Pengembangan Pengamanan Pertukaran Data pada Perangkat Internet of Things (IoT) Menggunakan Algoritma Advanced Encryption Standard (AES) dan Metode Shift Left Security = Development of Data Exchange Security on Internet of Things (IoT) Devices Using Advanced Encryption Standard (AES) Algorithm and Shift Left Security Method

Valya Sandria Akiela, author

Abstrak

Internet of Things (IoT) tidak hanya mengubah cara perangkat berinteraksi dan terhubung, tetapi juga membawa risiko keamanan serius, seperti kebocoran data. Penelitian ini mengatasi masalah tersebut dengan menggabungkan Advanced Encryption Standard (AES) dan shift left security. AES digunakan untuk mengenkripsi data yang ditransmisikan melalui perangkat IoT dengan mempertimbangkan keterbatasan sumber daya komputasi, khususnya pada perangkat Smart Fan System, yang bekerja dengan mengaktifkan mini fan berdasarkan threshold suhu tertentu yang dapat dimonitor melalui web app. Pada penelitian ini, shift left security diterapkan untuk mengidentifikasi dan mengatasi kerentanan sejak tahap awal pengembangan. Efektivitas integrasi AES dan shift left security diuji dengan membandingkan waktu eksekusi dan kerentanan keamanan. Penetration testing dilakukan terhadap SQL injection, Man in the Middle (MITM) attack, dan Distributed Denial of Service (DDoS) attack. Hasil penelitian menunjukkan peningkatan keamanan sebesar 66.67% dengan waktu eksekusi 485.51 ms pada sistem IoT yang mengintegrasikan AES dan shift left security, tanpa penurunan performa signifikan. Meskipun efektif terhadap SQL injection dan MITM attack, sistem masih rentan terhadap DDoS attack, sehingga diperlukan strategi tambahan yang lebih komprehensif. Penelitian ini diharapkan memberikan kontribusi penting dalam desain perangkat IoT yang lebih aman dan andal di masa depan.
.....The Internet of Things (IoT) not only transforms how devices interact and connect but also brings serious security risks, such as data breaches. This study addresses these issues by combining Advanced Encryption Standard (AES) and shift left security. AES is used to encrypt data transmitted through IoT devices, considering computational resource limitations, particularly in the Smart Fan System, which operates by activating a mini fan based on specific temperature threshold that can be monitored via a web app. In this research, shift left security is applied to identify and address vulnerabilities from the early stages of development. The effectiveness of integrating AES and shift left security is tested by comparing execution time and security vulnerabilities. Penetration testing is conducted against SQL injection, Man in the Middle (MITM) attack, and Distributed Denial of Service (DDoS) attack. The results show a 66.67% increase in security with an execution time of 485.51 ms in the IoT system integrating AES and shift left security, without significant performance degradation. Although effective against SQL injection and MITM attacks, the system remains vulnerable to DDoS attacks, indicating the need for more comprehensive strategies. This research is expected to make a significant contribution to the design of more secure and reliable IoT devices in the future.