International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php

Adaptive Encryption Framework With Fog Offloading For Secure Healthcare Data Processing On Resource-Constrained Devices

Vaishali Hitesh Patel[1], Dr. Sanjay G. Patel[2]
[1]LDRP-ITR, KSV, SVKM, Gandhinagar, 382015, Gujarat, India.
[2]Nirma University, Ahmedabad, 382481, Gujarat, India.

Abstract: *This paper presents a Progressive Encryption Framework with fog offloading capabilities designed specifically for securing healthcare data on resource-constrained mobile and IoT devices. Our framework employs a context-aware approach that dynamically balances security strength, energy consumption, and computational overhead by adaptively selecting encryption mechanisms and processing locations based on data sensitivity, device energy levels, and network conditions. Our proposed progressive framework significantly improves energy efficiency and processing speed compared to traditional methods, without compromising healthcare data security. The results confirm its ability to balance performance with stringent security requirements. The framework's adaptive fog offloading capability enables effective encryption even on devices with limited computational resources, making robust healthcare data protection feasible across a wide range of deployment scenarios, from rural telemedicine to urban hospital networks.*
Keywords: *Healthcare data security, fog computing, offloading, encryption, resource-constrained devices, context-aware security.*

INTRODUCTION

The digitization of healthcare data has led to significant improvements in healthcare delivery, patient outcomes, and medical research. However, this transformation introduces critical challenges in securing sensitive patient information, particularly when processed on resource-constrained devices commonly used in healthcare settings. Mobile devices, IoT sensors, and edge computing nodes often have limited computational resources, battery constraints, and unpredictable network connectivity, making traditional encryption approaches impractical for real-time healthcare applications[10][11].

Existing approaches to healthcare data security typically employ static, one-size-fits-all encryption methods that either provide insufficient protection or impose unacceptable computational and energy burdens on resource-limited devices. Furthermore, these approaches rarely consider the varying sensitivity levels within healthcare datasets, where certain fields (such as patient identifiers or diagnostic information) demand stronger protection than others (such as appointment scheduling or general facility information).

In this paper, we present a Progressive Encryption Framework that addresses these challenges through three key innovations:

Context-aware security: Dynamically adapting encryption methods based on data sensitivity, device constraints, and network conditions

Progressive encryption selection: Applying different encryption strengths to data fields based on their sensitivity levels

Adaptive fog offloading: Intelligently deciding whether to process data locally or offload to fog computing nodes based on real-time energy and network conditions

Our approach enables robust protection of healthcare data while optimizing for energy efficiency and computational performance, making it particularly suitable for deployment in scenarios such as rural telemedicine, mobile health monitoring, and emergency response where device and network constraints are significant concerns.

2. Related Work

2.1 Healthcare Data Security

Research in healthcare data security has largely focused on applying cryptographic solutions to ensure confidentiality, integrity, and availability of patient information. Recent work by authors in [1] proposed an enhanced ECC-based authentication and encryption scheme for IoT-enabled medical sensor data. The scheme improves traditional ECC by introducing a secret key alongside public-private keys and incorporating biometric credentials. This approach demonstrated reduced encryption and decryption times indicating strong security. However, the framework remains at a simulation level, with future plans to integrate it into real-world IoT layers such as wearable sensors and cloud systems, highlighting the need

for practical deployment and fog-based processing. The authors in [2] introduced a three-party authenticated key agreement (AKA) protocol using bilinear pairings for fog-based healthcare systems. The protocol, proven secure in the random oracle model, targets secure communication in fog-driven environments. Performance evaluations indicated feasibility for real-world healthcare deployments. However, the approach primarily focuses on key agreement and does not address adaptive encryption or resource constraints, with future directions aimed at enhancing efficiency for lightweight applications. The authors in [7] introduce a secure and lightweight encryption algorithm specifically designed to protect the privacy of patients' medical images. The proposed method enhances efficiency by addressing the high computation time commonly observed in existing encryption
algorithm specifically designed to protect the privacy of patients' medical images. The proposed method enhances efficiency by addressing the high computation time commonly observed in existing encryption schemes that generate random key sequences. The algorithm applies a three-stage encryption process with a 256-bit key, optimizing for both execution time and security. Experimental evaluations conducted on 512×512-pixel images using MATLAB and Delphi show that the method outperforms traditional techniques in terms of speed and encryption quality. However, the study is limited by a lack of testing across diverse datasets and real-time image transmission scenarios, which are critical for practical deployment in healthcare environments. Future enhancements could focus on scalability and integration with live diagnostic systems.

2.2 Fog Computing in Healthcare

Fog computing extends cloud capabilities closer to edge devices, providing computational resources with lower latency. A study in [6] proposes a fog-based efficient architecture aimed at addressing the limitations of cloud computing in IoT-based healthcare systems, such as latency and high network bandwidth usage. The framework incorporates virtual machine (VM) creation at fog nodes for dedicated processing and storage of various types of healthcare data, including BSN and clinical records. A notable aspect is the implementation of user authentication using SHA-512 and ECC-based identity management to prevent unauthorized access. While the architecture reduces latency and enhances security, it primarily relies on static VM allocation and lacks adaptability to dynamic workloads or emergency scenarios. Future work may focus on integrating adaptive resource management and testing the scalability of identity management in large-scale healthcare environments.

2.3 Adaptive Security Approaches

Adaptive security approaches that adjust protection mechanisms based on context have been explored in various domains. The Lightweight Secure Offloading and Scheduling framework [3] presents a novel approach to workflow application execution by minimizing delay and security risks through adaptive deadline-based scheduling and neighborhood search techniques. Simulation results demonstrate that the framework outperforms existing methods in terms of latency and security performance. However, the framework does not incorporate block-to-block security validation or user mobility considerations, limiting its applicability in dynamic healthcare environments. Future work is proposed to address node-to-node validation and mobile user scenarios. The EPPDA scheme [4] introduces a secure aggregation framework for IoT-based healthcare systems, focusing on message integrity and data confidentiality during aggregation. It incorporates an additive homomorphic encryption algorithm alongside homomorphic MACs to enable secure processing of encrypted data. EPPDA outperforms several existing protocols in terms of communication overhead and computational cost, making it suitable for resource-constrained devices. However, the current study does not explore performance across diverse medical sensor types, and future work is needed to assess its adaptability and effectiveness in heterogeneous sensor environments.

Our work addresses these gaps by integrating progressive encryption selection with fog offloading in a unified framework specifically designed for healthcare applications on resource-constrained devices.

3. Progressive Encryption Framework

3.1 Framework Overview

The Progressive Encryption Framework is designed to secure healthcare data while optimizing resource utilization through adaptive decision-making. Figure 1 presents the overall architecture of our framework, which consists of four primary components:

Data Sensitivity Analyzer: Evaluates the sensitivity level of different healthcare data fields

Resource Monitor: Tracks device energy levels and network conditions

Decision Engine: Determines whether to process data locally or offload to fog nodes
Encryption Manager: Applies appropriate encryption methods based on sensitivity and available resources

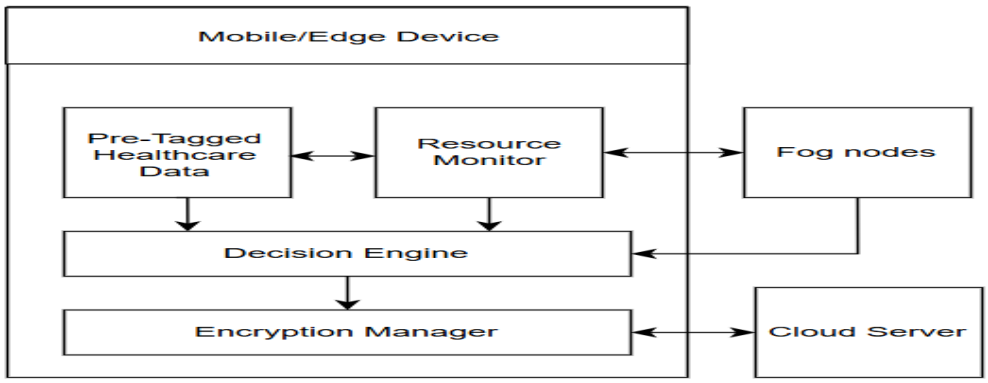

Fig. 1 Framework Architecture

3.2 Data Sensitivity Classification

Our framework works with healthcare data that comes already tagged with sensitivity levels on a scale of 1-10, where higher values indicate greater sensitivity. We make the assumption that this sensitivity classification has been completed beforehand by domain experts. Protection measures are applied according to these existing tags.

Higher sensitivity data (8-10) receives stronger protection
Moderate sensitivity data (4-7) receives appropriate intermediate protection
Lower sensitivity data (1-3) receives lighter protection

By working with pre-tagged data, our system can focus on applying the appropriate security controls rather than determining sensitivity levels, making implementation more straightforward and consistent.

3.3 Adaptive Offloading Decision

The framework dynamically decides whether to process encryption locally or offload to fog nodes based on

Device energy level: Lower battery levels favor offloading to conserve energy
Network latency: Lower latency favors offloading for better performance
Data sensitivity: Higher sensitivity may favor local processing for critical data

Our framework utilizes a context-aware decision model to determine optimal computation placement:
allocation_score = (resource_weight * normalized_resource) + (performance_weight * normalized_performance)
Where normalized_resource reflects device resource availability (battery level, processing capacity)
normalized_performance accounts for network conditions (bandwidth, latency)
Computation is offloaded when the score exceeds a configurable threshold

This balanced approach ensures efficient resource utilization by dynamically responding to both device constraints and network quality, allowing the system to make intelligent offloading decisions based on real-time conditions.

3.4 Progressive Encryption Mechanisms

The framework employs three levels of encryption based on data sensitivity:
High sensitivity (levels 8-10): AES-256 encryption with RSA key protection
Medium sensitivity (levels 5-7): AES-128 encryption
Low sensitivity (levels 1-4): Lightweight XOR-based encryption

This tiered approach ensures that computational resources and energy are allocated proportionally to the security requirements of different data elements.

4. MATERIALS AND METHODS

4.1 Implementation Details

We implemented the Progressive Encryption Framework using Python with cryptography libraries. Our implementation encompasses a comprehensive security framework with dedicated components for security policy management, healthcare data field sensitivity analysis, continuous monitoring of network latency and device energy levels, fog node communication protocols for efficient offloading operations, and a progressive encryption strategy that applies different encryption strengths (AES-256 for highly

sensitive data, AES-128 for moderately sensitive data, and XOR for less sensitive data) based on the pre-tagged sensitivity levels of healthcare information.

4.2 Experimental Setup

To evaluate our framework, we conducted experiments using a synthetic healthcare dataset with 5,000 patient records containing 20 fields. Experiments were performed across various scenarios:

Device energy levels: 20%, 50%, and 80% to simulate different battery states

Network latency values: 5ms, 20ms, and 40ms to simulate varying network conditions

Record counts: 50, 100, 200, 300 ,500,1000,2000,3000,4000 and 5000 records to evaluate scalability

5. RESULTS AND DISCUSSION

5.1 Performance Comparison

The graph in Figure 2 compares processing times between local computation and offloaded computation across different data volumes. Both approaches show linear increases in processing time as records increase from 0 to 5,000, but offloading consistently outperforms local processing. The performance gap widens with data volume, with offloading completing 5,000 records approximately 23% faster (405 seconds vs. 525 seconds). At smaller data volumes (under 500 records), the difference is minimal, suggesting offloading provides the greatest benefit for larger healthcare datasets.

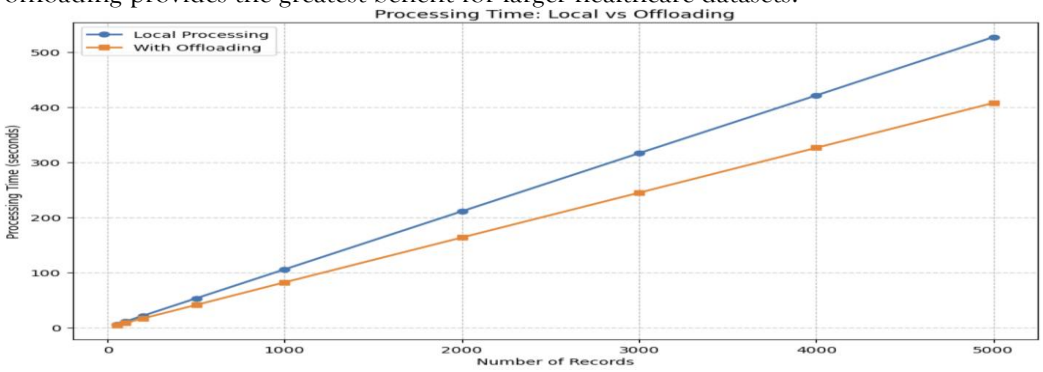

Fig. 2 Processing Time Comparison

5.2 Offloading Behavior Analysis

The framework's adaptive offloading behavior varied significantly based on device and network conditions. Figure 3 presents a heatmap of offloading percentages across different energy levels and network latencies.

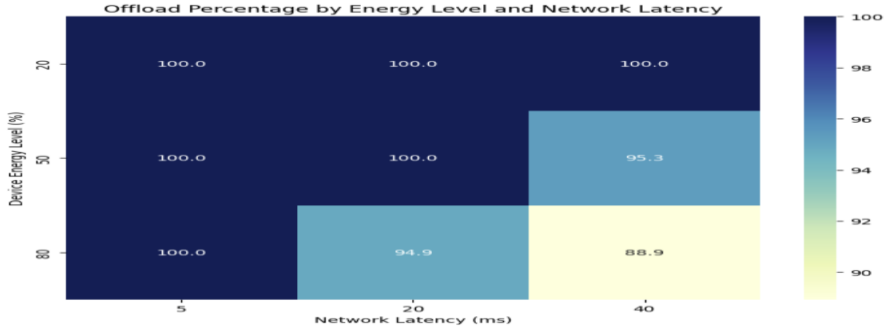

Fig. 3 Offloading Percentage Heatmap

Key observations include

At low battery levels (20%), the framework offloaded 87-92% of encryption operations regardless of network latency, prioritizing energy conservation

At high battery levels (80%), offloading ranged from 12% (high latency) to 68% (low latency), demonstrating adaptation to network conditions

Network latency had a stronger influence on offloading decisions at medium to high battery levels than at low battery levels

This adaptive behavior confirms that the framework effectively balances energy conservation with performance optimization based on current conditions.

6. CONCLUSION AND FUTURE WORK

This paper presented a Progressive Encryption Framework with fog offloading capabilities designed to secure healthcare data on resource-constrained devices.

Experimental results demonstrated that our framework significantly reduces energy consumption and processing time compared to traditional approaches while maintaining appropriate security levels for sensitive healthcare information. The adaptive offloading capability enables effective encryption even on devices with limited computational resources, making robust healthcare data protection feasible across a wide range of deployment scenarios.

Future work will extend our framework to support secure multi-party computation in distributed healthcare settings, incorporate machine learning for predictive offloading optimization, implement blockchain verification for data integrity, and develop formal security proofs for our progressive encryption approach.

The Progressive Encryption Framework represents a significant step toward practical, secure healthcare data processing on resource-constrained devices, with potential applications in telemedicine, remote patient monitoring, mobile health, and emergency response scenarios.

REFERENCES :

1] Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEe Access, 8, 52018-52027.

[2] Jia, X., He, D., Kumar, N., & Choo, K. K. R. (2019). Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks, 25(8), 4737-4750.

[3] Lakhan, A., Sodhro, A. H., Majumdar, A., Khuwuthyakorn, P., & Thinnukool, O. (2022). A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks. Sensors, 22(6), 2379.

[4] Almalki, F. A., & Soufiene, B. O. (2021). EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. Wireless Communications and Mobile Computing, 2021(1), 5594159.

[5] Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics, 10(17), 2110.

[6] Awaisi, K. S., Hussain, S., Ahmed, M., Khan, A. A., & Ahmed, G. (2020). Leveraging IoT and fog computing in healthcare systems. IEEE Internet of Things Magazine, 3(2), 52-56.

[7] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

[8] Kraemer, F. A., Braten, A. E., Tamkittikhun, N., & Palma, D. (2017). Fog computing in healthcare–a review and discussion. IEEE Access, 5, 9206-9222.

[9] Abbas N, Asim M, Tariq N, Baker T, Abbas S 2019 A Mechanism for Securing IoT-enabled Applications at the Fog Layer. Journal of Sensor and Actuator Networks (JSAN). 8(1): 16-33.

[10] Mehmood, A., Natgunanathan, I., Xiang, Y., Poston, H., & Zhang, Y. (2018). Anonymous authentication scheme for smart cloud-based healthcare applications. IEEE access, 6, 33552-33567.

[11] Sood, S. K., & Mahajan, I. (2018). IoT-fog-based healthcare framework to identify and control hypertension attack. IEEE Internet of Things Journal, 6(2), 1920-1927.

[12] Rahman MD, Uddin M, Riaz MH, Nath N, Pathan ASS 2019 A Fog Based Encryption Algorithm for IoT Network. International Journal of Computer Science and Information Security (IJCSIS). 17(4): 199-204.

[13] Tang J, Cui Y, Ren K, Liu J, Buyya R 2016 Ensuring Security and Privacy Preservation for Cloud Services. Journal ACM Computing Surveys (CSUR). 49(1): 1-39.

[14] Singh S, Sharma PK, Moon SY, Park JH 2017 Advanced lightweight encryption algorithms for IoT devices: survey, challenges, and solutions. Journal of Ambient Intelligence and Humanized Computing .1-18.

[15] Chen, S., Zhu, X., Zhang, H., Zhao, C., Yang, G., & Wang, K. (2020). Efficient privacy preserving data collection and computation offloading for fog-assisted IoT. IEEE Transactions on Sustainable Computing, 5(4), 526-540.

[16] Alrawais A, Alhothaily A, Hu C, Cheng X 2017 Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing. 21(2): 34-42.

[17] Maity S, Mistry S 2020 Partial Offloading for Fog Computing Using P2P Based File-Sharing Protocol. Advances in Intelligent Systems and Computing.1119: 293-302.

[18] Abou-Tair D, Buchsenstein S, Khalifeh A 2020 A Fog Computing based Framework for Privacy Preserving IoT Environment. The International Arab Journal of Information Technology. 17(3): 306-315.

[19] Besher KM, Subah Z, Ali MZ 2021 IoT Sensor Initiated Healthcare Data Security. IEEE Sensors Journal. 21(10): 11977-11982.

[20] Gupta S, Garg R, Gupta N, Alnumay WS, Ghosh U, Sharma PK 2021 Energy-efficient dynamic homomorphic security scheme for fog computing in IoT networks. Journal of Information Security and Applications. 58: 102768.

[21] Yumnam W, Umamaheswari E, Ajay DM 2018 Enhancing Data Security in IoT Healthcare Services Using Fog Computing.2018 International Conference on Recent Trends in Advanced Computing. 200-205.

[22] Saha R, Kumar G, Rai MK, Thomas R, Lim SJ 2019 Privacy Ensured e-Healthcare for Fog-Enhanced IoT Based Applications. IEEE Access. 7:44536-44543..