

Context-Awareness pada API Gateway sebagai Middleware dalam Menentukan Layanan Otentikasi (Skenario : *Smart Homes*)

Anom Sentanu Prayosa¹, Parman Sukarno², Rahmat Yasirandi³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

⁴Divisi Digital Service PT Telekomunikasi Indonesia

¹anomsentanu@students.telkomuniversity.ac.id, ²psukarno@telkomuniversity.ac.id,

³rahmat.yasirandi@telkomuniversity.ac.id

Abstrak

bertambahnya pengguna perangkat IoT pada saat ini membuat perangkat IoT semakin berkembang. Adanya layanan untuk *smart homes* seperti kamera pengintai, lampu pintar, pintu pintar yang dapat diakses dari jarak jauh menjadi bukti bahwa perangkat IoT semakin diminati dan semakin berkembang sampai saat ini. Dengan berkembangnya perangkat IoT maka akan semakin besar juga persentase terjadinya ancaman. Ancaman yang sangat sering terjadi adalah pada bagian otentikasi karena otentikasi merupakan pintu masuk yang harus dilewati oleh para peretas untuk bisa akses ke sebuah perangkat. Perangkat IoT pada *smart homes* juga tidak memiliki pembagian hak layanan, sehingga kapanpun dimanapun bisa akses perangkat tersebut selama pengguna memiliki otentikasi dasar dari perangkat seperti *username* dan *password*.

Pada studi ini akan dibuat *context awareness* pada sistem otentikasi untuk menentukan layanan yang ada pada *smart homes*. Pada dasarnya *smart homes* hanya memiliki satu *layer* otentikasi (*username/password*) dan ini adalah kelemahan *smart homes* pada bagian otentikasi. Pada penelitian ini akan dibuat *multi layer* pada otentikasi perangkat *smart homes* dengan menggunakan metode *context awareness*. Metode *context awareness* dapat membaca prilaku dari pengguna, sehingga keamanan dan kenyamanan dari pengguna bisa seimbang. Metode *context awareness* akan menjadi *multi layer* otentikasi pada perangkat IoT, dengan adanya metode ini hak layanan perangkat IoT pada *smart homes* dapat diatur.

Kata kunci : *context-awareness*, otentikasi, *layer*

Abstract

The increasing number of IoT device users is currently making IoT devices more developed. The existence of services for smart homes such as surveillance cameras, smart lights, smart doors that can be accessed remotely is proof that IoT devices are increasingly in demand and are increasingly developing until now. With the development of IoT devices, the proportion of threats will be greater. The threat that occurs very often is in the authentication section, because authentication is the entrance that hackers must pass to be able to access a device. IoT devices in smart homes also do not have shared service rights, so they can access the device anytime anywhere as long as the user has basic authentication from the device such as a username and password.

In this study, context awareness will be made on the authentication system to determine the existing services for smart homes. Basically, smart homes only have one authentication layer (*username / password*) and this is the weakness of smart homes in the authentication part. In this study, multi-layer authentication of smart homes devices will be created using the context awareness method. The context awareness method can read the behavior of the user, so that the safety and comfort of the user can be balanced. The context awareness method will be a multi-layer authentication on IoT devices, with this method the right to service IoT devices on smart homes can be managed.

Keywords: *context-awareness*, authentication, *layer*
