

Cybersecurity Portal for Effective Management of Servers and Firewall

¹Dr.G.Balram, ²Sandu Jyothirmmai , ³Sanjay Aryan

¹Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.

^{2,3}UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.

21eg105f55@anurag.edu.in

21eg105f49@anurag.edu.in

Abstract. Existing systems often lack a centralized platform for managing server and firewall operations, leading to fragmented oversight and delayed responses to cyber threats. This gap frequently results in increased vulnerabilities and operational inefficiencies within organizations. To address this issue, we propose the development of the Cybersecurity Portal, designed to provide real-time monitoring, predictive analytics, and streamlined resource allocation for server and firewall management. The portal will offer comprehensive insights into system performance, potential vulnerabilities, and proactive threat detection. By equipping administrators with timely and relevant data, this platform aims to empower organizations to make informed security decisions and implement effective risk mitigation strategies. Ultimately, the Cybersecurity Portal seeks to enhance the overall cybersecurity posture of organizations, ensuring better protection of their digital assets against evolving threats.

Keywords. Cybersecurity, Server Management, Firewall Optimization, Predictive Analytics, Real-Time Monitoring.

1 INTRODUCTION

In recent years, the rapid evolution of technology has significantly impacted the field of cybersecurity, especially as organizations face increasingly sophisticated cyber threats. The need for effective management solutions has driven the development of systems that streamline server and firewall operations while enhancing security measures. One such initiative is the Cybersecurity Portal, designed to provide comprehensive management capabilities for servers and firewalls, ultimately aiming to protect organizational assets.

The requirement for this research stems from the growing complexity of network infrastructures and the escalating frequency of cyberattacks. Recent studies indicate that organizations experience numerous security breaches annually, highlighting the urgency for innovative approaches that leverage technology to improve cybersecurity management. The Cybersecurity Portal addresses these challenges by offering features such as real-time monitoring, predictive analytics, and streamlined user management, thus creating a robust solution tailored to contemporary cybersecurity needs.

The primary problem statement for this research focuses on the lack of integrated platforms that effectively manage server and firewall configurations while proactively identifying threats. This research aims to fill this gap by presenting the Cybersecurity Portal as a viable solution, incorporating functionalities that enhance resource allocation and mitigate risks.

The authors' contributions include the conceptualization of the portal's framework, the development of user-centric features, and the integration of evidence-based practices to ensure operational efficacy. This research also emphasizes the importance of real-time data collection and analysis in enhancing cybersecurity strategies, underscoring the portal's role in fostering a proactive security posture.

In summary, this work aims to demonstrate the potential of the Cybersecurity Portal as an essential tool in the cybersecurity landscape, addressing current challenges in server and firewall management. Through this

research, we seek to contribute to the ongoing discourse surrounding effective cybersecurity solutions and their impact on organizational resilience.

2 RESEARCH METHODOLOGY

The research methodology for the Cybersecurity Portal employs a comprehensive approach to ensure robust data collection and analysis, facilitating reproducibility and validation of the findings.

2.1 User - Centered Design

The development of the Cybersecurity Portal follows a user-centered design process, gathering feedback from system administrators and IT professionals through surveys and focus groups. This initial phase aims to identify specific security management needs and preferences of the target audience. Insights gained from these interactions inform the portal's features and functionalities, ensuring they align with user requirements.

2.2 Development Framework

The Cybersecurity Portal utilizes an agile development framework, allowing for iterative testing and refinement of the system. This framework supports continuous integration and deployment, enabling rapid updates based on user feedback and emerging cybersecurity trends. Relevant methodologies for agile development have been highlighted in prior studies.

2.3 Evidence-Based Practices

To ensure the effectiveness of the portal's features, evidence-based practices from existing literature on cybersecurity management and risk assessment are integrated. Strategies derived from established security frameworks, such as NIST and ISO standards, are tailored to the portal based on user feedback and organizational contexts.

2.4 Data Collection and Analysis

Data collection occurs through system usage analytics, user surveys, and feedback mechanisms integrated within the Cybersecurity Portal. Key metrics include user engagement, system performance, and incident response rates. Both quantitative and qualitative methods are employed to assess the portal's impact on security management and operational efficiency.

2.5 Community Engagement

The Cybersecurity Portal emphasizes community support by facilitating collaboration among users through forums and shared resources. This methodology includes the creation of discussion boards and knowledge-sharing activities, allowing users to exchange experiences and best practices. The effectiveness of community engagement is monitored through user participation rates and qualitative feedback.

Through this comprehensive methodology, the Cybersecurity Portal aims to establish a robust platform that effectively supports server and firewall management while ensuring the reproducibility of reported data and findings.

3 THEORY AND CALCULATION

3.1. Theory

The theoretical foundation for the Cybersecurity Portal is grounded in systems theory and information security principles, particularly focusing on risk management and proactive security strategies. These frameworks emphasize the importance of understanding the interactions between various components of a network and the necessity of anticipating potential threats to maintain a secure environment.

3.1.1. Systems Theory

Systems theory posits that a network is a collection of interconnected components that work together to achieve a common goal. In the context of the Cybersecurity Portal, this theory informs the design of an integrated system where real-time monitoring, server management, and firewall configurations operate cohesively. By analyzing the relationships between different network elements, administrators can identify vulnerabilities and optimize configurations.

3.1.2. Risk Management Framework

The risk management framework focuses on identifying, assessing, and mitigating risks to information assets. The Cybersecurity Portal employs this framework by integrating predictive analytics to assess potential security threats based on historical data and current network conditions. This proactive approach enables organizations to address vulnerabilities before they can be exploited, ultimately enhancing their security posture.

3.2. Calculation

To evaluate the effectiveness of the Cybersecurity Portal in managing servers and firewalls, a series of calculations will be employed based on performance metrics and security assessments.

3.2.1. Performance Metrics

Key performance indicators (KPIs) will be calculated, including system uptime, response times for firewall rules, and the efficiency of load balancers. These metrics will help determine how effectively the portal manages resources and maintains network security.

3.2.2. Security Incident Analysis

The number of security incidents before and after implementing the Cybersecurity Portal will be tracked. Statistical analyses, such as Chi-square tests, will be conducted to assess whether there is a significant reduction in incidents, indicating the portal's effectiveness in enhancing security measures.

3.2.3. User Engagement Assessment

User engagement with the portal's features will be analyzed by calculating metrics such as frequency of logins, session duration, and feature utilization. Correlations between these engagement metrics and the effectiveness of security measures will be evaluated to understand the role of user interaction in enhancing cybersecurity outcomes.

By grounding the Cybersecurity Portal in established theories and employing systematic calculations for outcome evaluation, this research aims to demonstrate the portal's potential as a valuable tool for improving network security and management.

4 RESULTS AND DISCUSSION

The Cybersecurity Portal enhances server and firewall management through real-time monitoring of critical metrics such as CPU usage and network traffic. Unlike traditional systems that react to threats, this portal employs predictive analytics for proactive vulnerability identification. By centralizing operations and streamlining resource allocation, it significantly improves organizational cybersecurity posture. Its user-friendly interface makes it an essential tool for modern digital infrastructure management.

Results

- 1.User Management: The portal supports secure user login, distinguishing between regular users and administrators, ensuring that critical features are accessible only to authorized personnel.
- 2.Real-Time Monitoring: The dashboard provides an overview of system performance metrics like CPU and memory usage, allowing users to quickly identify and address potential issues.
- 3.Efficient Management: Administrators can easily add, remove, and configure servers and firewall rules, enabling quick adjustments to meet organizational needs.
- 4.Streamlined Provisioning: Users can submit server requests, which are efficiently reviewed and processed by administrators, facilitating resource allocation.
- 5.Load Balancer Management: The portal allows for effective configuration and management of load balancers, optimizing network traffic distribution

Discussion

The Cybersecurity Portal enhances operational efficiency through several innovative features:

Role Differentiation: By managing user roles, the portal improves security by restricting access to sensitive functionalities.

Centralized Control: The single dashboard simplifies monitoring and management, improving decision-making for administrators.

Proactive Security: Real-time data collection shifts the focus from reactive to preventive security measures, helping organizations address vulnerabilities before they are exploited.

While challenges such as user engagement and data security remain, the Cybersecurity Portal marks a significant advancement in server and firewall management. By integrating key functionalities into a user-friendly interface, it empowers organizations to enhance their cybersecurity strategies and protect their digital assets effectively.

4.1 Preparation of Figures and Tables

TABLE 1: Role and Access Level

Role	Access Level	Description
Admin	Full Access	Can manage all features
User	View only	Can only view dashboard data.

TABLE 2: Server Performance

Server	IP address	CPU Usage (%)	Memory Usage (%)	Status
Server 1	192.168.1.10	70	60	Active
Server 2	192.168.1.20	85	75	Active
Server 3	192.168.1.30	45	55	Inactive

TABLE 3 : Firewall Rules

Firewall ID	IP address	Action	Status
101	198.168.1.10	Allow	Active
102	10.0.0.12	Block	Active
103	198.168.1.20	Allow	Active

5 CONCLUSIONS

The Cybersecurity Portal builds upon traditional security management systems by evolving into a comprehensive platform for server and firewall management. It integrates real-time monitoring and predictive analytics to enhance an organization's defense against cyber threats. While conventional systems primarily focused on reactive measures, this portal emphasizes proactive management, allowing administrators to identify vulnerabilities before they can be exploited. Its capabilities in optimizing firewall rules and managing load balancers represent a significant advancement in cybersecurity solutions. By centralizing these functionalities within a user-friendly interface, the Cybersecurity Portal not only streamlines operations but also fosters a culture of security awareness, making it an essential tool for modern digital infrastructure management.

6 DECLARATIONS

6.1 Study Limitations

The study of the Cybersecurity Portal has several limitations that may impact the research outcomes:

1. **Data Security Risks:** Sensitive information regarding server configurations and firewall rules may expose organizations to cyber threats if not adequately protected, affecting data integrity.
2. **User Engagement:** The portal's effectiveness relies on consistent participation from administrators and users. Inconsistent usage or neglect of features can result in incomplete security monitoring.
3. **Technological Barriers:** Accessibility to advanced technologies and internet connectivity may limit the portal's implementation, particularly in organizations with fewer resources.
4. **Algorithm Limitations:** The accuracy of the portal's predictive analytics and load-balancing algorithms depends on the quality of input data; inadequate data can lead to inefficient traffic distribution or mismanagement of resources.

5. Variability in Network Conditions: Differences in network performance and infrastructure among organizations can affect the portal's monitoring capabilities, influenced by factors like bandwidth and latency.

6. Integration with Existing Systems: Limited interoperability with current IT frameworks may hinder comprehensive insights into system performance and security.

7. Cultural and Organizational Resistance: Varying attitudes towards cybersecurity practices and technology adoption may impact user engagement and trust in the portal.

These limitations should be considered when interpreting the effectiveness and applicability of the Cybersecurity Portal for effective management of servers and firewalls in real-world scenarios. Addressing these challenges can enhance the portal's reliability and user trust.

6.2 Funding Source

None

6.3 Acknowledgements

I would like to express my sincere thanks to my Guide and Head of the department of Anurag University for their constant encouragement and motivating in my research work.

6.4 Informed Consent

Informed consent was obtained from all participants involved in this research, ensuring that we fully informed ourselves about the study's purpose, procedures, and the use of our data in the publication of this work.

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., Kavin, 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, P. S. 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 Enabled the 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.