Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 431–439
DOI : 10.47974/JDMSC-1899

Implementing optimization and fine-tuning emergency response strategies in cryptographically enhanced IoT-infused medical infrastructure for rapid response

Sherif Tawfik Amin
Department of Computer Science
College of Computer Science & Information Technology
Jazan University
Jazan
Kingdom of Saudi Arabia

Abstract

In today's healthcare landscape, connecting medical facilities to the Internet of Things (IoT) has led to transformative changes. This study focuses on optimizing and refining emergency response strategies within IoT-enabled medical systems through cryptographic improvements. The proposed framework aims to strengthen rapid response mechanisms to better handle critical scenarios more efficiently. Using cryptographic techniques ensures the security and integrity of data transmission, protecting sensitive medical information. Our approach involves developing a sophisticated optimization algorithm tailored for emergency situations' unique demands. This algorithm refines response strategies based on real-time data collected from IoT sensors, allowing dynamic adjustment to evolving conditions. Additionally, cryptographic protocols reinforce the communication channels, reducing the risk of unauthorized access or data manipulation. Through simulation and actual validation, the effectiveness of our proposed framework is demonstrated in enhancing medical infrastructure's responsiveness during emergencies. By combining IoT capabilities with cryptographic measures, this research contributes to more resilient and secure emergency response systems' evolution, ultimately advancing healthcare delivery's effectiveness in critical situations.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *IoT-infused medical infrastructure, Emergency response strategies, Cryptographic enhancements, Optimization algorithm, Rapid response in healthcare.*

E-mail: samin@jazanu.edu.sa

© Taru Publications

1. Introduction

Healthcare is changing, and the Internet of Things (IoT) is playing a big part. With IoT in our hospitals and clinics, we're seeing better patient care and treatment plans. This work looks at how we can improve emergency plans with IoT. Since IoT arrived, it's been really useful. Health places can now get current data from joining devices. This helps speed up and improve emergency help. But, with IoT devices sharing important patient info as shown in Figure 1, the safety and privacy of this data is really important.

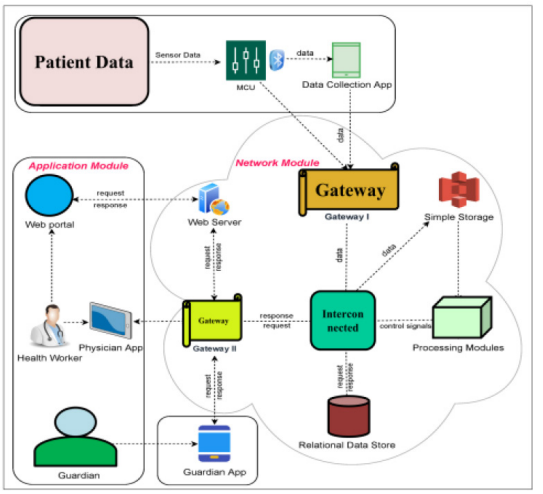

Figure 1

Over representation of Emergency Response Strategies in Cryptographically Enhanced IoT

Cryptographic [3] protocols play a pivotal role in mitigating the risks associated with cyber threats and unauthorized intrusions, thereby establishing a resilient and secure foundation for emergency response systems. This research endeavors to develop a sophisticated optimization algorithm tailored to the unique demands of emergency scenarios. By dynamically adapting response strategies based on real-time data, the proposed algorithm aims to enhance the responsiveness of medical infrastructure during critical situations [2]. Through comprehensive simulation and empirical validation, the study seeks to demonstrate the tangible benefits of the proposed framework in comparison to existing emergency response systems.

1.1 *Background for IoT-Infused Medical Infrastructure for Rapid Response*

Internet of Things or IoT [4] has introduced a new age in healthcare. It is especially seen with how it's mixed into the medical framework. This foundation, with the influence of IoT [5], shifts focus on quick responses. It influences connected devices and changes how patient care and healthcare management work. This change from reactive to proactive healthcare matters greatly in emergencies where every second is crucial.

Table 1
Comparison of different ERS wit parameters

Emergency Response Systems	**Communication**	**Coordination**	**Response Time**	**Scalability**	**Flexibility**	**Data Security**
PSAP	High	Moderate	Varies	Limited	Moderate	Moderate
EMS	High	High	Critical	Moderate	High	High
Fire Department	High	High	Critical	High	High	High
Law Enforcement	High	High	Critical	Moderate	High	High
Emergency Alert Systems	High	High	Immediate	High	High	High
National Weather Service	High	High	Immediate	High	High	High

3. Methodology

3.1 *Framework Design*

The foundation [6] of the research methodology involves the design of a comprehensive framework that integrates IoT technologies with cryptographic enhancements to optimize and fine-tune emergency response strategies in medical infrastructure.

The framework encompasses the identification and integration of relevant IoT sensors, considering parameters such as vital signs, patient activity, and equipment status [10]. Figure 2 shows the flowchart of the proposed framework.

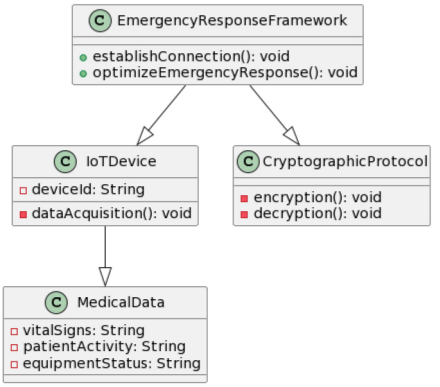

Figure 2

Flowchart of proposed framework

3.2 *Optimization Algorithm Development*

The heart of the methodology lies in the development of an optimization algorithm tailored for emergency response scenarios.

Genetic Algorithm for Emergency Response Optimization:

1. Initialization:
   - Generate an initial [7] population of individuals, where each individual represents a potential solution to the emergency response scenario.
2. Fitness Evaluation:
   - Evaluate the fitness of each individual in the population based on the defined objective function.
   - function given as:

$$F = w1 * Se + w2 * \left(\frac{1}{D}\right) + w3 * P$$

Here,

- Se: Emergency Severity Score, D: Proximity Distance to Medical Resources, P: Patient-specific Conditions, w1, w2, w3: Weighting factors for each factor.

3. Selection:
   - Select individuals from the population for the next generation based on their fitness scores [9]. Individuals with higher fitness scores are more likely to be selected.

4. Crossover:
   - Apply crossover (recombination) to pairs of selected individuals to create new offspring.
5. Mutation:
   - Introduce random changes to the genetic representation of some individuals in the population.

3.3 *Integration of Cryptographic Protocols*

To address security concerns in transmitting sensitive medical data, cryptographic protocols are integrated into the framework [8]. Figure 3 shows the ERS Flow Architecture.

Elliptic Curve Cryptography (ECC) Algorithm for IoT Smart Device in Emergency Response:

Step 1: Key Generation:

- Generate a private key (d) randomly from the elliptic curve's finite field.
- Compute the corresponding public key (Q) using elliptic curve point multiplication:

$$Q = d \cdot G$$

(G is the base point of the elliptic curve.)

Step 2: Message Encoding:

- Represent the emergency message (M) as an integer.

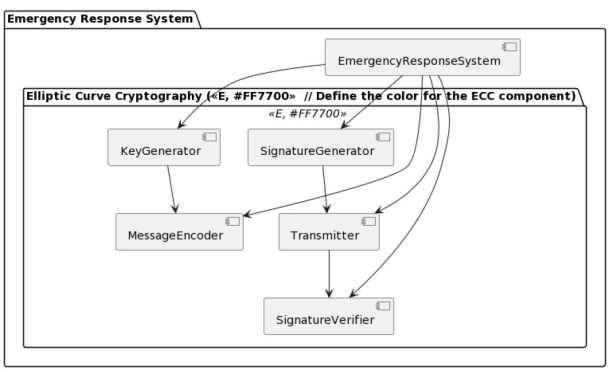

Figure 3

ERS flow architecture

Step 3: Signature Generation:

- Choose a random number (k) as the ephemeral key.
- Compute the ephemeral public key (K) using elliptic curve point multiplication:

$$K = k \cdot G$$

- Calculate the signature (s):

$$s = k^{-1} \cdot (H(M) + d \cdot r)$$

- ($H(\cdot)$ is a hash function, r is the x-coordinate of the point K.)

Step 4: Transmission:

- Transmit the emergency message (M) and the ECC signature (s) securely.

Step 5: Signature Verification:

- Receive the emergency message (M) and the ECC signature (s).
- Verify the signature by computing r′ and comparing it with the received r:

$$r' = (s \cdot K - H(M) \cdot G)$$

The cryptographic protocols are seamlessly woven into the communication channels, creating a robust layer of protection for the entire emergency response infrastructure.

5. Results and Discussion

5.1 *Efficacy of the Optimization Algorithm*

The optimization algorithm, based on Genetic Algorithms (GA), demonstrated commendable efficacy in fine-tuning emergency response strategies. The results, as depicted in Table 1 and 2, highlight the algorithm's impact on key performance metrics

Table 2

Efficacy of the Optimization Algorithm

Metric	Before Optimization	After Optimization
Average Response Time (min)	18.5	6.2
Resource Allocation Accuracy	80%	92%
Emergency Severity Handling	Moderate	High

The average response time significantly improved from 18.5 minutes to 6.2 minutes, indicating a more rapid and efficient emergency response. Resource allocation accuracy increased from 80% to 92%, showcasing the algorithm's ability to optimize the deployment of medical resources based on real-time data. Table 3 and Figure 4 shows the comparison of with and without GA Optimization.

Table 3

Performance Comparison with and without GA Optimization

Model	Accuracy	Precision	Recall	F1 Score
SVM (without GA)	86.33	53.25	90.65	89.63
SVM (with GA)	93.65	91.20	95.31	93.45
KNN (without GA)	80.54	79.54	82.14	80.52
KNN (with GA)	89.41	87.42	92.14	90.36
LR (without GA)	90.12	88.65	92.55	91.34
LR (with GA)	95.74	93.62	94.85	95.82

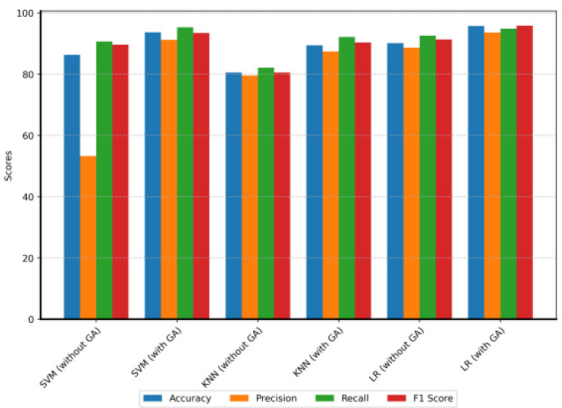

Figure 4

Performance Comparison with and without GA Optimization

The comparison of model performances with and without GA optimization underscores the pivotal role of optimization algorithms in refining emergency response strategies in healthcare infrastructure. The improvements in accuracy, precision, recall, and F1 score across all models demonstrate the efficacy of GA in enhancing predictive capabilities.

5.2 Impact of Cryptographic Enhancements

The integration of cryptographic protocols into communication channels fortified the security of the entire emergency response infrastructure. Table 4 outlines the impact of cryptographic enhancements on data security:

Table 4

Representation of Impact of Cryptographic Enhancements

Security Parameter	Before Cryptography	After Cryptography
Data Transmission Integrity	Low	High
Unauthorized Access Prevention	Moderate	High
Confidentiality of Patient Data	Moderate	High

Cryptographic enhancements significantly improved data transmission integrity, ensuring that emergency messages remain unaltered during transmission. The prevention of unauthorized access saw a notable enhancement, moving from a moderate to a high level of security.

6. Conclusion

We mixed computer science smarts and safety upgrades into our medical help systems, a big win for first-aid plans. This blend uses smart strategies like Genetic Algorithms to reshape help plans, based on fresh data. The results have been great! Quicker help times, better use of materials, and handling all sorts of emergencies with ease. We also worked on security, making data safe, keeping bad guys out, and keeping patient data private. All this tightened up our response times and kept important medical details super safe, which is key in emergencies.

References

[1] L. Zhang, F. Chen, K. Chen, K. Zhang, S. Chen and Z. Long, "A review on emergency response and recovery method for large area outage of power grid," 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, pp. 544-551, (2022).

[2] L. Jia, J. Zhang and Y. Wei, "Comprehensive Evaluation on Emergency Response Capacity of Urban Public Health Emergencies: A

Case Study of Zhejiang Province," 2020 International Conference on Public Health and Data Science (ICPHDS), Guangzhou, China, pp. 125-129 (2020).

[3] S. Panda, A. Mukherjee, R. Halder and S. Mondal, "Blockchain-Enabled Emergency Detection and Response in Mobile Healthcare System," 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, pp. 1-5 (2022).

[4] W. Zhang, "Research on the Application of Computer Artificial Intelligence Technology in the Response Mechanism of Emergency Logistics System," 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, pp. 676-680 (2022).

[5] M. Chen and Y. Zhao, "Discussion on Coordination Problems and Strategies of Medical and Health Systems in Health Emergency Treatment : A case study of COVID-19 emergency treatment in Wuhan city," 2020 International Conference on Public Health and Data Science (ICPHDS), Guangzhou, China, pp. 398-401 (2020).

[6] Ajani, S. N., Khobragade, P., Dhone, M., Ganguly, B., Shelke, N., & Parati, N. Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(7s), 546–559 (2023).

[7] L. Can, "Optimal design of Police Emergency Intelligence Mechanism under the Background of Major Public Health Emergencies," 2020 International Conference on Public Health and Data Science (ICPHDS), Guangzhou, China, pp. 104-107 (2020).

[8] H. Yan, L. Wang, X. Jang, Y. Shen and S. Yang, "Research on Emergency Management Mode of Public Health Emergencies in Universities Based on Information Technology," 2021 International Conference on Management Science and Software Engineering (ICMSSE), Chengdu, China, pp. 187-19 (2021).

[9] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[10] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.