ABSTRACT

The advancement of Internet of Things (IoT) technology brings numerous benefits but also poses risks to the security of sensitive data. This research aims to protect sensitive data communication in IoT using Zero Width Space (ZWSP) character-based steganography. This method allows sensitive data to be hidden within ordinary text without raising suspicion, ensuring that only authorized recipients can decrypt and access the message. The implementation of this research uses the ESP32 microcontroller and the DHT11 temperature sensor to collect data, which is then encrypted using ZWSP and transmitted to a server via the MQTT protocol. The encrypted data is displayed on a website.

The test results indicate that ZWSP-based steganography is effective in hiding sensitive data without altering the appearance of the original text. The tests show that the length of the original message increases significantly after encryption, with an average increase of 220% for 10-character messages, 110% for 20-character messages, 73.33% for 30-character messages, and 55% for 40-character messages. Quality of Service (QoS) measurements show that the system maintains good performance with HTTP throughput reaching 79-118 kbps, delay of 0.03-0.05 ms, and packet loss of 0.3%-17%. For the MQTT protocol, throughput reaches 486-14 Mbps, with low delay and minimal packet loss. Website performance testing with GTmetrix shows excellent performance with a score of 98%. Additionally, user survey results show that 97.1% of users feel comfortable with the website navigation, and 50% of users rate the visual design of the website as excellent.

Thus, ZWSP-based steganography can be an effective and efficient solution for protecting sensitive data in IoT communications, significantly contributing to enhancing data security in an increasingly connected IoT environment.

***Keywords**: Data security, Internet of Things (IoT), Steganography, Zero Width Space (ZWSP) characters*