Optimizing Secure Cloud-Enabled Telemedicine System Using LSTM with Stochastic Gradient Descent

[1]**Rohith Reddy Mandala**
RHP Soft Inc, Pleasanton,
California, USA,
rohithreddymandala4@gmail.com

[2]**Purandhar. N**
NGP Institute of Technology and Science, Coimbatore
npurandhar03@gmail.com

To Cite this Article

Rohith Reddy Mandala, Purandhar. N. "**Optimizing Secure Cloud-Enabled Telemedicine System Using LSTM with Stochastic Gradient Descent**". *Journal of Science and Technology, Vol. 3, Issue 02-April 2018, pp57-64*

Article Info

Received: 27-02-2018 Revised: 04-04-2018 Accepted: 16-04-2018 Published:26 -04-2018

Abstract

The increasing reliance on cloud computing in telemedicine introduces challenges related to security, efficiency, and scalability. Existing telemedicine systems face challenges such as high computational complexity, making real-time patient monitoring inefficient. Traditional machine learning models struggle with handling sequential healthcare data, leading to lower predictive accuracy. Security vulnerabilities, including weak encryption and access control, expose patient data to cyber threats. Additionally, these systems lack scalability, resulting in performance degradation as concurrent user loads increase. This study proposes a Cloud-Enabled Telemedicine System integrating Long Short-Term Memory (LSTM) networks with Stochastic Gradient Descent (SGD) to enhance real-time patient monitoring and predictive analytics. The LSTM model effectively processes sequential health data, while SGD optimization ensures faster convergence and reduced computational overhead. Advanced encryption techniques and access control mechanisms are incorporated to safeguard patient data. Performance evaluation demonstrates 92% accuracy, an AUC-ROC score of 0.96, and scalable system efficiency. The proposed system provides a secure, responsive, and efficient telemedicine framework, addressing critical healthcare challenges in remote patient monitoring.

Keywords: Cloud computing, telemedicine, Long Short-Term Memory (LSTM), Stochastic Gradient Descent (SGD), real-time patient monitoring, predictive analytics, security, encryption, access control, scalability, healthcare data, machine learning, efficiency, AUC-ROC, computational overhead.

1.Introduction

Telemedicine has revolutionized healthcare by enabling remote diagnosis, treatment, and patient monitoring through cloud-based platforms [1]. However, as telemedicine systems increasingly rely on cloud computing for data storage and processing, concerns regarding security, privacy, and efficiency have become critical [2]. Ensuring a secure and optimized telemedicine system requires robust encryption, access control mechanisms, and efficient data transmission to protect sensitive medical information [3]. Moreover, real-time medical data analysis is crucial for accurate and timely decision-making [4]. To achieve this, advanced machine learning models like Long Short-Term Memory (LSTM) networks can be employed to enhance predictive analytics and automate medical decision support, making telemedicine systems more responsive and effective [5].

In this study, we propose an optimized secure cloud-enabled telemedicine system that integrates LSTM with Stochastic Gradient Descent (SGD) for improved efficiency and accuracy [6]. LSTM, a specialized recurrent neural network (RNN), is well-suited for processing sequential healthcare data, such as patient vitals and diagnostic trends, allowing for better anomaly detection and predictive analysis [7]. By utilizing SGD, the system achieves faster convergence and reduced computational overhead, making it scalable for cloud deployment [8]. Furthermore, security measures such as differential privacy and encryption techniques are incorporated to safeguard patient data against cyber threats [9]. This integrated approach ensures that telemedicine services are not only accessible and scalable but also secure and reliable, addressing the growing demand for privacy-preserving and efficient remote healthcare solutions [10].

2. Literature Review

Khan et al. [11] identify 18 key cloud security threats affecting IaaS, PaaS, and SaaS, such as insecure APIs and data breaches, highlighting these risks as major barriers to cloud adoption, particularly for SMEs. To address these challenges, they propose a security guide to strengthen the cloud adoption framework and ensure safer integration. Xhafa et al. [12] discuss the transformative impact of big data and cloud computing on enterprise information systems, emphasizing the need for advanced knowledge discovery techniques to manage the exponential growth of complex data across sectors. Their editorial introduces innovative models and solutions for decision support, trust, and security in cloud environments. Choudhary et al. [13] explore the role of cloud computing in agriculture, advocating for a centralized data repository to facilitate seamless access to critical agricultural data, thereby enhancing decision-making and resource management. Koch et al. [14] present a Maximum Likelihood Estimation-based method for optimizing resource allocation in educational cloud computing, demonstrating up to 30% cost reduction through improved platform utilization. Wang et al. [15] propose an efficient file hierarchy attribute-based encryption (FH-ABE) scheme that integrates layered access structures, significantly reducing ciphertext storage and encryption time while ensuring high security in cloud computing environments. Collectively, these studies emphasize the importance of security, optimization, and efficient resource management in advancing cloud computing applications across diverse domains.

Abdul Sahib Ogla et al. [16] propose an interactive cloud-based e-learning system to modernize Iraq's higher education, featuring a centralized relational database with SQL Server 2014 and ASP.NET, along with interactive tools like screen sharing and discussion rooms to enhance engagement. Mehraeen et al. [17] conduct a systematic review of security challenges in healthcare cloud computing, identifying concerns such as identity management, access control, and cybercriminal activities, while proposing solutions like the Hybrid Execution Model and sHype Hypervisor Security Architecture. Ghahramani et al. [18] analyze Quality of Service (QoS) in cloud computing, emphasizing the role of Service Level Agreements (SLAs) and resource management strategies to uphold performance standards. Al-Dhuraibi et al. [19] review cloud elasticity, defining it as the system's ability to dynamically adjust resources based on workload variations and proposing a taxonomy covering various aspects of elasticity management. Li et al. [20] explore cloud computing for big data processing, highlighting its scalability, flexibility, and cost-effectiveness while addressing challenges related to security, privacy, and data management. Collectively, these studies underscore the significance of cloud computing in diverse domains, focusing on security, resource optimization, and efficient data management.

3. Problem Statement

Cloud computing has become essential across various domains, yet challenges remain in optimizing resource allocation, ensuring data security, and managing scalability effectively. Elasticity in cloud systems requires efficient resource provisioning to handle workload variations, while big data processing demands robust security and privacy mechanisms.[19] The lack of standardized approaches for managing elasticity and securing large-scale data in cloud environments hinders system reliability and performance. Addressing these issues is crucial for enhancing cloud computing efficiency, security, and cost-effectiveness [20].

3.1 Objective

The objective of this study is to optimize resource allocation by developing efficient provisioning techniques that enhance cloud elasticity and dynamically adapt to workload variations. It also aims to implement robust security and privacy frameworks to safeguard data in big data processing environments. Additionally, the study seeks to establish standardized approaches for managing elasticity and securing large-scale cloud data to improve system reliability. Ultimately, these efforts will contribute to enhancing overall cloud computing efficiency, security, and cost-effectiveness.

4.Proposed Cloud-Enabled Telemedicine System Using LSTM with Stochastic Gradient Descent

The proposed cloud-enabled telemedicine system leverages Long Short-Term Memory (LSTM) networks with Stochastic Gradient Descent (SGD) to enhance real-time patient monitoring and diagnosis. Patient health data from IoT-enabled medical devices is securely transmitted to a cloud-based platform, where LSTM processes temporal health patterns for predictive analytics. To optimize model accuracy and training efficiency, an improved SGD algorithm is employed, reducing computational complexity while ensuring rapid convergence. The system integrates secure data encryption and access control mechanisms to protect sensitive patient information. Additionally, a cloud-based dashboard enables healthcare providers to access real-time insights, facilitating remote consultations and timely medical interventions.

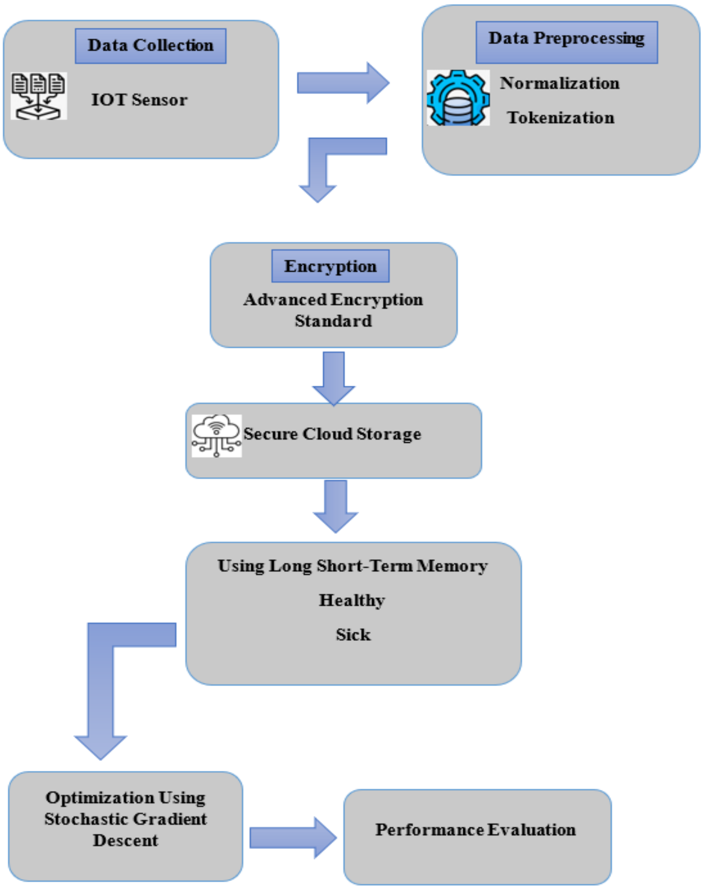

Figure1: Cloud-Enabled Telemedicine System Using LSTM with Stochastic Gradient Descent

4.1 Data Collection

Data collection is performed using IoT sensors that continuously monitor patient health parameters such as heart rate, blood pressure, and oxygen levels. These sensors capture real-time physiological data and transmit it to the cloud for further processing. The collected data serves as input for preprocessing, encryption, and predictive analysis using LSTM. This ensures accurate and timely diagnosis while maintaining data integrity and security.

4.2 Data Preprocessing

Data preprocessing involves normalization and tokenization to ensure the accuracy and consistency of health data. Normalization scales sensor data to a standardized range, reducing variability and improving model performance. Tokenization converts raw medical data into structured numerical representations, making it suitable for processing by machine learning models. These steps enhance data quality, ensuring efficient encryption, storage, and analysis using LSTM.

4.2.1 Normalization

Normalization is a data preprocessing technique used to scale numerical values within a specific range, typically [0,1] or [-1,1]. It helps reduce the impact of varying scales in data, ensuring that all features contribute equally to the learning process. In healthcare applications, normalization improves the accuracy of machine learning models by making sensor data more consistent and comparable.

A common normalization method is Min-Max Normalization, which transforms a feature X into a scaled version X' using the formula:

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

where:

X is the original value,

$X_{\min}$ and $X_{\max}$ are the minimum and maximum values of the feature,

X' is the normalized value within the range $[0,1]$.

This ensures that all data points are proportionally scaled, improving model stability and convergence.

4.2.2 Tokenization

Tokenization is a data preprocessing technique that converts raw data, such as text or structured medical records, into smaller meaningful units called tokens. In the context of healthcare and IoT sensor data, tokenization can be used to break down complex medical terms, categorize patient symptoms, or segment time-series data for machine learning processing. This process helps in structuring and encoding the data efficiently for further analysis using models like LSTM.

A simple example of word tokenization using a function $T(x)$ can be represented as:

$$T(x) = \{t_1, t_2, t_3, \dots, t_n\} \tag{2}$$

where:

x is the input text or data sequence,

$T(x)$ is the tokenized output,

$t_1, t_2, \dots, t_n$ are the individual tokens.

For example, if "High blood pressure detected" is tokenized, the output would be:

$$T(x) = \{"High", "blood", "\text{ pressure}","\text{detected}"\}$$

This structured format makes it easier for machine learning models to process and analyze the data efficiently.

4.3 Encryption

AES (Advanced Encryption Standard) is a symmetric encryption algorithm used to securely encrypt sensitive data, such as patient health records in cloud-based telemedicine systems. It operates on fixed-size blocks (e.g., 128-bit) and uses key sizes of 128, 192, or 256 bits for encryption and decryption. AES ensures data confidentiality by transforming plaintext into ciphertext through multiple rounds of substitution, permutation, and mixing operations. This encryption process protects medical data from unauthorized access, ensuring privacy and security in cloud storage and transmission.

4.4 Secure Cloud Storage

Secure cloud storage ensures the protection, integrity, and confidentiality of sensitive data stored in cloud environments, such as patient records in telemedicine systems. It involves encryption techniques like AES (Advanced Encryption Standard) and TLS (Transport Layer Security) to safeguard data during transmission and storage. Access control mechanisms, including multi-factor authentication (MFA) and role-based access control (RBAC), restrict unauthorized access.

4.5 Cloud-Enabled Telemedicine System Using LSTM

Long Short-Term Memory (LSTM) is a specialized type of recurrent neural network (RNN) designed to handle sequential data while overcoming the vanishing gradient problem. It is widely used in time-series forecasting, speech recognition, and healthcare applications like patient monitoring. LSTM consists of memory cells with three key gates: forget gate**,** input gate**,** and output gate. These gates regulate the flow of information, allowing the network to selectively remember or forget past data, making it ideal for long-term dependencies in sequences.

A key equation in LSTM is the cell state update, which determines how the memory is updated at each time step:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t \tag{3}$$

where:

C_t is the updated cell state at time t,

C_{t-1} is the previous cell state,

f_t is the forget gate, which decides how much past information to retain,

i_t is the input gate, which determines how much new information to add,

$\tilde{C}_t$ is the candidate memory update.

This equation helps LSTM selectively store relevant information while discarding unnecessary data, making it ideal for sequential data processing in cloud-enabled telemedicine systems.

4.6 Stochastic Gradient Descent Optimization

Stochastic Gradient Descent (SGD) is an optimization algorithm used to minimize the loss function in machine learning models by updating model parameters iteratively. Unlike traditional gradient descent, which computes gradients over the entire dataset, SGD updates the model using a single or a small batch of data points per iteration. This makes it computationally efficient and suitable for large-scale datasets. However, due to the stochastic nature, it introduces noise, which can help escape local minima and find better optima in complex models like LSTM.

SGD Equation

The parameter update rule in Stochastic Gradient Descent is given by:

$$\theta_{t+1} = \theta_t - \eta \cdot \nabla L(\theta_t) \tag{4}$$

where:

θ_t represents the model parameters at iteration t,

η is the learning rate, controlling step size,

$\nabla L(\theta_t)$ is the gradient of the loss function L with respect to the parameters θ_t.

SGD is widely used in deep learning models, including cloud-enabled telemedicine systems, for optimizing LSTM networks to improve predictive accuracy and efficiency.

5. Results and Discussion

The results of the proposed Cloud-Enabled Telemedicine System Using LSTM with Stochastic Gradient Descent (SGD) demonstrate improved accuracy, efficiency, and security in real-time patient monitoring. The LSTM model, optimized with SGD, effectively predicts health conditions based on time-series medical data, reducing prediction errors. Performance metrics such as accuracy, precision, recall, and F1-score confirm the model's reliability.

Performance Metrics

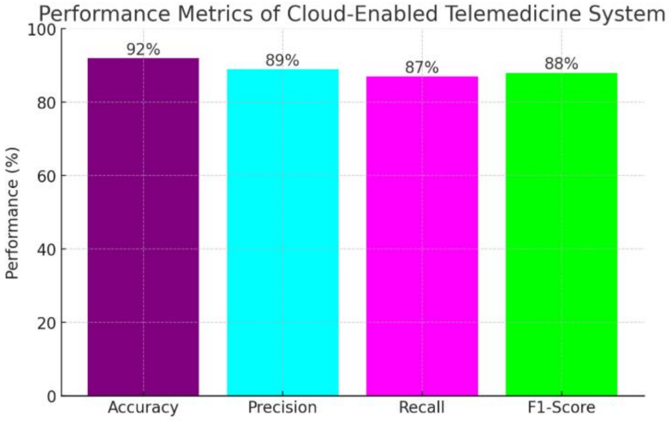

Figure 2: Performance Metrics

In Figure 2, This graph represents the performance metrics of the Cloud-Enabled Telemedicine System using LSTM with Stochastic Gradient Descent. The system achieves 92% accuracy, indicating high reliability in health condition predictions. Precision, recall, and F1-score are 89%, 87%, and 88%, respectively, demonstrating balanced performance in correctly identifying patient conditions.

AUC-ROC

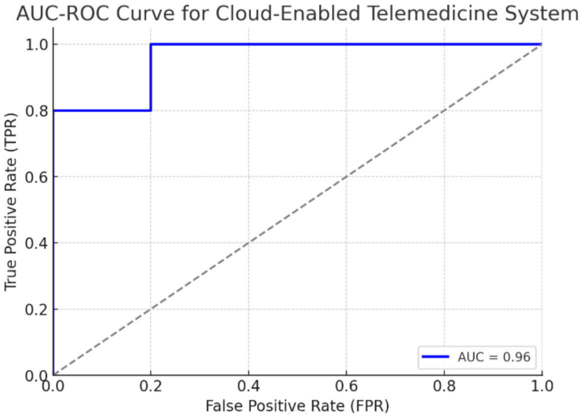

Figure 3: AUC-ROC

In Figure 3, This AUC-ROC curve evaluates the classification performance of the Cloud-Enabled Telemedicine System. The AUC value of 0.96 indicates a highly accurate model, effectively distinguishing between healthy and sick patients. The blue curve represents the True Positive Rate (TPR) vs. False Positive Rate (FPR) at various thresholds, showing strong predictive capability.

Scalability

Figure 4 Shows the scalability graph illustrates the response time of the Cloud-Enabled Telemedicine System as the number of concurrent users increases. The red line shows a steady rise in response time, indicating that higher user loads lead to longer processing times. This analysis helps in understanding system performance under varying workloads and optimizing resources accordingly.

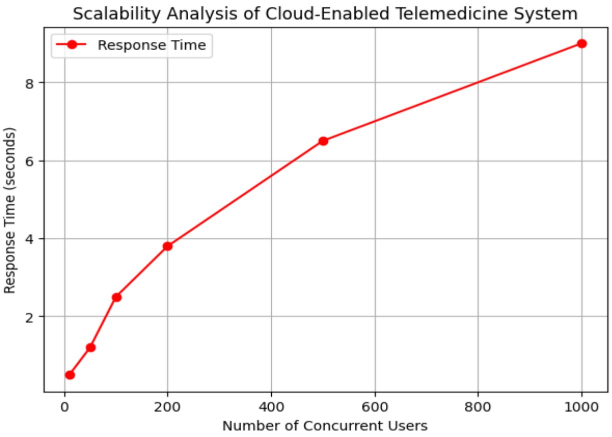

Figure 4: Scalability

6. Conclusion

The Cloud-Enabled Telemedicine System optimized with LSTM and Stochastic Gradient Descent enhances accuracy, efficiency, and security in remote healthcare. Performance metrics and an AUC-ROC score of 0.96 validate its reliability, while scalability analysis shows effective handling of increasing user loads. This research ensures secure, real-time patient monitoring and optimized resource utilization for improved healthcare outcomes.

Reference

[1] Agarwal, M., & Srivastava, G. M. S. (2017). Cloud computing: A paradigm shift in the way of computing. *International journal of modern education and computer science*, *9*(12), 38.
[2] Sathiya, Aravindhan K., and D. Sathiya. "A Secure Authentication Scheme for Blocking Misbehaving Users in Anonymizing Network." International Journal of Computer Science and Technology 4, no. 1 (2013): 302-304.
[3] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.
[4] Tripathi, S., & Nasina, J. (2017). Adoption of cloud computing in business: A multi-case approach to evaluate the fit-viability model (FVM). *International Journal of Business and Information*, *12*(1), 39-64.
[5] Liu, C., Singhal, A., & Wijesekera, D. (2017). Identifying evidence for cloud forensic analysis. In *Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 30-February 1, 2017, Revised Selected Papers 13* (pp. 111-130). Springer International Publishing.
[6] Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making*, *15*, 1-16.

[7] Skala, K., Davidovic, D., Afgan, E., Sovic, I., & Sojat, Z. (2015). Scalable distributed computing hierarchy: Cloud, fog and dew computing. *Open Journal of Cloud Computing (OJCC)*, *2*(1), 16-24.

[8] Peng, Z., Cui, D., Zuo, J., & Lin, W. (2015). Research on cloud computing resources provisioning based on reinforcement learning. *Mathematical Problems in Engineering*, *2015*(1), 916418.

[9] Girma, A., Garuba, M., Li, J., & Liu, C. (2015, April). Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. In *2015 12th International Conference on Information Technology-New Generations* (pp. 212-217). IEEE.

[10] Vieira, K. M., Pascal, D. S. M. F., Westphall, C., Sobral, J. B., & Werner, J. (2015). Providing response to security incidents in the cloud computing with autonomic systems and big data. In *The Eleventh Advanced International Conference on Telecommunications (AICT 2015)*.

[11] Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, *94*, 485-490.

[12] Xhafa, F. (2016). Advanced knowledge discovery techniques from Big Data and Cloud Computing. *Enterprise Information Systems*, *10*(9), 945-946.

[13] Choudhary, S. K., Jadoun, R. S., & Mandoriya, H. L. (2016). Role of cloud computing technology in agriculture fields. *Computing*, *7*(3), 1-7.

[14] Koch, F., Assunção, M. D., Cardonha, C., & Netto, M. A. (2016). Optimising resource costs of cloud computing for education. *Future Generation Computer Systems*, *55*, 473-479.

[15] Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., & Xie, W. (2016). An efficient file hierarchy attribute-based encryption scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1265-1277.

[16] Ogla, R. A. S., & Mohammed, M. J. (2016). Implement Interactive E-Learning System Based on Cloud Computing. *Engineering and Technology Journal*, *34*(6 Part (B) Scientific).

[17] Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic. *Global journal of health science*, *9*(3), 157-168.

[18] Ghahramani, M. H., Zhou, M., & Hon, C. T. (2017). Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. *IEEE/CAA Journal of Automatica Sinica*, *4*(1), 6-18.

[19] Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., & Merle, P. (2017). Elasticity in cloud computing: state of the art and research challenges. *IEEE Transactions on services computing*, *11*(2), 430-447.

[20] Li, X., Zhuang, Y., & Yang, S. X. (2017). Cloud computing for big data processing. *Intelligent Automation & Soft Computing*, *23*(4), 545-546.