

ABSTRAK

Internet of Things (IoT) merupakan sebuah paradigma yang muncul dalam teknologi informasi yang mengintegrasikan kemajuan dalam *sensing*, komputasi, dan komunikasi untuk meningkatkan layanan yang ada dalam kehidupan sehari-hari. Pada umumnya, IoT mengacu pada suatu objek fisik yang terhubung dengan jaringan. Objek fisik tersebut terdiri atas sensor dan aktuator yang dapat bertukar data untuk menawarkan peningkatan kualitas layanan dalam kehidupan sehari-hari. Pada saat pertukaran data terjadi, data yang ditukarkan merupakan data sensitif sehingga data tersebut rentan terhadap ancaman keamanan yang diluncurkan oleh penyerang, salah satunya adalah serangan *sybil*. Pada penelitian ini, penulis mengajukan metode manajemen *trustworthiness* berdasarkan pada autentikasi dan *trust value*. Setelah dilakukan pengujian pada dua skenario, sistem mampu mendeteksi serangan *sybil* dengan cepat dan akurat. Rata-rata waktu yang dibutuhkan untuk mendeteksi serangan *sybil* adalah 9,3287 detik. Selain itu, sistem juga mampu memproses nilai *trust* yang telah disimpan di dalam *database* sehingga dapat menentukan objek mana yang memiliki nilai *trust* tertinggi dan terendah.

Kata Kunci : IoT, Serangan Sybil, Manajemen Trustworthiness, Authentication.