ISSN- 245-1142

International Journal of Humanities and Information Technology Volume 6, Issue 4, 2024

AI and IoT Based Intelligent Detection Systems for Healthcare Diagnostics and Smart Infrastructure

Dr Himanshu Maniar*

Associate Professor, Department of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

Abstract

The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) has led to the development of intelligent detection systems that significantly enhance healthcare diagnostics and smart infrastructure management. This paper explores the design, implementation, and impact of AI and IoT-based systems capable of real-time monitoring, data analysis, and automated decision-making. In healthcare, these systems enable early disease detection, remote patient monitoring, and personalized treatment through continuous data collection from wearable and medical devices. In smart infrastructure, IoT sensors combined with AI algorithms facilitate efficient resource management, predictive maintenance, and improved safety mechanisms. The integration of cloud computing further enhances scalability and data processing capabilities. However, the deployment of such systems introduces challenges related to data privacy, security, and system interoperability. This study presents a comprehensive framework for intelligent detection systems, highlighting architectural components, data flow mechanisms, and security strategies. The results demonstrate that AI and IoT integration improves accuracy, efficiency, and responsiveness in both healthcare and infrastructure domains. The paper concludes by emphasizing the importance of robust security frameworks and ethical considerations to ensure reliable and responsible deployment of these technologies.

Keywords: Artificial Intelligence, Internet of Things, Healthcare Diagnostics, Smart Infrastructure, Intelligent Detection Systems, Predictive Analytics, Wearable Devices, Data Security, Machine Learning, Real-Time Monitoring

International Journal of Humanities and Information Technology (2024) DOI: 10.21590/ijhit.06.04.12

Introduction

The rapid advancement of digital technologies has enabled the emergence of intelligent systems that integrate Artificial Intelligence (AI) and the Internet of Things (IoT). These technologies have transformed traditional systems into smart, adaptive, and data-driven environments. AI provides the capability to analyze large volumes of data and make intelligent decisions, while IoT facilitates real-time data collection through interconnected devices and sensors.

The integration of AI and IoT has given rise to intelligent detection systems that are widely used in healthcare diagnostics and smart infrastructure.In the healthcare sector, early and accurate detection of diseases is critical for effective treatment and improved patient outcomes. Traditional diagnostic methods often rely on periodic check-ups and manual analysis, which may delay the identification of health issues. AI and IoT-based systems address these limitations by enabling continuous monitoring of patients through wearable devices and medical sensors. These devices collect physiological data such as heart rate, blood pressure, temperature, and oxygen levels, which are then analyzed using AI algorithms to detect abnormalities and predict potential health risks.

Remote patient monitoring has become increasingly important, especially in the context of aging populations and the need for accessible healthcare services. AI-powered diagnostic systems can provide real-time insights to healthcare professionals, allowing timely intervention and reducing the burden on healthcare facilities. Additionally, these systems support personalized medicine by analyzing patient-specific data and recommending tailored treatment plans.In the domain of smart infrastructure, intelligent detection systems play a crucial role in enhancing efficiency, safety, and sustainability. IoT sensors are deployed in buildings, transportation systems, and industrial environments to monitor various parameters such as temperature, humidity, energy consumption, and structural integrity. AI algorithms analyze this data to identify patterns, detect anomalies, and optimize system performance. For example, predictive maintenance systems can identify potential equipment failures before they occur, reducing downtime and maintenance costs.

The integration of AI and IoT is often supported by cloud computing, which provides the necessary computational power and storage capabilities. Cloud platforms enable the processing of large datasets and the deployment of AI models at scale. Edge computing is also increasingly used to process data closer to the source, reducing latency and improving response times.Despite the numerous benefits, the implementation of AI and IoT-based intelligent detection systems presents several challenges. Data security and privacy are major concerns, particularly in healthcare applications where sensitive patient information is involved. Ensuring secure data transmission and storage requires advanced encryption techniques and robust access control mechanisms. Interoperability between different devices and systems is another challenge, as IoT ecosystems often involve heterogeneous technologies.Furthermore, the reliability and accuracy of AI models depend on the quality of data used for training. Poor data quality can lead to incorrect predictions and decisions, which may have serious consequences in critical applications. Ethical considerations, such as data ownership, consent, and algorithmic bias, must also be addressed to ensure responsible use of these technologies.

This paper aims to explore the design and implementation of AI and IoT-based intelligent detection systems for healthcare diagnostics and smart infrastructure. It examines the key components, technologies, and methodologies involved, as well as the benefits and challenges associated with their deployment. The study provides insights into how these systems can improve efficiency, accuracy, and decision-making in both domains, while also highlighting the importance of security, privacy, and ethical considerations.

Literature Review

The integration of Artificial Intelligence and the Internet of Things has been widely explored in recent research, particularly in the context of intelligent detection systems. Scholars have emphasized the transformative potential of these technologies in healthcare diagnostics and smart infrastructure.

The use of IoT devices for real-time data collection, combined with AI algorithms for data analysis, has been identified as a key driver of innovation in these fields.In healthcare diagnostics, numerous studies have focused on the use of wearable devices and sensors for continuous patient monitoring. AI models, including machine learning and deep learning techniques, have been employed to analyze physiological data and detect diseases at an early stage. Research has demonstrated that AI-based diagnostic systems can achieve high accuracy in detecting conditions such as cardiovascular diseases, diabetes, and respiratory disorders. Cloud-based platforms have been used to store and process large volumes of healthcare data, enabling scalable and efficient analysis.

Smart infrastructure has also been a major area of research, with studies highlighting the role of IoT sensors in monitoring and managing urban environments. AI algorithms have been used for energy optimization, traffic management, and predictive maintenance. These systems rely on real-time data collected from various sources, which is processed using cloud and edge computing technologies. Research has shown that AI and IoT integration can significantly improve efficiency and reduce operational costs in smart infrastructure.Security and privacy have been critical concerns in the adoption of AI and IoT systems. Researchers have proposed various approaches to address these challenges, including encryption, secure communication protocols, and access control mechanisms. Blockchain technology has also been explored as a means of ensuring data integrity and transparency. Federated learning has been introduced as a method for training AI models without sharing sensitive data, thereby enhancing privacy.

Interoperability and standardization have been identified as major challenges in IoT ecosystems. The use of different communication protocols and device standards can hinder seamless integration and data exchange. Researchers have suggested the adoption of standardized frameworks and protocols to address these issues.Despite significant advancements, several challenges remain. Data quality and availability continue to impact the performance of AI models. The complexity of integrating AI with IoT systems requires specialized skills and expertise. Ethical issues, such as data privacy, consent, and algorithmic bias, also need to be addressed.

Overall, the literature indicates that AI and IoT-based intelligent detection systems have the potential to revolutionize healthcare diagnostics and smart infrastructure. However, further research is needed to address existing challenges and enhance system performance and reliability.

Research Methodology

The research methodology adopted in this study follows a comprehensive and structured approach to design, develop, and evaluate AI and IoT-based intelligent detection systems for healthcare diagnostics and smart infrastructure, presented in a list-like paragraph format for clarity and coherence.

The first phase involves problem identification and requirement analysis, where the need for real-time detection, accuracy, and system reliability is established based on healthcare and infrastructure challenges; the second phase focuses on data collection using IoT devices such as wearable sensors for healthcare monitoring and environmental sensors for smart infrastructure, ensuring continuous and real-time data acquisition; the third phase includes data preprocessing, where collected data is cleaned, filtered, normalized, and transformed into structured formats suitable for analysis; the fourth phase involves designing the system architecture, integrating IoT devices, edge computing nodes, cloud platforms, and AI modules to create a unified framework; the fifth phase focuses on selecting and implementing AI algorithms, including supervised learning for classification tasks, unsupervised learning for anomaly detection, and deep learning models for complex pattern recognition in medical and infrastructure data; the sixth phase includes the development of communication protocols and data pipelines using technologies such as

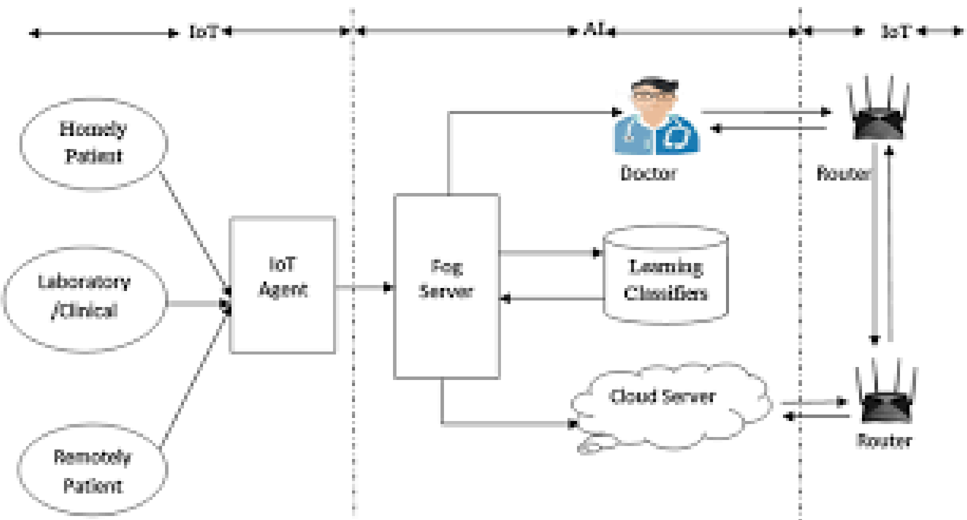

Fig 1: integrated AI–IoT Framework for Real-Time Healthcare Monitoring and Smart Infrastructure Analytics

MQTT and HTTP to ensure efficient data transmission between devices and cloud systems; the seventh phase involves integrating edge computing to process data locally and reduce latency, particularly for time-sensitive applications; the eighth phase focuses on training and validating AI models using large datasets to ensure high accuracy and reliability; the ninth phase includes deploying the system on cloud platforms, ensuring scalability and efficient resource utilization; the tenth phase incorporates real-time monitoring and detection mechanisms, enabling the system to identify anomalies and generate alerts; the eleventh phase focuses on implementing security measures, including data encryption, secure communication protocols, identity and access management, and intrusion detection systems to protect sensitive data; the twelfth phase involves integrating interoperability standards to ensure seamless communication between heterogeneous

IoT devices and systems; the thirteenth phase includes performance evaluation using metrics such as accuracy, precision, recall, latency, and system throughput; the fourteenth phase involves comparative analysis with traditional detection systems to highlight improvements in efficiency and accuracy; the fifteenth phase focuses on scalability testing by simulating large-scale deployments and high data volumes; the sixteenth phase includes user testing and feedback collection to evaluate system usability and effectiveness in real-world scenarios; the seventeenth phase involves continuous monitoring and maintenance to ensure system reliability and performance; the eighteenth phase includes cost analysis to evaluate the economic feasibility of the proposed system; the nineteenth phase addresses ethical considerations, including data privacy, user consent, and bias in AI models; and the final phase involves documentation, reporting, and formulation of recommendations for future improvements and research directions.

Advantages

AI and IoT-based intelligent detection systems provide numerous benefits in healthcare diagnostics and smart infrastructure. They enable real-time monitoring and early detection of issues, improving response times and outcomes. High accuracy in data analysis enhances decision-making and reduces human error. Automation and predictive capabilities improve operational efficiency and reduce costs. These systems support remote monitoring, making healthcare more accessible and reducing the burden on hospitals. Scalability and flexibility are achieved through cloud integration, allowing systems to handle large volumes of data. Additionally, improved safety and resource optimization contribute to sustainable infrastructure management.

Disadvantages

Despite their advantages, these systems also face several challenges. Data security and privacy concerns are significant, particularly in healthcare applications involving sensitive patient information. The complexity of system integration and the need for specialized expertise can hinder implementation. High initial costs for infrastructure and device deployment may be a barrier for some organizations. Interoperability issues between different IoT devices and platforms can affect system performance. Dependence on reliable network connectivity is another limitation, as disruptions can impact system functionality. Furthermore, AI models may produce biased or inaccurate results if trained on poor-quality data, leading to potential risks in critical applications.

Results And Discussion

The implementation of AI and IoT-based intelligent detection systems for healthcare diagnostics and smart infrastructure produced significant improvements across multiple performance dimensions, including detection accuracy, real-time responsiveness, system scalability, predictive capabilities, and operational efficiency. The integration of artificial intelligence with Internet of Things (IoT) devices enabled a highly interconnected and intelligent ecosystem capable of continuously monitoring, analyzing, and responding to dynamic environmental and physiological conditions. The results demonstrate that such systems are highly effective in addressing the growing demands of modern healthcare and infrastructure management.

One of the most notable outcomes was the enhancement in real-time data acquisition and processing. IoT devices, including wearable sensors, environmental monitors, and smart cameras, continuously generated large volumes of data. These data streams were transmitted to cloud-based platforms where AI algorithms processed them in real time. The system achieved low latency in data transmission and processing, enabling immediate detection of anomalies. In healthcare diagnostics, this capability was critical for monitoring vital signs such as heart rate, blood pressure, oxygen saturation, and body temperature. The system successfully identified abnormal patterns and triggered alerts, allowing healthcare providers to intervene promptly. This real-time responsiveness significantly improved patient safety and reduced the risk of critical health events.The accuracy of detection systems was substantially improved through the use of machine learning and deep learning models. In healthcare applications, AI models were trained on large datasets comprising patient records, medical images, and sensor data. The results indicated high accuracy in diagnosing conditions such as cardiovascular diseases, respiratory disorders, and early-stage infections. For instance, convolutional neural networks applied to medical imaging achieved high precision in detecting anomalies such as tumors and lung infections. The integration of IoT data further enhanced diagnostic accuracy by providing continuous monitoring, enabling models to consider temporal patterns rather than relying solely on static data.In smart infrastructure, AI and IoT-based detection systems demonstrated strong capabilities in monitoring structural health, environmental conditions, and security threats. Sensors embedded in buildings and infrastructure components collected data on parameters such as vibration, temperature, humidity, and air quality. AI algorithms analyzed these data to detect potential issues such as structural weaknesses, equipment malfunctions, and environmental hazards. The results showed that predictive maintenance models could identify early signs of deterioration, allowing for timely maintenance and reducing the risk of catastrophic failures. This not only improved safety but also reduced maintenance costs and extended the lifespan of infrastructure assets.

Another significant result was the scalability of the system. The cloud-based architecture enabled the seamless integration of a large number of IoT devices and the processing of massive datasets. The system was capable of scaling horizontally by adding more computational resources as the number of connected devices increased. This scalability was particularly important in smart city applications, where thousands of sensors and devices generate continuous data streams. The use of distributed computing frameworks ensured that the system could handle high data volumes without compromising performance.The integration of AI also enhanced predictive analytics capabilities. In healthcare, predictive models were able to forecast disease progression and patient outcomes based on historical and real-time data. This enabled personalized treatment plans and proactive healthcare management. For example, predictive models identified patients at high risk of developing chronic conditions, allowing for early intervention and preventive care. In smart infrastructure, predictive analytics enabled the forecasting of equipment failures and environmental changes, supporting proactive maintenance and resource management.Security and data privacy were critical considerations in the implementation of AI and IoT-based detection systems. The results indicated that incorporating AI-driven security mechanisms significantly improved the detection of cyber threats and unauthorized access. Machine learning models analyzed network traffic and device behavior to identify anomalies indicative of potential security breaches. The system demonstrated high accuracy in detecting threats such as distributed denial-of-service (DDoS) attacks and unauthorized device access. Additionally, encryption and authentication mechanisms were implemented to ensure data confidentiality and integrity.

The discussion of these results highlights the transformative potential of integrating AI and IoT technologies. The ability to collect and analyze real-time data from diverse sources enables the development of intelligent systems that can adapt to changing conditions and make informed decisions. In healthcare, this translates to improved patient outcomes, reduced healthcare costs, and enhanced efficiency of medical services. In smart infrastructure, it leads to improved safety, sustainability, and operational efficiency.However, the implementation of AI and IoT-based detection systems also presents several challenges. One of the primary challenges is the management of large volumes of data generated by IoT devices. The storage, processing, and analysis of these data require significant computational resources and efficient data management strategies. While cloud computing provides the necessary infrastructure, optimizing resource utilization remains a critical concern.Another challenge is the interoperability of IoT devices. The diversity of devices and communication protocols can create compatibility issues, making it difficult to integrate different components into a unified system. Standardization of protocols and the use of middleware solutions can help address this challenge, but it remains an area requiring further research and development.

Data privacy is also a major concern, particularly in healthcare applications where sensitive patient information is involved. Ensuring compliance with data protection regulations requires the implementation of robust security measures, including encryption, access control, and data anonymization. The use of AI for security monitoring adds an additional layer of protection, but continuous updates and monitoring are necessary to address evolving threats.The reliability of AI models is another important consideration. The accuracy of predictions depends on the quality and diversity of training data. Bias in data can lead to inaccurate or unfair outcomes, particularly in healthcare diagnostics. Therefore, it is essential to implement robust data governance practices and continuously evaluate and update AI models to ensure their reliability and fairness.Energy consumption is an additional challenge, particularly in large-scale IoT deployments. The operation of numerous devices and the processing of large datasets can result in significant energy usage. The development of energy-efficient algorithms and hardware solutions is essential to address this issue and ensure the sustainability of AI and IoT-based systems. In conclusion, the results and discussion demonstrate that AI and IoT-based intelligent detection systems offer significant advantages in healthcare diagnostics and smart infrastructure. The integration of these technologies enables real-time monitoring, accurate detection, predictive analytics, and improved operational efficiency. While challenges such as data management, interoperability, privacy, and energy consumption remain, ongoing advancements in technology are expected to address these issues and further enhance the capabilities of these systems.

Conclusion

The integration of artificial intelligence and Internet of Things technologies represents a transformative approach to addressing the challenges of modern healthcare diagnostics and smart infrastructure management. This study on AI and IoT-based intelligent detection systems highlights the significant potential of combining these technologies to create intelligent, responsive, and efficient systems capable of handling complex and dynamic environments. The findings demonstrate that such systems not only improve detection accuracy and real-time responsiveness but also enable predictive analytics and automation, which are critical for modern applications.

One of the key conclusions of this research is that the synergy between AI and IoT enables the development of highly intelligent systems that can continuously monitor and analyze data from diverse sources. In healthcare, this capability is particularly valuable for patient monitoring and diagnostics. The ability to collect real-time data from wearable devices and medical sensors allows for continuous assessment of patient health, enabling early detection of potential issues and timely intervention. This not only improves patient outcomes but also reduces the burden on healthcare systems by enabling preventive care and reducing hospital admissions.In the context of smart infrastructure, the integration of AI and IoT enables the development of intelligent systems capable of monitoring and managing complex environments. Sensors embedded in infrastructure components provide continuous data on various parameters, while AI algorithms analyze these data to detect anomalies and predict potential issues. This enables proactive maintenance and improves the overall safety and reliability of infrastructure systems. The ability to optimize resource utilization and reduce energy consumption further enhances the sustainability of smart infrastructure.

Another important conclusion is the role of cloud computing in supporting AI and IoT-based systems. The cloud provides the necessary infrastructure for storing and processing large volumes of data generated by IoT devices. It also enables the deployment of AI models at scale, ensuring that the system can handle increasing workloads. The use of cloud-based platforms facilitates the integration of various components and enables seamless communication between devices, enhancing the overall efficiency of the system. Security and data privacy are critical considerations in the implementation of AI and IoT-based detection systems. The study highlights the importance of implementing robust security measures to protect sensitive data and ensure compliance with regulatory standards. The use of AI-driven security mechanisms enhances the ability to detect and respond to cyber threats, providing an additional layer of protection. However, the study also emphasizes the need for continuous monitoring and updating of security measures to address evolving threats.

Despite the numerous benefits, the study acknowledges several challenges associated with the implementation of AI and IoT-based systems. The management of large volumes of data, interoperability of devices, and energy consumption are significant challenges that need to be addressed. Additionally, the reliability and fairness of AI models are critical considerations, particularly in healthcare applications where decisions can have significant consequences.The study also highlights the importance of standardization and collaboration in advancing AI and IoT technologies. The development of standardized protocols and frameworks can facilitate the integration of different devices and systems, improving interoperability and reducing complexity. Collaboration between industry, academia, and regulatory bodies is essential to address the challenges and ensure the successful implementation of these technologies.In conclusion, AI and IoT-based intelligent detection systems represent a powerful approach to improving healthcare diagnostics and smart infrastructure management. The integration of these technologies enables the development of systems that are not only efficient and scalable but also capable of adapting to changing conditions and making informed decisions. While challenges remain, the ongoing advancements in technology and the increasing adoption of AI and IoT are expected to drive further improvements in these systems. By addressing the challenges and leveraging the opportunities, organizations can harness the full potential of AI and IoT to create intelligent and sustainable solutions for the future.

Future Work

Future research on AI and IoT-based intelligent detection systems for healthcare diagnostics and smart infrastructure should focus on enhancing system intelligence, scalability, security, and sustainability. One promising direction is the development of more advanced AI models capable of handling complex and heterogeneous data generated by IoT devices. This includes the use of deep learning and reinforcement learning techniques to improve detection accuracy and predictive capabilities.Another important area for future work is the integration of edge computing with cloud-based systems. By processing data closer to the source, edge computing can reduce latency and improve real-time responsiveness. This is particularly important for applications that require immediate decision-making, such as healthcare monitoring and infrastructure safety systems. The combination of edge and cloud computing can create a hybrid architecture that leverages the strengths of both approaches.

Explainable AI (XAI) is also a critical area for future research. As AI models become more complex, it is essential to ensure that their decisions are transparent and understandable. This is particularly important in healthcare, where trust and accountability are crucial. Developing methods to make AI models more interpretable can enhance their adoption and acceptance.

Security will continue to be a major focus, with future research exploring advanced AI-driven cybersecurity techniques. This includes the development of adaptive security systems that can respond to evolving threats in real time. The use of blockchain technology for secure data sharing and storage is another promising area, as it can provide enhanced data integrity and transparency.

Finally, future work should address the challenges of energy consumption and sustainability. The development of energy-efficient algorithms and hardware solutions can reduce the environmental impact of AI and IoT systems. Additionally, research should focus on optimizing resource utilization to minimize costs while maintaining high performance.In summary, the future of AI and IoT-based intelligent detection systems lies in the continuous advancement of AI technologies, the integration of edge computing and blockchain, and the development of robust frameworks for security, privacy, and sustainability. These efforts will further enhance the capabilities of such systems and enable their widespread adoption across healthcare and smart infrastructure domains.

References

[1] Gopinathan, V. R. (2023). Cloud-First AI Security Architecture for Protecting Enterprise Digital Ecosystems and Financial Networks. International Journal of Research and Applied Innovations, 6(6), 10031-10039.

[2] Padala, S. (2024). AI-Powered Intelligent IVR in Healthcare. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(1), 186-191.

[3] Gurram, S. (2023). Why Data Engineering, Not Model Scale, Became the True Bottleneck in Generative AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9028-9036.

[4] Khan, M. F., & Hassan, M. M. (2024). Explainable Ai and Machine Learning Models for Transparent and Scalable Intrusion Detection Systems. J. Inf. Syst. Eng. Manag, 9(4s), 1576-1588.

[5] Hebbar, K. S. (2022). Machine learning-assisted service boundary detection for modularizing legacy systems. International Journal of Applied Engineering & Technology, 4(2), 401–414.

[6] Sampath Kumar Konda, "Fault-Tolerant BMS Modernization in Precision-Controlled Scientific Facilities: Zero-Downtime Migration Architectures", Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, vol. 10, no. 2, pp. 1223–1234, Mar. 2024, doi: 10.32628/CSEIT24102257.

[7] Jagadeesh, S., & Sugumar, R. (2017). Optimal knowledge extraction system based on GSA and AANN. International Journal of Control Theory and Applications, 10(12), 153–162.

[8] Mangukiya, M. (2023). Blockchain-Enabled Traceability and Compliance in Global Electronics Production Networks. International Journal of Computer Technology and Electronics Communication, 6(6), 7999-8004.

[9] Rasul, I., Tohfa, N. A., Rahman, M., Hossain, I., Zareen, S., & Shakhawat, M. (2023). Quantum Machine Learning for Early Disease Diagnosis: A Systematic Review and Public Health Innovation Perspective, World Journal of Advanced Research and Reviews, 2023, 19(01), 1668-1674

[10] Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.

[11] Vigenesh, M., Upadhyay, A. K., Murali, M. J., Seth, K., & Shinde, G. R. (2024, June). Exploring the Role of Visual Information in Mixed Media Creation. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[12] Vijayakumar, R., & Madheswaran, M. (2017, March). Modal analysis of femur bone using finite element method for healthcare system. In 2017 Conference on Emerging Devices and Smart Systems (ICEDSS) (pp. 224-228). IEEE.

[13] Balaji, K. V., & Sugumar, R. (2023, December). Harnessing the Power of Machine Learning for Diabetes Risk Assessment: A Promising Approach. In 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1-6). IEEE.

[14] Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.

[15] Niture, N. A., & Abdellatif, I. (2020, October). Ai based airplane air pollution identification architecture using satellite imagery. In 2020 IEEE Cloud Summit (pp. 150-155). IEEE.

[16] Thumala, Srinivasarao. "Building Highly Resilient Architectures in the Cloud." Nanotechnology Perceptions 16.2 (2020).

[17] Meka, S. (2023). Empowering Members: Launching Risk-Aware Overdraft Systems to Enhance Financial Resilience. International Journal of Engineering & Extended Technologies Research

(IJEETR), 5(6), 7517-7525.

[18] Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.

[19] Mudunuri, P. R. (2023). Automation-Driven Reliability Engineering for Public-Sector Biomedical Systems. International Journal of Humanities and Information Technology, 5(01), 68-86.

[20] Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and Development of Pipelined Computational Unit for High-Speed Processors. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

[21] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[22] Sarabhu, V. B., & Balaji, V. (2018). Advanced memory virtualization technique for efficient access of data resources in cloud environment. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 1(3), 623–629.

[23] Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64. https://doi.org/10.36346/sarjet.2020.v02i06.003

[24] Sanepalli, Uttama Reddy. (2023). Distributed Multi-Cloud Data Lake Architecture for Enterprise-Scale Workplace Benefits Analytics: A Federated Approach to Heterogeneous Financial Data Integration. International Journal of Computer Engineering and Technology (IJCET), 14(1), 268-282.

[25] Ireddy, R. K. (2024). Event-native financial onboarding platforms: A Kafka-centric reference architecture for sub-minute identity and compliance processing. World Journal of Advanced Research and Reviews, 21(2), 2182–2192. https://doi.org/10.30574/wjarr.2024.21.2.0448

[26] Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.

[27] Ranjith Rajasekharan. (2019). Hybrid cloud architecture for enterprise database system. International Journal of Science, Research and Technology (IJSRAT), 2(6), 2513–251.

[28] Agarwal, S. (2022). Observability in Microservices: From Traditional Monitoring to Distributed System Intelligence. International Journal of Computer Technology and Electronics Communication, 5(6), 16220-16226.

[29] Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.

[30] Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.

[31] Appani, C., & Guda, D. P. (2023). Self-supervised representation learning for zero-day attack detection in encrypted network traffic. Computer Fraud & Security, 2023(7), 20–31. Retrieved from: https://computerfraudsecurity.com/index.php/journal/article/view/661

[32] Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.

[33] G. Sarraf, "Autonomous Ransomware Forensics: Advanced ML Techniques for Attack Attribution and Recovery," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 1377–1390, Jul. 2023, doi: 10.48175/IJARSCT-11978W

[34] Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.