

ABSTRAK

IMPLEMENTASI NETWORK INTRUSION DETECTION SYTEM (NIDS) *RULE-BASED* PADA JARINGAN *SMART DOOR LOCK* DENGAN MEDIA NOTIFIKASI TELEGRAM

Dalam perkembangannya teknologi dari *Internet of things* (IoT) saat ini telah mencapai titik dimana manusia telah mengembangkan sedemikian rupa hingga menjadi suatu alat yang berguna pada suatu bidang. Teknologi IoT memudahkan suatu pekerjaan manusia dalam aspek tertentu. Seperti dalam bidang infrastruktur, perancangan suatu sistem IoT yaitu *smart door lock* berguna dalam pembuatan suatu akses pada sebuah ruangan. Dengan demikian setiap orang yang ingin masuk kedalam ruangan tersebut harus memiliki izin terlebih dahulu, selain itu siapapun yang masuk kedalam ruangan akan tercatat pada suatu *database*. Pengembangan teknologi ini menggunakan *radio frequency identification* (RFID), sebagai sarana dari sistem pintu pintar tersebut. RFID bekerja secara *wireless*, dengan demikian RFID menggunakan gelombang radio untuk pengambilan data. Hasil dari RFID berupa *tag* yang berisikan nilai unik dari kartu yang dibaca oleh *reader*. Dalam studi perkembangan sebuah sistem, tidak luput dari suatu daya kerapuhan dari sistem tersebut. Setiap sistem yang menggunakan sebuah jaringan dalam beroperasi membutuhkan suatu pengamanan tertentu. *Data* pribadi yang saling bertukar pada jaringan sistem harus dilindungi agar tidak dicuri oleh *Attacker*. Dengan demikian dalam perancangan sebuah IoT harus memiliki sistem keamanan yang terpercaya dan dapat diandalkan. Dalam pengembangan tugas akhir saya ini akan mengimplementasikan sebuah sistem keamanan yang bekerja untuk melindungi jaringan IoT *smart door lock*. Sistem keamanan yang dirancang yaitu *network intrusion detection system* (NIDS). Sistem NIDS memungkinkan kita untuk mengobservasi setiap *traffic* jaringan yang terjadi pada jaringan IoT tersebut. Dengan menggunakan suatu metode *rules-based* sistem NIDS ini akan mencatat apabila terjadi sebuah anomali jaringan berdasarkan *rules* yang ada. NIDS yang dikembangkan menggunakan *software open-source* Snort. Perancangan Snort IDS diharapkan dapat melindungi *traffic* jaringan dari *smart door lock*. Untuk memudahkan *Administrator* dalam memitigasi setiap anomali yang terjadi pada jaringan tersebut, Snort IDS akan dilengkapi dengan *interface* yang digunakan untuk *Administrator* memantau jaringan *smart door lock*. Dengan demikian pengamanan jaringan pada sistem pintu pintar ini dapat dengan mudah diobservasi pada suatu waktu.

Kata kunci ; RFID, *Smart door lock*, NIDS, Snort, *Rule-base*

ABSTRACT

IMPLEMENTATION OF RULE-BASED NETWORK INTRUSION DETECTION SYSTEM (NIDS) SMART DOOR LOCK NETWORK WITH TELEGRAM NOTIFICATION

In its development of internet of things (IoT) technology has grown respectively at some of human's life aspect. At this moment human have developed some IoT technology that is useful for certain area. This IoT technology facilities human work in many ways. As in infrastructure, one of the technology IoT example is smart door lock, the use of it is making an access to a spesific room. Thus for every person that wants to access the room or building must have a permission. Smart door lock system also have database that makes every user that accessing the room or building will be recorded into database. This tech using a module named radio frequency identification (RFID). The smart door lock system use this module to operate. RFID module works wirelessly, so that RFID uses radio waves for data retrieval. When RFID module receive an input from a card, RFID contain a tag that have unique value of the card. In development of an IoT system, vulnerability of the system is one of the concern for making a great system with vulnerability is on the lowest level. So that system need a proper security to makes sure that the vulnerability of the system monitorized by the administrator. The system network must be protected while it exchanging any personal data for some point. The system must have a trusted and reliable security. In this final project, I will implement a security for an IoT system, this security section will protect smart door lock IoT network system. The security design is the network intrusion detection system (NIDS). NIDS system allows us to observe network traffic that occurs on IoT. By using a rules-based method, NIDS will record every anomaly on the IoT network based on the rules. In this implementation of a security system, NIDS will be develop by using an open-source software called Snort. This Snort software will protect network traffic from the IoT smart door lock system. In this implementation of a solid system, NIDS will have an interface that is used for administrator monitor the traffic network on smart door lock system. So that administrator will easily can mitigate every anomalies that occurs on the network and traffic of smart door lock system also secured in that moment.

Keywords : RFID, Smart door lock, NIDS, Snort, Rule-Based