

INTISARI

IMPLEMENTASI KRIPTOGRAFI PADA KOMUNIKASI PERANGKAT IOT MENGGUNAKAN ADVANCED ENCRYPTION STANDARD (AES)

Pada saat ini internet merupakan kebutuhan primer dimana hampir semua orang memiliki akses terhadap jaringan internet. Saat ini perkembangan internet tidak hanya digunakan sebagai media akses terhadap informasi bahkan sebagai media kendali atau *remote access* terhadap *hardware* atau perangkat apa pun didalamnya.

Seseorang dapat melihat, mengendalikan segala perangkat yang letaknya bahkan tidak diketahui seperti *cloud computer* atau *Internet of Things* (IoT). Mulai era inilah IoT berkembang begitu pesat menjadikan jumlah perangkat yang terkoneksi dengan jaringan internet semakin banyak. Data yang dikirimkan lewat jaringan dapat dilihat siapa saja yang memiliki akses sehingga apabila data yang dikirimkan adalah informasi yang penting akan sangat berbahaya.

Komunikasi perangkat IoT yang dilakukan lewat jaringan juga merupakan sasaran kejahatan dunia maya. *Advanced Encryption Standard* 128 (AES 128) digunakan dalam metode pengamanan karena beberapa sifatnya yang fleksibel diantaranya relatif cepat, aman dan membutuhkan resource yang lebih sedikit. AES 128 sendiri merupakan jenis enkripsi simetrik dimana menggunakan kunci yang sama untuk enkripsi-dekripsi. Maka dari itu AES 128 dapat digunakan dalam perangkat dengan resource yang kecil serta memiliki kecepatan yang baik sehingga efektif meningkatkan keamanan perangkat IoT dari penyerang dan penyadap informasi penting yang dikirimkannya lewat jaringan.

Kata Kunci : *Advanced Encryption Standard*, AES, *Internet of Things*, IoT, Kriptografi

ABSTRACT

IMPLEMENTATION OF CRYPTOGRAPHY ON IOT DEVICE COMMUNICATION USE ADVANCED ENCRYPTION STANDARD ALGORITHM (AES)

At present the internet is a primary need where almost everyone has access to internet networks. At present the development of the internet is not only used as a medium of access to information even as a medium of control or remote access to any hardware or devices in it.

One can see, control all devices that are even unknown, such as cloud computers or Internet of Things (IoT). Starting from this era IoT is growing so rapidly that the number of devices connected to the internet network is increasing. Data sent over the network can be seen by anyone who has access so that if the data sent is important information, it will be very dangerous.

Communication of IoT devices that are carried out over the network is also the target of cyber crime. The Advanced Encryption Standard 128 (AES 128) is used in security methods because some of its flexible properties are relatively fast, safe and require fewer resources. AES 128 itself is a type of symmetric encryption which uses the same key for encryption-decryption. Therefore AES 128 can be used in devices with small resources and has good speed so that it effectively increases the security of IoT devices from attackers and tappers of important information that they send over the network.

Keywords : *Advanced Stanadard Encryption, AES, Internet of Things, IoT, Crtiptography*