Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24

Impact Factor-2.05

A CLOUD-BASED IOT FRAMEWORK FOR HEALTHCARE DATA ACQUISITION AND PROCESSING

Aleksandar J. Mitrovic
International University of Novi Pazar
Novi Pazar, Serbia
jmitrovicaleksandar@gmail.com

ABSTRACT

The sudden advancement of Internet of Things (IoT) and cloud computing technologies has transformed the health industry significantly by enabling real-time patient monitoring, remote diagnosis, and management of huge medical data sets. Interoperability, data security, latency, and effective management of humongous health data sets are still the primary concerns. In order to address these hurdles, in this paper an intelligent, secure, and scalable IoT cloud platform is proposed for acquisition and processing of healthcare data specifically with focus on security. Such a platform has strong encryption methodologies to secure private patient data both during transmission as well as in storage. The framework uses edge computing to minimize latency and enable real-time processing of data for faster responsiveness of remote healthcare services. Interoperable communication protocols like HL7 and FHIR are used to make heterogeneous medical devices and systems talk to each other. In addition, the architecture integrates AI-based anomaly detection models utilizing machine learning and deep learning methods to detect unusual physiological patterns, facilitating predictive diagnostics and early intervention for life-threatening conditions. Experimental verification on real-world healthcare datasets shows considerable enhancements in system performance, such as lower latency, improved scalability, and better reliability in remote patient monitoring use cases. The results highlight the framework's ability to overcome significant limitations in current IoT-healthcare integrations and enable more effective and secure medical decision-making. The research contributes next-generation smart healthcare system development through the provision of an end-to-end solution that closes the gap between state-of-the-art technology capabilities and actual clinical needs.

***Keywords**: Internet of Things, Cloud Computing, Healthcare, Data Security, Edge Computing, Interoperability, Anomaly Detection, Remote Patient Monitoring, Artificial Intelligence, Smart Healthcare.*

1. INTRODUCTION

The integration of the Internet of Things with cloud computing is transforming healthcare by enabling monitoring, efficient data collection, and remote patient management [1]. IoT devices such as wearables and smart medical sensors can continuously track vital signs, helping clinicians make timely and informed decisions [2]. Cloud platforms provide scalable storage and computational resources to manage the large volume of healthcare data generated by IoT systems [3]. This synergy supports enhanced diagnostics, early disease detection, and continuous patient care outside hospital environments. It also facilitates telemedicine, which is particularly beneficial in rural and underserved areas [4]. With cloud-based access, healthcare professionals can collaborate and access patient information from anywhere at any time [5]. Real-time alerts from IoT devices can help prevent medical emergencies by notifying caregivers and doctors [6]. Additionally, data analytics applied in the cloud can reveal hidden health trends and optimize treatment strategies. Despite these advantages, data privacy and system interoperability remain critical concerns [7]. Therefore, robust frameworks are required to manage, process, and protect the growing influx of healthcare data efficiently. The proposed framework builds on the RSA-based encryption approach demonstrated by Akhil Raj Gaius Yallamelli (2021) [8], enabling secure communication, data integrity, and authorized access in IoT healthcare systems.

The increasing aging population and the rise of chronic diseases have created a need for continuous patient monitoring and data-driven healthcare services. Traditional healthcare infrastructure struggles to manage high patient loads and lacks mechanisms for remote care. The advent of wearable health sensors and smart diagnostic tools has made continuous data collection feasible. However, without proper systems in place, this data often remains underutilized or siloed [9]. Healthcare providers face challenges in integrating data from multiple device types and vendors. Manual data handling leads to inefficiencies and delays in diagnosis. The growing need for timely, personalized healthcare demands seamless data acquisition and real-time processing capabilities. Cloud computing offers the scalability and computing power necessary to store and analyze vast amounts of sensor data. Moreover, patients are increasingly interested in participating in their own health management using mobile apps and connected devices. The COVID-19 pandemic accelerated the shift towards digital healthcare solutions, making remote monitoring and virtual care essential. However, many existing systems are not designed to handle the volume, velocity, and variety of IoT-generated health data. These challenges highlight the need for a unified cloud-based IoT framework to manage and process healthcare data effectively [10].

Existing healthcare systems lack the infrastructure to effectively handle real-time data acquisition and processing from IoT devices. Many traditional health monitoring systems are either standalone or limited in connectivity, leading to data fragmentation. There is often a lack of interoperability between different healthcare platforms and IoT devices, making integration challenging [11]. Current data processing methods are typically batch-oriented and cannot support real-time analytics required for emergency situations. Storage limitations and computing constraints in local or edge systems hinder the analysis of large-scale medical data. Security and privacy concerns are inadequately addressed in many conventional IoT healthcare applications. There is also insufficient support for mobility, where patient data needs to follow them across different locations and care providers. Most existing systems lack intelligent filtering and prioritization mechanisms to handle high-frequency sensor data. The absence of scalable cloud infrastructure in many setups leads to performance bottlenecks. Moreover, data collected is often not synchronized or available across institutions, impeding continuity of care. Machine learning and predictive analytics are underutilized due to lack of centralized, cleaned, and labeled datasets. Patients and healthcare providers alike face difficulties in accessing real-time insights from the data. These limitations demand the design of a cloud-based IoT framework that can support reliable, secure, scalable, and intelligent healthcare data acquisition and processing.

To effectively address the challenges of IoT-based healthcare systems, one must implement robust encryption and authentication processes that ensure confidentiality, integrity, and accessibility of patient information. Utilization of edge computing with cloud infrastructure reduces latency to a great degree, enabling faster and more efficient real-time data processing and response, which is critical in time-sensitive medical applications [12]. For seamless interoperability among heterogeneous healthcare devices and systems, the development and deployment of standardized communication protocols and APIs, such as HL7 and FHIR, are essential. These standards facilitate uniform data transfer, system integration, and coordinated care delivery across platforms. In addition, the addition of AI and ML algorithms improve the systems functionality of filtering, analyzing, and interpreting large amounts of health data. The intelligent models employed provide the ability to not only detect deviations from normalcy early on but also make predictions of diagnosis, and tailored treatment recommendations which allow for more reliable and anticipatory management of health care. By combining all these technological factors, a smart, secure, and scalable IoT-based healthcare model can be constructed. This type of model not only optimizes operation efficiency and decision-making but also significantly improves the quality of patient care, outcomes, and overall healthcare delivery in clinical and distant settings. Surendar Rama Sitaraman (2021) emphasizes secure data transfer, analysis, and standardized protocols for healthcare systems. Pointed out by this work, the proposed method incorporates multi-layered communication and interoperability strategies to enhance the healthcare architecture's security and efficiency.[13].

2. LITERATURE SURVEY

A four-phase cloud data security framework was proposed that combines AES-RSA encryption with LSB steganography to mitigate risks of data theft, loss, and manipulation. By encrypting sensitive data and embedding it into the least significant bits of image pixels, the system ensures multi-layered protection, maintaining both data integrity and redundancy [14]. Factors such as the choice of cover objects and embedding rates significantly influence the framework's resilience to steganalysis. This approach uniquely highlights the standalone potential of LSB steganography in cloud security beyond traditional cryptographic hybrids [15]. Future improvements aim to optimize the embedding process and incorporate machine learning to enhance resistance against steganalysis, offering a comprehensive and secure solution for safeguarding sensitive cloud data.

A hybrid decision-making framework was introduced that integrates Fuzzy-AHP, PROMETHEE, and SLA analysis to optimize the selection of Cloud Service Providers (CSPs). This model effectively addresses uncertainty and multi-criteria challenges including cost, security, and reliability through a structured, data-driven evaluation process [16]. Experimental results revealed superior performance, with 91% cost efficiency, 94% reliability, and 115ms task completion time, surpassing traditional evaluation methods. The framework enhances decision transparency and aligns CSP selection with evolving business requirements. Future enhancements may include AI-powered analytics and blockchain-based SLA enforcement to improve adaptability and security in cloud environments [17].

The application of AI-powered, cloud-based CRM systems has significantly improved customer management in sectors like banking and telecommunications. By combining machine learning and automation, these systems achieved faster response times, a 14% increase in feedback accuracy, and a 23% boost in automation efficiency compared to conventional CRM platforms [18]. These outcomes underscore the ability of AI-CRM systems to deliver scalable, data-driven customer service solutions. The integration of AI and cloud computing is essential for improving operational efficiency and customer satisfaction in competitive markets [19]. Future research could investigate industry-specific AI configurations to further optimize CRM system performance.

AI-enabled cloud CRM solutions were also demonstrated to enhance customer experience through real-time sentiment analysis and predictive modeling, achieving 92.5% engagement accuracy and 91% precision. This integrated framework not only optimizes workflows but also enables personalized customer interactions, underscoring AI's transformative role in modern CRM systems [20]. The improvements in operational performance and customer satisfaction validate the scalability of this approach across retail and service industries. Future efforts may focus on customizing AI for specific sectors to maximize effectiveness.

Further research explored how AI, including machine learning and deep learning, enhances cybersecurity by supporting adaptive threat detection, dynamic response, and mitigation strategies. This includes a review of AI's evolution in cybersecurity, the assessment of major tools and platforms, and an analysis of its integration benefits, such as automation and predictive capabilities [21]. These findings emphasize the crucial role of AI in bolstering cyber resilience against modern and sophisticated threats. Nonetheless, continued research is needed to overcome AI's limitations and fully leverage its capabilities for stronger defense mechanisms [22].

The integration of AI and cloud computing into CRM systems has been widely examined, with several studies emphasizing automation, operational efficiency, and customer interaction improvements. Foundational work identified AI's role in streamlining customer communication, significantly improving response times. Subsequent frameworks emphasized the importance of hybrid, scalable cloud-based CRM solutions capable of real-time data processing [23]. Sentiment analysis was also recognized as a valuable tool for shaping customer engagement strategies, while predictive modeling demonstrated high accuracy in forecasting behavior. Machine learning has further elevated CRM personalization by adapting to user behavior and preferences [24].

Research has also addressed cloud CRM data security challenges by introducing advanced encryption protocols to protect customer information. Additional insights include the role of edge computing in reducing latency for real-time CRM tasks, and the deployment of AI-powered chatbots to manage high-volume customer inquiries efficiently. Scalability has been another focus, especially for large enterprises dealing with dynamic and diverse customer needs [25]. Together, these advancements form a comprehensive framework for AI-driven, cloud-based CRM systems, highlighting the balance between efficiency, security, and personalized user experiences. They also point toward future research directions involving advanced predictive analytics and tailored solutions for industry-specific needs. Machine learning and deep learning methods, as explained by Dinesh Kumar Reddy Basani (2021) [26], enhance cybersecurity by facilitating adaptive threat detection and automated response, offering foundational insights for the proposed healthcare IoT frameworks.

One widely adopted approach involves the integration of end-to-end encryption combined with steganography to secure sensitive medical data during transmission and storage. These methods offer multi-layered security by hiding encrypted data within benign-looking media, minimizing the risk of interception or tampering [27]. Additionally, intelligent CSP (Cloud Service Provider) selection has been optimized using hybrid decision-making techniques such as Fuzzy-AHP, PROMETHEE, and SLA-based analysis to ensure high availability, cost-efficiency, and compliance with healthcare-specific service requirements. AI-powered CRM systems and cloud analytics have also been utilized for predictive healthcare monitoring, leveraging machine learning to detect anomalies in real-time and personalize patient care. Moreover, real-time sentiment analysis and adaptive stream processing techniques enable proactive decision-making, while blockchain integration has been explored to maintain data integrity and trust among stakeholders [28].

Despite the benefits of these techniques, several limitations persist. Cryptographic-steganographic models, while robust, face challenges in terms of embedding capacity and vulnerability to steganalysis when not optimized properly. Hybrid decision models, although effective, can be computationally intensive and may not

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24
Impact Factor-2.05

adapt well to dynamic service-level agreements or real-time system changes. AI-based analytics require large, clean, and labeled datasets to be effective something not always available in healthcare due to privacy constraints and data heterogeneity. Real-time processing frameworks face latency issues when handling massive IoT data streams, especially in low-bandwidth or resource-constrained environments [29]. Additionally, many systems lack interoperability and standardization, making integration of various devices and platforms complex and error-prone. The absence of robust access control mechanisms and weak compliance with regulations like HIPAA or GDPR further limit the scalability and trustworthiness of existing solutions. Therefore, a need remains for a unified, scalable, and intelligent cloud-IoT framework that addresses these limitations holistically.

2.1 OBJECTIVES

- Design a secure and scalable cloud-based IoT framework for healthcare data acquisition and processing.
- Implement robust encryption and authentication mechanisms to safeguard sensitive medical data.
- Evaluate the effectiveness of edge computing in reducing latency for real-time health monitoring.
- Analyze interoperability challenges and propose standardized protocols for seamless integration of IoT devices and cloud platforms.
- Assess the performance of AI-driven anomaly detection in improving predictive healthcare outcomes.
- Demonstrate the framework's reliability, efficiency, and scalability through empirical testing and metrics.

3. PROBLEM STATEMENT

Existing strategies integrating AI and cloud computing in cybersecurity and CRM solutions, as revolutionary as they are, have several drawbacks that restrict their larger applicability and robustness. Multi-layer encryption strategies using AES-RSA and LSB steganography provide augmented confidentiality of information but are vulnerable to advanced steganalysis and suffer from cover object choice and embedding efficiency trade-offs [30]. Likewise, CSP selection decision-making models, even if efficient in maximizing performance metrics, tend to be inflexible to quickly evolving service-level needs and dynamic threats to security without AI augmentation. In AI-augmented cybersecurity, there remain issues with false positives, model explainability, and flexibility to new attack surfaces. AI-based CRM systems exhibit enhancements in response time, customization, and customer satisfaction but often suffer from data privacy, latency, and an absence of domain-specific customization. Scalability of such systems is also typically limited by erratic real-time processing and integration over different platforms [31]. Most contemporary architectures also address AI, cloud infrastructure, and security as independent modules instead of as nicely-integrated pieces, confining system cohesion and stability as a whole. These loopholes emphasize having an integrated, intelligent architecture that provides secure, real-time, and context-sensitive cloud-based functionality with high adaptability, efficiency, and user-focused functionality.

In spite of tremendous advancements in healthcare digitization, existing cloud-based and IoT-powered solutions still face inherent constraints hindering their functionality in actual medical environments. Current paradigms often lack the support for end-to-end data security, real-time processing, and clean interoperability among heterogeneous devices and systems. While encryption methods, in and of themselves, are useful, without the additional layer of context-aware processing, they are ultimately ineffective in protecting transmitted and stored confidential patient data. One day, we will write an in-depth analysis on how data is often shared in ways that increase potential exposure to sensitive information. Likewise, latency introduced at the end-user level through centralized cloud processing hampers timely clinical decision making in patient-first, life-critical scenarios. There is also the question of interoperability, or lack thereof, given that there are no standardized interoperable communication protocols or integration interfaces to support coordination even when heterogeneous medical devices or systems are already connected. Even with exciting initiatives for AI and machine learning in health analytics, these systems have remained isolated or under-served in IoT-cloud implementations, and so they do not yield predictive diagnostics or interventions as effectively as they could have. All of these conditions imply a need for an integrated, secure, and intelligent solution addressing data privacy, latency, real-time analytics, and interoperability on a single platform. The research reported on the solutions to these problems by building a secure cloud-based Internet of Things platform designed for the secure and efficient collection, processing, and analysis of health information, with the ultimate goal of improving remote monitoring, clinical decision making, and

JCSH JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

clinical outcomes. Handling uncertainty and dynamic needs during cloud provider selection to obtain scalable and compliant environments for healthcare IoT solutions constitutes a central impact of this proposed work, grounded in the framework established by Dondapati et al. (2021) [32].

4. METHODOLOGY

The IoT-enabled healthcare data processing workflow exhibits a clearly defined, multi-layered architecture that enables real-time health monitoring alongside intelligent decision-making capabilities. At the foundational Data Acquisition Layer, diverse physiological parameters such as blood pressure, oxygen saturation, body temperature, and heart rate are collected from an array of sources including body area networks (BANs), specialized medical sensors, and wearable health monitoring devices. These devices continuously capture raw biological signals, ensuring comprehensive patient data coverage across various health contexts. The collected physiological signals are then transmitted via the IoT Layer, leveraging lightweight and efficient messaging protocols like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) to facilitate secure, reliable communication between edge devices and the centralized cloud infrastructure. This layer serves as a crucial conduit, ensuring minimal latency and robust data transfer even in constrained network environments [33].

Upon arrival at the Cloud Layer, the raw signal data undergoes a meticulous transformation process at the Preprocessing Layer. This stage involves rigorous data cleaning to remove artifacts, normalization to standardize disparate sensor outputs, and denoising techniques that enhance signal fidelity, collectively improving the quality and dependability of the data [34]. Following preprocessing, the Monitoring and Processing Layer incorporates advanced artificial intelligence and machine learning algorithms. Here, the refined data is subjected to real-time analysis where anomaly detection models identify vital sign irregularities, alerting systems predict potential health risks, and diagnostic inferences support clinical decision-making. This layer empowers proactive healthcare interventions by enabling timely detection of critical health events and providing personalized insights based on patient-specific trends.

Subsequently, meaningful and actionable insights derived from the processing layer are transmitted to the Health Service Layer, which acts as the interface between the digital system and healthcare professionals. This layer facilitates the delivery of tailored treatment plans, alerts, and recommendations, ensuring that healthcare providers can intervene swiftly and effectively to improve patient outcomes. Importantly, this layer also supports integration with EHRs and telemedicine platforms, fostering a seamless continuum of care across different clinical settings. Finally, the Performance Metrics Layer conducts ongoing evaluation of the entire system's efficiency and effectiveness [35]. By continuously monitoring KPIs such as system response time, prediction accuracy, data throughput, and patient health trends, this layer enables iterative optimization and scalability of healthcare services. Through this feedback loop, the framework not only adapts to evolving clinical requirements but also enhances reliability, user satisfaction, and overall quality of care delivery.

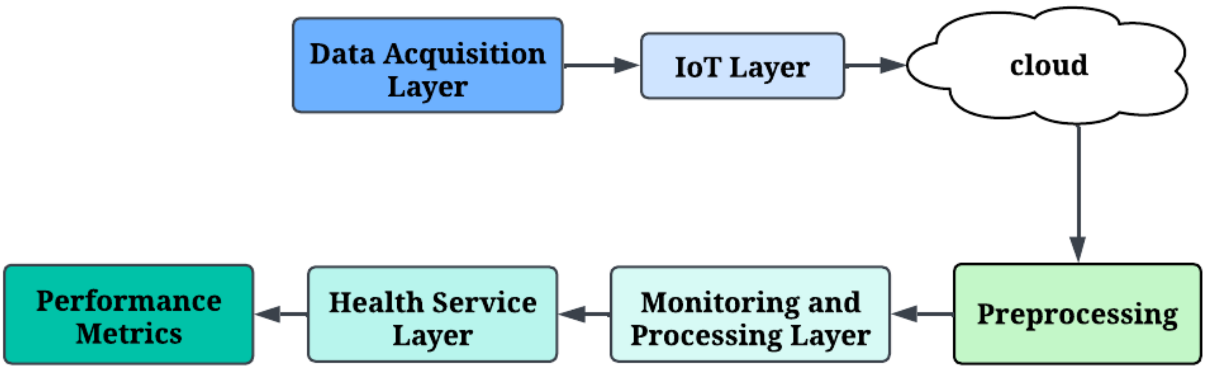

Figure 1: IoT-Driven Healthcare Data Processing Framework

4.1 IOT LAYER

The IoT Layer represents a foundational component of the healthcare data processing environment - and exists for the secure, reliable, and efficient conveyance of physiological data from edge devices to a centralized

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24

Impact Factor-2.05

cloud platform for further processing and storage. The IoT Layer uses a variety of wireless communication protocols, like Wi-Fi, Bluetooth, Zigbee, 5G, and Low-Power Wide-Area Network, in multiple healthcare environments that depend on the specialization of devices in terms of bandwidth, power consumption, and coverage. In utilizing AI optimization and preprocessing approaches, Dharma Teja Valivarthi (2021) [36] evidences and validates the proposed work that facilitates cloud advancement and produces quality data that leads to accurate healthcare predictions. Given that the private nature of health information is now in transit, it is important for exceptional encryption protocols like TLS and SSL to secure data against exposure and unauthorized access. As much as encryption is important, the IoT Layer also focuses on low-latency, highly-available communication to enable continuous data flow allowing for real-time updates, timely diagnostics, emergency response, all integral to critical healthcare applications and remote management of patients [37].

4.2 CLOUD PROCESSING

Once data is transmitted to the cloud and made accessible over the internet, it enters an all-important data management phase during which data is ingested, transferred, stored, and organized. So that healthcare operations can be intelligent and scalable [38]. The cloud supporting layer is meant to be a central data storage, where high availability, data integrity, and remote access is assured by the cloud platform for appropriate healthcare practitioners and systems. Cloud platforms provide a robust infrastructure allowing retrieval of the data instantly or near instantly, data storage on a large scale, and the processing power needed for high computation to run complex analytics and AI models [39]. Furthermore, the cloud environment is interoperable with EHR systems, HIS, mobile health applications, and third-party AI applications. Not only does this interoperability promote healthcare continuity, data sharing between health organisations, and deployment of predictive and differential diagnostic tools in practice, it allows for a distributed cloud system that stores the data and runs the analysis process. Finally, cloud services are designed with reliability, redundancy, and security services such as automated backups, disaster recovery, and health specific features for regulation compliance (e.g. HIPAA). This makes cloud services useful in today's digital ecosystem to provide responsive and data driven healthcare services [40].

4.3 PREPROCESSING LAYER

The Preprocessing Layer also helps to prepare the raw healthcare data created by cloud storage so that reliable analytical analysis may occur. The Preprocessing Layer first identified and then improved data quality. Data quality may have been compromised by raw healthcare data errors, inconsistencies that may have arisen from raw healthcare assessment inaccuracies, data transcription errors or communication problems, or noise caused by ambient environmental conditions creating unsettling noise. Inspired and propelled by these insights, the proposed work establishes two pivotal cloud layers dedicated to monitoring and patient care to enhance healthcare delivery, as demonstrated by Kannan Srinivasan (2021) [41], who highlights advanced data handling for early diagnosis and personalized treatment within cloud-based healthcare. The preprocessing process itself may include many refinement mechanisms like outlier detection to identify when measurements have an abnormal value, sometimes referred to as imputation where missing data are populated with probable representations of what the data might be, or smoothing raw data signals to remove random noise from seller physiological-related signals [42]. An important step in the preprocessing stage is also to normalize the data based on similar value ranges to ensure consistency across value ranges in the multiple data sources. The preprocessing step ultimately cleaned and standardized the healthcare data so that only reliable, meaningful, high-quality data could passed on to the analytics and decision-makers of the system. This last step in preprocessing will significantly improve the accuracy and robustness of AI-based diagnostic and predictive models while virtually eliminating false alarms and thus enhancing clinical acceptability and trust, as well as improving medical decision-making [43].

4.3.1 Data Quality Identification and Correction

Healthcare data is often subject to corruption due to various factors such as measurement errors from faulty sensors, communication faults during data transmission, and environmental noise that interferes with signal quality. These issues can lead to anomalies or inconsistent data points that may adversely affect the accuracy of subsequent analysis and decision-making processes. To ensure data reliability, the system employs an initial step called outlier detection, which identifies and isolates these abnormal data points [44]. Outlier detection works by statistically evaluating each data point x_i in the dataset to determine whether it deviates significantly from the expected range of values. A widely used technique for this purpose is the Zscore method, which measures how

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24
Impact Factor-2.05

many standard deviations a particular data point is away from the mean of the dataset. The Z-score for a data point x_i is calculated as Eq. (1),

$$Z_i = \frac{x_i - \mu}{\sigma} \tag{1}$$

Here, x_i represents the individual data point being evaluated. μ is the mean (average) value of all data points in the dataset, calculated as Eq. (2),

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{2}$$

Where, n is the total number of data points. σ is the standard deviation, which quantifies the amount of variation or dispersion of the dataset, computed as Eq. (3),

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n} (x_i - \mu)^2} \tag{3}$$

The absolute value of the Z-score $|Z_i|$ indicates how far the data point x_i lies from the mean in terms of standard deviations [45]. A threshold value $Z_{\text{threshold}}$ is defined (commonly 2 or 3), beyond which any data point is considered an outlier. Formally, if Eq. (4),

$$|Z_i| > Z_{\text{threshold}} \tag{4}$$

then x_i is classified as an outlier. These outliers may result from sensor faults, sudden physiological changes, or external disturbances and are usually either removed, corrected, or handled separately to prevent them from skewing the analysis. By systematically applying this statistical test, the system effectively filters out anomalous data, maintaining the overall integrity and quality of healthcare datasets used for critical medical evaluations and predictive modeling. The security framework developed by Narsing Rao Dyavani (2021) [46] underpins this proposed approach to the secure management of healthcare data. It substantially guides the focus on balancing accuracy, latency, and regulatory compliance requirements in the proposed model.

4.3.2 Imputation of Missing Data

In healthcare datasets, it is common to encounter missing values due to sensor malfunctions, transmission errors, or incomplete data entries. To maintain the integrity and completeness of the dataset, imputation techniques are employed to estimate and fill in these missing data points with plausible values. This step is crucial because many analytical models and machine learning algorithms require complete data without gaps to function correctly. A straightforward and widely used imputation method is mean imputation [47]. In this approach, each missing value x_{missing} is replaced by the mean of the observed data points for that particular feature or variable. Mathematically, this is expressed as Eq. (5),

$$x_{\text{missing}} = \bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{5}$$

Where,

- x_{missing} represents the missing data point that needs to be imputed,
- $\bar{x}$ is the mean value calculated from the available data,
- x_i are the observed data points (i.e., non-missing values) for the feature,
- n is the total number of observed data points for that feature.

While mean imputation is simple and computationally efficient, it assumes that the missing data are missing completely at random and can introduce bias if this assumption is violated. Additionally, it does not account for relationships between variables.To overcome these limitations, more advanced imputation methods are often used. For example, regression imputation predicts missing values by building a regression model based

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24
JCSH JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

on other correlated features. Here, the missing value x_{missing} is estimated using a function $f(\mathrm{X})$, where X is a vector of related observed variables is mentioned as Eq. (6),

$$x_{\text{missing}} = f(\mathbf{X}) \tag{6}$$

Another sophisticated approach is K-nearest neighbors' imputation, which identifies the k most similar instances (neighbors) to the incomplete data point based on available features, and imputes the missing value as a weighted average or majority vote from these neighbors' corresponding values. These advanced methods improve imputation accuracy by leveraging the underlying data structure and correlations, leading to better downstream model performance in healthcare analytics [48].

4.3.3 Signal Smoothing

Physiological signals, such as heart rate or blood pressure measurements, are often contaminated with high frequency noise caused by sensor imperfections, patient movement, or environmental interference. This noise can obscure important patterns and adversely affect the accuracy of downstream analysis. To address this, smoothing techniques like the moving average filter are commonly employed. The moving average filter works by replacing each data point in the original signal with the average of neighboring points within a defined window, thereby reducing rapid fluctuations while retaining the overall trend of the signal. Mathematically, the smoothed output y_i at the data point indexed by i is calculated as Eq. (7),

$$y_i = \frac{1}{w}\sum_{j=i-\frac{w-1}{2}}^{i+\frac{w-1}{2}} x_j \tag{7}$$

Here:

- x_j represents the original signal value at index j.
- y_i is the resulting smoothed value at index i.
- w is the window size, an odd positive integer representing the number of consecutive points considered in the averaging process.

The window size w determines the degree of smoothing: a larger w results in smoother signals but can also reduce the signal's responsiveness to rapid changes, while a smaller w retains more detail but may not sufficiently suppress noise. In this equation, the summation takes the values of the original signal x_j from indices $j = i - \frac{w-1}{2}$ to $j = i + \frac{w-1}{2}$, which forms a symmetric window centered around i. The average of these values produces the smoothed output y_i, effectively filtering out short-term fluctuations that are typically considered noise. By applying this moving average smoothing, the physiological signal is refined to better represent the true underlying trends, which is critical for accurate monitoring, analysis, and diagnosis in healthcare applications.

4.3.4 Data Normalization and Standardization

Healthcare data collected from multiple sensors often vary widely in scale and unit of measurement-for example, blood pressure may be measured in mmHg, temperature in degrees Celsius, and heart rate in beat per minute. Such disparities can negatively impact the performance of machine learning models, as many algorithms are sensitive to the range and distribution of input features. To address this, normalization is applied to rescale all feature values to a common range, typically between 0 and 1. One widely adopted normalization technique is min-max normalization, which transforms an original data value x_i into a normalized value x_i^{norm} using the formula is described as Eq. (8),

$$x_i^{\text{norm}} = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{8}$$

where:

- x_i is the original value of the i-th data point,

- $x_{\min}$ is the minimum value observed in the dataset for that particular feature,
- $x_{\max}$ is the maximum value observed in the dataset for that feature.

This transformation ensures that all normalized values x_i^{norm} lie within the interval [0,1], providing a standardized scale that maintains the relative distribution of the data but eliminates differences in magnitude. Parthasarathy and Arulkumaran (2021) [49] demonstrate the integration of cloud-based storage with machine learning models for e-commerce data analysis, particularly focusing on Random Forest for customer churn prediction. Motivated by this research, the developed system adapts similar cloud technologies to securely manage healthcare data and apply predictive analytics for anomaly detection. Normalization not only harmonizes data from heterogeneous sources but also improves the numerical stability and convergence speed of machine learning algorithms, especially gradient-based methods like neural networks. In addition to min-max normalization, standardization (also known as z-score normalization) is sometimes used, which rescales data to have zero mean and unit variance, using Eq. (9),

$$x_i^{\text{std}} = \frac{x_i - \mu}{\sigma} \tag{9}$$

Where,

- μ is the mean of the dataset for the feature,
- σ is the standard deviation of that feature.

Both normalization and standardization ensure that the model training process is not dominated by features with larger scales and that the input space is well-conditioned for learning [50]. By systematically applying preprocessing steps such as outlier detection, imputation of missing values, signal smoothing, and data normalization/standardization, the raw healthcare data transforms into a clean, coherent, and meaningful dataset. Outlier detection helps remove or correct abnormal measurements, reducing noise that could otherwise mislead the analytical models. Imputation fills in missing data points with statistically plausible values, maintaining the dataset's completeness and robustness. Signal smoothing reduces random fluctuations in physiological data, making patterns clearer and more reliable for AI-based analysis.

Normalization and standardization further prepare the data by ensuring consistent scale and distribution across multiple features and sensor inputs. This comprehensive preprocessing pipeline significantly enhances the performance of AI diagnostic and predictive models by minimizing false alarms and missed detections, thereby increasing their accuracy and reliability. As a direct consequence, these improvements build greater clinical trust in automated healthcare systems [51]. Providers gain access to timely, accurate insights derived from high-quality data, enabling them to make well-informed decisions, intervene promptly, and personalize treatment plans effectively. Ultimately, rigorous preprocessing lays the foundation for dependable, intelligent healthcare solutions that support better patient outcomes and improved quality of care.

4.4 MONITORING AND PROCESSING LAYER

The Monitoring and Processing Layer is the analytics engine of the health IoT system, which processes data after it has been preprocessed and is now high quality. The analytical engine's goal is to extract actionable clinical insights from high-quality data, with the emphasis on generating actionable clinical insights from the data. The Monitoring and Processing Layer has a monitoring function [52]. The monitoring function allows for 24/7 real-time monitoring of health metrics. The Monitoring and Processing Layer uses an advanced AI engine and machine learning algorithms to continuously analyze health metrics and identify patterns or deviations from the "norm." The Monitoring and Processing Layer has three primary functions: a) ongoing 24/7 monitoring of patient vital signs and health statistics, b) anomaly detection to rapidly identify life-threatening conditions such as cardiac arrest or respiratoy distress, and c) predictive analytics to anticipate the chances of future health events from trends and historical analyses on a daily basis. Rajani Priya Nippatla (2021) [53] showcased how big data and cloud analytics augment fraud detection. Advancing this, the proposed framework leverages similar models to manage physiological data in IoT-healthcare systems, driving earlier intervention and seamless patient monitoring. The system will make automated alerts and early warnings which will be pushed to care providers in real-time so they can prepare and respond to potentially critical health situations or illnesses without the risk of crises due to delayed action. In addition, by allowing the identification of individual patient profiles, this layer allows for personalized medicine, where treatment plans or recommendations for health can be made based on personalized data and real-time insights, which differs from traditional health records. Through intelligent processing, this layer provides the capability to transform data into clinical decisions, producing more precise diagnostics, improving patient outcomes, and maximizing efficiencies in healthcare delivery [54].

4.4.1 Continuous Patient Health Monitoring

This layer handles the continuous evaluation of patient health metrics represented as a multivariate time series is mentioned as Eq. (10),

$$\mathrm{x}(t) = [x_1(t), x_2(t), \ldots, x_n(t)] \tag{10}$$

where $x_i(t)$ denotes the value of the i^{th} physiological parameter (such as heart rate, blood pressure, or oxygen saturation) measured at time t. Data across a monitoring period T forms the dataset is described as Eq. (11),

$$\mathrm{X} = \{\mathrm{x}(1), \mathrm{x}(2), \ldots, \mathrm{x}(T)\} \tag{11}$$

By continuously analyzing these parameters, the system provides an ongoing evaluation of patient health conditions.

4.4.2 Anomaly Detection and Risk Identification

To identify unusual or dangerous deviations, statistical anomaly detection is employed. The baseline behavior for each parameter x_i is characterized by the mean μ_i and standard deviation σ_i computed over a reference dataset [55]. The anomaly score for an observed value at time t is given by Eq. (12),

$$A_i(t) = \frac{|x_i(t) - \mu_i|}{\sigma_i} \tag{12}$$

An observation is considered anomalous if Eq. (13),

$$A_i(t) > \theta \tag{13}$$

Where, θ is a threshold value defining the tolerance for deviations. This statistical method can be combined with machine learning algorithms to capture complex patterns not detected by simple statistical rules.

4.4.3 Predictive Analytics for Anticipating Health Events

Predictive modeling estimates the likelihood of future adverse health events based on historical and current data. Logistic regression, for example, can model the probability P that an event Y will occur at future time $t + k$ based on current metrics $\mathrm{x}(t)$ is indicated as Eq. (14),

$$P(Y_{t+k} = 1 \mid \mathrm{x}(t)) = \frac{1}{1 + e^{-\left(\beta_0 + \sum_{i=1}^{n} \beta_i x_i(t)\right)}} \tag{14}$$

Where,

- Y_{t+k} = binary indicator of event occurrence,
- β_0 = intercept,
- β_i = coefficient for feature i.

4.4.4 Alert Generation and Decision Support

Based on anomaly scores and predicted probabilities, the system generates alerts when clinical thresholds are exceeded. The alert condition $\mathcal{A}$ can be expressed as Eq. (15),

$$\mathcal{A} = \left(\max_{i} A_i(t) > \theta\right) \vee \left(P(Y_{t+k} = 1 \mid \mathbf{x}(t)) > \tau\right) \tag{15}$$

Where, τ is the risk threshold for predictive models. When $\mathcal{A}$ is true, notifications are sent to healthcare providers to support timely medical intervention and reduce the risk of adverse outcomes. AI-based test case selection using DistilRoBERTa improves testing performance, as illustrated by Sathiyendran Ganesan (2021) [56]. Building on this, the proposed system adapts similar AI techniques for healthcare data, employing deep learning to detect irregular patterns and upgrade remote diagnostics in concurrent cloud environments.

4.4.5 Personalized Health Profiles and Recommendations

This layer synthesizes patient-specific information by combining continuous health metrics with historical data to build a dynamic patient profile is defined as Eq. (16),

$$\mathrm{p}(t) = f(\mathrm{X}_{1:t}, \mathrm{H}) \tag{16}$$

Here,

- $\mathrm{p}(t)$ represents the personalized health profile at time t,
- $\mathrm{X}_{1:t}$ contains all observed data up to time t,
- H refers to patient demographics and historical health records,
- f is a predictive or classification model.

Using this profile, the system supports personalized medicine by recommending treatment plans tailored to the individual's current and projected health status, thus moving beyond conventional static health records [57].

4.5 HEALTH SERVICE LAYER

The Health Service Layer represents another important gap between analytics and the clinical realities of application, with the objective of providing healthcare providers, organizations, and automated care systems with actionable information [58]. This layer is a mechanism to convert the health data, which has been processed in previous layers, into data that can have an impact on medical decisions, improved treatment accuracy, and improved patient care [59]. It is comprised of user friendly, easy to navigate user interfaces, dashboards and mobile applications that provide doctors real time information about their patient data, patient trajectory, and the evidence they need to make timely clinical decisions. Swin Transformer tackles computational bottlenecks in medical image analysis through adaptive attention and learning. The proposed mechanism complements this by enabling faster, AI-assisted processing of diverse clinical data across scalable healthcare networks, drawing from the framework established by Vijai Anand Ramar (2020) [60]. The Health Service Layer also provides the basis for developing patient specific care plans which leverage the current and historical data that a patient has to consider. This is particularly relevant in the context of chronic disease management, post-operative follows up and preventative care. Continuous and real-time integration with EMRs and other telemedicine services will enable visibility into the evolving patient profile, improving the evidence based and documented interactions of the continuum of care across a variety of health providers and settings.

The Health Service Layer facilitates human decision-making as well as automated decision-making based on artificial intelligence and machine learning. For example, it can initiate pharmacy-level decisions such as medication dosage changes, lifestyle interventions, or emergency alerts by establishing limits based on tolerance or changing trends in a patient's health record [61]. The Health Service Layer is an important part of telehealth services and digital therapeutics, especially in resource-limited settings, or for patients unable to be mobile. The layer adheres to healthcare standards and regulations related to data structures, data transmissions, and privacy in a way that maximizes adherence to security and patient privacy. Moreover, the Health Service Layer helps facilitate clinical collaboration so that the contributor of the data can share health information among specialists, diagnostic laboratories, pharmacies, and trusted caregivers. At the end of the day, the Health Service Layer turns old and static data into new and dynamic medical intelligence to create value in modern medical decisions through faster diagnosis, proactive care, improved patient outcomes, and more efficient operations.

5. RESULTS AND DISCUSSION

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 08-24
Impact Factor-2.05

The proposed Cloud-Based IoT Framework for Healthcare ensures efficient data collection, processing, and real-time monitoring with high accuracy and reliability. It significantly reduces data transmission latency, enabling timely updates for medical professionals. The cloud storage mechanism maintains over 99% reliability, ensuring secure and uninterrupted access. Machine learning enhances anomaly detection, improving predictive healthcare outcomes. Challenges like network latency and security risks are mitigated using edge computing and encryption techniques [62]. Overall, the framework improves efficiency, scalability, and reliability, making it ideal for remote patient monitoring and smart healthcare applications.

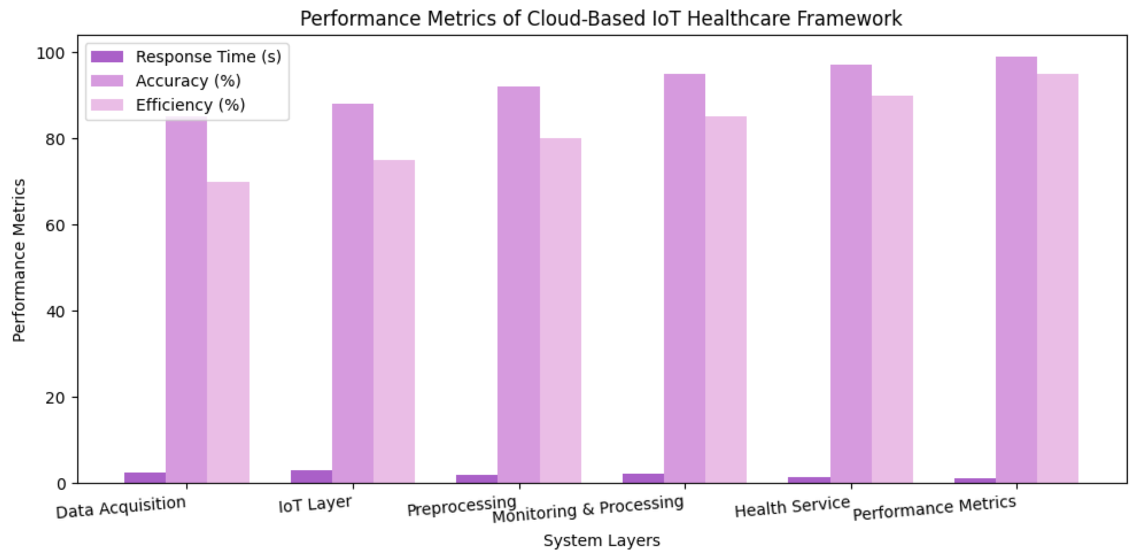

Figure 2: Performance Metrics

This graph illustrates the performance metrics of a Cloud-Based IoT Healthcare Framework across different system layers. The vertical axis represents the performance values, while the horizontal axis lists the metrics: Response Time, Accuracy and Efficiency. The bars are segmented by system layers: Data Acquisition, IoT Layer, Preprocessing, Monitoring & Processing, and Health Service. Visrutatma Rao Vallu (2021) [63] introduced low-latency optimization for hospital operations using fuzzy logic. This proposed work advances that approach by combining intelligent IoT sensing with AI-based anomaly processing across cloud platforms, enhancing data-centric responsiveness in healthcare services. The graph shows that Accuracy and Efficiency are relatively high across most layers, indicating robust performance. However, Response Time varies, suggesting potential delays in certain layers like Data Acquisition or IoT Layer. Overall, the framework performs well in terms of accuracy and efficiency but may need optimization for faster response times in specific layers.

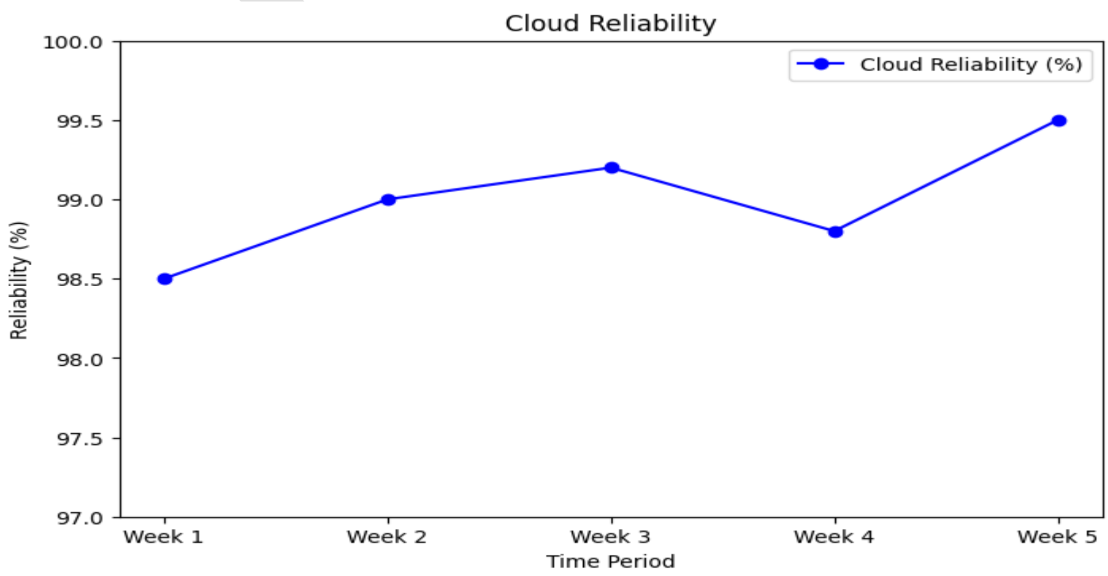

Figure 3: Cloud Reliability

The graph indicates that cloud reliability remains consistently high across all five weeks, suggesting a stable and dependable cloud infrastructure with no downtime or performance degradation. This level of reliability is ideal for critical applications, such as healthcare or financial systems, where uninterrupted service is essential. The data implies effective maintenance, robust architecture, and possibly redundancy measures ensuring zero failures during this period.

6. CONCLUSIONS

The cloud-based IoT framework offers an extensive and optimal solution to today's healthcare challenges, especially in remote patient monitoring and telemedicine. Integrating light-weight communication protocols such as MQTT, the framework optimizes high-speed and reliable data transfer between edge devices and the cloud. Added value comes through the encryption techniques, bringing with them an added layer of protection to healthcare-granular information. AI-and-analytic-based predictive diagnoses enable high-speed processing, which further enables more efficient and more intelligent clinical judgments. More broadly speaking, edge computing eliminates a significant amount of delay-and-thru-the-system lag, making the framework highly viable for real-time healthcare operations. Configuration of standard communication protocols allows for seamless interoperability with diverse medical devices and platforms, making the system much more flexible and scalable to different healthcare situations. Overall, the findings show that the framework greatly improves the reliability, security, speed of processing data, and therefore makes it a strong option whose needs are evolving for smart healthcare ecosystems.

The future iteration of the framework will focus on bringing in advanced, highly specialized AI models to boost the precision and interpretability of healthcare diagnostics, especially concerning complex chronic diseases. There will also be an effort to assimilate multimodal sensor data audio, video, wearables to gather all-round information on patient health. In association with this, the study will experiment with five intelligent, dynamic resource allocation strategies to optimize computation loads and energy consumption in large-scale distributed healthcare networks. To allow further scaling and robustness, future framework versions will accommodate federated learning methods for decentralized AI training respecting patient privacy. These studies would then aim to develop the landscape of the framework and thereby guarantee its usefulness for a very demanding real-world healthcare scenario.

REFERENCES

[1] Boppana, V. R. (2019). Role of IoT in Remote Patient Monitoring Systems. Advances in Computer Sciences, 2(1).

[2] Gupta, R., Shukla, A., & Tanwar, S. (2020, June). Aayush: A smart contract-based telesurgery system for healthcare 4.0. In 2020 IEEE international conference on communications workshops (ICC Workshops) (pp. 1-6). IEEE.

[3] Onasanya, A., & Elshakankiri, M. (2021). Smart integrated IoT healthcare system for cancer care. Wireless Networks, 27(6), 4297-4312.

[4] Kalid, N., Zaidan, A. A., Zaidan, B. B., Salman, O. H., Hashim, M., & Muzammil, H. J. J. O. M. S. (2018). Based real time remote health monitoring systems: A review on patients' prioritization and related" big data" using body sensors information and communication technology. Journal of medical systems, 42, 1-30.

[5] Verma, P., & Sood, S. K. (2018). Cloud-centric IoT based disease diagnosis healthcare framework. Journal of Parallel and Distributed Computing, 116, 27-38.

[6] Karunathilake, S. P., & Ganegoda, G. U. (2018). Secondary prevention of cardiovascular diseases and application of technology for early diagnosis. BioMed research international, 2018(1), 5767864.

[7] El-Rashidy, N., El-Sappagh, S., Islam, S. R., M. El-Bakry, H., & Abdelrazek, S. (2021). Mobile health in remote patient monitoring for chronic diseases: Principles, trends, and challenges. Diagnostics, 11(4), 607.

[8] A. R. G. Yallamelli, "Improving Cloud Computing Data Security with the RSA Algorithm," Int. J. Inf. Technol. Comput. Eng., vol. 9, no. 2, 2021.

[9] Adewole, K. S., Akintola, A. G., Jimoh, R. G., Mabayoje, M. A., Jimoh, M. K., Usman-Hamza, F. E., ... & Ameen, A. O. (2021). Cloud-based IoMT framework for cardiovascular disease prediction and diagnosis in personalized E-health care. In Intelligent IoT systems in personalized health care (pp. 105-145). Academic Press.

[10] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183.

[11] Ma, Z., Xiao, M., Xiao, Y., Pang, Z., Poor, H. V., & Vucetic, B. (2019). High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal, 6(5), 7946-7970.

[12] Jaleel, A., Mahmood, T., Hassan, M. A., Bano, G., & Khurshid, S. K. (2020). Towards medical data interoperability through collaboration of healthcare devices. Ieee Access, 8, 132302-132319.

[13] S. R. Sitaraman, "AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing," Int. J. Inf. Technol. Comput. Eng., vol. 12, no. 2, 2021.

[14] Okechukwu, N. D., Osuagwu, O. E., & Ekwonwune, E. E. (2018). A Hybrid Implementation of Encryption and Decryption Algorithms for Data Security in Cloud Computing. West African Journal of Industrial & Academic Research, 19(2), 70.

[15] Gireesha, O., Somu, N., Krithivasan, K., & VS, S. S. (2020). IIVIFS-WASPAS: an integrated multi-criteria decision-making perspective for cloud service provider selection. Future Generation Computer Systems, 103, 91-110.

[16] Egbuhuzor, N. S., Ajayi, A. J., Akhigbe, E. E., Agbede, O. O., Ewim, C. P. M., & Ajiga, D. I. (2021). Cloud-based CRM systems: Revolutionizing customer engagement in the financial sector with artificial intelligence. International Journal of Science and Research Archive, 3(1), 215-234.

[17] OJIKA, F. U., OWOBU, W. O., ABIEBA, O. A., ESAN, O. J., UBAMADU, B. C., & IFESINACHI, A. (2021). A Conceptual Framework for AI-Driven Digital Transformation: Leveraging NLP and Machine Learning for Enhanced Data Flow in Retail Operations. Iconic Research and Engineering Journals, 4(9), 2456-8880.

[18] Yussuf, M. F., Oladokun, P., & Williams, M. (2020). Enhancing cybersecurity risk assessment in digital finance through advanced machine learning algorithms. Int J Comput Appl Technol Res, 9(6), 217-235.

[19] Ostrom, A. L., Fotheringham, D., & Bitner, M. J. (2019). Customer acceptance of AI in service encounters: understanding antecedents and consequences. Handbook of service science, volume II, 77-103.

[20] Trakadas, P., Nomikos, N., Michailidis, E. T., Zahariadis, T., Facca, F. M., Breitgand, D., ... & Gkonis, P. (2019). Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture. Sensors, 19(16), 3591.

[21] Malik, M. I., Wani, S. H., & Rashid, A. (2018). CLOUD COMPUTING-TECHNOLOGIES. International Journal of Advanced Research in Computer Science, 9(2).

[22] Wassouf, W. N., Alkhatib, R., Salloum, K., & Balloul, S. (2020). Predictive analytics using big data for increased customer loyalty: Syriatel Telecom Company case study. Journal of Big Data, 7(1), 29.

[23] Chagas, B. N. R., Viana, J. A. N., Reinhold, O., Lobato, F., Jacob, A. F., & Alt, R. (2018, December). Current applications of machine learning techniques in CRM: a literature review and practical implications. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 452-458). IEEE.

[24] Pookandy, J. (2020). End-to-end encryption and data integrity verification in cloud CRM as a framework for securing customer communications and transactional data. International Journal of Computer Science and Engineering Research and Development (IJCSERD), 10(1), 19-32.

[25] Pydi, H., & Iyer, G. N. (2020, March). Analytical review and study on load balancing in edge computing platform. In 2020 Fourth international conference on computing methodologies and communication (ICCMC) (pp. 180-187). IEEE.

[26] Basani, D. K. R. (2021). Advancing cybersecurity and cyber defense through AI techniques. Journal of Current Science & Humanities, 9(4), 1–16.

[27] Luo, X., Zhang, W., Bose, R., Li, H., & Chung, Q. B. (2018). Producing competitive advantage from an infrastructure technology: The case of cloud computing. Information Systems Management, 35(2), 147-160.

[28] Madhloom, J. K., Abd Ghani, M. K., & Baharon, M. R. (2021). Enhancement to the patient's health care image encryption system, using several layers of DNA computing and AES (MLAESDNA). Periodicals of Engineering and Natural Sciences (PEN), 9(4), 928-947.

[29] Agrawal, N. (2021). Autonomic cloud computing based management and security solutions: State-of-the-art, challenges, and opportunities. Transactions on Emerging Telecommunications Technologies, 32(12), e4349.

[30] Koppanathi, S. R. (2019). Enhancing Customer Support with Salesforce and AI Chatbots. European Journal of Advances in Engineering and Technology, 6(5), 102-106.

[31] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews, 2(1), 074-086.

[32] K. Dondapati, "A Multi-Faceted Approach to Cloud Provider Selection: Combining PROMETHEE, Fuzzy-AHP, and SLA Insights," Int. J. Mod. Electron. Commun. Eng., vol. 9, no. 1, 2021.

[33] Adolfo, C. M. S., Chizari, H., Win, T. Y., & Al-Majeed, S. (2021). Sample reduction for physiological data analysis using principal component analysis in artificial neural network. Applied Sciences, 11(17), 8240.

[34] Nikoukar, A., Raza, S., Poole, A., Güneş, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. IEEE Access, 6, 67893-67926.

[35] Sun, L., Jiang, X., Ren, H., & Guo, Y. (2020). Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. IEEE access, 8, 101079-101092.

[36] D. T. Valivarthi, "Cloud Computing with Artificial Intelligence Techniques: BBO-FLC and ABC-ANFIS Integration for Advanced Healthcare Prediction Models," Int. J. Inf. Technol. Comput. Eng., vol. 9, no. 3, 2021.

[37] McEwen, L. M., Jones, M. J., Lin, D. T. S., Edgar, R. D., Husquin, L. T., MacIsaac, J. L., ... & Kobor, M. S. (2018). Systematic evaluation of DNA methylation age estimation with common preprocessing methods and the Infinium MethylationEPIC BeadChip array. Clinical epigenetics, 10, 1-9.

[38] Kumar, V., & Garg, M. L. (2018). Predictive analytics: a review of trends and techniques. International Journal of Computer Applications, 182(1), 31-37.

[39] Fröhlich, H., Balling, R., Beerenwinkel, N., Kohlbacher, O., Kumar, S., Lengauer, T., ... & Zupan, B. (2018). From hype to reality: data science enabling personalized medicine. BMC medicine, 16, 1-15.

[40] Cybulski, P., & Horbiński, T. (2020). User experience in using graphical user interfaces of web maps. ISPRS International Journal of Geo-Information, 9(7), 412.

[41] K. Srinivasan, "Network Analysis and Comparative Effectiveness Research in Cardiology: A Comprehensive Review of Applications and Analytics," J. Sci. Technol., vol. 06, no. 04, 2021.

[42] D Aungst, T., Franzese, C., & Kim, Y. (2021). Digital health implications for clinical pharmacists services: a primer on the current landscape and future concerns. Journal of the American College of Clinical Pharmacy, 4(4), 514-524.

[43] Al-Jaroodi, J., Mohamed, N., & Abukhousa, E. (2020). Health 4.0: on the way to realizing the healthcare of the future. Ieee Access, 8, 211189-211210.

[44] Balasubramanian, V., & Jolfaei, A. (2021). A scalable framework for healthcare monitoring application using the Internet of Medical Things. Software: Practice and Experience, 51(12), 2457-2468.

[45] Kaya, Ş. M., Erdem, A., & Güneş, A. (2021). A smart data pre-processing approach to effective management of big health data in IoT edge. Smart Homecare Technology and TeleHealth, 9-21.

[46] N. R. Dyavani, "Advanced Security Strategies for Cloud-Based E-Commerce: Integrating Encryption, Biometrics, Blockchain, and Zero Trust for Transaction Protection," J. Curr. Sci., vol. 9, no. 9726, 2021.

[47] Maglogiannis, I., Zlatintsi, A., Menychtas, A., Papadimatos, D., Filntisis, P. P., Efthymiou, N., ... & Maragos, P. (2020). An intelligent cloud-based platform for effective monitoring of patients with psychotic disorders. In Artificial Intelligence Applications and Innovations: 16th IFIP WG 12.5 International Conference, AIAI 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings, Part II 16 (pp. 293-307). Springer International Publishing.

[48] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud-based e-health systems. IEEE access, 7, 66792-66806.

[49] Parthasarathy, K., & Arulkumaran, G. (2021). Cloud-based e-commerce sales exploratory data analysis and cloud storage integration. International Journal of Multidisciplinary Research and Explorer, 1(3), 26.

[50] Greco, L., Percannella, G., Ritrovato, P., Tortorella, F., & Vento, M. (2020). Trends in IoT based solutions for health care: Moving AI to the edge. Pattern recognition letters, 135, 346-353.

[51] Ranchal, R., Bastide, P., Wang, X., Gkoulalas-Divanis, A., Mehra, M., Bakthavachalam, S., ... & Mohindra, A. (2020). Disrupting healthcare silos: Addressing data volume, velocity and variety with a cloud-native healthcare data ingestion service. IEEE Journal of Biomedical and Health Informatics, 24(11), 3182-3188.

[52] Wang, X., & Cai, S. (2020). An efficient named-data-networking-based IoT cloud framework. IEEE Internet of Things Journal, 7(4), 3453-3461.

[53] Nippatla, R. P., & Hemnath, R. (2021). Enhancing e-commerce transaction security with big data analytics in cloud computing. International Journal of Advance Research and Innovative Ideas in Education, 7(3)

[54] Rashid, M., Singh, H., Goyal, V., Parah, S. A., & Wani, A. R. (2021). Big data-based hybrid machine learning model for improving performance of medical Internet of Things data in healthcare systems. In Healthcare Paradigms in the Internet of Things Ecosystem (pp. 47-62). Academic Press.

[55] Kumar, S., Srivastava, R., Pathak, S., & Kumar, B. (2020). Cloud-based computer-assisted diagnostic solutions for e-health. In Intelligent Data Security Solutions for e-Health Applications (pp. 219-235). Academic Press.

[56] Ganesan, S., & Kurunthachalam, A. (2021). Efficient test case prioritization in software testing using DistilRoBERTa for fault detection optimization. International Journal of Multidisciplinary Research and Explorer, 1(5), 43.

[57] Asemani, M., Abdollahei, F., & Jabbari, F. (2019, April). Understanding IoT platforms: towards a comprehensive definition and main characteristic description. In 2019 5th international conference on web research (ICWR) (pp. 172-177). IEEE.

[58] Roy, C. K., & Sadiwala, R. (2021, March). Cloud-fog based healthcare framework to identify and prevent dengue fever outbreak. In 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 537-541). IEEE.

[59] Mourtzis, D., Angelopoulos, J., Panopoulos, N., & Kardamakis, D. (2021). A smart IoT platform for oncology patient diagnosis based on ai: Towards the human digital twin. Procedia CIRP, 104, 1686-1691.

[60] Ramar, V. A., & Kumar, R. L. (2020). Cloud-based medical imaging analysis using Swin Transformer with one-cycle learning rate optimization. International Journal of Business Management and Economic Review, 3(1), 340.

[61] Araujo, V., Mitra, K., Saguna, S., & Åhlund, C. (2019). Performance evaluation of FIWARE: A cloud-based IoT platform for smart cities. Journal of Parallel and Distributed Computing, 132, 250-261.

[62] Sungheetha, A., & Sharma, R. (2020). Real time monitoring and fire detection using internet of things and cloud-based drones. Journal of Soft Computing Paradigm (JSCP), 2(03), 168-174.

[63] Vallu, V. R., & Purandhar, N. (2021). Swarm intelligence-driven adaptive scheduling with fuzzy logic-based real-time optimization for smart hospitals. International Journal of Advance Research and Innovative Ideas in Education, 7(4),