ABSTRACT

The Internet of Health Things (IoHT) is crucial in modern healthcare, enabling real-time patient monitoring and remote diagnostics through interconnected devices. However, protocols like MQTT, while efficient, lack strong security features, exposing sensitive health data to cyberattacks. As IoT technologies grow in healthcare, securing both the data payload and metadata is vital to maintaining patient privacy and trust.

This study proposes a dual-layer security scheme designed to address these vulnerabilities by integrating ASCON (Authenticated Encryption with Associated Data) encryption for payload protection with Zero-Width Characters (ZWC) for covert metadata concealment. The combination of these two techniques provides a comprehensive security solution, ensuring that both the medical data and the associated metadata such as device identifiers, patient information, and QoS levels are securely transmitted without exposing them to potential threats like metadata inference attacks or traffic analysis. Experimental results show that while implementing ASCON with ZWC results in a slight increase in latency from 0.54 ms for smaller payloads (8 KB) to 18.93 ms for larger payloads (1 MB) the trade-off between performance and security remains acceptable. The system also exhibits a strong avalanche effect, ranging from 51.02% to 51.25%, demonstrating its high sensitivity to changes in input and reinforcing its resilience against cryptographic attacks. Furthermore, the computational overhead remains manageable, with a modest increase in CPU load by only 1.2%, from 88.93% to 90.14%, as payload size increases.

By providing encryption for payloads and concealment metadata, this approach addresses critical security concerns in real-time healthcare applications. The integration of ZWC as a covert channel ensures that sensitive metadata is concealed without disrupting the MQTT protocol's structure, making this solution ideal for IoHT communication.

Keywords: MQTT, AEAD, ASCON, Covert Channel, Metadata Protection, Lightweight Encryption, Secure Communication, Health IoT.