ABSTRACT

Secure key exchange is essential to ensuring the integrity and confidentiality of communications in IoT-based Early Warning Systems (EWS). This research evaluates the performance of the Boneh-Boyen Hierarchical Identity-Based Encryption (BB-HIBE) scheme as an alternative to conventional key exchange mechanisms such as TLS/ECDH. Simulations were conducted in a Microsoft Azure virtual machine environment to compare BB-HIBE and TLS/ECDH in terms of communication overhead and key storage requirements. Additionally, BB-HIBE was evaluated at two security levels (128-bit and 256-bit key sizes) to assess its execution time, CPU usage, and memory requirements. The results show that BB-HIBE significantly reduces both communication overhead and key storage compared to TLS/ECDH, especially as the number of users increases. Furthermore, the 128-bit implementation of BB-HIBE meets the international latency standard of less than 100 ms recommended for real-time IoT communications.

Keywords: BB-HIBE, Key Exchange, Early Warning Systems.