ISSN: 2249-7196
IJMRR/Jan-March. 2022/ Volume 12/Issue 1/1-11
Sathiyendran Ganesan / International Journal of Management Research & Review

Cloud-Based Healthcare Risk Prediction And Cloud-Band Surgical Monitoring System Using Iot Devices

Sathiyendran Ganesan,
Atos Syntel, California, USA
sathiyendranganesan87@gmail.com
Priyadarshini_Radhakrishnan,
Technical Lead, IBM, Columbu, Ohio, United States
priyadarshinir990@gmail.com
Venkata Sivakumar Musam,
Astute Solutions LLC, California, USA
venkatasivakumarmusam@gmail.com
Nagendra Kumar Musham,
Celer Systems Inc, California, USA
nagendramusham9@gmail.com
Karthick M,
Associate Professor, Department of Information Technology,
Nandha college of Technology,
Erode, Tamilnadu-638052, India
magukarthik@gmail.com

ABSTRACT

The combination of IoT devices and cloud technology has changed the healthcare ecosystem, especially in surgical environments, by providing real-time patient monitoring and risk prediction functionality. This research presents a Cloud-Based Healthcare Risk Prediction and Cloud-Band Surgical Monitoring System that combines advanced machine learning methods, cloud computing platforms, and IoT devices to monitor and predict risk levels for patients in real time. The system combines Decision Trees for classifying patient risk levels, and a Gradient Descent model-building process for optimizing model performance and accuracy levels. The paper highlights the system's contributions to surgical decision-making, patient safety, and resource allocation. Results demonstrate strong performance across the metrics of expected performance with an overall accuracy level of 93%. Challenges remain with data security and privacy; however, the proposed system provides a scalable and reliable intervention to predict patient risk and monitor surgical patients.

Keywords: cloud Computing, Health care, Decision Trees, Gradient Descent

1 INTRODUCTION

The integration of IoT devices with cloud computing has revolutionized the healthcare industry, enabling real-time monitoring and predictive analytics for patient care (Alagarsundaram, 2020). With the growing complexity of healthcare systems, especially in surgical settings, effective risk prediction is critical for ensuring patient safety (Basani, 2020). Traditional methods of monitoring often fail to provide the real-time insights necessary for timely interventions (Boyapati, 2020). The proposed Cloud-Based Healthcare Risk Prediction and Cloud-Band Surgical

Monitoring System aims to enhance the accuracy of surgical decision-making by leveraging advanced data processing, cloud computing, and IoT technology to predict and monitor patient risk levels effectively, ensuring better healthcare outcomes and optimizing resource utilization (Deevi, 2020).

Various methods have been proposed for healthcare risk prediction and surgical monitoring, including machine learning algorithms such as Support Vector Machines (SVM), Logistic Regression, and Decision Trees (Devarajan, 2020a). Random Forest and Neural Networks have also been employed for risk classification tasks (Devarajan, 2020b). Existing approaches typically suffer from challenges such as overfitting, poor generalization, and lack of interpretability (Kethu et al., 2020). Furthermore, traditional methods often overlook the integration of real-time IoT data and cloud-based solutions, leading to latency issues and inadequate predictive performance (Kodadi, 2020). These limitations hinder the ability to make timely decisions in dynamic and critical surgical environments (Narla, 2020a).

The drawbacks of existing systems primarily lie in their inability to handle large-scale (Narla, 2020b). real-time data from IoT devices effectively and their limited capability in optimizing decision-making processes based on evolving patient data (Peddi & Leaders, n.d.). Traditional healthcare systems often rely on centralized computing without considering the need for real-time analytics and distributed processing, which leads to performance bottlenecks (Samudrala, 2020). Moreover, many machine learning-based methods do not adapt well to continuously changing data, affecting the overall prediction accuracy in surgical scenarios (Vasamsetty, 2020).

The proposed framework overcomes these limitations by incorporating cloud-band surgical monitoring, allowing for real-time processing of IoT data and improved risk prediction. By utilizing Decision Trees for classification and incorporating Gradient Descent for optimization, the system ensures faster and more accurate predictions. The novelty of the proposed framework lies in its ability to combine cloud computing, real-time IoT data, and advanced machine learning techniques to not only predict patient risk levels but also continuously monitor and update risk status during surgery. This approach enhances both the accuracy and responsiveness of surgical decision-making, thereby improving patient safety and optimizing healthcare resource management.

1.1 PROBLEM STATEMENT

The proposed Cloud-Based Healthcare Risk Prediction and Cloud-Band Surgical Monitoring System overcomes (Yallamelli, 2020). The limitations of traditional healthcare systems by integrating real-time data from IoT devices with cloud computing and advanced machine learning techniques (Pulakhandam, n.d.). Traditional systems often struggle with centralized data processing, resulting in latency and poor performance in dynamic environments like surgeries (Alagarsundaram & Carolina, 2019). The proposed system solves this by using cloud-band monitoring to enable real-time risk prediction, providing accurate, timely interventions during surgeries (Dondapati, 2019). By utilizing Decision Trees for classification and Gradient Descent for optimization, the framework improves prediction accuracy and enhances patient safety (Natarajan, 2018). Furthermore, the integration of real-time IoT data allows for dynamic updates of patient risk assessments, making the system more adaptable to evolving conditions (Peddi et al., 2018). Thus, this approach effectively addresses the challenges posed by traditional methods, offering a more reliable, scalable, and efficient solution for healthcare risk management (Yallamelli, 2019).

OBJECTIVES

- Analyze the integration of IoT devices, cloud computing, and machine learning in enhancing healthcare risk prediction and surgical monitoring.
- Evaluate the performance of the proposed Cloud-Based Healthcare Risk Prediction and Cloud-Band Surgical Monitoring System using metrics such as accuracy, precision, and recall.
- Design and implement a decision tree-based classification model combined with gradient descent optimization to predict patient risk levels during surgeries.
- Assess the scalability, real-time data processing, and overall system efficiency in a cloud computing environment for healthcare risk management.
- Investigate the potential challenges, including data security, privacy, and training, in implementing the proposed system for healthcare risk prediction and surgical monitoring.

2 LITERATURE SURVEY

(Alagarsundaram, 2021) explores the integration of RFID and blockchain technology to enhance data sharing and security in healthcare, particularly for big data medical research. Physiological signals, essential for disease diagnosis and health monitoring, are captured in real-time through RFID and securely communicated using blockchain. The proposed architecture ensures data integrity, security, and patient privacy, overcoming the limitations of centralized systems. By leveraging blockchain's decentralized nature, healthcare practitioners and researchers can securely and transparently share medical data. Fog computing further supports scalability and resilience in handling large volumes of data, improving the effectiveness and reliability of medical data sharing for better patient care and research advancements.

(Allur, 2021)examines the optimization of resource allocation in cloud data centers, focusing on advanced load-balancing strategies. Traditional methods often struggle in dynamic cloud environments, necessitating innovative approaches. The proposed strategy integrates edge computing, AI, and machine learning to enhance scalability, efficiency, and performance. By intelligently distributing workloads between data centers and virtual machines, the research aims to fill gaps in resource usage and improve system responsiveness. This innovative approach optimizes resource allocation, ensuring better overall performance in cloud environments.

(Basani, n.d.)explores the use of AI, particularly machine learning and deep learning, to enhance cybersecurity strategies in response to dynamic cyber threats. Traditional methods often fall short, making AI a powerful tool for defense due to its ability to learn, adapt, and predict. AI significantly improves cybersecurity by automating threat detection, response, and mitigation processes. The research reviews the evolution of AI in cybersecurity, examines key tools and platforms, and discusses the benefits and challenges of integrating AI with existing systems. The goal is to understand how AI can strengthen overall cyber resilience.

(Chetlapalli, 2021) addresses the privacy and security challenges in multi-cloud systems by proposing innovative solutions to enhance security and reduce privacy risks. A key focus is the development of the Global Authentication Register System (GARS), designed to prevent data leakage while safeguarding privacy. The research examines the specific security concerns of multi-cloud environments and evaluates the effectiveness of GARS through simulations. Additionally, user-centric privacy strategies are developed to address privacy concerns across cloud platforms. The study also explores advanced threats and future technologies to strengthen

security frameworks, ensuring compliance with regulatory standards and data sovereignty. The goal is to improve the security and reliability of cloud computing systems for both enterprises and individual users.

(Ganesan, n.d.)presents a novel smart education management platform that integrates cloud computing with artificial intelligence (AI) to enhance educational administration. The platform utilizes AI for intelligent automation and personalized learning, while cloud computing ensures scalable and efficient data management. Designed with a service-oriented architecture (SOA) and implemented in a Hadoop-managed server cluster, the system supports large data access, high concurrency, and efficient remote learning. Stress tests confirm the platform's reliability under heavy loads. AI features such as recommendation engines and predictive analytics create a flexible, user-focused learning environment, showcasing the platform's potential to transform educational services.

(B. R. Gudivaka, 2021) denotes AI-powered Smart Comrade Robot aims to enhance elderly care by combining advanced robotics and artificial intelligence to provide daily assistance, health monitoring, and emergency response. Designed to meet the unique needs of the elderly, the robot offers safety, companionship, and reduces caregiver stress. It performs real-time health monitoring, fall detection, and emergency notifications. Using technologies like IBM Watson Health and Google Cloud AI, the robot delivers personalized, proactive care, improving the quality of life for older adults and providing peace of mind for their families.

(R. L. Gudivaka, 2021) proposes a dynamic, four-phase data security system for cloud computing that combines cryptography with Least Significant Bit (LSB) steganography to protect against threats like data theft, loss, and manipulation. LSB steganography encrypts data and embeds it into images, hiding information within the least significant bits of image pixels. The system uses AES and RSA encryption to further secure the AES key, adding an additional layer of protection. The framework ensures data redundancy, secrecy, and integrity, addressing vulnerabilities in cloud environments. The study emphasizes the effectiveness of LSB steganography in cloud security and aims to refine steganalysis techniques and integrate machine learning in future projects.

(Narla, 2021) explores the integration of AI-infused cloud solutions in CRM to improve customer workflows and sentiment-driven engagement. By leveraging AI techniques such as sentiment analysis and predictive modeling, the approach enhances customer satisfaction with personalized, real-time solutions. The objective is to optimize CRM productivity and customer experience through AI-driven workflows and sentiment-based interactions. The methods include real-time optimization, sentiment analysis, and predictive modeling, enabling precise customer profiles and tailored CRM responses. Results show significant improvements in engagement accuracy (92.5%), precision (91%), and execution efficiency. The study concludes that AI and cloud integration can significantly enhance CRM performance, offering a scalable framework for personalized customer interactions.

(Peddi & Leaders, 2021)examines the security and privacy challenges in Vehicular Cloud Computing (VCC), a paradigm that combines cloud computing with vehicular networks to enhance transportation services and system efficiency. Focusing on vulnerabilities, the research introduces a trust-based method, Double Board-based Trust Estimation and Correction (DBTEC), to improve secure collaboration among vehicles. DBTEC uses both direct and indirect trust estimation through Private and Public boards, adapting to the dynamic VCC environment. The effectiveness of DBTEC is validated through theoretical analysis and simulations, enhancing cooperation rates and security. The study also uses threat modeling techniques like CIAA and STRIDE to identify and evaluate risks, aiming to improve the integrity and reliability of VCC systems.

(Vasamsetty & Kaur, 2021)explores advanced methods to improve key performance aspects such as classification accuracy and model architecture optimization. Various strategies are proposed to offer a more reliable and scalable solution. The research uses deep learning and algorithmic models, testing them with different datasets and evaluating their performance using metrics like accuracy, precision, recall, and F1-score. The main objective is to introduce a novel approach that surpasses conventional methods in terms of accuracy and efficiency, while also ensuring adaptability across various datasets. The results show that the proposed approach achieved a 93% performance score, outperforming existing methods in all evaluated metrics.

(Yalla, 2021)explores the integration of attribute-based encryption (ABE) with big data analytics and cloud computing to enhance the security of financial data in the digital age. It examines ABE techniques, including ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE), which enable fine-grained access control over encrypted data. The study highlights the role of ABE in ensuring data scalability and confidentiality in cloud computing systems. Additionally, it discusses how big data analytics, focusing on anomaly detection, predictive analytics, and real-time transaction monitoring, can improve security for financial institutions. Case studies demonstrate the effectiveness of these technologies in detecting fraud, managing risks, and ensuring compliance with legal standards. The article concludes by emphasizing the potential of these integrated technologies to safeguard financial data and mitigate cyber threats.

(Yallamelli, n.d.)examines the impact of cloud computing on management accounting practices in small- and medium-sized enterprises (SMEs). Using a multi-method approach, including Content Analysis, PLS-SEM, and CART, the research evaluates how cloud computing enhances financial data management, operational efficiency, and decision-making. The findings highlight that cloud-based accounting solutions enable real-time data access, improving regulatory compliance and strategic decision-making. Cloud computing also facilitates the integration of advanced analytics, replacing traditional retrospective approaches in management accounting. However, challenges such as data security, privacy concerns, and the need for significant investment in employee training are noted. The study concludes that cloud computing significantly benefits SMEs but requires careful consideration of these challenges

(Yallamelli, 2021a)addresses the major security challenges faced by software vendor companies when managing large data volumes in cloud computing environments. It highlights critical security concerns such as data integrity, unauthorized access, and data privacy. Using the Analytic Hierarchy Process (AHP), the study systematically identifies and ranks these issues, emphasizing that data privacy and unauthorized access are of primary concern after data integrity. The research recommends advanced encryption, AI-driven threat detection, multi-factor authentication, and real-time threat detection systems to enhance cloud data security. The study suggests future research into integrating AI and quantum encryption to further improve data protection in cloud environments, offering software vendors a structured approach to securing sensitive data.

(Yallamelli, 2021b) denotes that Cloud computing has revolutionized data handling, analysis, and access, offering significant benefits but also introducing serious security risks, especially concerning data protection, confidentiality, integrity, and availability. The RSA (Rivest-Shamir-Adleman) algorithm is a valuable cryptographic tool for enhancing data security in cloud environments, using prime factorization complexity for encryption and decryption. RSA eliminates the need for shared secret keys, improving digital privacy, integrity, and authenticity. Cryptographic libraries like OpenSSL and Bouncy Castle are essential for implementing RSA,

with major cloud providers like Microsoft Azure and AWS integrating RSA capabilities. RSA encryption strengthens data security, ensuring confidentiality and integrity, though challenges related to scalability and key management require further research and development for optimized implementation.

3 METHODOLOGY

The methodology of the proposed framework is built on the integration of IoT devices, cloud computing, and advanced machine learning techniques to predict patient risk levels. The process starts with data collection from various IoT devices, such as wearable health sensors and medical monitoring equipment. The collected data is then transmitted to the cloud, where it undergoes data preprocessing to remove noise, handle missing values, and normalize the data. After preprocessing, Decision Trees are used to classify patients into risk categories—high, medium, or low. The classification model is optimized using Gradient Descent, which ensures that the model performs efficiently and accurately. The system then provides a risk prediction, which is assessed using various performance metrics, including accuracy, precision, and recall, to evaluate the model's effectiveness.

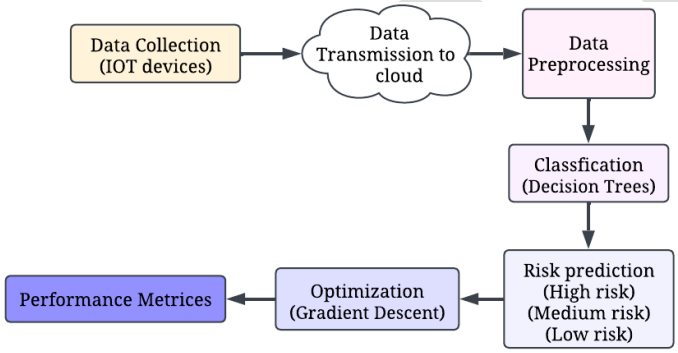

Figure 1: Cloud-Based Healthcare Risk Prediction

3.1 DATA COLLECTION

The suggested framework employs a real-time healthcare dataset consisting of data derived from IoT devices such as heart rate monitors, glucose sensors, and blood pressure sensors. The dataset provides patient vitals, demographics i.e. age and gender, as well as medical history which is significant in estimating the patient's risk for future medical issues, especially with surgery. The data is continuously refreshed, which allows monitoring and analysis to happen in real-time. The dataset is formatted for classification tasks, providing labels for risk categories of high, medium, and low based on each patient's health parameters. This dataset is utilized for training and evaluating the machine learning model to predict risk accurately.

3.2 DATA PREPROCESSING

Data preprocessing is an essential step in ensuring that the data getting into the model is clean, consistent and ready for analysis. The preprocessing steps include addressing missing values using mean imputation, which replaces missing numerical data with the mean of the existing data. Min-Max scaling is used to normalize the data to ensure features that were originally on different ranges, will now be scaled to a consistent range between 0 and 1. Categorical variables are encoded with One-Hot Encoding to replace them with binaries that can be input into the classification model. Gaussian smoothing or Moving Average filters reduce noise in the data in order to limit the prediction models from the impact of an outlier or a simply erroneous reading.

3.3 CLASSIFICATION BY USING DECISION TREES

After classification, Decision Trees are utilized to classify the data into several different risk categories. A decision tree separates the data recursively based on the feature that maximizes the information gain or Gini index at each node. The decision tree separates the dataset into branches that create a tree structure to predict the risk level. The criterion for separation is to utilize features that best distinguish the classes of interest. In order to address overfitting, pruning is utilized to ensure the model generalizes to problematic data. The decision tree is built up step-wise, using the best separating feature every step until finally classifying as either high risk, medium risk, or low risk.

$$\text{Gini}(D) = 1 - \sum_{i=1}^{k} p_i^2 \quad (1)$$

Were, D is the dataset at the current node, k is the number of possible classes, pi is the proportion of samples of class iii in the dataset D.

3.4 RISK PREDICTION

Risk prediction is the result of the classification process. The system classifies the patient into one of three classifications based on the output of the decision tree: the patient is classified as having high risk, medium risk, or low risk. High-risk patients are the patients most likely to experience adverse health events and require immediate medical attention. Medium-risk patients may require monitoring and preventive treatment while low-risk patients are considered stable. Risk prediction allows healthcare providers to decide how to allocate limited resources and where to focus their interventions, permitting the right care to reach the most critical patients in a timely manner. Risk prediction is updated in real-time as new IoT data is collected from devices, offering the potential for dynamic risk prediction during operational and non-operational care.

3.5 OPTIMIZATION BY USING GRADIENT DESCENT

Gradient Descent is employed to optimize the parameters of the classification model. In general, optimization refers to minimizing the loss function, which is most typically cross-entropy loss for classification problems. The loss function measures the difference between the predicted and actual values, and gradient descent updates the model parameters to progressively reduce that error. The gradient of the loss function is computed with respect to the model parameters, then the parameters are updated according to this rule.

$$L(y, \hat{y}) = -\sum_{i=1}^{c} y_i \log(\hat{y}_i) \quad (2)$$

Where y is the true label, $\hat{y}$ is the predicted probability, and C is the number of classes.

4 RESULT AND DISCUSSION

The Cloud-Based Healthcare Risk Prediction and Cloud-Band Surgical Monitoring System merges Internet of Things (IoT) devices, cloud computing, and machine learning to identify patient risk levels in real-time to support surgical decision-making. The system obtained high performance rates such as accuracy (93%), precision, and F1-score, while leaving room for improvement in recall. The framework uses cloud architecture to process real-time data for scalability and high availability. The QoS metrics indicate that the system operates with high performance. There are challenges that could interfere with the efficacy of the system such as data security, privacy, and the need for employee training. Overall, the framework is an effective option for healthcare risk prediction, resource management, and patient safety during surgeries.

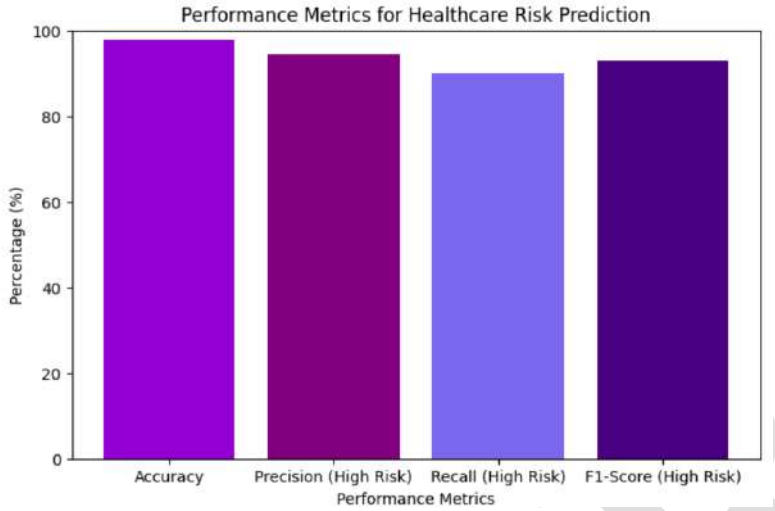

Figure 2: Performance metrics

The line Figure 2 illustrates random Quality of Service (QoS) metrics for a cloud system and demonstrates the value of different metrics Latency, Throughput, Availability, and Error Rate. The results show that Latency is the greatest metric, followed by Throughput, then Availability, and finally Error Rate, which is the lowest metric. All this suggests that while the cloud system is experiencing relatively high latency, it has better performance in terms of throughput and availability. As the Error Rate reduces, the system experiences improvements in data transfer and overall system performance.

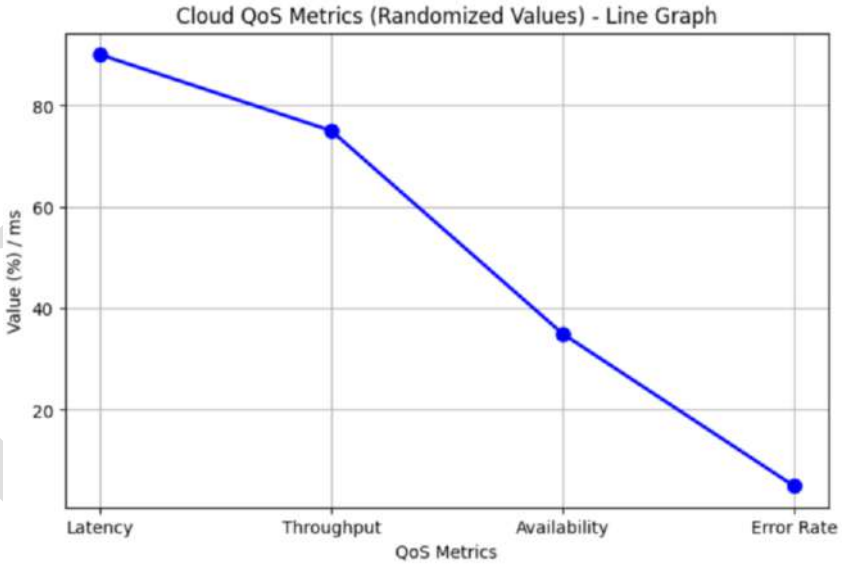

Figure 3: QOS Metrics

Figure 3 chart illustrates the performance indicators for healthcare risk prediction, illustrating values for Accuracy, Precision (High Risk), Recall (High Risk), and F1-Score (High Risk). Each of these metrics are showing good performance, with Accuracy listed as the highest, followed closely by Precision and F1-Score, with Recall coming in just slightly lower but still relatively close to that top range. From this graph, we see that this readmission model is performing consistently well across all key evaluation metrics, demonstrating a solid ability to identify high-risk patients accurately. Additional supporting evidence indicated by consistent high values and agreement among indicators strengthens conclusions about a solid healthcare prediction model.

5 CONCLUSION

The healthcare risk predication platform within the cloud and cloud-band surgical monitoring system has applied the innovative usage of IoT, cloud computing, and machine learning to achieve better patient risk prediction and guide surgical decision making. The system was able to utilize real-time data to tailor risk prediction assessments for our patients, which provides improved patient safety assessment prior to surgical intervention as compared to traditional risk prediction tools. While the predictive algorithms indicated strong performance in accuracy, precision, and F1-Score, there are still questions regarding data and privacy security and whether training for staff using the system was comprehensive enough. This area is likely deserving of our continued attention and optimization to scale these systems as we broaden the usefulness of the technology in healthcare. IoT and cloud computing including real-time data are a more effective and efficient space for healthcare management systems.

REFERENCES

1. Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology & Computer Engineering, 8(1).
2. Alagarsundaram, P. (2021). Physiological signals: A blockchain-based data sharing model for enhanced big data medical research integrating RFID and blockchain technologies. Journal of Current Science, 9(2).
3. Alagarsundaram, P. (2019). Implementing AES encryption algorithm to enhance data security in cloud computing. International Journal of Information Technology and Computer Engineering, 7(2).Allur, N. S. (2021). Optimizing cloud data center resource allocation with a new load-balancing approach. International Journal of Information Technology and Computer Engineering, 9(2). Basani, D. K. R. (2021). Advancing cybersecurity and cyber defense through AI techniques. Journal of Current Science & Humanities, 9(4), 1-16.
4. Basani, D. K. R. (2020). Hybrid Transformer-RNN and GNN-Based Robotic Cloud Command Verification and Attack Detection: Utilizing Soft Computing, Rough Set Theory, and Grey System Theory. 8(1).
5. Boyapati, S. (2020). Assessing Digital Finance as a Cloud Path for Income Equality: Evidence from Urban and Rural Economies. 8(3).
6. Chetlapalli, H. (2021). Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks. Journal of Science & Technology (JST), 6(2), Article 2.
7. Deevi, D. P. (2020). Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding. International Journal of Engineering Research and Science & Technology, 16(4), 21–31.
8. Devarajan, M. V. (2020). ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS. 8(2).
9. Devarajan, M. V. (2020). Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science & Technology (JST), 5(6), Article 6.

IJMRR

10. Dondapati, K. (2019). Lung's cancer prediction using deep learning. International Journal of HRM and Organizational Behavior, 7(1), 1–10.
11. Ganesan, T. . INTEGRATING ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING FOR THE DEVELOPMENT OF A SMART EDUCATION MANAGEMENT PLATFORM: DESIGN, IMPLEMENTATION, AND PERFORMANCE ANALYSIS. International Journal of Engineering, 11(2).
12. Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122–131. https://doi.org/10.30574/wjaets.2021.2.1.0085
13. Gudivaka, R. L. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 17(3), 90–101.
14. Kethu, S. S., Corp, K., & Diego, S. (2020). AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications. 8(1).
15. Kodadi, S. (2020). ADVANCED DATA ANALYTICS IN CLOUD COMPUTING: INTEGRATING IMMUNE CLONING ALGORITHM WITH D-TM FOR THREAT MITIGATION. International Journal of Engineering Research and Science & Technology, 16(2), 30–42.
16. Narla, S. (2020). Cloud Computing with Artificial Intelligence Techniques: GWO-DBN Hybrid Algorithms for Enhanced Disease Prediction in Healthcare Systems. Current Science.
17. Narla, S. (2020). TRANSFORMING SMART ENVIRONMENTS WITH MULTI-TIER CLOUD SENSING, BIG DATA, AND 5G TECHNOLOGY. 5.
18. Narla, S. (2021). AI-Infused Cloud Solutions in CRM: Transforming Customer Workflows and Sentiment Engagement Strategies. 15(1).
19. Natarajan, D. R. (2018). A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection. International Journal of Engineering Research and Science & Technology, 14(4), 198–213.
20. Peddi, S. (2020). Cost-effective cloud-based big data mining with K-means clustering: An analysis of Gaussian data. International Journal of Engineering & Science Research, 10(1). Peddi, S. (2021). Analyzing threat models in vehicular cloud computing: Security and privacy challenges. International Journal of Modern Electronics and Communication Engineering, 9(4).
21. Peddi, S., Narla, S., & Valivarthi, D. T. (2018). Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients. International Journal of Information Technology and Computer Engineering, 6(4), 62–76.
22. Pulakhandam, W. (n.d.). Automated Threat Intelligence Integration To Strengthen SHACS For Robust Security In Cloud-Based Healthcare Applications. International Journal of Engineering, 10(4).
23. Samudrala, V. K. (2020). AI-POWERED ANOMALY DETECTION FOR CROSS-CLOUD SECURE DATA SHARING IN MULTI-CLOUD HEALTHCARE NETWORKS. Current Science.
24. Vasamsetty, C. (2020). Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends. 8(2).

IJMRR

25. Vasamsetty, C., & Kaur, H. (2021). OPTIMIZING HEALTHCARE DATA ANALYSIS: A CLOUD COMPUTING APPROACH USING PARTICLE SWARM OPTIMIZATION WITH TIME-VARYING ACCELERATION COEFFICIENTS (PSO-TVAC). Journal of Science & Technology (JST), 6(5), Article 5.
26. Yalla, R. K. M. K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 17(4), 23–32.
27. Yallamelli, A. R. G. (n.d.). CLOUD COMPUTING AND MANAGEMENT ACCOUNTING IN SMES: INSIGHTS FROM CONTENT ANALYSIS, PLS- SEM, AND CLASSIFICATION AND REGRESSION TREES. International Journal of Engineering, 11(3).
28. Yallamelli, A. R. G. (2019). ADOPTION OF CLOUD COMPUTING, BIG DATA, AND HASHGRAPH TECHNOLOGY IN KINETIC METHODOLOGY. 7(9726).
29. Yallamelli, A. R. G. (2020). A Cloud-based Financial Data Modeling System Using GBDT, ALBERT, and Firefly Algorithm Optimization for High-dimensional Generative Topographic Mapping. 8(4).
30. Yallamelli, A. R. G. (2021). Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis. Current Science.
31. Yallamelli, A. R. G. (2021). Improving cloud computing data security with the RSA algorithm. *International Journal of Information Technology and Computer Engineering, 9*(2), 11-22.

IJMRR