INTEGRATING CLOUD COMPUTING WITH PREDICTIVE AI MODELS FOR EFFICIENT FAULT DETECTION IN ROBOTIC SOFTWARE

[1]Venkat Garikipati
Network Architect,
latidude 36,
California, USA
venkat44556@gmail.com
[2]R. Pushpakumar
Assistant Professor,
Department of Information Technology,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of
Science and Technology, Tamil Nadu, Chennai, India.
pushpakumar@veltech.edu.in

Abstract

With multiple breakthroughs in robotics being propelled for aspirations like machine production, healthcare provision, and logistics, intelligent fault detection has turned out to be extremely important to sustain machines' reliability. The project aims to use advanced cloud computing, predictive AI models, and IoT technologies for real-time monitoring and fault detection of robotic systems. This proposes to implement an intelligent fault detection system utilizing machine-learning methods for RNN, predicting faults through the analysis of several sensor data, logs, and performance metrics captured. The preparation of the data starts with the cleaning and normalization of data and then moves on to the anomaly detection of the frequency components which indicate fault occurrence by Fast Fourier Transform-(FFT)-based features. The processed data are uploaded to the cloud for centralized and scalable management for future use. In subsequent research, the RNN model is applied to classify the robotic systems into faulty and non-faulty classes based on the learned features. The average system performance yielded excellent results with 98.80% accuracy, 98.25% precision, 97.87% recall, and 98.06% F1 score. Therefore, these results verify the robustness of the model for fault detection with few false positives/negatives. The work here contributes to fault detection and provides a scalable solution to monitor robotic systems in real-time, thus improving overall performance.

Keywords: *Cloud Computing Predictive AI Models Fault Detection Robotic Systems Machine Learning IoT Integration.*

1. Introduction

With the new cloud coupled with predictive AI models, the revolutionizing method of robotic software fault detection enables continuous monitoring and predictive maintenance [1]. Hence, with robotics being one of the rapidly developing technologies across industries such as manufacturing, healthcare, and logistics, it has become immensely important to look into the uninterrupted working of robotic systems [2]. For robotic software, responsible for controlling a robot's behavior, one is expected to stay completely bug-free; otherwise, any downtime and operational inefficiencies could turn expensive [3]. As systems grow in complexity, the likelihood of faults or failures creeps up exponentially, especially in activities where critical decision-making, motion control, and sensor integration are involved [4]. Considering the intention behind cloud computing is to store huge amounts of data and provide processing power remotely, such a platform fits very well for developing predictive AI models [5]. Through these models, real-time analysis of sensor data from robots can detect irregularities or patterns indicative of potential faults, allowing preventive actions to take place before the occurrence of actual system failure [6]. Predictive AI-cloud integration not only provides scalability features, but also enhances fault detection by means of advanced machine learning algorithms, which continuously learn from operational data to enhance their accuracy over time [7].

The various kinds of faults that robotic software suffers can be caused by the following: hardware problems, software bugs, sensor failures, external environmental factors which affect the quality of sensor data [8]. These might include external or internal factors [9]. The very minor glitches in software with robotics can end up bringing failure of a high order; thus, fault detection is vital [10]. Complexity in software itself may be an important factor in failure [11]. Most robotic-software systems are built on very complicated and rigorous algorithms related to motion planning, decision making, and machine learning [12]. Therefore, the errors in such algorithms can create escalation and loss of unexpected behaviors [13]. Environmental changes in terms of lighting or temperature and, more importantly, the presence or absence of physical obstructions might affect sensor performance and will give wrong data into the robotic system [14]. Moreover, the integration of different components, part by part, from different respective manufacturers creates a fault, as there are interoperability issues with each other [15]. Now that robotics is taking more autonomy with its critical applications, detection of faults early enough before any disruption to operations or safety demand has become even more important [16]. This has resulted in the development of predictive AI models whereby cloud computing can analyze this high volume of data to be able to detect emerging failed condition characteristics early in the operation process [17].

While there are many benefits to the fusion of cloud computing and predictive AI models for fault detection for robotic software, there are still a number of challenges [18]. One, for example, is that when a robotic system generates huge volumes of data, traditional fault diagnosis methods are likely to fail-the methods will not have the efficiency needed to handle the raw data inputs without advanced algorithms and cloud infrastructure handling and processing the data [19]. Latency is also a common issues where transmitting sensor data, which is data collected from robots, to the cloud for processing takes time, thus impairing real-time fault detection [20]. Besides, the performance of predictive models is highly dependent on the quality of data collected. Because of the common sources of error-sensor inaccuracies, environmental noise, and so forth-data collection may often be inconsistent [21]. Then predictive models can report false alarms or fail to detect incidents, both of which lead to unreliable fault predictions. Integrating AI models into robotic software systems is complex; also, AI models must be specifically designed for robot configurations with their respective operational environments and tasks [22]. There is a lack of standardization regarding robotic platforms, making it difficult to create fault detection models that would apply to all of them [23]. Also, confidentiality and compliance with the data protection laws make important sensitive transmission and storage security in the cloud to be an issue that may risk things in some industries [24].

To overcome these challenges, several strategies can be employed. One approach is to improve the efficiency and scalability of cloud platforms by leveraging edge computing, which processes data closer to the source, reducing latency and minimizing the need for constant data transmission to the cloud. This allows for real-time monitoring and quick decision-making in robotic systems [25]. Additionally, enhancing data quality through sensor calibration, noise filtering, and sensor fusion techniques can reduce inaccuracies, ensuring that AI models receive reliable inputs for fault detection. Implementing robust AI model training with diverse datasets that include edge cases can help improve model accuracy, reducing false positives and false negatives. Standardizing protocols for data exchange and integrating modular AI models can also enable more flexible and scalable systems, making it easier to adapt the fault detection system to different robotic platforms. Finally, addressing cloud security concerns through encryption, secure data transmission protocols, and compliance with regulatory standards will help mitigate risks and ensure the integrity of the data used for predictive maintenance. By combining these strategies, the integration of cloud computing and predictive AI can be made more efficient, accurate, and secure, thus improving fault detection in robotic software.

1.1 Objective

- ➢ Combined run a cloud, Machine Learning models and IoT all in real-time fault detection of robotic systems.
- ➢ Analyze those predictive AI models in terms of performance improvements concerning accuracy and scalability in monitoring and fault detection of robotic systems.
- ➢ Developing a scalable artificial intelligence framework including cloud storage for managing and processing huge amounts of robot-generated datasets.

- Use machine learning architectures like Recurrent Neural Networks (RNN) to classify the states of robotic systems under fault and non-fault conditions.

2. Literature Survey

[26] Memory-augmented neural networks (MANNs), hierarchical multi-agent learning (HMAL), and concept bottleneck models (CBMs) into a n AI system. The integrated functioning of MANNs-the memory retention feature, HMAL-the agent coordination tool, and CBMs-the interpretability mechanism-helps in better robustness, adaptability, and transparency in the decision-making process during tasks varying in complexity. Memory enhancement, coordination among agents, and increased transparency in decision-making are the goals here; hence, solving dynamic challenging situations dependent on memory and providing an effective and flexible AI framework for various applications.

[27] The building blocks of cloud computing, AI, and IoT for real-time healthcare monitoring and diagnosis. A hybrid neural fuzzy learning model that foments a fusion of fuzzy logic and neural networks is used for processing data from IoT devices through cloud platforms for the forecasting of health conditions. The working model is trained using machine learning methods on medical datasets. The objectives of this study are to analyze the scalability of real-time data processing and to assess the hybrid learning models' effectiveness in enhancing diagnostic accuracy for healthcare applications.

[28] SCLC and NSCLC as the two main subtypes of lung carcinoma. Graph theory will visualize genes and proteins as nodes and give insight into the complex molecular networks of the disease. Some of the core components include structural property analysis, algorithm development, multi-omics integration, predictive modeling, and selection of therapeutic targets. Machine learning facilitates data processing to enable reliable prediction and detection. The logistic regression model performs very well in predicting lung cancer, thereby rendering furtherance to personalized treatment strategies.

[29] A method in which Cloud computing-based machine learning techniques enhance fraud detection in e-commerce transactions. The method uses the Online Payments Fraud Detection Dataset for preprocessing with MinMax scaling and enables real-time processing through AWS Lambda and S3. The proposed model includes a hybrid of XGBoost for classification for structured data and Autoencoders for anomaly detection to improve fraud detection accuracy. The performance of the system is evaluated based on the effect of the batch size on processing efficiency. The proposed solution ensures e-commerce fraud detection that is scalable, real-time, and minimized false positives [30].

[31] Cloud computing and internet-enabled finances on income disparities between urban and rural areas in this research. In carrying out another analysis upon the panel data, it was established how such regional aspects of digital finance usage affected income levels. The findings show that, in general, the access to financial and internet-related services has lowered income disparity more than it would have in the absence of such interventions, thus playing its role in financial inclusion and growth of rural areas. The role of access to digital finance in promoting interregional equity and sustainability is made clear by this study [32].

[33] A hybrid cryptographic key generation scheme specifically for IoT networks using Super Singular Elliptic Curve Isogeny Cryptography (SSEIC) combined with optimization algorithms such as MultiSwarm Adaptive Differential Evolution (MSADE) and Gaussian Walk Group Search Optimization (GWGSO). The proposed method enhances encryption by increasing the speed at which keys are generated as well as the key level of security and then resistance to quantum attacks. In addition, safeguarded against resource consumption, it ensures efficient and secure data exchange within IoT environments. The method can be extended and robustly secured for any IoT ecosystem in the future [34].

[35] Network analysis, comparative effectiveness research (CER), and ethnographic research for the evaluation of heart medicines and patient care plans with the use of big data tools, such as EHRs and AI-driven analytics. The aim is to assess how well the methods work in identifying cost-effective and personalized treatments based on genetic, clinical, and social factors to improve clinical results and further decrease costs. However, different new approaches are needed in improved care due to considerable global health issues posed by cardiovascular disease (CVD) [36].

[37] A model for the optimization of cloud computing systems that offer better performance,

scalability, and cost-effectiveness in handling all associated challenges such as data security, energy efficiency, resource management, and systems reliability during the processing of big data. Among these strategies are load balancing-triggered auto-scaling, dynamic resource allocation, vertical and horizontal scaling. It should also be equipped with very stringent data security protocols per energy-efficient methods automated network optimization, and online monitoring. Implementing these methods will buttress concentrated building up a big and resilient infrastructure able to house various types of applications and workload management while driving the operational costs down [38].

[39] Superior techniques regarding [specific area/field] has been carried out, concentrating towards the resolutions of major issues involving accuracy of classification and optimization of model architecture. A strategy was thus developed and tested through deep learning and algorithmic models, specific datasets and evaluation metrics available for area comparison against other existing ones. Further research intent is therefore aimed at presenting a new approach that beats traditional accuracies and efficiencies while improving on such other measures as applicability across datasets [40].

[41] SURGE-Ahead Project that aims to apply machine learning models in predicting and managing chronic illnesses in geriatric care, thereby assisting clinical decision-making. The study will lead to the design of individualized, patient-oriented models based on techniques like support-vector method, decision tree, and neural network, in conjunction with either feature selection or data preprocessing [42]. The findings indicate the effectiveness of machine-learning-based approaches for chronic illness prediction to support individualized care and real-time intervention with a view to maximizing positive patient outcomes and refining clinical decisions.

2.1 Problem Statement

It is very challenging now to integrate cutting-edge machine learning models, cloud computing, and the Internet of Things (IoT) into an entire real-time healthcare monitoring and diagnosis system due to critical challenges in scalability, accuracy, and personalization of patient care [43]. Most often, current healthcare systems are stalled in dealing with excessive amounts of data produced by real-time monitoring through IoT devices while it was expected that individualized care should be provided as well during the timely intervention stages [44]. The existing methodologies for chronic disease prediction and fraud detection in different healthcare applications are at times not very clear in their adaptability and robustness [45] [46]. Consequently, effective decision-making with the allocation of resources is hindered with patient outcome and operational efficiency being adversely affected [47] [48] [49]. This high complexity of healthcare systems now requires AI-enabled solutions for the ingestion of multiple data sources, such as EHRs and medical datasets, towards personalized care [50]. Some gaps like those mentioned above have to be covered through the design of scalable, accurate, and transparent AI frameworks for advancing healthcare diagnostics, management of patients, and processes of decision-making [51].

3. Proposed Methodology

Your project methodology includes several important steps: data collection, preprocessing, feature extraction, classification, and cloud storage integration. The raw input is derived from sensor signals along with logs and the performance metrics from robotic systems. The subsequent data processing involves two processes: cleaning, whereby some missing or noisy data can be discarded; and normalization, by which all features are scaled to a common range. For identifying potential fault-indicative frequency patterns, Fast Fourier Transform (FFT) is employed on the data for feature extraction. This data is stored on cloud platforms that provide further centralized and scalable management for analyses and operations. The recurrent neural network (RNN) model analyzes the time-series data and classifies the system state into faulty or non-faulty. The cloud storage allows data to be accessed flexibly, thus promoting real-time access for efficient integration into the continuous analysis and classification of robotic faults.

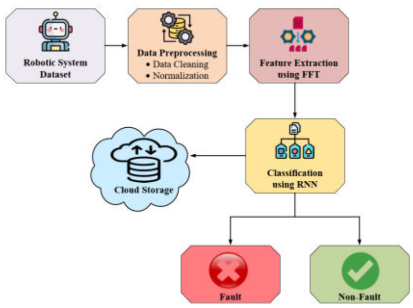

Figure 1: Workflow for Fault Detection Using Cloud Computing and Predictive AI Models

3.1 Dataset

Sensor data, logs, and performance metrics are vital input channels into the fault detection model in the robotic system dataset. Mainly, the dataset consists of time series information regarding vibrations, temperatures, speeds, and other signals of the robot. Such extensive information will help capture the system behavior and provide training data for the machine-learning models that can detect faults and anomalies in robotic systems, thereby improving operational efficiency and minimizing downtime of the given system.

3.2 Data Preprocessing

It is an integral part of data preprocessing that the raw data undergoes four basic processes before being introduced as input to the model. These processes include cleaning the data (removing noisy, missing, or irrelevant data points) and normalizing them. Normalization helps to maintain uniformity by ensuring that all features are on an equal scale so that no feature with a large scale would dominate the learning process.

3.2.1 Data Cleaning

Data Cleansing refers to the detection and cleaning of dirty or missing entries within a dataset. Missing values in the data can lead to trained models with less precision. Missing values frequently replaced with the mean of the feature are one of the common techniques of data cleansing. Since mean filling does not affect any of the sizes of the dataset, it achieves overall statistics balanced in the dataset.

3.2.2 Normalization

The main goal of normalization is to scale the features of the data into a standard range to maintain uniformity as input to the model, thus preventing the domination of variables with larger magnitude values. Common techniques include Min-Max scaling and Z-score normalization.

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (1)$$

where X is the original value, $X_{\min}$ is the minimum value, and $X_{\max}$ is the maximum value of the feature.

3.3 Feature Extraction using FFT

Fast Fourier Transform (FFT) for Feature Extraction means converting time-series data from the time domain to the frequency domain for anomaly detection in robotic systems so that some frequency patterns, which are not usual relative to normal conditions, can be identified with respect to the fault conditions. It is a computationally efficient version of the Discrete Fourier Transform (DFT) and is given by:

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-2\pi i \frac{kn}{N}}, k = 0,1, \ldots, N-1 \quad (2)$$

where x_n is the time-domain signal, and X_k represents its frequency components. Peaks in $|X_k|$ (the magnitude spectrum) can reveal abnormal vibrations or behaviors, serving as key features for predictive models like RNNs to classify robotic states as fault or non-fault.

3.4 Classification using RNN

In an RNN that detects faults, robotic system data are fed into the sequential model by using time series to present an input at some time step x_t that integrates with the earlier hidden state h_{t-1} in generating an output hidden state as h_t.The function of time that RNNs serve captures the transient dependence of the data one from another as it will determine whether the sequence is Fault or Non-Fault based on what has been learned. The last judgment is made through a sigmoid function that provides a chance of detecting fault; this may be represented as:

$$y_t = \text{sigmoid}\left(W_y \cdot \tanh\left(W_h \cdot x_t + U_h \cdot h_{t-1} + b_h\right) + b_y\right) \quad (3)$$

3.5 Cloud Storage

By then, data will pass through multiple steps of preprocessing, with features extracted for eventual storage in cloud storage for centralized and scalable management. Cloud storage guarantees efficiency in handling large amounts of robotic systems' datasets with easy access and seamless integration for further analysis. These cloud platforms allow the system to extend as data volume increases in terms of real-time access for machine learning models to classify and detect faults in robotic systems while effectively storing and retrieving data for advance analysis.

4. Result and Discussion

In the Result and Discussion section, the accent is mainly on the performance of the fault detection model implemented for robotic systems. The classification results are shown by a confusion matrix with true positive, true negative, false positive, and false negative counts. The model exhibited great performance in detecting faults with barely any misclassifications, which was evident in accuracy, precision, and recall. The remaining performance measures, including the F1-score, dictate how adept the model is in assessing a fault with minimum false alarms. The tremendous efficiency of the model indicates that it could be used in real-time monitoring of robotic systems where early fault detection is imperative to rule out operational downtime.

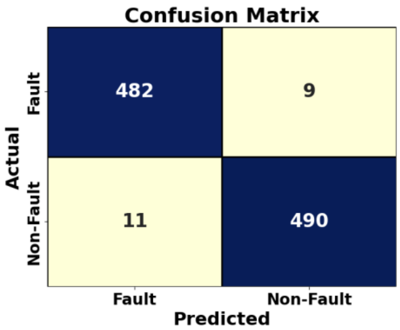

Figure 2: Confusion Matrix

Figure 2 shows the results of a classification done by a model able to detect faults in robotic systems. With this model, 482 true positives (Fault detected as Fault) and 490 true negatives (non-fault detected as non-fault) showed a correct prediction. The respective numbers for false positives (non-fault misclassified as Fault) and false negatives (Fault misclassified as non-fault) are 9 and 11. The model is well-developed and displays a high degree of accuracy, precision, and recall in identifying faults while also minimizing misclassifications.

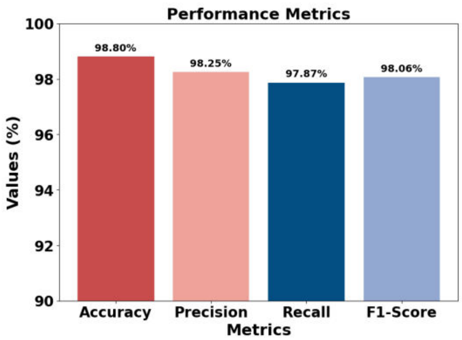

Figure 3: Performance Metrics

Figure 3 illustrates the bar chart indicating the performance metrics for the fault detection algorithm on robotic systems. The algorithm reported accuracy of 98.80%, showing it most of the time classifies cases correctly. With precision of 98.25%, this shows that it marks the faults most of the times. The recall of 97.87% reflects how the model can reflect actual fault detection. The final measure of performance, the F1-Score, which is the sum of precision and recall, would measure 98.06%. All of these indicate fair performance measures for fault detection.

5. Conclusion

Real-time fault detection of robotic systems is accomplished by integration of cloud computing, predictive AI models, and IoT technologies. The combination of sensor data, logs, and performance metrics is forwarded to machine learning models, specifically RNNs, for classifying the fault condition in the robot states as either faulty or not faulty. The results achieved are excellent in terms of performance metrics, with 98.80% accuracy, 98.25% precision, 97.87% recall, and 98.06% F1-score. This attests to the robustness and excellent capability of the fault detection with minimum misclassification. The clouds provide storage for large data sets and real-time data access for continuous monitoring and evaluation. Future work involves edge computing for low-latency and real-time responsiveness. Further enhancements in AI model training as well as sensor data quality will improve the model accuracy and broad applicability across many different robotic platforms, making further significant contributions to more advanced fault detection systems.

References

[1] Bezobrazov, S., Sachenko, A., Komar, M., & Rubanau, V. (2016). The methods of artificial intelligence for malicious applications detection in Android OS. Computing, (15, Issue 3), 184-190.

[2] Chetlapalli, H., & Bharathidasan, S. (2018). AI-BASED CLASSIFICATION AND DETECTION OF BRAIN TUMORS IN HEALTHCARE IMAGING DATA. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(2), 18-26.

[3] Gai, K., Qiu, M., Tao, L., & Zhu, Y. (2016). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and communication networks, 9(16), 3049-3058.

[4] Gaius Yallamelli, A. R., & Prasaath, V. R. (2018). AI-enhanced cloud computing for optimized healthcare information systems and resource management using reinforcement learning. International Journal of Information Technology and Computer Engineering, 6(3).

[5] Sun, L., Wei, J., Wang, J., Mi, X., Guo, Y., Lv, Y., ... & Tian, X. (2016). A universal dynamic threshold cloud detection algorithm (UDTCDA) supported by a prior surface reflectance database. Journal of Geophysical Research: Atmospheres, 121(12), 7172-7196.

[6] Yalla, R. K. M. K., & Prema, R. (2018). ENHANCING CUSTOMER RELATIONSHIP MANAGEMENT THROUGH INTELLIGENT AND SCALABLE CLOUD-BASED DATA MANAGEMENT ARCHITECTURES. International Journal of HRM and Organizational Behavior, 6(2), 1-7.

[7] Ma, L., Li, Y., Li, J., Wang, C., Wang, R., & Chapman, M. A. (2018). Mobile laser scanned point-clouds for road object detection and extraction: A review. Remote Sensing, 10(10), 1531.
[8] Ganesan, T., & Hemnath, R. (2018). Lightweight AI for smart home security: IoT sensor-based automated botnet detection. International Journal of Engineering Research and Science & Technology. 14(1).
[9] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity to Improve Detection and Response to Cyber Threats. Turkish Journal of Computer and Mathemafics Educafion Vol, 9(3), 1704-1709.
[10] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.
[11] Ali, Z. A., & Ameen, S. Y. (2018). Detection and Prevention Cyber-Attacks for Smart Buildings via Private Cloud Environment. International Journal of Computing Network Technology, 6(1).
[12] Panga, N. K. R. (2018). ENHANCING CUSTOMER PERSONALIZATION IN HEALTH INSURANCE PLANS USING VAE-LSTM AND PREDICTIVE ANALYTICS. International Journal of HRM and Organizational Behavior, 6(4), 12-19.
[13] Zhang, P., Shu, S., & Zhou, M. (2018). An online fault detection model and strategies based on SVM-grid in clouds. IEEE/CAA Journal of Automatica Sinica, 5(2), 445-456.
[14] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).
[15] Narani, S. R., Ayyalasomayajula, M. M. T., & Chintala, S. (2018). Strategies For Migrating Large, Mission-Critical Database Workloads to The Cloud. Webology (ISSN: 1735-188X), 15(1).
[16] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).
[17] Tang, A., Tam, R., Cadrin-Chênevert, A., Guest, W., Chong, J., Barfett, J., ... & Canadian Association of Radiologists (CAR) Artificial Intelligence Working Group. (2018). Canadian Association of Radiologists white paper on artificial intelligence in radiology. Canadian Association of Radiologists Journal, 69(2), 120-135.
[18] Srinivasan, K., & Arulkumaran, G. (2018). LSTM-based threat detection in healthcare: A cloud-native security framework using Azure services. International Journal of Modern Electronics and Communication Engineering, 6(2)
[19] Li, J., Zhao, Z., Li, R., & Zhang, H. (2018). Ai-based two-stage intrusion detection for software defined iot networks. IEEE internet of Things Journal, 6(2), 2093-2102.
[20] Mandala, R. R., & N, P. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. Journal of Science and Technology, 3(2).
[21] Ye, X., Chen, X., Wang, H., Zeng, X., Shao, G., Yin, X., & Xu, C. (2016). An anomalous behavior detection model in cloud computing. Tsinghua Science and Technology, 21(3), 322-332.
[22] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. Chinese Traditional Medicine Journal, 1(3), 10-15.
[23] Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.
[24] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)
[25] Andročec, D., & Vrček, N. (2016). Methodology for detection of cloud Interoperability problems. International journal of electrical and computer engineering systems, 7(2.), 53-59.
[26] Grandhi, S. H., & Padmavathy, R (2018). Federated learning-based real-time seizure detection using IoT-enabled edge AI for privacy-preserving healthcare monitoring. International Journal of Research in Engineering Technology, 3(1).
[27] Nutalapati, P. (2018). Threat Detection and Incident Response in Cloud Infrastructures. Journal of Scientific and Engineering Research, 5(9), 393-399.
[28] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions.

International Journal of Computer Science Engineering Techniques, 3(4), 10–16.

[29] Fu, H., Shen, Y., Liu, J., He, G., Chen, J., Liu, P., ... & Li, J. (2018). Cloud detection for FY meteorology satellite based on ensemble thresholds and random forests approach. Remote Sensing, 11(1), 44.

[30] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.

[31] Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology, 57(4), 312-324.

[32] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[33] Bedka, K. M., & Khlopenkov, K. (2016). A probabilistic multispectral pattern recognition method for detection of overshooting cloud tops using passive satellite imager observations. Journal of Applied Meteorology and Climatology, 55(9), 1983-2005.

[34] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.

[35] Castaño, F., Beruvides, G., Villalonga, A., & Haber, R. E. (2018). Self-tuning method for increased obstacle detection reliability based on internet of things LiDAR sensor models. Sensors, 18(5), 1508.

[36] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[37] Pentyala, D. (2017). Hybrid Cloud Computing Architectures for Enhancing Data Reliability Through AI. Revista de Inteligencia Artificial en Medicina, 8(1), 27-61.

[38] Jayaprakasam, B. S., & Hemnath, R. (2018). Optimized microgrid energy management with cloud-based data analytics and predictive modelling. International Journal of Mechanical Engineering and Computer Science, 6(3), 79–87.

[39] Shah, H. (2017). Deep Learning in Cloud Environments: Innovations in AI and Cybersecurity Challenges. Revista Espanola de Documentacion Cientifica, 11(1), 146-160.

[40] Ayyadurai, R., & Vinayagam, S. (2018). Transforming customer experience in banking with cloud-based robo-advisors and chatbot integration. International Journal of Marketing Management, 6(3), 9–17.

[41] Deng, S., Zhou, A. H., Yue, D., Hu, B., & Zhu, L. P. (2017). Distributed intrusion detection based on hybrid gene expression programming and cloud computing in a cyber physical power system. IET Control Theory & Applications, 11(11), 1822-1829.

[42] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.

[43] Ai, Y., Li, J., Shi, W., Schmit, T. J., Cao, C., & Li, W. (2017). Deep convective cloud characterizations from both broadband imager and hyperspectral infrared sounder measurements. Journal of Geophysical Research: Atmospheres, 122(3), 1700-1712.

[44] Valivarthi, D. T., & Hemnath, R. (2018). Cloud-integrated wavelet transform and particle swarm optimization for automated medical anomaly detection. International Journal of Engineering Research & Science & Technology, 14(1), 17–27.

[45] Bai, T., Li, D., Sun, K., Chen, Y., & Li, W. (2016). Cloud detection for high-resolution satellite imagery using machine learning and multi-feature fusion. Remote Sensing, 8(9), 715.

[46] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.

[47] Saljoughi, A. S., Mehrvarz, M., & Mirvaziri, H. (2017). Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms. Emerging Science Journal, 1(4), 179-191.

[48] Sareddy, M. R., & Jayanthi, S. (2018). Temporal convolutional network-based shortlisting model for sustainability of human resource

management. International Journal of Applied Sciences, Engineering, and Management, 12(1).
[49] Sun, H., Wang, X., Buyya, R., & Su, J. (2017). CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices. Software: Practice and Experience, 47(3), 421-441.
[50] Gollapalli, V. S. T., & Arulkumaran, G. (2018). Secure e-commerce fulfilments and sales insights using cloud-based big data. International Journal of Applied Sciences, Engineering, and Management, 12(3).
[51] Lo'ai, A. T., Basalamah, A., Mehmood, R., & Tawalbeh, H. (2016). Greener and smarter phones for future cities: Characterizing the impact of GPS signal strength on power consumption. IEEE access, 4, 858-868.