ABSTRAK

Ilham, Irvantoni. 2024. Perancangan Sistem Keamanan Data Pada Perangkat *Internet of Things* (IoT) Dengan Algoritma *PRESENT*, Skripsi. Tanjungpinang: Jurusan Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Univeristas Maritim Raja Ali Haji. Pembimbing I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Pembimbing II: M. Radzi Rathomi, S.Kom., M.Cs.

Penelitian ini bertujuan untuk merancang sistem keamanan data untuk perangkat Internet of Things (IoT) dengan menggunakan algoritma PRESENT. Fokusnya adalah meningkatkan keamanan saat data sensor dikirimkan ke media penyimpanan dan ditampilkan di antarmuka, seperti situs web. Metodologinya melibatkan pengujian prototipe sistem yang mengenkripsi data sensor menggunakan web server, menyimpannya sebagai ciphertext dalam database Firebase, dan mendekripsinya di web client. Hasil penelitian menunjukkan bahwa enkripsi PRESENT efektif dalam melindungi data dari serangan sniffing jaringan. Tanpa enkripsi, data mudah dibaca oleh penyerang. Namun, dengan enkripsi, data hanya muncul sebagai ciphertext, sehingga informasi sensitif tetap aman meskipun database diretas. Dari uji coba, penggunaan algoritma PRESENT secara signifikan meningkatkan keamanan data IoT, memperkuat kerahasiaan, dan mengurangi risiko serangan siber. Penelitian ini memperkuat pemahaman tentang pentingnya algoritma keamanan yang kuat untuk melindungi data IoT dari akses yang tidak sah dan serangan eksternal.

Kata kunci: ***Algoritma PRESENT, IoT (Internet of Things), Keamanan Data***

ABSTRACT

Ilham, Irvantoni. 2024. Designing Data Security System on Internet of Things (IoT) Devices with PRESENT Algorithm, Thesis. Tanjungpinang: Department of Informatics Engineering, Faculty of Maritime Engineering and Technology, University of Maritim Raja Ali Haji. Advisor I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Advisor II: M. Radzi Rathomi, S.Kom., M.Cs.

This research aims to design a data security system for Internet of Things (IoT) devices using the PRESENT algorithm. The focus is on enhancing security during the transfer of sensor data to storage media and displaying it on interfaces such as websites. The methodology involves testing a prototype system that encrypts sensor data using a web server, stores it as ciphertext in a Firebase database, and decrypts it on the web client. The results show that PRESENT encryption is effective in protecting data from network sniffing attacks. Without encryption, data is easily readable by attackers. However, with encryption, the data only appears as ciphertext, ensuring that sensitive information remains secure even if the database is hacked. The tests demonstrate that using the PRESENT algorithm significantly improves IoT data security, strengthens confidentiality, and reduces the risk of cyber-attacks. This research emphasizes the importance of strong security algorithms in protecting IoT data from unauthorized access and external attacks.

Keywords: ***PRESENT Algorithm, IoT (Internet of Things), Data Security***