

ABSTRACT

INTERNET OF THINGS (IoT) DATA SECURITY USING AES ALGORITHM

By :

Nisa Hayati

Faculty of Computer, Informatics and Business Institution

nisahayati.1711060012@mail.darmajaya.ac.id

Internet of Things (IoT) is not new in this modernization era. Along with the rapid growth of the Internet of Things today, it is necessary to have a data security method on the Internet of Things. This study will propose an Internet of Things (IoT) data security method using AES 128, where AES 128 uses 10 repetitions to perform the encryption process. The microcontroller will process the data in such a way and after that the data will be transferred to the web server. This data will be encrypted using the AES algorithm. The AES algorithm encryption process consists of 4 types of bytes transformation, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. Testing begins by ensuring that every component on the hardware and software can work according to the previous design, then testing the encryption and decryption of data. Based on the results of research that has been carried out in the overall test, it can be seen that encryption and decryption of sensor data on the 128 bit AES algorithm can be done. Based on the results of the tool trials that have been carried out, it can be concluded that this research has been running according to the design, this research has been able to secure internet of things devices by encrypting and decrypting using the 128 bit AES algorithm.