ABSTRACT

The development of Internet of Things (IoT) technology has brought significant benefits in automation and monitoring across various sectors, including aquaculture. The My I-Pond system was developed as a real-time water quality monitoring solution for fish ponds using IoT devices. However, the open nature of networks and the limited capability of edge devices such as Raspberry Pi pose major challenges in ensuring data security and system performance. The main problem addressed in this research is how to design a secure, responsive, and efficient IoT security system within a resource-constrained edge computing environment.

The proposed solution is the development of an Edge Computing IoT Security (ECIS) system that integrates the Suricata Intrusion Prevention System (IPS) and AES-256 encryption algorithm, deployed on a Raspberry Pi. Suricata functions as a real-time threat detection and mitigation engine, while AES-256 ensures data confidentiality during transmission to the Firebase cloud. System performance was evaluated based on parameters including latency, throughput, processing overhead, response time, and scalability under various traffic loads and client counts.

The test results showed that ECIS successfully detected and mitigated 100% of common attacks, with an average response time of 206 ms and minimal overhead at 0.775%. The system remained stable with up to 50 active clients and no packet loss. Based on TIPHON parameters, the system performance is classified as Good to Excellent, establishing ECIS as an effective security solution for small- to medium-scale IoT deployments.

Keywords: AES-256, Edge Computing, IoT, Suricata, TIPHON