Performance Analysis of the Latest Encryption Algorithms in VANET-SDN for Healthcare in Smart CitiesSmart Cities

Dr.Moawiah El-Dalahmeh, Al-zaytoonah University of Jordan. Jordan

Abstract (300 word limit)

The The integration of Vehicular Ad Hoc Networks (VANET) with Software-Defined Networking (SDN) is revolutionizing healthcare in smart cities by enabling real-time communication between ambulances, hospitals, and healthcare infrastructure. This integration enhances

emergency response efficiency, remote diagnostics, and medical data transmission. However, the dynamic and open nature of VANET-SDN poses significant cybersecurity risks, particularly

regarding sensitive patient data. Traditional encryption methods struggle to provide both security and performance, especially against emerging threats such as quantum attacks, Man-in-the-

Middle (MITM) attacks, and DDoS attacks.

This study evaluates the performance of next-generation encryption algorithms for securing VANET-SDN healthcare environments, focusing on:

1. Post-Quantum Cryptography (PQC): Secure encryption schemes resistant to quantum attacks, including CRYSTALS-Kyber and SPHINCS+.

2. Neural Cryptography: AI-driven encryption leveraging deep neural networks for adaptive key generation, reducing energy consumption.

3. Deep Learning-Based Encryption: A novel approach enhancing security and computationaln efficiency for real-time medical data transmission.

Using NS-3 and Qiskit, we simulated a smart city environment with 200 smart medical vehicles, 30 hospitals, and 1,000 infrastructure units. Results showed that deep learning-based encryption

reduced energy consumption by 55% compared to AES-256, while Quantum Digital Signatures (QDS) provided an 8192-bit security level with minimal latency impact. Additionally, our Quantum-Optimized Routing (QOR) algorithm improved ambulance response time by 62%.

These findings highlight the potential of AI and quantum-secure encryption for ensuring fast, secure, and efficient healthcare communications in smart citiesintegration of Vehicular Ad Hoc Networks (VANET) with Software-Defined Networking (SDN) is revolutionizing healthcare in smart cities by enabling real-time communication

between ambulances, hospitals, and healthcare infrastructure. This integration enhances emergency response efficiency, remote diagnostics, and medical data transmission. However, the

dynamic and open nature of VANET-SDN poses significant cybersecurity risks, particularly regarding sensitive patient data. Traditional encryption methods struggle to provide both security and performance, especially against emerging threats such as quantum attacks, Man-in-the-Middle (MITM) attacks, and DDoS attacks.

This study evaluates the performance of next-generation encryption a algorithms for securing VANET-SDN healthcare environments, focusing on:

1. Post-Quantum Cryptography (PQC): Secure encryption schemes resistant to quantum attacks, including CRYSTALS-Kyber and SPHINCS+.

2. Neural Cryptography: AI-driven encryption leveraging deep neural networks for adaptive key generation, reducing energy consumption.

3. Deep Learning-Based Encryption: A novel approach enhancing security and computational efficiency for real-time medical data transmission.

Using NS-3 and Qiskit, we simulated a smart city environment with 200 smart medical vehicles, 30 hospitals, and 1,000 infrastructure units. Results showed that deep learning-based encryption reduced energy consumption by 55% compared to AES-256, while Quantum Digital Signatures (QDS) provided an 8192-bit security level with minimal latency impact. Additionally, our Quantum-Optimized Routing (QOR) algorithm improved ambulance response time by 62%.

These findings highlight the potential of AI and quantum-secure encryption for ensuring fast, secure, and efficient healthcare communications in smart cities.

Image



Recent Publications (minimum 5)

1. El-Dalahmeh, M. and Adeel, U., 2023, May. Intrusion detection system for SDN based VANETs using a deep belief network, decision tree, and ToN-IoT dataset. In *2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET)* (pp. 1-6). IEEE.
2. El-Dalahmeh, A., El-Dalahmeh, M., Razzaque, M.A. and Li, J., 2024. Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. *Security and Privacy*, *7*(6), p.e446
3. El-Dalahmeh, M., El-Dalahmeh, A. and Adeel, U., 2023. A Critical Review of Software Defined Networks Enabled Vehicular Ad Hoc Network. *International Journal of Future Computer and Communication*, *12*(3).
4. El-Dalahmeh, A., El-Dalahmeh, M. and Li, J., 2024, June. Enhanced Vehicle Detection through Multi-Sensor Fusion Utilizing YOLO-NAS and Faster R-CNN. In *2024 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-6). IEEE.
5. El-Dalahmeh, M., El-Dalahmeh, A. and Adeel, U., 2024. Analysing the performance of AODV, OLSR, and DSDV routing protocols in VANET based on the ECIE method. *IET Networks*, *13*(5-6), pp.377-394.

Photograph



Biography (150 word limit)

I am a cybersecurity researcher with a PhD in Computer Science (Cybersecurity) from Teesside University, specializing in cloud computing, network security, and instructional technology. I also hold an MSc in Network Systems from the University of Sunderland and have extensive experience in course development for cloud computing and cybersecurity principles. My research focuses on emerging security challenges in smart cities, particularly the integration of Vehicular Ad Hoc Networks (VANET) with Software-Defined Networking (SDN) for healthcare applications. I explore next-generation encryption techniques, including post-quantum cryptography, neural cryptography, and deep learning-based encryption, to enhance data security and emergency response efficiency. Additionally, I am passionate about developing innovative educational frameworks to equip future cybersecurity professionals with practical skills. I have designed and delivered a 16-week university-level course on Cloud Computing Security, blending theoretical concepts with hands-on applications. My goal is to advance secure, intelligent, and resilient network infrastructures for the digital future.

Email:M.eldalahmeh@zuj.edu.jo

Notes/Comments: