SYBIL ATTACK MITIGATION WITH BEHAVIOUR DETECTION ON FOG COMPUTING NETWORK

Yusuf Agung Purnomo[1], Vera Suryani, S.T., M.T.[2], Aulia Arif Wardana, S.Kom., M.T.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]yusufap@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstract

Nowadays, Internet of Things are fastly being develop, the application of this technology had already been done on several fields. But, it doesn't mean that this technology is safe from cyber attacks, one of cyber attacks that could attack this network is Sybil where the attackers will impersonating other user on the network. So. a detection method is needed to filter and separate these attackers in order to maintain the performance of the network.

One of the methods that can be use to detect Sybil activities is Behaviour Detection method which it will check every communications in and out of the network and separated the sybil node out of the network if detected. The criteria of a node can be called as a sybil is when it pass certain thresholds that has been already set, one of the threshold components are how fast the interval of an ID and locations of a node changed.

The end result is this system can detect sybil node with success rate up to 90%. The result came from arranging the threshold sensitivity that being used to do detection.

Key Words : ***internet of things, sybil, fog computing, honeypot, behavioral detection, iot.***