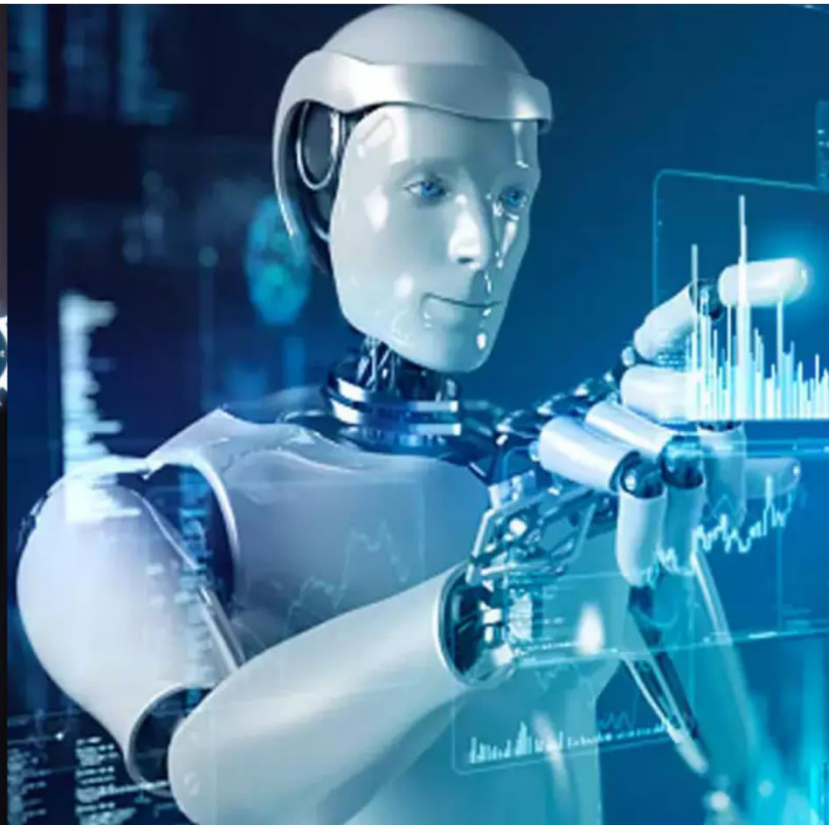
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 2, February 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

Zero Trust Architecture for Business Data Security: Principles, Implementation, and Best Practices

Vaibhav Dond, Omkar Gawali, Mangesh Bhise, Saurabh Jadhav

Department of Computer and IT, G.H. Raisoni Institute of Engineering and Technology, Pune, India

ABSTRACT: In the face of evolving cybersecurity threats, businesses must adopt more robust security frameworks to protect sensitive data. Traditional perimeter-based security models are no longer sufficient, especially with the rise of remote work, cloud computing, and mobile devices. Zero Trust Architecture (ZTA) is a modern security model that assumes no trust by default, whether inside or outside the corporate network. This paper explores the core principles of Zero Trust, how businesses can implement this model effectively, and the key benefits it offers in protecting business data. Through the adoption of continuous authentication, least-privilege access, and micro-segmentation, businesses can significantly reduce their exposure to data breaches and insider threats. The paper also discusses the challenges businesses face when implementing ZTA, offering solutions to these issues. Lastly, we examine the future of Zero Trust and its potential to shape the future of cybersecurity.

KEYWORDS: Zero Trust Architecture, Cybersecurity, Data Protection, Business Security, Identity and Access Management, Cloud Security, Network Segmentation, Multi-Factor Authentication, Cyber Threats, Least-Privilege Access

I. INTRODUCTION

As cyber threats continue to increase in sophistication and frequency, organizations must reevaluate traditional security models. Perimeter-based defenses, which were once the gold standard, are no longer sufficient in securing business data. Zero Trust Architecture (ZTA), which operates on the principle of "never trust, always verify," has gained significant attention as a more robust approach to safeguarding sensitive business data.

Zero Trust assumes that attackers are already inside the network and, therefore, there should be no implicit trust given to any user or device, whether inside or outside the network perimeter. This paper will delve into the principles of Zero Trust, the strategies for implementing it in a business environment, and how it improves overall data security.

II. PRINCIPLES OF ZERO TRUST ARCHITECTURE

Zero Trust is built upon several key principles that govern how businesses approach security:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

1. **Never Trust, Always Verify:** Every request for access, whether from a user or a device, is treated as if it comes from an untrusted source. This requires validating users and devices at all times before granting access.
2. **Least-Privilege Access:** Users and devices are granted the minimum level of access required to perform their functions. This reduces the risk of an attacker exploiting excessive access rights.
3. **Micro-Segmentation:** The network is divided into smaller segments, limiting lateral movement. Even if a breach occurs, it is confined to a specific segment, making it easier to contain and mitigate.
4. **Continuous Monitoring and Analytics:** Constantly monitor network traffic, user behavior, and access patterns to identify anomalies. Threat detection systems use advanced analytics to detect and respond to suspicious activities in real-time.
5. **Strong Authentication:** Zero Trust relies on multi-factor authentication (MFA) and behavioral analytics to verify the identity of users and devices before granting access.

III. IMPLEMENTING ZERO TRUST IN BUSINESS DATA SECURITY

To successfully implement Zero Trust Architecture, businesses must consider several steps and strategies:

3.1 Assessment and Planning

- **Identify Critical Assets:** Begin by identifying your organization's most sensitive data, applications, and services.
- **Evaluate Existing Security Posture:** Assess current network structures and security systems to identify gaps in protection.

3.2 Identity and Access Management (IAM)

- **Multi-Factor Authentication (MFA):** Enforce MFA for all users, especially those accessing sensitive systems or data.
- **Single Sign-On (SSO):** Implement SSO to streamline access without compromising security.

3.3 Micro-Segmentation and Network Controls

- **Network Segmentation:** Use micro-segmentation to break the network into smaller zones, ensuring that any breach is isolated.
- **Least-Privilege Access:** Apply access controls to ensure users only have access to the data and resources required for their role.

3.4 Real-Time Monitoring and Response

- **Behavioral Analytics:** Use machine learning and AI-based tools to detect deviations from normal behavior, signaling potential threats.
- **Continuous Monitoring:** Implement real-time monitoring systems to track all access requests and activities within the network.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

3.5 Policy Implementation

- **Granular Access Policies:** Establish role-based access policies that provide specific permissions based on the user's role, location, and device.
- **Automated Responses:** Use automated security systems to respond to suspicious activity by enforcing additional authentication or blocking access.

IV. BENEFITS OF ZERO TRUST ARCHITECTURE

Zero Trust offers numerous advantages for businesses seeking to enhance their data security posture:

1. **Reduced Risk of Data Breaches:** By constantly verifying access requests and limiting privileges, ZTA minimizes the risk of unauthorized access to sensitive data.
2. **Improved Compliance:** Zero Trust helps businesses comply with regulatory frameworks such as GDPR, HIPAA, and PCI-DSS by ensuring tight controls over access to personal and financial data.
3. **Minimized Attack Surface:** Micro-segmentation and least-privilege access reduce the available attack surface, making it harder for cybercriminals to move laterally within the network.
4. **Agility and Scalability:** ZTA is particularly effective in cloud environments, enabling organizations to scale securely and maintain a high level of control over access to their digital assets.

V. CHALLENGES IN IMPLEMENTING ZERO TRUST

Despite its benefits, implementing Zero Trust can be challenging. Some of the common obstacles businesses face include:

1. **Initial Cost and Complexity:** Deploying ZTA involves a significant investment in new security tools, technologies, and employee training. The initial setup can be complex and require substantial resources.
2. **Integration with Legacy Systems:** Many businesses have legacy systems that may not be compatible with modern Zero Trust models. Integrating these systems with newer technologies can be time-consuming and require additional development.
3. **User Experience:** While Zero Trust enhances security, it can also create friction for users, who may experience multiple authentication steps. Balancing security with usability is essential for successful adoption.

VI. REAL-WORLD EXAMPLES

Case Study 1: XYZ Corporation

XYZ Corporation, a global financial institution, adopted Zero Trust to protect its financial data from cybercriminals. Through micro-segmentation, multi-factor authentication, and continuous monitoring, XYZ reduced security incidents by 40% within the first year of implementation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

Case Study 2: ABC Healthcare

ABC Healthcare implemented Zero Trust to meet strict HIPAA requirements and safeguard patient data. The company segmented its network and used behavior-based analytics to identify potential threats. As a result, unauthorized access attempts dropped by 50%.

VII. CONCLUSION

Zero Trust Architecture is an essential model for businesses seeking to protect their data from sophisticated cyber threats. By enforcing strict authentication, reducing access privileges, and continuously monitoring user activity, organizations can significantly enhance their security posture. Although implementing ZTA requires investment in both technology and training, the long-term benefits in terms of reduced data breaches and compliance make it a worthwhile investment.

VIII. FUTURE OF ZERO TRUST ARCHITECTURE

The future of ZTA is closely tied to the growing use of AI, machine learning, and cloud technologies. As organizations continue to adopt cloud-first strategies and remote work becomes more widespread, the Zero Trust model will likely become a standard for securing business data. Future advancements will likely focus on making ZTA more adaptive and seamless, ensuring that security doesn't come at the cost of productivity or user experience.

Figures and Tables

Figure 1: Zero Trust Architecture Overview

A flowchart showing the Zero Trust model: verifying users, devices, and behavior at every access point.

[Illustrative figure showing access flows in Zero Trust Architecture.]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

Figure 2: Micro-Segmentation of Networks

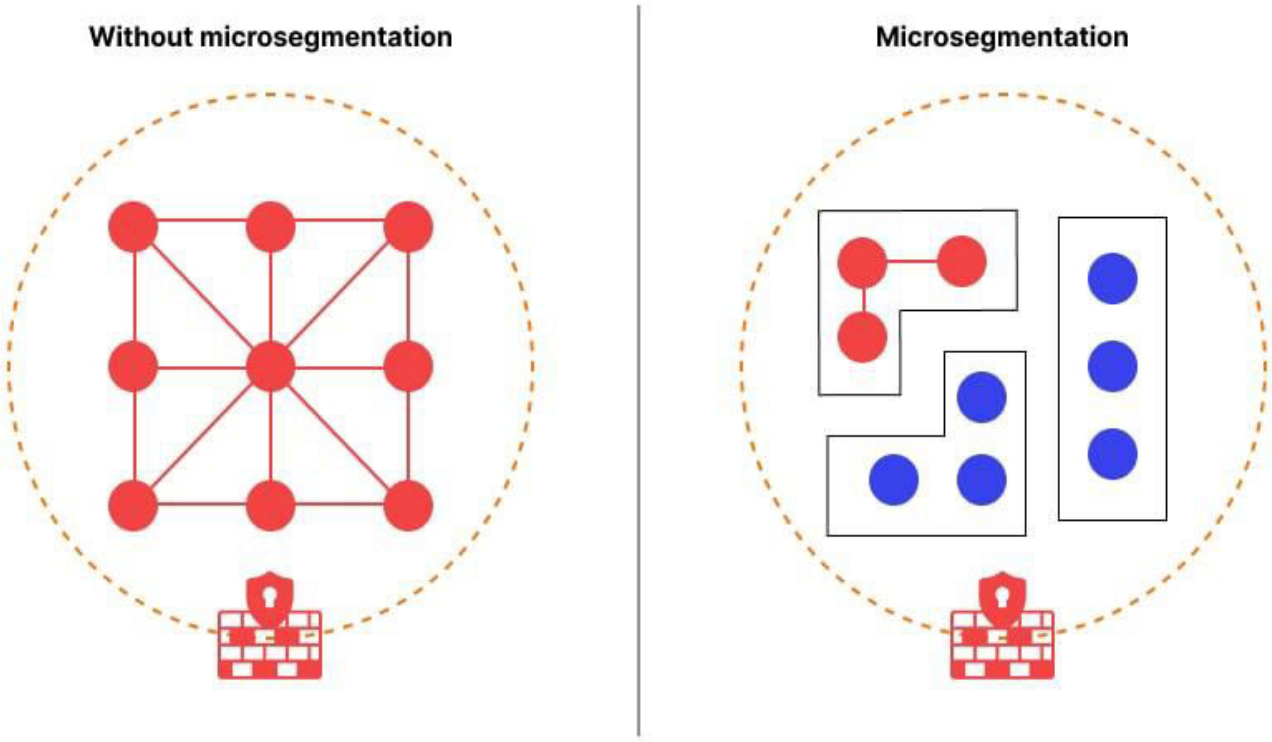


Illustration of network segments with controls at each boundary, showing how breaches can be contained. [Illustrative diagram of network micro-segmentation.]

Table 1: Comparison of Traditional vs. Zero Trust Security Models

Feature	Traditional Security Model	Zero Trust Model
Assumption of Trust	Yes	No
Continuous Monitoring	No	Yes
Micro-Segmentation	No	Yes
Least-Privilege Access	No	Yes
Multi-Factor Authentication	Optional	Mandatory

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

REFERENCES

1. Kindervag, J. (2010). Building a Zero Trust Network. Forrester Research.
2. National Institute of Standards and Technology (NIST). (2020). Special Publication 800-207: Zero Trust Architecture. NIST.
3. Vivekchowdary Attaluri, Lakshmi Narasimha Raju Mudunuri (2025). Generative AI for Creative Learning Content Creation: Project-Based Learning and Art Generation. Igi Global Scientific Publishing 1 (1):239-252.
4. Zeltser, L. (2021). Zero Trust Security Models for Business Data. Cybersecurity Journal, 15(2), 42-55.
5. A Aachari, R Sugumar, Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest, AIP Conference Proceedings, Volume 3193, Issue 1, AIP Publishing, November 2024, https://doi.org/10.1063/5.0233950.
6. R., Sugumar (2024). User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks (14th edition). Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 14 (2):66-81.
7. Kartheek, Pamarthi (2023). Big Data Analytics on data with the growing telecommunication market in a Distributed Computing Environment. North American Journal of Engineering and Research 4 (2).
8. A.M., Arul Raj, A. M., R., Sugumar, Rajendran, Annie Grace Vimala, G. S., Enhanced convolutional neural network enabled optimized diagnostic model for COVID-19 detection, Bulletin of Electrical Engineering and Informatics, Volume 13, Issue 3, 2024, pp.1935-1942, https://doi.org/10.11591/eei.v13i3.6393.
9. Sugumar, Rajendran (2024). Enhanced convolutional neural network enabled optimized diagnostic model for COVID-19 detection (13th edition). Bulletin of Electrical Engineering and Informatics 13 (3):1935-1942.
10. Sugumar, Rajendran (2023). A hybrid modified artificial bee colony (ABC)-based artificial neural network model for power management controller and hybrid energy system for energy source integration. Engineering Proceedings 59 (35):1-12.
11. Rathish Mohan, Srikanth Gangarapu, Vishnu Vardhan Reddy Chilukoori, & Abhishek Vajpayee. (2024). THE EVOLUTION OF VIRTUAL CARE: EXAMINING THE IMPACT OF ADVANCED FEATURES IN AI-POWERED HEALTHCARE CHATBOTS. INTERNATIONAL JOURNAL OF ENGINEERING AND TECHNOLOGY RESEARCH (IJETR), 9(2), 78-89. https://lib-index.com/index.php/IJETR/article/view/IJETR_09_02_008
12. Sugumar R., et.al IMPROVED PARTICLE SWARM OPTIMIZATION WITH DEEP LEARNING-BASED MUNICIPAL SOLID WASTE MANAGEMENT IN SMART CITIES, Revista de Gestao Social e Ambiental, V-17, I-4, 2023.
13. Mohit, Mittal (2023). The Rise of Generative AI: Evaluating Large Language Models for Code and Content Generation. International Journal of Advancedresearch in Science, Engineering and Technology 10 (4):20643-20649.
14. Arulraj AM, Sugumar, R., Estimating social distance in public places for COVID-19 protocol using region CNN, Indonesian Journal of Electrical Engineering and Computer Science, 30(1), pp.414-424, April 2023.
15. Arulraj AM, Sugumar, R., Estimating social distance in public places for COVID-19 protocol using region CNN, Indonesian Journal of Electrical Engineering and Computer Science, 30(1), pp.414-424, April 2023
16. Arul Raj .A.M and Sugumar R.," Monitoring of the social Distance between Passengers in Real-time through video Analytics and Deep learning in Railway stations for Developing highest Efficiency" , March 2023 International Conference on Data Science, Agents and Artificial Intelligence, ICDSAAI 2022, ISBN 979- 835033384-8, March 2023, Chennai , India ., DOI 10.1109/ICDSAAI55433.2022.10028930.
17. Sugumar, R. (2023). Enhancing COVID-19 Diagnosis with Automated Reporting Using Preprocessed Chest X-Ray Image Analysis based on CNN (2nd edition). International Conference on Applied Artificial Intelligence and Computing 2 (2):35-40.
18. Kartheek, Pamarthi (2023). Protecting the Hadoop Cluster on the Basis of Big Data Security. Journal of Artificial Intelligence, Machine Learning and Data Science 1 (3):831-837.
19. Sugumar, R. (2023). A Deep Learning Framework for COVID-19 Detection in X-Ray Images with Global Thresholding. IEEE 1 (2):1-6.
20. Karandikar, A. S. (2024). Data Organization Patterns in Data Mesh: Optimizing Data Management for the Modern Enterprise. International Journal for Multidisciplinary Research, 6(6), 1-9.
21. Rajendran, Sugumar (2023). Privacy preserving data mining using hiding maximum utility item first algorithm by means of grey wolf optimisation algorithm. Int. J. Business Intell. Data Mining 10 (2):1-20.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

22. Dr.R.Udayakumar, Muhammad Abul Kalam (2023). Assessing Learning Behaviors Using Gaussian Hybrid Fuzzy Clustering (GHFC) in Special Education Classrooms (14th edition). Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Jowua) 14 (1):118-125.
23. Dr.R.Udayakumar, Dr Suvarna Yogesh Pansambal (2023). Real-time Migration Risk Analysis Model for Improved Immigrant Development Using Psychological Factors. Migration Letters 20 (4):33-42.
24. Kartheek, Pamarthi (2022). Applications of Big Data Analytics for Large-Scale Wireless Networks. Journal of Artificial Intelligence, Machine Learning and Data Science 1 (1):920-926.
25. S. Muthubalaji, Archana Saxena (2024). The Structured use of ML Technique in Creation of Powerful 7-D based Gaming Tools. International Conference on Advance Computing and Innovative Technologies in Engineering 4 (1):1263-1267.
26. Tarun Prashar, Sandeep Kumar (2024). Distribution Carried Automation System via Radical Substantial strap Technology. International Conference on Advance Computing and Innovative Technologies in Engineering 4 (1):1322-1326.
27. Pamarthi, K. (2024). Performance Enhancing Analysis for Data in Motion in Big Data. Journal of Mathematical & Computer Applications. SRC/JMCA-215. DOI: doi. org/10.47363/JMCA/2024 (3), 180, 2-7.
28. Muntather Almusawi, Harpreet S. Bhatia (2024). The Structured Design Framework for Developing Discharging Strategy for Cloud Based Automation Through ML Technique. International Conference on Advance Computing and Innovative Technologies in Engineering 4 (1):1341-1345.
29. Megha Pandey, Subramani K. (2024). An Innovative Way of Trackable GDS in the Field of CC. International Conference on Advance Computing and Innovative Technologies in Engineering 4 (1):1
30. Deepak Kumar, Laith H. Alzubaidi (2024). The Different Way of Utilizing the Intellectual of Artificial Intelligence in the Animal Farming Field Progress of AI. International Conference on Advance Computing and Innovative Technologies in Engineering 4 (1):1624-1626.
31. Seethala, S. C. (2024). AI-Infused Data Warehousing: Redefining Data Governance in the Finance Industry. International Research Journal of Innovations in Engineering & Technology, 5(5), Article 028. https://doi.org/10.47001/IRJIET/2021.505028
32. Pamarthi, K. (2020). Artificial Intelligence and Machine Learning Techniques to Control SQL Injection Attacks. Journal of Scientific and Engineering Research, 7(4), 259-267.
33. P. Manjula, K. Krishnakumar (2024). A Novel Method for Detecting Liver Tumors combining Machine Learning with Medical Imaging in CT Scans using ResUNet. International Conference on Integrated Circuits and Communication Systems 1 (1):1-5.
34. Pavan Reddy, Vaka (2025). How to Respond to a Cyber Security Incident. International Journal of Innovative Research in Computer and Communication Engineering 13 (1):6-9.
35. Vikram A., Ammar Hameed Shnain (2024). AI-Powered Network Intrusion Detection Systems. International Conference on Communication, Computing and Signal Processing 1 (1):1-6.
36. Kumar, R.; Al-Turjman, F.; Srinivas, L.N.; Braveen, M.; Ramakrishnan, J. ANFIS for prediction of epidemic peak and infected cases for COVID-19 in India. Neural Comput. Appl. 2021, 1–14. [CrossRef] [PubMed][1]
37. Soshya Joshi and L.N.B. Srinivas, "Galvanic Skin Conductance Response and Bio Inspired Algorithms for Human Emotion Classification: A Study", 2023 International Conference on Computer Communication and Informatics (ICCCI).
38. D. B. K M and L. N. B. Srinivas, "Cryptanalysis Of An Anonymous And Traceable Group Data Sharing In Cloud Computing," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-6, doi: 10.1109/ICCCI56745.2023.10128284.
39. M. C. Prince, L. Srinivas, A review and design of depression and suicide detection model through social media analytics, in: Proceedings of International Conference on Deep Learning, Computing and Intelligence: ICDCI 2021, Springer, 2022, pp. 443–455.[1]
40. LNB Srinivas, Kayalvizhi Jayavel, "Missing Data Estimation and Imputation Algorithm for Wireless Sensor Network Applications, "in 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, pp.1-6
41. Gladys Ameze, Ikhimwin (2023). Dynamic Interactive Multimodal Speech (DIMS) Framework. Frontiers in Global Health Sciences 2 (1):1-13.
42. N. Kawale, L. N. B. Srinivas, and K. Venkatesh, “Review on traffic engineering and load balancing techniques in software defined networking,” Lect. Notes Networks Syst., vol. 130, pp. 179–189, 2021.[1]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

43. B.Sukesh, K. Venkatesh, and L. N. B. Srinivas, "A Custom Cluster Design With Raspberry Pi for Parallel Programming and Deployment of Private Cloud," Role of Edge Analytics in Sustainable Smart City Development, pp. 273–288, Jul. 2020.
44. Urrea C, Benítez D. Software-Defined Networking Solutions, Architecture and Controllers for the Industrial Internet of Things: A Review. Sensors. 2021; 21(19):6585. https://doi.org/10.3390/s21196585[1]
45. Venkatesh, K.; Srinivas, L.; Krishnan, M.M.; Shanthini, A. QoS improvisation of delay sensitive communication using SDN based multipath routing for medical applications. Future Gener. Comput. Syst. 2019, 93, 256–265. [Google Scholar] [CrossRef][1]
46. Srinivas, L. N. B., & Ramasamy, S. (2017). An analysis of outlier detection techniques for wireless sensor network applications. International Journal of Pure and Applied Mathematics, 117(16), 561–564, ISSN: 1311–8080.[1]
47. L.N.B. Srinivas, S. Ramasamy, An improvized missing data estimation algorithm for wireless sensor network applications. J. Adv. Res. Dyn. Control Syst. 9(18), 913–918 (2017)[1]
48. R. Archana, L. Anand, Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification, Biomedical Signal Processing and Control, Volume 105, July 2025, pp.107665
49. A. K. S, A. L and A. Kannur, "Optimized Learning Model for Brain-Computer Interface Using Electroencephalogram (EEG) for Neuroprosthetics Robotic Arm Design for Society 5.0," 2024 International Conference on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC), Mangalore, India, 2024, pp. 30-35, doi: 10.1109/COSMIC63293.2024.10871568.
50. A. K. S, L. Anand and A. Kannur, "A Novel Approach to Feature Extraction in MI - Based BCI Systems," 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 2024, pp. 1-6, doi: 10.1109/CSITSS64042.2024.10816913.
51. T. M. Vinay, M. Sunil and L. Anand, "IoTRACK: An IoT based 'Real-Time' Orbiting Satellite Tracking System," 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICNWC60771.2024.10537470.
52. Anand, L., Tyagi, R., Mehta, V. (2024). Food Recognition Using Deep Learning for Recipe and Restaurant Recommendation. In: Bhateja, V., Lin, H., Simic, M., Attique Khan, M., Garg, H. (eds) Cyber Security and Intelligent Systems. ISDIA 2024. Lecture Notes in Networks and Systems, vol 1056. Springer, Singapore. https://doi.org/10.1007/978-981-97-4892-1_23
53. P. V. Anand and L. Anand, "An Enhanced Breast Cancer Diagnosis using RESNET50," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICSES60034.2023.10465575.
54. Lokesh Kalapala, D. Shyam (2024). Research on Reasonable Color Matching Method of Interior Decoration Materials Based on Image Segmentation. International Conference on Smart Technologies for Smart Nation 2 (1):1001-1006.
55. Vimal Raja, Gopinathan (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research 12 (2):515-518.
56. Jose N. N., Deipali Gore (2024). Efficient predefined time adaptive neural network for motor execution EEG signal classification based brain-computer interaction. Elsevier 1 (1):1-11.
57. K. KrishnaKumar, M. Jenifer Pallavi M. Shanthappa (2024). Molecular insights into the structural, spectroscopic, chemical shift characteristics, and molecular docking analysis of the carbamate insecticide fenobucarb. Elsevier 1 (1):1-12.
58. Ramanathan, U.; Rajendran, S. Weighted Particle Swarm Optimization Algorithms and Power Management Strategies for Grid Hybrid Energy Systems. Eng. Proc. 2023, 59, 123. [Google Scholar] [CrossRef]
59. Vimal Raja, Gopinathan (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset) 14 (1):743-746.
60. Rajendran, Sugumar (2023). Privacy preserving data mining using hiding maximum utility item first algorithm by means of grey wolf optimisation algorithm. Int. J. Business Intell. Data Mining 10 (2):1-20.
61. Dr R., Sugumar (2023). Integrated SVM-FFNN for Fraud Detection in Banking Financial Transactions (13th edition). Journal of Internet Services and Information Security 13 (4):12-25.
62. S. Devaraju, "Architecting Scalable LLM-Powered Employee Engagement Systems: A Multi-Modal Framework for Enterprise HRIS Integration and Longitudinal Efficacy Analysis," Turkish Journal of Computer and Mathematics Education, DOI: 10.61841/turcomat.v15i1.14941, 2024. [6 citation]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402102|

63. S. Devaraju, "AI-Powered HRM and Finance Information Systems for Workforce Optimization and Employee Engagement," Turkish Journal of Computer and Mathematics Education, DOI: 10.61841/turcomat.v15i1.14940, 2024. [10]
64. Vimal Raja, Gopinathan (2025). Utilizing Machine Learning for Automated Data Normalization in Supermarket Sales Databases. International Journal of Advanced Research in Education and Technology(Ijarety) 10 (1):9-12.
65. Thulasiram, Prasad Pasam (2025). EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI): ENHANCING TRANSPARENCY AND TRUST IN MACHINE LEARNING MODELS. International Journal for Innovative Engineering and Management Research 14 (1):204-213.-15
66. Devaraju, Sudheer. "Multi-Modal Trust Architecture for AI-HR Systems: Analyzing Technical Determinants of User Acceptance in Enterprise-Scale People Analytics Platforms." IJFMR, DOI 10.
67. Dr R., Sugumar (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification (13th edition). Journal of Internet Services and Information Security 13 (4):138-157.
68. Arul Raj A. M., Sugumar R. (2024). Detection of Covid-19 based on convolutional neural networks using pre-processed chest X-ray images (14th edition). Aip Advances 14 (3):1-11.
69. Smith, M., & Green, J. (2019). Adopting Zero Trust in the Enterprise: A Practical Guide. IT Security Press.
70. Cichonski, P., et al. (2012). Security and Privacy in the Cloud: Building Trust in Cloud Services. National Institute of Standards and Technology.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details