

# MITIGASI SERANGAN SYBIL DENGAN METODE *BEHAVIOUR DETECTION* PADA JARINGAN *FOG COMPUTING*

Yusuf Agung Purnomo<sup>1</sup>, Vera Suryani, S.T., M.T.<sup>2</sup>, Aulia Arif Wardana, S.Kom., M.T.<sup>3</sup>

<sup>1,2,3</sup>Fakultas Informatika, Universitas Telkom, Bandung

<sup>1</sup>yusufap@student.telkomuniversity.ac.id, <sup>2</sup>verasuryani@telkomuniversity.ac.id,

<sup>3</sup>auliawardan@telkomuniversity.ac.id

---

## Abstrak

*Internet of Things* saat ini berkembang dengan pesat, pengaplikasian teknologi ini sudah banyak dilakukan di berbagai macam lini. Tetapi, tidak berarti bahwa teknologi ini aman dari serangan *cyber*, salah satu jenis serangan yang bisa menyerang jaringan ini ialah *Sybil* yaitu sebuah jenis serangan di mana penyerang akan meniru identitas *node* lokal yang ada di jaringan tersebut. Sehingga diperlukan metode pendeteksian yang bisa menyaring dan memisahkan penyerang ini sehingga performansi jaringan tetap terjaga.

Salah satu metode yang bisa dilakukan untuk mendeteksi aktifitas *Sybil* adalah dengan metode *Behaviour Detection*, di mana metode ini akan memeriksa setiap komunikasi keluar masuk jaringan dan memisahkan *sybil node* keluar jaringan jika terdeteksi. Kriteria sebuah *node* dikatakan *sybil* adalah ketika ia melewati sebuah *threshold* yang telah ditentukan, komponen *threshold* itu di antara nya adalah cepat nya perubahan *ID*, dan lokasi dari suatu *node*.

Hasil yang didapatkan adalah sistem ini dapat mendeteksi *sybil node* dengan tingkat keberhasilan hingga 90%. Hasil ini didapatkan dengan mengatur sensitivitas *threshold* yang digunakan untuk proses pendeteksian.

**Kata Kunci:** *internet of things, sybil, fog computing, honeypot, behavioral detection, iot.*