ABSTRACT

IoT or the Internet of Things is a network that can link various objects that have identity identities and IP addresses, so they can connect to each other and exchange information. In this simulation of security design of smart electricity network, the implementation of Smart KWH Meter utilizes Internet connection and connect it with Android device to display the power data consumed. But the process of sending information by utilizing the Internet network to an Android device through the Firebase server is sometimes not always going well. There are several factors that may cause the data delivery process to be hampered by one of them is with network attacks such as DOS attack (Smurults attack) and Sniffing attack which can cause failure in Data transmission, not only the failure of data transmission may also lead to the loss of user data.

At the end of this task is implemented a network security system for the process of sending power usage data on Smart KWH meters. To avoid attacks that can cause failures in the transmission of such data. Using the hping3 command on the attack simulation DOS attack and Sniffing attack using Etttercap tools.

From the results of research and analysis that has been done it can be concluded that by using IP tables that have been configured and then tested with a DOS attack simulation and Sniffing attack can protect the network or Smart KWH Meter connection when sending data using the internet network.

***Keywords**: Internet of Things, Android, Firebase, Cyber Security, DOS Attack, Sniffing Attack*

.