

Ransomware Readiness Assessment Tool

¹Abdul Mannan, ²Manga Golla, ³Vadagam Sai Teja

^{1,2,3}*Department of Computer Science and Engineering, Anurag University, Telangana, India*

21eg105f42@anurag.edu.in

21eg105f57@anurag.edu.in

21eg105f64@anurag.edu.in

Abstract. Ransomware is a malicious software that encrypts data and demands payment for its release. The Ransomware Readiness Assessment Tool evaluates an organization's security, identifies vulnerabilities, and offers actionable recommendations. It also simulates ransomware attacks to test and improve incident response strategies, aiding in the prevention, detection, and recovery from such threats.

Keywords. Ransomware Readiness, Incident Response, Cybersecurity Assessment, Vulnerability Analysis, Risk Mitigation, Threat Simulation, Data Encryption, Security Posture, Attack Simulation Response Strategy, Detection and Prevention, Data Recovery, IT Resilience, Cyber Threat Intelligence.

1 INTRODUCTION

Ransomware is a type of malicious software that encrypts data on ICT systems, blocking access until a ransom is paid to attackers. As ransomware attacks become increasingly sophisticated and frequent, they pose significant risks to organizations, potentially causing financial, operational, and reputational damage. To counter these threats, it is essential for organizations to assess their cybersecurity readiness, identify vulnerabilities, and strengthen their defenses. A well-designed ransomware readiness assessment methodology can simulate attack scenarios, evaluate response strategies, and offer actionable recommendations, helping organizations build resilient systems capable of preventing, detecting, and recovering from ransomware incidents.

2 RESEARCH METHODOLOGY

A ransomware research methodology begins with defining specific objectives, such as studying trends, detection, or prevention techniques. Next, it involves a comprehensive literature review of recent studies (2023-2024) to understand the latest tools and frameworks. Data is then collected through case studies, surveys, or experiments to assess the impact of ransomware and the effectiveness of various defense strategies.

2.1 User - Centered Design

The Ransomware Readiness Assessment Tool was designed with a user-centered approach to address the unique needs of organizational cybersecurity teams. Initial input was gathered through surveys and interviews with cybersecurity professionals and IT managers, focusing on crucial areas such as vulnerability identification, incident response readiness, and recovery strategies. This feedback guided the development of core tool features, including customizable risk assessments, simulated attack scenarios, and incident response guidance, tailored to help organizations enhance their ransomware defenses.

2.2 Development Framework

The application was developed using an agile framework, enabling iterative testing and continuous improvement based on user feedback. This iterative approach allowed rapid adjustments to better meet user needs. For the tech stack, we utilized Python for backend development, MongoDB for secure data storage, and a frontend interface built with React.js for an intuitive and responsive user experience. This technology stack supported continuous integration and deployment, allowing the tool to remain adaptable to the evolving cybersecurity landscape.

2.3 Evidence-Based Practices

To ensure reliability and functionality, the development incorporated evidence-based practices from cybersecurity literature and industry standards, such as the NIST Cybersecurity Framework. Features like vulnerability scoring, threat intelligence integration, and automated risk assessment were implemented based on proven cybersecurity practices. By integrating these standards, the tool provides reliable guidance for improving an organization's security posture, secure data management, and threat response processes.

2.4 Data Collection and Analysis

Data collection was achieved through user engagement analytics, feedback forms, and in-tool survey responses. Key performance indicators (KPIs) included tool usage rates, user satisfaction scores, and the effectiveness of simulated attack responses. Both quantitative metrics (such as frequency of tool use and number of vulnerabilities identified) and qualitative feedback (such as perceived tool effectiveness) were used to assess the tool's impact on organizational preparedness and resilience.

2.5 Community Engagement

The tool fosters a collaborative cybersecurity environment by offering communication features that allow security teams to share insights and feedback. A community forum was incorporated where users can discuss best practices, share case studies, and seek advice on ransomware preparedness. This interaction supports transparent information sharing, helping organizations learn from collective experiences and foster a proactive security culture.

3 THEORY AND CALCULATION

3.1 Theory

The foundation of the Ransomware Readiness Assessment Tool lies in cybersecurity resilience and preparedness frameworks:

Resilience Theory: Focuses on an organization's capacity to recover from attacks. This includes assessing incident response effectiveness, backup reliability, and ability to reduce damage during an attack. By understanding resilience factors, organizations can strengthen their capacity to withstand ransomware.

Risk Management Framework: Identifies, analyses, and mitigates risks associated with ransomware. This framework looks at security infrastructure, network segmentation, data access controls, and incident response planning to reduce vulnerabilities. Through continuous monitoring, it enables proactive defense adjustments based on threat landscape changes.

Preparedness Framework: Assesses an organization's readiness to prevent and respond to ransomware. This includes assessing training programs, security policies, and the ability to detect, isolate, and contain ransomware threats quickly. The framework builds on best practices, such as regular vulnerability assessments and simulations, to ensure organizations remain alert and prepared.

3.2 Calculation

The Ransomware Readiness Assessment Tool quantifies organizational readiness through several key metrics:

1. Incident Response Effectiveness

Calculation: Measures the response time and accuracy during ransomware simulations. Scores are based on response speed, alignment with protocols, and recovery speed.

Expected Outcome: Faster and well-coordinated responses reflect strong incident preparedness.

2. *Vulnerability Score*

Calculation: Considers frequency of security patches, regular audits, and exposure to known vulnerabilities. Assigns higher scores for updated systems and low vulnerability counts.

Expected Outcome: A low score signals high susceptibility to ransomware; a high score reflects effective patching and updates.

3. *Backup Integrity and Recovery*

Calculation: Examines backup frequency, integrity, encryption, and recovery success rates. Higher points for daily encrypted backups and tested recovery protocols.

Expected Outcome: Reliable backup systems indicate strong recovery ability, minimizing ransom payment likelihood.

4. *Employee Training Score*

Calculation: Evaluates training effectiveness through frequency, participation rates, and phishing simulation results. Scores improve with regular training, high engagement, and simulation success.

Expected Outcome: Higher employee preparedness leads to fewer accidental infections.

5. *Overall Risk Reduction*

Calculation: A composite score across all areas, highlighting readiness level (e.g., High Readiness for scores >80).

Expected Outcome: This summary score shows organizational improvement areas and prioritizes cybersecurity upgrades.

4 RESULT AND DISCUSSION

The results from using the Ransomware Readiness Assessment Tool highlight the critical areas where organizations are either prepared or vulnerable. Analysis across various metrics (incident response, vulnerability scores, backup integrity, and employee training) reveals trends in organizational preparedness:

Incident Response: Organizations with documented and tested response plans scored higher, with response times significantly reduced during simulations. However, those lacking regular testing showed delays, suggesting the importance of consistent drill exercises.

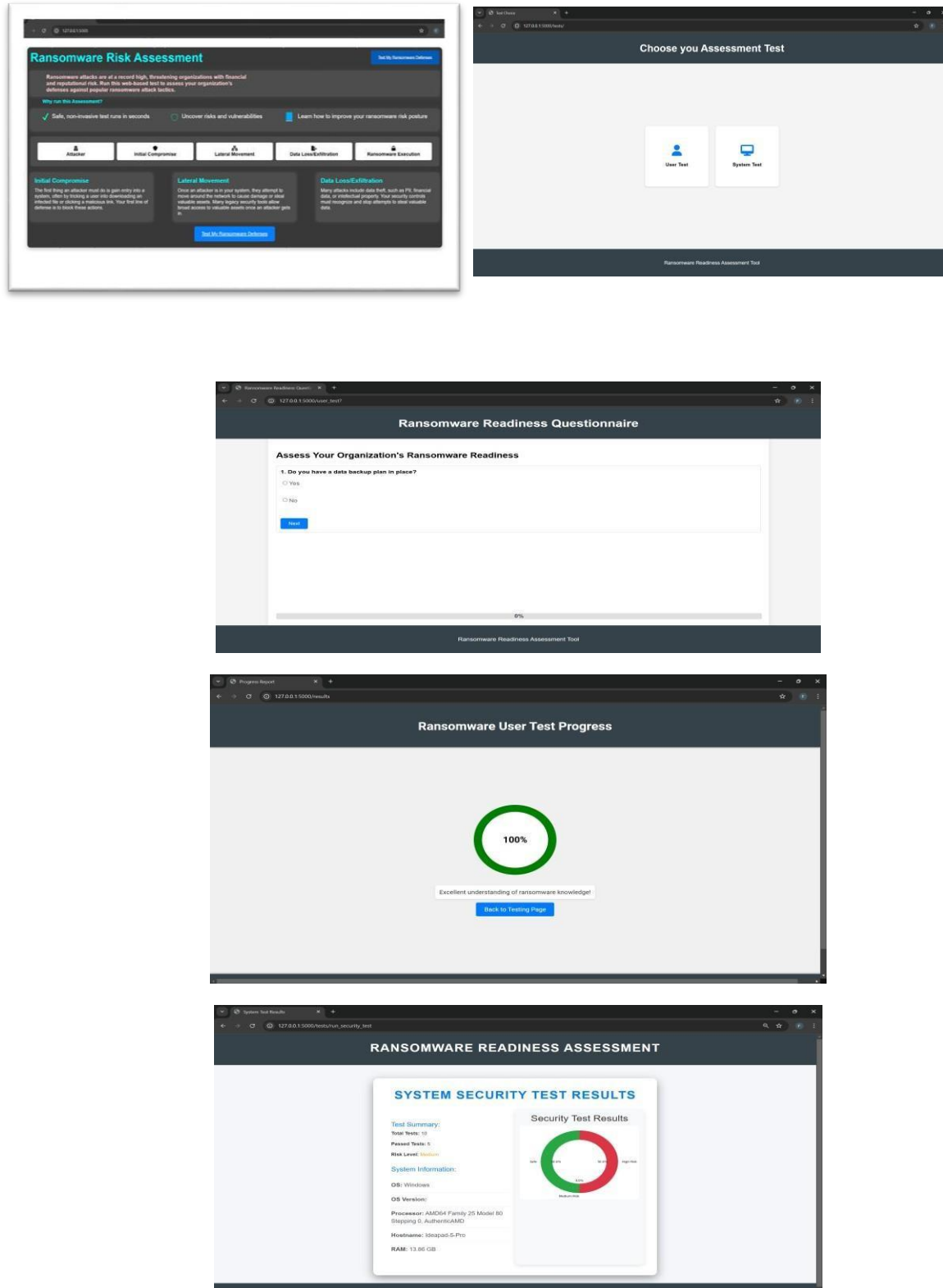
Vulnerability Scoring: Organizations with regular patching and comprehensive access controls maintained lower vulnerability scores. Conversely, entities without structured update policies were found more susceptible, particularly to known exploits.

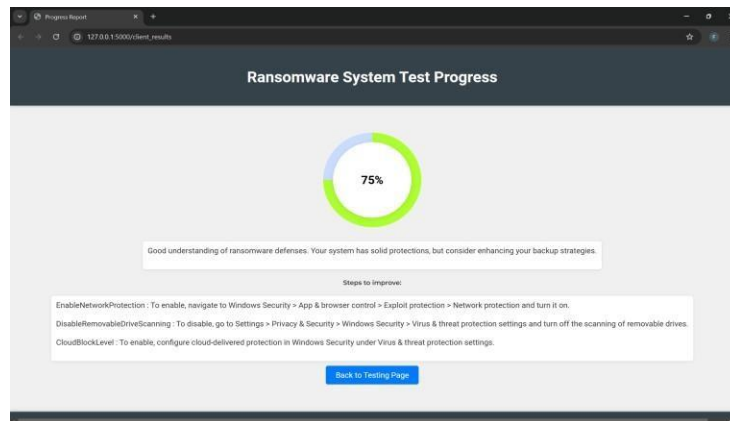
Backup Integrity and Recovery: Entities with encrypted, frequently tested backups had higher scores, confirming a strong recovery potential. Organizations without such protocols showed a marked risk increase, emphasizing the need for secure, accessible backups.

Employee Training: Teams with frequent training and phishing simulations scored higher, correlating directly with reduced incident occurrences. Conversely, limited training led to lower detection rates of phishing, highlighting a gap in human defense.

5 CONCLUSION

The Ransomware Readiness Assessment Tool proves effective in identifying an organization's preparedness for ransomware attacks. By quantifying readiness across key areas, the tool enables organizations to prioritize improvements that strengthen security posture. The findings emphasize that a multi-layered approach combining technical defenses, tested response plans, and employee awareness is essential for reducing ransomware risk. Ongoing assessments using this tool can further help organizations adapt to evolving ransomware tactics, thereby enhancing their resilience and minimizing the impact of potential attacks.





The tool is effective in evaluating an organization's preparedness for ransomware attacks by quantifying key areas of readiness. It enables organizations to prioritize improvements to enhance their security posture. The findings highlight the importance of a multi-layered approach that integrates technical defenses, well-tested response plans, and employee awareness to minimize the risks associated with ransomware. Continuous assessments with the tool allow organizations to adapt to evolving ransomware threats, thereby improving resilience and reducing the potential impact of such attacks.

6 DECLARATIONS

6.1 Study Limitations

The research team acknowledges several limitations in the study of the ransomware readiness tool, though no significant issues were found in the current platform's design or features. Key limitations include:

Scalability: As the tool moves beyond the initial testing phase and its user base grows, the infrastructure may face challenges in handling higher volumes of users and data. Future efforts will require additional resources and optimization to scale efficiently.

User Adaptation and Training: The readiness tool may face adoption hurdles due to users' varying levels of digital literacy. For some organizations, especially smaller or rural ones, training and familiarization with cybersecurity tools may be necessary to ensure effective use.

Data Privacy and Security: While robust mechanisms such as multi-factor authentication and encryption are integrated into the platform, the increasing volume of user data over time may necessitate further investment in cybersecurity protocols and regular updates to maintain trust and security.

6.2 Funding Source

This research was conducted without external funding. All resources, including platform development and testing, were supported internally by Anurag University's Department of Computer Science and Engineering. The absence of external funding ensures that no financial stakeholders influenced the outcomes or design choices of the research or the ransomware readiness tool.

6.3 Acknowledgments

The authors express deep gratitude to Mrs. S.R. Shailaja, Assistant Professor at Anurag University, for her invaluable guidance throughout the project. Mrs. Shailaja provided insightful contributions to the

research design, assisted in shaping the project's objectives, and offered technical expertise during the development and testing phases. Her mentorship was crucial to the successful execution of the study and the development of the web platform.

6.4 Competing Interests

The authors declare no competing interests. There are no financial or professional conflicts that could influence the findings, ensuring the integrity of the research process and a focus on producing a reliable and unbiased ransomware readiness tool.

REFERENCES

1. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM)*, Amity University Rajasthan, Jaipur-India.
2. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
3. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
4. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.
5. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.
6. Narayana, M. S., Babu, N., Prasad, B. V. V. S., & Kumar, B. S. (2011). Clustering Categorical Data--Study of Mining Tools for Data Labeling. *International Journal of Advanced Research in Computer Science*, 2(4).
7. Shankar, G. S., Onyema, E. M., Kavim, B. P., Gude, V., & Prasad, B. S. (2024). Breast Cancer Diagnosis Using Virtualization and Extreme Learning Algorithm Based on Deep Feed Forward Networks. *Biomedical Engineering and Computational Biology*, 15, 11795972241278907.
8. Kulkarni, R., & Prasad, B. S. (2022). Predictive Modeling Of Heart Disease Using Artificial Intelligence. *Journal of Survey in Fisheries Sciences*, 791-801.
9. Gowda, B. M. V., Murthy, G. V. K., Upadhye, A. S., & Raghavan, R. (1996). Serotypes of Escherichia coli from pathological conditions in poultry and their antibiogram.
10. Balasubbareddy, M., Murthy, G. V. K., & Kumar, K. S. (2021). Performance evaluation of different structures of power system stabilizers. *International Journal of Electrical and Computer Engineering (IJECE)*, 11(1), 114-123.
11. Murthy, G. V. K., & Sivanagaraju, S. (2012). S. Satyana rayana, B. Hanumantha Rao, " Voltage stability index of radial distribution networks with distributed generation,". *Int. J. Electr. Eng*, 5(6), 791-803.
12. Anuja, P. S., Kiran, V. U., Kalavathi, C., Murthy, G. N., & Kumari, G. S. (2015). Design of elliptical patch antenna with single & double U-slot for wireless applications: a comparative approach. *International Journal of Computer Science and Network Security (IJCSNS)*, 15(2), 60.
13. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2015). Voltage stability enhancement of distribution system using network reconfiguration in the presence of DG. *Distributed Generation & Alternative Energy Journal*, 30(4), 37-54.
14. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, 3(2), 3328-3333.
15. Madhavi, M., & Murthy, G. V. (2020). Role of certifications in improving the quality of Education in Outcome Based Education. *Journal of Engineering Education Transformations*, 33(Special Issue).
16. Varaprasad Rao, M., Srujan Raju, K., Vishnu Murthy, G., & Kavitha Rani, B. (2020). Configure and management of internet of things. In *Data Engineering and Communication Technology: Proceedings of 3rd ICDECT-2K19* (pp. 163-172). Springer Singapore.
17. Murthy, G. V. K., Suresh, C. H. V., Sowjankumar, K., & Hanumantharao, B. (2019). Impact of distributed generation on unbalanced radial distribution system. *International Journal of Scientific and Technology Research*, 8(9), 539-542.

18. Balram, G., & Kumar, K. K. (2022). Crop field monitoring and disease detection of plants in smart agriculture using internet of things. *International Journal of Advanced Computer Science and Applications*, 13(7).
19. Balram, G., & Kumar, K. K. (2018). Smart farming: Disease detection in crops. *Int. J. Eng. Technol*, 7(2.7), 33-36.
20. Balram, G., Rani, G. R., Mansour, S. Y., & Jafar, A. M. (2001). Medical management of otitis media with effusion. *Kuwait Medical Journal*, 33(4), 317-319.
21. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
22. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, 13(2), 2749-2757.
23. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, 7(2), 01-12.
24. Prasad, PVS Siva, and S. Krishna Mohan Rao. "A Survey on Performance Analysis of ManetsUnder Security Attacks." *network* 6, no. 7 (2017).
25. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
26. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, 33(Special Issue).
27. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 1190-1198.
28. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, 30(3).
29. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
30. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, 32, 101054.
31. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(7 S).
32. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
33. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, 13(1), 159-168.
34. DASTAGIRIAH, D. (2024). A SYSTEM FOR ANALYSING CALL DROP DYNAMICS IN THE TELECOM INDUSTRY USING MACHINE LEARNING AND FEATURE SELECTION. *Journal of Theoretical and Applied Information Technology*, 102(22).
35. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
36. Sudhakar, R. V., Dastagiraiah, C., Pattem, S., & Bhukya, S. (2024). Multi-Objective Reinforcement Learning Based Algorithm for Dynamic Workflow Scheduling in Cloud Computing. *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, 12(3), 640-649.
37. PushpaRani, K., Roja, G., Anusha, R., Dastagiraiah, C., Srilatha, B., & Manjusha, B. (2024, June). Geological Information Extraction from Satellite Imagery Using Deep Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
38. Rani, K. P., Reddy, Y. S., Sreedevi, P., Dastagiraiah, C., Shekar, K., & Rao, K. S. (2024, June). Tracking The Impact of PM Poshan on Child's Nutritional Status. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
39. Sravan, K., Gunakar Rao, L., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2023, July). Analyze the Quality of Wine Based on Machine Learning Approach. In *International Conference on Data Science and Applications* (pp. 351-360). Singapore: Springer Nature Singapore.
40. LAASSIRI, J., EL HAJJI, S. A. İ. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, 15(1).

41. Ramineni, K., Harshith Reddy, K., Sai Thrikoteswara Chary, L., Nikhil, L., & Akanksha, P. (2024, February). Designing an Intelligent Chatbot with Deep Learning: Leveraging FNN Algorithm for Conversational Agents to Improve the Chatbot Performance. In *World Conference on Artificial Intelligence: Advances and Applications* (pp. 143-151). Singapore: Springer Nature Singapore.
42. Samya, B., Archana, M., Ramana, T. V., Raju, K. B., & Ramineni, K. (2024, February). Automated Student Assignment Evaluation Based on Information Retrieval and Statistical Techniques. In *Congress on Control, Robotics, and Mechatronics* (pp. 157-167). Singapore: Springer Nature Singapore.
43. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
44. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, 11, 503-512.
45. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, 38(Special Issue 1).
46. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
47. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, 17(4), 1265-1282.
48. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, 83(16), 48761-48797.
49. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
50. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
51. Ravinder Reddy, B., & Anil Kumar, A. (2020). Survey on access control mechanisms in cloud environments. In *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019* (pp. 141-149). Springer Singapore.
52. Reddy, M. B. R., Nandini, J., & Sathwik, P. S. Y. (2019). Handwritten text recognition and digital text conversion. *International Journal of Trend in Research and Development*, 3(3), 1826-1827.
53. Reddy, B. R., & Adilakshmi, T. (2023). Proof-of-Work for Merkle based Access Tree in Patient Centric Data. *structure*, 14(1).
54. Reddy, B. R., Adilakshmi, T., & Kumar, C. P. (2020). Access Control Methods in Cloud Enabledthe Cloud-Enabled Internet of Things. In *Managing Security Services in Heterogenous Networks* (pp. 1-17). CRC Press.
55. Reddy, M. B. R., Akhil, V., Preetham, G. S., & Poojitha, P. S. (2019). Profile Identification through Face Recognition.
56. Dutta, P. K., & Mitra, S. (2021). Application of agricultural drones and IoT to understand food supply chain during post COVID-19. *Agricultural informatics: automation using the IoT and machine learning*, 67-87.
57. Matuka, A., Asafo, S. S., Eweke, G. O., Mishra, P., Ray, S., Abotaleb, M., ... & Chowdhury, S. (2022, December). Analysing the impact of COVID-19 outbreak and economic policy uncertainty on stock markets in major affected economies. In *6th Smart Cities Symposium (SCS 2022)* (Vol. 2022, pp. 372-378). IET.
58. Saber, M., & Dutta, P. K. (2022). Uniform and Nonuniform Filter Banks Design Based on Fusion Optimization. *Fusion: Practice and Applications*, 9(1), 29-37.
59. Mensah, G. B., & Dutta, P. K. (2024). Evaluating if Ghana's Health Institutions and Facilities Act 2011 (Act 829) Sufficiently Addresses Medical Negligence Risks from Integration of Artificial Intelligence Systems. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, 2024, 35-41.
60. Aydın, Ö., Karaarslan, E., & Gökçe Narin, N. (2023). Artificial intelligence, vr, ar and metaverse technologies for human resources management. *VR, AR and Metaverse Technologies for Human Resources Management* (June 15, 2023).
61. Chidambaram, R., Balamurugan, M., Senthilkumar, R., Srinivasan, T., Rajmohan, M., Karthick, R., & Abraham, S. (2013). Combining AIET with chemotherapy—lessons learnt from our experience. *J Stem Cells Regen Med*, 9(2), 42-43.
62. Karthick, R., & Sundhararajan, M. (2014). Hardware Evaluation of Second Round SHA-3 Candidates Using FPGA. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, 2(2).
63. Sudhan, K., Deepak, S., & Karthick, R. (2016). SUSTAINABILITY ANALYSIS OF KEVLAR AND BANANA FIBER COMPOSITE.
64. Karthick, R., Gopalakrishnan, S., & Ramesh, C. (2020). Mechanical Properties and Characterization of Palmyra Fiber and Polyester Resins Composite. *International Journal of Emerging Trends in Science & Technology*, 6(2).

65. Karthick, R., Pandi, M., Dawood, M. S., Prabakaran, A. M., & Selvaprasanth, P. (2021). ADHAAR: A RELIABLE DATA HIDING TECHNIQUES WITH (NNP2) ALGORITHMIC APPROACH USING X-RAY IMAGES. *3C Tecnologia*, 597-608.
66. Deepa, R., Karthick, R., Velusamy, J., & Senthilkumar, R. (2025). Performance analysis of multiple-input multiple-output orthogonal frequency division multiplexing system using arithmetic optimization algorithm. *Computer Standards & Interfaces*, 92, 103934.
67. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
68. Selvan, M. Arul. "Fire Management System For Industrial Safety Applications." (2023).
69. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.
70. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
71. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
72. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, 8(2).
73. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
74. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
75. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
76. Arora, P., & Bhardwaj, S. (2017). Investigation and Evaluation of Strategic Approaches Critically before Approving Cloud Computing Service Frameworks.
77. Arora, P., & Bhardwaj, S. (2017). Enhancing Security using Knowledge Discovery and Data Mining Methods in Cloud Computing.
78. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. *machine learning*, 8(7).
79. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
80. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
81. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
82. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
83. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
84. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
85. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.
86. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
87. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. *Technology*, 2(2).
88. Karthick, R., & Pragasam, J. (2019). D "Design of Low Power MPSoC Architecture using DR Method" Asian Journal of Applied Science and Technology (AJAST) Volume 3, Issue 2.
89. Karthick, R. (2018). Deep Learning For Age Group Classification System. *International Journal Of Advances In Signal And Image Sciences*, 4(2), 16-22.
90. Karthick, R., Akram, M., & Selvaprasanth, P. (2020). A Geographical Review: Novel Coronavirus (COVID-19) Pandemic. *A Geographical Review: Novel Coronavirus (COVID-19) Pandemic (October 16, 2020). Asian Journal of Applied Science and Technology (AJAST)(Quarterly International Journal) Volume, 4*, 44-50.
91. Karthick, R. (2018). Integrated System For Regional Navigator And Seasons Management. *Journal of Global Research in Computer Science*, 9(4), 11-15.
92. Kavitha, N., Soundar, K. R., Karthick, R., & Kohila, J. (2024). Automatic video captioning using tree hierarchical deep convolutional neural network and ASRNN-bi-directional LSTM. *Computing*, 106(11), 3691-3709.
93. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
94. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
95. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
96. Lokhande, M., Kalpanadevi, D., Kate, V., Tripathi, A. K., & Bethapudi, P. (2023). Study of Computer Vision Applications in Healthcare Industry 4.0. In *Healthcare Industry 4.0* (pp. 151-166). CRC Press.

97. Parganiha, R., Tripathi, A., Prathyusha, S., Baghel, P., Lanjhiyana, S., Lanjhiyana, S., ... & Sarkar, D. (2022). A review of plants for hepatic disorders. *J. Complement. Med. Res*, 13(46), 10-5455.
98. Tripathi, A. K., Soni, R., & Verma, S. (2022). A review on ethnopharmacological applications, pharmacological activities, and bioactive compounds of *Mimosa pudica* (linn.). *Research Journal of Pharmacy and Technology*, 15(9), 4293-4299.
99. Tripathi, A. K., Dwivedi, C. P., Bansal, P., Pradhan, D. K., Parganiha, R., & Sahu, D. An Ethnoveterinary Important Plant Terminalia Arjuna. *International Journal of Health Sciences*, (II), 10601-10607.
100. Mishra, S., Grewal, J., Wal, P., Bhivshet, G. U., Tripathi, A. K., & Walia, V. (2024). Therapeutic potential of vasopressin in the treatment of neurological disorders. *Peptides*, 174, 171166.
101. Koliqi, R., Fathima, A., Tripathi, A. K., Sohi, N., Jesudasan, R. E., & Mahapatra, C. (2023). Innovative and Effective Machine Learning-Based Method to Analyze Alcoholic Brain Activity with Nonlinear Dynamics and Electroencephalography Data. *SN Computer Science*, 5(1), 113.
102. Tripathi, A. K., Diwedi, P., Kumar, N., Yadav, B. K., & Rathod, D. (2022). Trigonella Foenum Grecum L. Seed (Fenugreek) Pharmacological Effects on Cardiovascular and Stress Associated Disease. *NeuroQuantology*, 20(8), 4599.
103. Sahu, P., Sharma, G., Verma, V. S., Mishra, A., Deshmukh, N., Pandey, A., ... & Chauhan, P. (2022). Statistical optimization of microwave assisted acrylamide grafting of Linum usitatissimum Gum. *NeuroQuantology*, 20(11), 4008.
104. Biswas, D., Sharma, G., Pandey, A., Tripathi, A. K., Pandey, A., Sahu, P., ... & Chauhan, P. (2022). Magnetic Nanosphere: Promising approach to deliver the drug to the site of action. *NeuroQuantology*, 20(11), 4038.
105. Kumar, D. P., & Kumar, P. G. (2025). Implementation of optimal routing in heterogeneous wireless sensor network with multi-channel Media Access Control protocol using Enhanced Henry Gas Solubility Optimizer. *International Journal of Communication Systems*, 38(1), e5980.
106. Avhankar, Madhavi S., et al. "Mobile ad hoc network routing protocols using opnet simulator." *International Journal on Recent and Innovation Trends in Computing and Communication* 10.1 (2022): 1-7.
107. Pawar, J. A., Avhankar, M. S., Gupta, A., Barve, A., Patil, H., & Maranan, R. (2024, May). Enhancing Network Security: Leveraging Isolation Forest for Malware Detection. In 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT) (pp. 230-234). IEEE.
108. Avhankar, M. S., Pawar, J., & Byagar, S. (2022, December). Localization Algorithms in Wireless Sensor Networks: Classification, Case Studies and Evaluation Frameworks. In 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 01-07). IEEE.
109. Avhankar, M. S., Pawar, J., Singh, G., Asokan, A., Kaliappan, S., & Purohit, K. C. (2023, May). Simulation Environment for the I9 Vanet Platform. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-8). IEEE.