IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

www.ijitce.com

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 10, Issue 3, 2022

INTEGRATING IOT DEVICES WITH CLOUD HEALTHCARE SYSTEMS FOR ENHANCED DATA MANAGEMENT

Kannan Srinivasan,
Senior Software Engineer, Saiana Technologies Inc,
South Plainfield, New Jersey, USA
kannan.srini3108@gmail.com

Guman Singh Chauhan,
John Tesla Inc,
Dallas, USA
gumanc38@gmail.com

Rahul Jadon,
CarGurus Inc,
Massachusetts, USA
rahuljadon974@gmail.com

Rajababu Budda,
Senior Integration Developer,
Tata Consultancy Services, London, England
rahuljadon974@gmail.com

Venkata Surya Teja Gollapalli,
Senior System Engineer, Centene Management LLC, Tampa, Florida, USA
venkatasuryagollapalli@gmail.com

Aravindhan Kurunthachalam,
Associate Professor, School of Computing and Information Technology,
REVA University, Bangalore
Aravindhan03@gmail.com

ABSTRACT

The rapid advancements in Internet of Things-based healthcare systems have revolutionized patient monitoring by enabling continuous and data collection from various devices like heart rate monitors, blood pressure sensors, and glucose meters. However, existing systems face critical challenges such as scalability issues and inconsistent data quality, which hinder their effectiveness in applications. This paper proposes a novel framework that addresses these challenges by designing a robust framework that seamlessly integrates IoT devices with cloud healthcare systems, focusing on enhancing data management. The framework starts with data collection from IoT devices, followed by data preprocessing using k-Nearest Neighbors for handling missing values and Z-score normalization for consistent sensor data. The data is then encrypted using the ChaCha20 encryption algorithm. The encrypted data is stored in cloud storage, which facilitates scalability and efficient management of large datasets. The system's performance is evaluated based on metrics such as encryption time and latency time, with results showing encryption times increasing from 0.09 seconds to 0.25 seconds as the data size grows, and latency times ranging from 0.05 seconds to 0.35 seconds with larger data volumes. The proposed framework contributes to efficient and scalable healthcare data management, ensuring reliable and timely patient monitoring.

Keywords: IoT Data, Data Encryption, Scalability, ChaCha20, Healthcare Monitoring and Cloud Storage.

1 INTRODUCTION

The integration of IoT devices with cloud healthcare systems has revolutionized patient monitoring by enabling continuous health data collection and analysis [1]. IoT devices, such as wearables and sensors, provide valuable insights into vital signs, which can enhance personalized care and decision-making [2]. However, managing and processing this large volume of data securely and efficiently remains a significant challenge [3]. Cloud computing platforms offer a promising solution, ensuring scalability and accessibility of data, yet concerns regarding data security and latency need to be addressed [4]. The proposed framework aims to bridge these gaps, offering an efficient solution for healthcare systems [5].

Various existing methods have explored the integration of IoT with cloud healthcare systems, such as edge computing, fog computing, and cloud-based storage solutions [6]. Edge computing has been used to process data locally, reducing latency, while fog computing extends cloud capabilities to the network's edge for faster decision-making [7]. Additionally, cloud-based systems have provided scalable solutions for data storage and analysis [8]. Despite these advancements, existing methods often face limitations in ensuring data privacy, handling data processing, and providing a seamless integration between devices and cloud platforms [9]. Security vulnerabilities, high latency, and inefficient data processing remain significant drawbacks [10].

The proposed framework overcomes these challenges by combining edge computing and cloud systems in a hybrid approach, ensuring both security and processing of health data [11]. The novelty of this study lies in its integration of advanced encryption techniques for data security, health monitoring using edge devices, and seamless cloud synchronization [12] [13]. By leveraging edge computing for local data processing, the framework reduces latency and dependency on cloud resources, while maintaining high security through encryption and access control mechanisms [14]. This integrated approach provides a scalable, efficient solution for patient monitoring in healthcare systems [15].

The paper is structured as follows: Section 2 presents a literature survey, reviewing existing works. Section 3 discusses the methodology. Section 4 presents the results, including performance analysis and system evaluation. Section 5 the concludes the paper with future work.

2 LITERATURE SURVEY

Several advancements in the integration of IoT and cloud healthcare systems have been made, providing the groundwork for improving patient monitoring and healthcare delivery [16]. In the context of artificial intelligence, Crow Search Optimization (CSO) has emerged as a prominent metaheuristic algorithm for optimizing diagnostic models [17]. Grandhi demonstrated how CSO, by mimicking crows' foraging behavior, enhances the performance of deep learning models like CNNs and LSTMs. The algorithm's ability to handle complex, high-dimensional data made it particularly suitable for the healthcare domain, where data processing is critical [18]. However, while CSO contributed significantly to enhancing model accuracy and precision, it highlighted the ongoing challenge of ensuring data integration and secure processing in healthcare systems.

Further developments in AI-driven healthcare systems were examined by Panga, who explored the transformative effects of big data analytics and mobile computing [19]. The integration of AI, particularly neural networks, with mobile health (m-Health) systems was shown to optimize healthcare delivery by providing predictive models and personalized care [20]. Despite the success of these technologies, issues such as data privacy, data management, and the handling of unstructured data from wearable devices remain prevalent in the field. These gaps present significant challenges in achieving a fully optimized system for patient monitoring, calling for more refined solutions in data integration and analysis [21].

Additionally, Sareddy investigated the use of machine learning for detecting financial fraud in IoT environments, underlining the importance of integrating AI for anomaly detection [22]. While the study focused on financial fraud, the same principles of anomaly detection and machine learning models could be applied to healthcare data, especially for monitoring patient health [23]. The application of adaptive learning systems, capable of retraining models based on new data, ensures that the system evolves to detect emerging threats or issues. This study's relevance lies in its emphasis on scalability and integration, which are essential elements for building an effective IoT-cloud healthcare framework [24].

In the domain of healthcare data stream optimization, Allur highlighted the effectiveness of analytics using big data frameworks like Apache Spark and Hadoop [25]. This research illustrated how these technologies can significantly reduce data processing times, crucial for timely interventions in healthcare settings [26]. However, despite the advancements in processing, challenges persist in handling the vast amount of data produced by IoT-enabled devices and ensuring that data privacy and security are not compromised [27].

Lastly, Parthasarathy reviewed the role of predictive analytics and multi-modal AI interfaces in revolutionizing customer relationship management (CRM) systems [28]. While the study primarily focused on CRM, the methodologies discussed can be adapted for healthcare applications, particularly in improving patient engagement through AI-driven predictive models [29]. The integration of AI with multi-modal interfaces could provide a more personalized healthcare experience by analyzing various patient data sources and improving decision-making [30]. However, the research also pointed out the challenges of ethical decision-making, data privacy, and operational integration, which are directly applicable to healthcare systems dealing with sensitive patient information.

2.1 Problem Statement

While existing works have made significant strides in IoT-based healthcare systems, there are still several critical challenges that need to be addressed. These include the integration of encryption methods, many systems are still susceptible to security breaches, compromising sensitive health data [31]. As the number of IoT devices grows, scalability becomes an issue, hindering efficient data management and processing. Additionally, the quality of data collected from various devices can be inconsistent, leading to inaccuracies in patient monitoring and decision-making. The work is proposed to overcome these challenges by enhancing security, optimizing scalability, and improving data preprocessing for more reliable and accurate healthcare outcomes.

3 METHODOLOGIES

The proposed framework begins with Data Collection, where IoT-enabled devices such as heart rate monitors, blood pressure sensors, glucose meters, ECGs, and temperature sensors continuously gather patient health data. This data is then Pre-processed using k-Nearest Neighbors (k-NN) for handling missing data and Z-score Normalization to standardize the values across different sensors. The pre-processed data is then encrypted using ChaCha20 encryption to protect sensitive health information. Finally, the encrypted data is stored in Cloud Storage, ensuring scalability, accessibility, and security, enabling healthcare professionals to efficiently access and manage patient data for analysis and timely decision-making.

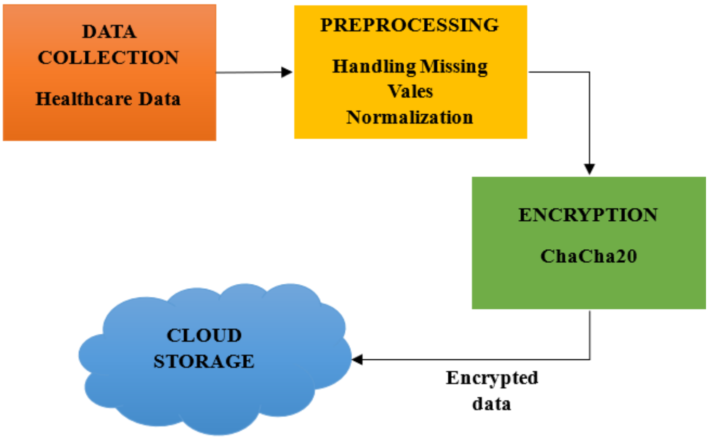

Figure 1: Workflow of IoT-based Healthcare Data Management and Encryption

3.1 Data Collection

The dataset used in the proposed framework consists of health data collected from various IoT-enabled wearable devices such as heart rate monitors, blood pressure sensors, glucose meters, ECGs, and temperature sensors. These devices continuously record vital signs like heart rate, blood pressure, glucose levels, and temperature. The dataset also includes timestamps to track when the data was recorded. The data is recorded along with timestamps, which helps in tracking the temporal changes in a patient's health metrics. This continuous, data collection forms the foundation for further preprocessing, analysis, and decision-making within the framework.

3.2 Data Preprocessing

Preprocessing in the proposed framework involves preparing the raw data collected from IoT devices to ensure it is accurate and ready for analysis.

3.2.1 Missing Data Handling

The first step is Missing Data Handling, where missing values in the dataset are addressed using the k-Nearest Neighbors (k-NN) imputation technique. This method estimates missing data based on the values of the nearest neighbors, ensuring the dataset remains complete and usable for further analysis.

3.2.2 Normalization

Next, Normalization is performed using Z-score Normalization, which standardizes the sensor data by subtracting the mean and dividing by the standard deviation. This step ensures that all data points, such as heart rate, blood pressure, and glucose levels, are on a comparable scale. Normalization is crucial for maintaining consistency across the different types of sensor data, which might otherwise vary in scale. After these preprocessing steps, the data is ready for encryption and storage in the cloud, making it accessible for analysis and decision-making.

3.3 Data Encryption

After preprocessing the data, Data Encryption is performed using ChaCha20. ChaCha20 is a stream cipher that encrypts data by generating a key stream from a 256-bit key, a 64-bit nonce, and a 32-bit counter. This key stream is then XORed with the preprocessed data to produce the encrypted ciphertext. The encryption process involves 20 rounds of operations on a 512-bit state matrix, ensuring strong security. ChaCha20 is chosen for its efficiency and robust resistance to cryptographic attacks, ensuring that sensitive health data remains protected during transmission and storage in the cloud.

Quarter Round Operation is represented as equation (1),

$$a = (a + b) \oplus \text{rotate}(a + b, 7) \tag{1}$$

This equation adds the values of a and b, then rotates the result by 7 bits and XORs it with a, applying the same operation to other pairs of words in the state matrix. This diffusion step spreads the influence of each value throughout the matrix.

Encryption (XOR with Key Stream) is expressed as equation (2),

$$\text{Ciphertext} = \text{Plaintext} \oplus \text{KeyStream} \tag{2}$$

After generating the key stream through repeated quarter rounds, this equation XORs the key stream with the plaintext to produce the ciphertext. The same process is used in reverse for decryption, making ChaCha20 a symmetric cipher.

3.4 Cloud Storage

After Data Encryption using ChaCha20, the encrypted data is stored in Cloud Storage on platforms like AWS or Microsoft Azure. These platforms provide scalable, secure storage for large volumes of IoT health data, ensuring easy access by authorized healthcare professionals. The data is stored in databases like NoSQL or Object Storage for efficient management. Cloud storage also offers high availability, redundancy, and integration with data processing tools for quick analysis. Additionally, data sharding is used to optimize access and performance.

4 RESULTS

The results section evaluates the impact of increasing data size on encryption time and latency in the proposed framework. These metrics are vital for assessing the system's efficiency and scalability. The findings highlight the importance of managing data volume for optimal performance in healthcare applications.

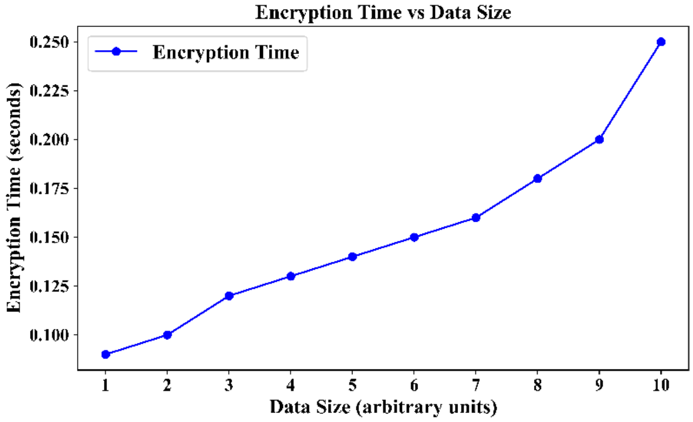

Figure 2: Encryption Time

Figure 2 shows the relationship between encryption time and data size for the ChaCha20 encryption algorithm. As the data size increases from 1 to 10 arbitrary units, the encryption time increases from 0.09 seconds to 0.25 seconds. This illustrates the typical behavior where larger datasets require more time to process and encrypt. The graph highlights the efficiency of the encryption process and how it scales with data size. It also emphasizes the need to manage data volume efficiently for applications like healthcare monitoring.

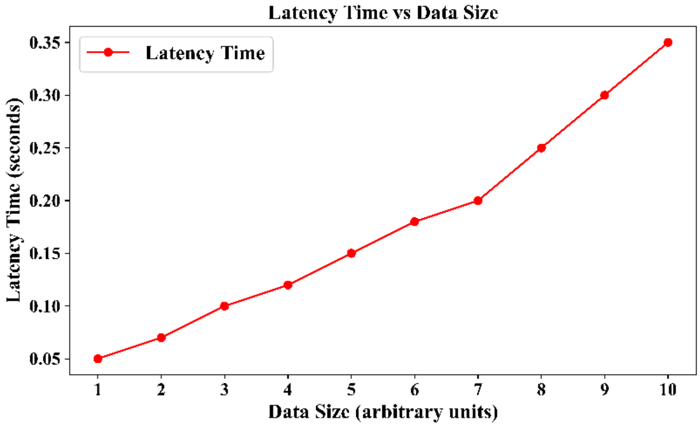

Figure 3: Latency Time and Data Size

Figure 3 depicts the relationship between latency time and data size. As the data size increases from 1 to 10 arbitrary units, the latency time gradually increases from 0.05 seconds to 0.35 seconds. This reflects the typical trend where larger data volumes lead to higher latency due to more processing time required for handling the data. The graph highlights the scalability of the system and the need to optimize latency for healthcare applications. It emphasizes the importance of managing data size to minimize delays in IoT healthcare systems.

5 CONCLUSIONS

This work aims to develop a scalable framework for healthcare monitoring using IoT devices, focusing on improving data security, scalability, and consistency. The proposed framework effectively addresses the challenges of encryption, data management, and scalability by integrating ChaCha20 encryption, cloud storage, and data preprocessing techniques. The performance evaluation showed that the encryption time increased from 0.09 seconds to 0.25 seconds as data size grew, while latency times ranged from 0.05 seconds to 0.35 seconds with increasing data volumes. These results highlight the system’s efficiency in handling growing data sizes while maintaining scalable data management. The proposed framework significantly enhances healthcare monitoring, ensuring timely interventions and management of health data. Furthermore, the system's ability to handle large datasets with minimal delay makes it suitable for IoT-based healthcare applications. Future work will focus on incorporating AI-driven predictive analytics to further enhance the accuracy of health predictions, optimizing the encryption process for faster performance, and improving the integration of the framework with other healthcare systems for greater interoperability.

REFERENCES

[1] R. L. Gudivaka, “A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography,” *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 3, pp. 90–101, Aug. 2021.

[2] D. R. Natarajan, “A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection,” *Int. J. Eng. Res. Sci. Technol.*, vol. 14, no. 4, pp. 198–213, Dec. 2018.

[3] R. P. Nippatla, “A Secure Cloud-Based Financial Analysis System for Enhancing Monte Carlo Simulations and Deep Belief Network Models Using Bulk Synchronous Parallel Processing,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 3, pp. 89–100, Jul. 2018.

[4] D. K. R. Basani, “Advancing Cybersecurity and Cyber Defense through AI Techniques”.

[5] S. Peddi, S. Narla, and D. T. Valivarthi, “Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 4, pp. 62–76, Nov. 2018.

[6] B. R. Gudivaka, “AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system,” *World J. Adv. Eng. Technol. Sci.*, vol. 2, no. 1, pp. 122–131, 2021, doi: 10.30574/wjaets.2021.2.1.0085.

[7] S. Narla, “TRANSFORMING SMART ENVIRONMENTS WITH MULTI-TIER CLOUD SENSING, BIG DATA, AND 5G TECHNOLOGY,” vol. 5, 2020.

[8] P. Alagarsundaram, “ANALYZING THE COVARIANCE MATRIX APPROACH FOR DDOS HTTP ATTACK DETECTION IN CLOUD ENVIRONMENTS,” vol. 8, no. 1, 2020.

[9] S. Peddi, “Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges,” vol. 9, no. 4, 2021.

[10] M. V. Devarajan, “ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS,” vol. 8, no. 2, 2020.

[11] R. K. M. K. Yalla, “Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data,” *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 4, pp. 23–32, Oct. 2021.

[12] S. Peddi and T. Leaders, “Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data,” *Int. J. Eng.*, vol. 10, no. 1.

[13] N. K. R. Panga, “FINANCIAL FRAUD DETECTION IN HEALTHCARE USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES,” vol. 10, no. 3, 2021.

[14] B. R. Gudivaka, “Designing AI-Assisted Music Teaching with Big Data Analysis,” *Curr. Sci.*, 2021.

[15] A. R. G. Yallamelli, “Improving Cloud Computing Data Security with the RSA Algorithm,” vol. 9, no. 2, 2021.

[16] D. P. Deevi, “Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding,” *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 4, pp. 21–31, Dec. 2020.

[17] M. V. Devarajan, “Improving Security Control in Cloud Computing for Healthcare Environments,” *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[18] S. H. Grandhi, “Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction,” *World J. Adv. Eng. Technol. Sci.*, vol. 2, no. 1, pp. 132–139, 2021, doi: 10.30574/wjaets.2021.2.1.0087.

[19] N. K. R. Panga, “LEVERAGING HEURISTIC SAMPLING AND ENSEMBLE LEARNING FOR ENHANCED INSURANCE BIG DATA CLASSIFICATION”.

[20] K. Dondapati, “Lung’s cancer prediction using deep learning,” *Int. J. HRM Organ. Behav.*, vol. 7, no. 1, pp. 1–10, Jan. 2019.

[21] G. Thirusubramanian, “Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments,” *Int. J. HRM Organ. Behav.*, vol. 8, no. 4, pp. 1–16, Oct. 2020.

[22] M. R. Sareddy and O. Llc, “Next-Generation Workforce Optimization: The Role of AI and Machine Learning,” vol. 5, no. 5, 2020.

[23] H. Chetlapalli, “Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks,” *J. Sci. Technol. JST*, vol. 6, no. 2, Art. no. 2, Mar. 2021.

[24] R. Jadon, “Optimized Machine Learning Pipelines: Leveraging RFE, ELM, and SRC for Advanced Software Development in AI Applications,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 1, pp. 18–30, Jan. 2018.

[25] N. S. Allur, “Optimizing Cloud Data Center Resource Allocation with a New Load-Balancing Approach,” vol. 9, no. 2, 2021.

[26] R. Ayyadurai, “Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions,” *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 110–120, 2020, doi: 10.30574/wjaets.2020.1.1.0023.

[27] P. Alagarsundaram, “PHYSIOLOGICAL SIGNALS: A BLOCKCHAIN-BASED DATA SHARING MODEL FOR ENHANCED BIG DATA MEDICAL RESEARCH INTEGRATING RFID AND BLOCKCHAIN TECHNOLOGIES,” vol. 9, no. 9726, 2021.

[28] K. Parthasarathy, “REAL-TIME DATA WAREHOUSING: PERFORMANCE INSIGHTS OF SEMI-STREAM JOINS USING MONGODB,” vol. 10, no. 4.

[29] H. Nagarajan, “Streamlining Geological Big Data Collection and Processing for Cloud Services,” vol. 9, no. 9726, 2021.

[30] Gudivaka, R. L. (2020). Robotic process automation meets cloud computing: A framework for automated scheduling in social robots. *IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM), 8*

[31] K. Dondapati, “Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios,” vol. 8, no. 2, 2020.