machine learning," Int. J. Mod. Phys. B, vol. 37, no. 07, 2023.
43. G. A. Ogunmola, M. E. Lourens, A. Chaudhary, V. Tripathi, F. Effendy, and D. K. Sharma, "A holistic and state of the art of understanding the linkages of smart-city healthcare technologies," in 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 2022.
44. P. Sindhuja, A. Kousalya, N. R. R. Paul, B. Pant, P. Kumar, and D. K. Sharma, "A Novel Technique for Ensembled Learning based on Convolution Neural Network," in 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, 2022, pp. 1087–1091.
45. A. R. B. M. Saleh, S. Venkatasubramanian, N. R. R. Paul, F. I. Maulana, F. Effendy, and D. K. Sharma, "Real-time monitoring system in IoT for achieving sustainability in the agricultural field," in 2022 International Conference on Edge Computing and Applications (ICECAA), 2022.
46. Srinivasa, D. Baliga, N. Devi, D. Verma, P. P. Selvam, and D. K. Sharma, "Identifying lung nodules on MRR connected feature streams for tumor segmentation," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), 2022.
47. C. Goswami, A. Das, K. I. Ogaili, V. K. Verma, V. Singh, and D. K. Sharma, "Device to device communication in 5G network using device-centric resource allocation algorithm," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), 2022.
48. M. Yuvarasu, A. Balaram, S. Chandramohan, and D. K. Sharma, "A Performance Analysis of an Enhanced Graded Precision Localization Algorithm for Wireless Sensor Networks," Cybernetics and Systems, pp. 1–16, 2023.
49. P. P. Dwivedi and D. K. Sharma, "Evaluation and ranking of battery electric vehicles by Shannon's entropy and TOPSIS methods," Math. Comput. Simul., vol. 212, pp. 457–474, 2023.
50. P. P. Dwivedi and D. K. Sharma, "Assessment of Appropriate Renewable Energy Resources for India using Entropy and WASPAS Techniques," Renewable Energy Research and Applications, vol. 5, no. 1, pp. 51–61, 2024.
51. P. P. Dwivedi and D. K. Sharma, "Selection of combat aircraft by using Shannon entropy and VIKOR method," Def. Sci. J., vol. 73, no. 4, pp. 411–419, 2023.
52. B. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Lecture Notes in Computer Science, Singapore: Springer Nature Singapore, 2023, pp. 22–39.
53. B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 1, no. 100019, p. 100019, 2023.
54. B. Senapati et al., "Wrist crack classification using deep learning and X-ray imaging," in Proceedings of the Second International Conference on Advances in Computing Research (ACR'24), Cham: Springer Nature Switzerland, 2024, pp. 60–69.
55. A. B. Naeem et al., "Heart disease detection using feature extraction and artificial neural networks: A sensor-based approach," IEEE Access, vol. 12, pp. 37349–37362, 2024.
56. R. Tsarev et al., "Automatic generation of an algebraic expression for a Boolean function in the basis ∧, ∨, ¬," in Data Analytics in System Engineering, Cham: Springer International Publishing, 2024, pp. 128–136.

57. R. Tsarev, B. Senapati, S. H. Alshahrani, A. Mirzagitova, S. Irgasheva, and J. Ascencio, “Evaluating the effectiveness of flipped classrooms using linear regression,” in Data Analytics in System Engineering, Cham: Springer International Publishing, 2024, pp. 418–427.
58. M. Sabugaa, B. Senapati, Y. Kupriyanov, Y. Danilova, S. Irgasheva, and E. Potekhina, "Evaluation of the prognostic significance and accuracy of screening tests for alcohol dependence based on the results of building a multilayer perceptron," in Artificial Intelligence Application in Networks and Systems. CSOC 2023, Lecture Notes in Networks and Systems, vol. 724, R. Silhavy and P. Silhavy, Eds., Cham: Springer, 2023, pp. 373–384.
59. P. P. Anand, U. K. Kanike, P. Paramasivan, S. S. Rajest, R. Regin, and S. S. Priscila, “Embracing Industry 5.0: Pioneering Next-Generation Technology for a Flourishing Human Experience and Societal Advancement,” FMDB Transactions on Sustainable Social Sciences Letters, vol.1, no. 1, pp. 43–55, 2023.
60. G. Gnanaguru, S. S. Priscila, M. Sakthivanitha, S. Radhakrishnan, S. S. Rajest, and S. Singh, “Thorough analysis of deep learning methods for diagnosis of COVID-19 CT images,” in Advances in Medical Technologies and Clinical Practice, IGI Global, pp. 46–65, 2024.
61. G. Gowthami and S. S. Priscila, “Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach,” Int. J. Crit. Comput.-based Syst., vol. 10, no. 4, pp. 355–374, 2023.
62. A. J. Obaid, S. Suman Rajest, S. Silvia Priscila, T. Shynu, and S. A. Ettyem, “Dense convolution neural network for lung cancer classification and staging of the diseases using NSCLC images,” in Proceedings of Data Analytics and Management, Singapore; Singapore: Springer Nature, pp. 361–372, 2023.
63. S. S. Priscila and A. Jayanthiladevi, “A study on different hybrid deep learning approaches to forecast air pollution concentration of particulate matter,” in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023.
64. S. S. Priscila, S. S. Rajest, R. Regin, and T. Shynu, “Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm,” Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.
65. S. S. Priscila and S. S. Rajest, “An Improvised Virtual Queue Algorithm to Manipulate the Congestion in High-Speed Network”,” Central Asian Journal of Medical and Natural Science, vol. 3, no. 6, pp. 343–360, 2022.
66. S. S. Priscila, S. S. Rajest, S. N. Tadiboina, R. Regin, and S. András, “Analysis of Machine Learning and Deep Learning Methods for Superstore Sales Prediction,” FMDB Transactions on Sustainable Computer Letters, vol. 1, no. 1, pp. 1–11, 2023.
67. R. Regin, Shynu, S. R. George, M. Bhattacharya, D. Datta, and S. S. Priscila, “Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting,” Int. J. Bioinform. Res. Appl., vol. 19, no. 3, 2023.
68. S. Silvia Priscila, S. Rajest, R. Regin, T. Shynu, and R. Steffi, “Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm,” Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.
69. S. S. Rajest, S. Silvia Priscila, R. Regin, T. Shynu, and R. Steffi, “Application of Machine Learning to the Process of Crop Selection Based on Land Dataset,” International Journal on Orange Technologies, vol. 5, no. 6, pp. 91–112, 2023.
70. T. Shynu, A. J. Singh, B. Rajest, S. S. Regin, and R. Priscila, “Sustainable intelligent outbreak with self-directed learning system and feature extraction approach in technology,” International Journal of Intelligent Engineering Informatics, vol. 10, no. 6, pp.484-503, 2022.
71. S. S. Priscila, D. Celin Pappa, M. S. Banu, E. S. Soji, A. T. A. Christus, and V. S. Kumar, “Technological frontier on hybrid deep learning paradigm for global air quality intelligence,” in Cross-Industry AI Applications, IGI Global, pp. 144–162, 2024.
72. S. S. Priscila, E. S. Soji, N. Hossó, P. Paramasivan, and S. Suman Rajest, “Digital Realms and Mental Health: Examining the Influence of Online Learning Systems on Students,” FMDB Transactions on Sustainable Techno Learning, vol. 1, no. 3, pp. 156–164, 2023.
73. S. R. S. Steffi, R. Rajest, T. Shynu, and S. S. Priscila, “Analysis of an Interview Based on Emotion Detection Using Convolutional Neural Networks,” Central Asian Journal of Theoretical and Applied Science, vol. 4, no. 6, pp. 78–102, 2023.

74. S. G. A. Hasan, G. A. V. S. S. K. S., B. V. Reddi, and G. S. Reddy, "A critical review on preparation of Fe3O4 magnetic nanoparticles and their potential application," International Journal of Current Engineering and Technology, vol. 8,no.6, pp. 1613-1618, 2018.
75. S.G.A. Hasan and M.D.A. Rasool, "Preparation and Study of Magnetic Nanoparticles (Fe2O3 and Fe3O4) by Arc-Discharge Technique" ," IJSRSET, vol. 3, no. 2, pp. 730-732, 2017.
76. S.G.A. Hasan, A. Gupta, and B.V. Reddi, "Effect of Voltage on the Size of Magnetic Nanoparticles Synthesized Using Arc-Discharge Method," Innovations in Mechanical Engineering: Select Proceedings of ICIME 2021, pp. 339-346, 2022.
77. S.G.A. Hasan, A. Gupta, and B.V. Reddi, "Influence of Electrolyte on the Size of Magnetic Iron Oxide Nanoparticles Produced Using Arc-Discharge Technique," International Journal of Mechanical Engineering , vol. 7, no. 1, pp. 326-335, 2022.
78. S.G.A. Hasan, A. Gupta, and B.V. Reddi, "The Effect of Heat Treatment on Phase changes in Magnetite (Fe3O4) and Hematite (Fe2O3) nanoparticles Synthesized by Arc-Discharge method," Advanced Engineering Sciences, vol. 46, no. 1, pp. 49-57, 2021.
79. S.G.A. Hasan, A.V. Gupta, and B.V. Reddi, "Estimation of size and lattice parameter of magnetic nanoparticles based on XRD synthesized using arc-discharge technique," Materials Today: Proceedings, vol. 47, pp. 4137-4141, 2021.
80. S.G.A. Hasan, A.V. Gupta, and B.V. Reddi, "Synthesis and characterization of magnetic Nano crystallites using ARC-discharge method," Solid State Technology, vol. 63, no. 5, pp. 578-587, 2020.
81. S.G.A. Hasan, G. A.V.S.S.K.S., and B.V. Reddi, "Comparison of ER70S-2 with ER309L in synthesis of magnetic nanoparticles using arc-discharge method," Int. J. Curr. Eng. Technol, vol. 11,no.1, pp. 22-25, 2021.
82. S.G.A. Hasan, A. Gupta, and B.V. Reddi, "Investigation on the Morphological size and physical parameters of magnetic nanoparticles synthesized using arc-Discharge method" Advanced Engineering Sciences, vol. 46, no. 1, pp. 58-65, 2021.
83. S.G.A. Hasan, G.S. Kumar, and S.S. Fatima, "Finite Element Analysis and Fatigue Analysis of Spur Gear Under Random Loading," International Journal of Engineering Sciences & Research Technology, vol. 4, no. 7, pp. 523-534, 2015.
84. S.G.A. Hasan, S.M. Amoodi, and G.S. Kumar, "Starring of Hydrogen as a Compression Ignition Engine Fuel: A Review," International Journal of Engineering and Management Research (IJEMR), vol. 5, no. 3, pp.738-743, 2015.
85. S.G.A. Hasan, S.M. Amoodi, and G.S. Kumar, "Under Floor Air Distribution for Better Indoor Air Quality," International Journal of Engineering and Management Research (IJEMR), vol. 5, no. 3, pp.744-755, 2015.
86. S.G.A. Hasan, S.S. Fatima, and G.S. Kumar, "Design of a VRF Air Conditioning System with Energy Conservation on Commercial Building," International Journal of Engineering Sciences & Research Technology, vol. 4, no. 7, pp. 535-549, 2015.
87. S.M. Amoodi, G.S. Kumar, and S.G.A. Hasan, "Design of II Stage Evaporative Cooling System for Residential," International Journal of Engineering and Management Research (IJEMR), vol. 5, no. 3, pp. 810-815, 2015.
88. T. Wahidi, S.A.P. Quadri, S.G.A. Hasan, M.G. Sundkey, and P.R. Kumar, "Experimental investigation on performance, emission and combustion analysis of CNG-Diesel enrichment with varying injection operating pressures," IOSR Journal of Mechanical And Civil Engineering, vol. 12,no.2, pp. 23-29, 2015.
89. K.S. Goud, K.U. Reddy, P.B. Kumar, and S.G.A. Hasan, "Magnetic Iron Oxide Nanoparticles: Various Preparation Methods and Properties," ," IJSRSET, vol. 3, no. 2, pp. 535-538, 2017.
90. M.S. Reddy, R. Kumaraswami, B.K. Reddy, B.A. Sai, and S.G.A. Hasan, "Extraction of Water from Ambient Air by Using Thermoelectric Modules," IJSRSET, vol. 3, no. 2, pp. 733-737, 2017.
91. P.C. Kumar, S. Ramakrishna, S.G.A. Hasan, and C. Rakesh, "Find the Performance of Dual Fuel Engine Followed by Waste Cooking Oil Blends with Acetylene," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 2, pp. 127-131, 2019.
92. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 100019, 2023.