# Pengembangan Sistem Keamanan Internet of Things (IoT) Skala Kecil Berbasis Network Intrusion Detection System (NIDS) dan Secure Access Point Menggunakan Raspberry Pi = Development of Small Scale Internet of Things (IoT) Security System Based on Intrusion Detection System and Secure Access Point on Raspberry Pi

Kevin Darmawan, author



---

Abstrak

Pesatnya perkembangan teknologi informasi di era revolusi industri 4.0 memicu berkembangnya paradigma Internet of Things (IoT) yang memudahkan otomasi dan monitoring rumah. Artinya bertambah pula kerentanan pada jaringan rumah yang menyebabkan resiko penurunan performa jaringan, hingga kebocoran data. Penelitian ini mengusulkan sistem keamanan jaringan IoT berbasis Raspberry Pi sebagai solusi IDS beserta tambahan secure access point yang terjangkau. Sistem keamanan yang dikembangkan dipercaya dapat mengisolasi jaringan IoT dengan lebih baik agar serangan tidak mempengaruhi kinerja perangkat IoT, dan memberikan alerting mengenai intrusion kepada pengguna untuk mengambil langkah terhadap resiko yang dapat terjadi. Intrusion Detection System berhasil mendeteksi serangan yang ada pada skenario dengan hasil maksimum: tingkat false alarm dibawah 15%, tingkat keberhasilan deteksi diatas 50% dan akurasi deteksi diatas 75% untuk skenario serangan Evil Twin, Reconnaissance, Distributed Denial of Service (DDoS), dan Man In The Middle (MITM) dan dapat mencegah serangan Evil Twin dan MITM.

.....

The rapid development of information technology in the industrial revolution 4.0 era triggers the development of the Internet of Things (IoT) paradigm in everyday life, facilitating automation and monitoring for home. This phenomenon introduces vulnerabilities in the home network and may lead to the risk of decreased network performance, and privacy leak. This study proposes an IoT network security system implementing Network Intrusion Detection System (NIDS) and secure access point based on Raspberry Pi as an affordable IDS solution. The proposed security system is believed to better isolate the IoT network and not affect the performance of IoT devices in case of attacks, also providing  intrusion alerts to encourage users to take steps against risks that may occur. The system is able to detect a maximum of: false alarm rate under 15%, successful detection rate above 50% and detection accuracy of 75% for Evil Twin, Reconnaissance, Distributed Denial of Service (DDoS), and Man In The Middle (MITM) attack scenarios with increased robustness in case of Evil Twin deauthentication and MITM attacks.