ABSTRACT

In the rapid development of the Internet there is one utilization of the development in the Internet is a emergance Internet of Things (IoT) concept. In the application of this IoT concept, it turns out that many cases found on IoT devices are a cyber crime target, with the connection of the device to the Internet network, there is a vulnerability in the IoT network, so it's where the biggest challenge for IoT.

With this problem, security systems are developed by making security from IoT devices and IoT networks by adopting the Advanced Encryption Standard (AES) and MD5 algorithms. Security on IoT device side purpose make only legal devices be able to respond data from the server in other words only legitimate users can be access, then encrypt-decrypt purpose makes process of sending data is kept confidential and validity.

The security system tested by using DoS attack scenarios. Testing was conducted to determine the formation of QoS and CPU Usage on the designed system. The result of the test is the delay of 0, 26284968s on the security system without any attack, the difference of delay between that implements the system and without a system with Dos attack tool ApacheJMeter of 10% and with Loic DOS tools by 4%. As for the results of increased CPU usage difference between 9% on systems designed with DoS attacks and without DoS attacks.

Keywords : Internet of Things (IoT), Advanced Encryption Standard (AES), MD5, DDoS