Pengamanan Objek IoT Terhadap Serangan *Sybil* Menggunakan Manajemen *Trustworthiness*

Ridwan Hadiansyah[1], Vera Suryani[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]rhd.learn@gmail.com, [2]verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

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 tiga skenario, sistem mampu mendeteksi serangan *sybil* dengan cepat dan akurat. Rata-rata waktu yang dibutuhkan untuk mendeteksi serangan *sybil* adalah 9,3287 detik. Lalu, rata-rata waktu yang dibutuhkan untuk mendeteksi objek *intruder* pada sistem adalah 18,1029 detik. Akurasi yang dihasilkan pada setiap skenario adalah 100%, sehingga dapat disimpulkan bahwa akurasi yang dihasilkan oleh sistem untuk mendeteksi serangan *sybil* adalah 100%.**

Kata kunci : Manajemen *Trustworthiness*, Serangan *Sybil*, Autentikasi.

Abstract

Internet of Things (IoT) is an emerging paradigm in information technology that integrates development in sensing, computing, and communication to improve existing services in everyday life. In general, IoT refers to physical objects that are connected to the network. These physical objects consist of sensors and actuators that can exchange data to offer improved quality of service in everyday life. When data transfer occurs, the data exchanged is sensitive data so that the data is vulnerable to security launched by the attacker, one of which is the Sybil attack. Sybil attacks allow IoT users to be cheated by other devices because there is no prior checking of device information. In this study, the authors propose a trust management method based on authentication and the value of trust. After testing on two scenarios, the system is able to detect Sybil attacks quickly and accurately. The average time needed to detect a sybil attack is 9,3287 seconds. Then, the average time needed to detect intruder objects in the system is 18.1029 seconds. The accuracy produced in each scenario is 100%, so it can be concluded that the accuracy generated by the system for detecting Sybil attacks is 100%.

1. Pendahuluan

Latar Belakang

Kemunculan *Internet of Things* (IoT) pada saat ini telah merubah cara pandang manusia berinteraksi dengan teknologi. Dengan adanya peningkatan di bidang jaringan, komunikasi, komputasi, *software* dan *hardware* menyebabkan IoT berkembang dengan cepat [1]. Dengan perkembangan IoT saat ini, memungkinkan perangkat elektronik di lingkungan sekitar kita untuk menjadi partisipan aktif dengan berbagi informasi melalui jarigan yang terhubung sehingga memungkinkan mengenali peristiwa dan perubahan di sekitarnya dan mampu bertindak secara mandiri tanpa harus ada campur tangan manusia [6]. 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 [2]. Selain itu juga, dengan keberadaan jaringan yang besar dari suatu objek yang terhubung pasti akan menimbulkan ancaman keamanan, privasi, dan *trust threats* yang memungkinkan objek berada dalam risiko yang tinggi [6].

John R. Douceur dalam penelitian [13] mengatakan bahwa jika satu objek dapat menampilkan banyak identitas sehingga mampu mengontrol sebagian kecil dari sistem, maka kondisi tersebut disebut dengan serangan

sybil. Berdasarkan [4] untuk menghindari ancaman yang ada pada IoT, dibutuhkan manajemen *trust* agar dapat membantu pengguna memberikan rasa aman dari ancaman yang beredar di jaringan. Manajemen *trust* memainkan peran yang penting di dalam IoT karena terdapat informasi yang dibutuhkan oleh pengguna, salah satunya adalah reputasi. Reputasi adalah ukuran yang berasal dari pengetahuan atau pengalaman langsung atau tidak langsung pada saat melakukan interaksi antar perangkat dan digunakan untuk menilai tingkat kepercayaan suatu perangkat.

Pada penulisan penelitian ini untuk mengamankan suatu objek IoT, penulis mengajukan metode manajemen *trustworthiness* yang berdasarkan pada autentikasi dan *trust value* untuk mengamankan objek IoT dari serangan *sybil*. Metode ini akan di simulasi dan di analisis pada objek Raspberry Pi 3b+ dan ESP8266.

Topik dan Batasannya

Rumusan masalah yang diangkat di dalam penelitian ini adalah bagaimana cara untuk mendeteksi penyerangan *sybil* terhadap objek IoT menggunakan manajemen *Trustworthiness* dan batasan masalah yang digunakan pada penelitian ini adalah sebagai berikut:

1. Perangkat yang digunakan untuk pengujian adalah tiga buah ESP8266 dan satu buah Raspberry Pi 3b+.
2. Protokol komunikasi yang digunakan pada pengujian adalah MQTT.

Tujuan

Tujuan pada penelitian ini adalah untuk melakukan pengamanan objek IoT dari serangan *sybil* dengan memanfaatkan komunikasi antar objek yang mengacu pada metode manajemen *trustworthiness* serta mengukur performansi pada objek IoT berdasarkan parameter akurasi dan waktu.

Organisasi Tulisan

Penulisan penelitian ini tersusun atas 5 bab. Pada bab 2 akan dijelaskan tentang Studi Terkait, bab 3 dijelaskan tentang sistem yang dibangun, yaitu pembuatan simulasi MQTT. Bab 4 akan dijelaskan tentang evaluasi, dan bab 5 dijelaskan kesimpulan dan saran.

2. Studi Terkait

Manajemen *Trustworthiness*

Manajemen *Trustworthiness* merupakan salah satu bagian dari aspek keamanan yang dapat digunakan untuk mengamankan objek IoT. Tujuan dari penggunaan metode tersebut adalah untuk memprediksi *behaviour* dari suatu objek [8]. Pada penelitian [12] menjelaskan bahwa salah satu cara untuk mencari objek yang dapat dipercaya, dapat menggunakan manajemen *trustworthiness*. Manajemen *trustworthiness* digunakan untuk memverifikasi keamanan suatu objek. Alat yang digunakan di dalam manajemen *trustworthiness* untuk memverifikasi suatu objek yaitu menggunakan *trust assessment*. Penelitian [7] menjelaskan bahwa salah satu bagian dari manajemen *trustworthiness* yaitu *trust assessment* yang fungsinya adalah untuk menilai objek lain berdasarkan *behavior* objek tersebut. Proses ini sangat penting karena objek IoT cenderung diserang oleh *trust-based attack* yang diantaranya yaitu *good mouthing* dan *bad mouthing*.

Autentikasi

Autentikasi adalah sebuah metode yang digunakan untuk memfilter objek yang valid atau mencurigakan [7,11]. Pada penelitian [11] mengajukan sebuah metode manajemen *trust* dalam IoT menggunakan autentikasi dan otorisasi berbasis *locally centralized*. Metode ini dikatakan mampu mengantisipasi ancaman serangan DoS dan dapat menghindari *single point of failure*.

Serangan *sybil*

Penelitian [5] menjelaskan bahwa serangan *sybil* adalah serangan di mana penyerang memanipulasi sebuah *node* untuk menghadirkan banyak identitas sehingga dapat menghasilkan informasi yang salah.

Pada penelitian [1] untuk mendeteksi adanya serangan *sybil*, digunakan metode *VisIoT*. Metode tersebut terdiri dari dua buah komponen utama yaitu *anomaly detection engine* (ADE) dan *radial visualitation engine* (RVE). Hasil dari penelitian tersebut diperoleh bahwa untuk mendeteksi sebuah *node* yang mengklaim bahwa *node* tersebut adalah *neighbor node*, perlu dilakukan pengecekan apakah jangkauan komunikasi node tersebut melebihi jangkauan maksimum. Jika melebihi, maka dapat disimpulkan bahwa *node* tersebut merupakan *sybil node*.

Pada penelitian [2] mengajukan metode *enhanced AODV* (EAODV) untuk mendeteksi serangan *sybil*. Metode ini menggunakan pendekatan *behavior* untuk mendapatkan rute yang optimal. Rute akan dipilih berdasarkan dari nilai *trust* dan jumlah *hop*. *Node* nantinya akan diidentifikasi dan jika terdeteksi bahwa *node* tersebut adalah *sybil node*, maka *node* tersebut akan dibuang. Di dalam penelitian ini, metode EAODV akan dibandingkan dengan AODV, dan hasilnya menyatakan bahwa EAODV lebih efektif untuk mengidentifikasi dan mendeteksi *sybil node* pada jaringan IoT.

Pada penelitian [3] untuk mendeteksi dan mengurangi serangan *sybil*, digunakan metode komunikasi V2V. Metode ini menggunakan *trust value* dan perhitungan sederhana. Pada penelitian ini hanya bisa dilakukan pada kondisi tertentu, sehingga penelitian ini masih memiliki kekurangan.

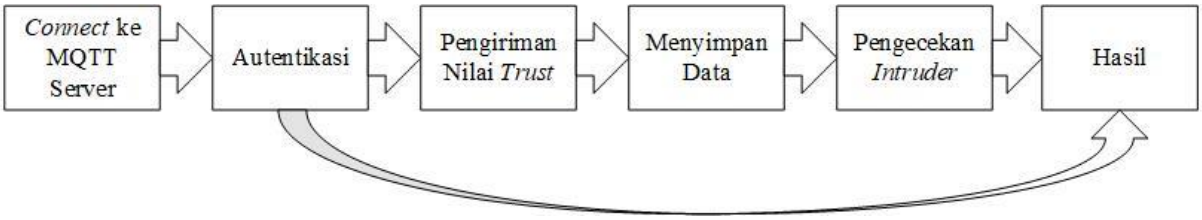
Pada penelitian [7] mengajukan metode *two-phase security protection* untuk mengamankan objek IoT. Metode tersebut menggunakan kombinasi dari autentikasi dan model statistik. Autentikasi digunakan untuk mendeteksi serangan *sybil* berdasarkan ID dari suatu objek sedangkan model statistik digunakan untuk mendeteksi *trust-based attacks*. Hasil dari penelitian tersebut menyatakan bahwa metode yang diajukan mampu menangani serangan *sybil* dan *trust-based attacks*.

Dari studi terkait diatas diperoleh bahwa untuk mempertahankan aspek keamanan pada suatu objek IoT, dibutuhkan nilai *trust* untuk mengetahui apakah suatu objek sedang melakukan serangan atau tidak. Di dalam penelitian ini, penulis mengajukan metode manajemen *trustworthiness* dengan menggunakan kombinasi dari autentikasi dan penilaian *trust*. Autentikasi digunakan untuk memeriksa apakah objek yang terhubung ke dalam server valid atau tidak, sedangkan penilaian *trust* digunakan untuk mengetahui apakah objek tersebut dapat dipercaya atau tidak.

3. Sistem yang Dibangun

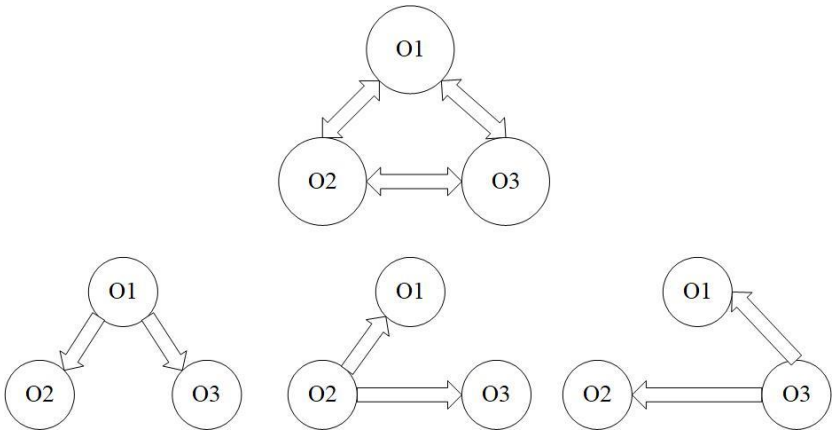
Gambaran Umum Sistem

Sistem yang dibangun pada penelitian ini merupakan sistem yang bertujuan untuk mendeteksi serangan *sybil* dengan menggunakan manajemen *trustworthiness*. Salah satu parameter yang digunakan dalam manajemen *trustworthiness* adalah penilaian *trust*. Penilaian *trust* yang digunakan dalam sistem ini menggunakan model ConTrust [12]. Penilaian *trust* bersifat rentan karena dapat diubah oleh objek yang *malicious*. Untuk menghindari hal tersebut, penulis menambahkan parameter autentikasi ke dalam manajemen *trustworthiness*. Berikut adalah penjelasan tentang sistem yang dibangun pada penelitian ini:



Gambar 1 Perancangan Model

1. Proses pertama yang dilakukan di dalam sistem adalah autentikasi. Autentikasi pada sistem ini terdiri dari dua fase. Pada fase pertama, sistem akan memeriksa objek berdasarkan *username* dan *password*. Pada fase kedua, sistem akan memeriksa objek berdasarkan ID objek tersebut. ID objek terdiri dari *IP Address* dan *MAC Address*.
2. Proses kedua yang dilakukan di dalam sistem adalah pengiriman nilai *trust*. Proses ini hanya dapat dilakukan oleh objek yang terautentikasi oleh sistem. Pada gambar 2 ditunjukan bagaimana objek melakukan penilaian *trust* terhadap objek lainnya.

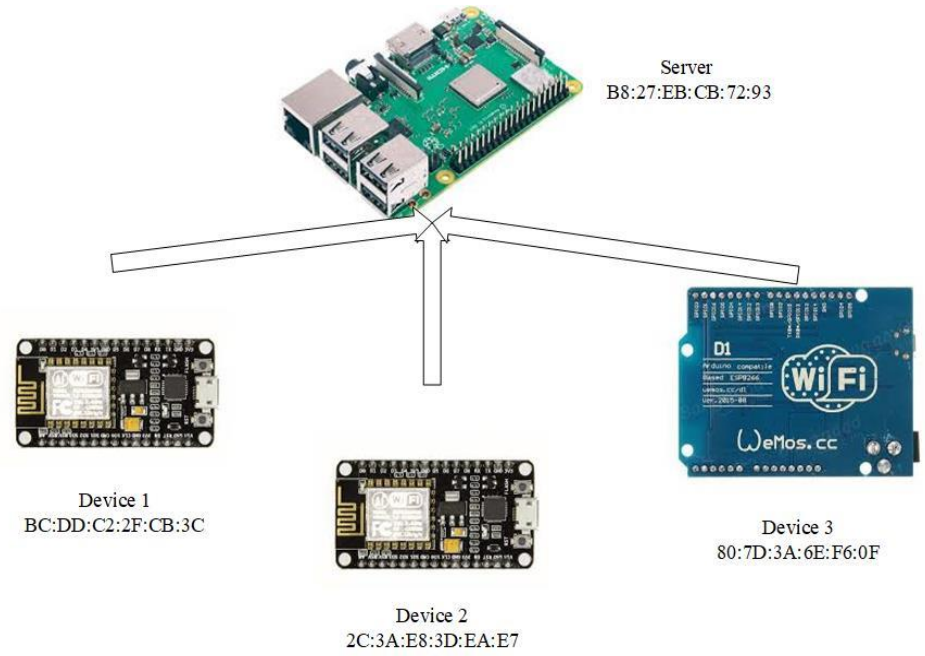


Gambar 2 Topologi Penilaian *Trust*

Pada gambar 2 ditampilkan tiga buah objek O1, O2, dan O3. Ketiga objek tersebut terhubung oleh sebuah protokol komunikasi sehingga seluruh objek tersebut dapat berkomunikasi. Setiap objek nantinya akan melakukan penilaian *trust* terhadap objek lainnya.

3. Proses ketiga pada sistem ini adalah penyimpanan data. Penilaian *trust* yang dilakukan oleh antar objek nantinya akan disimpan datanya di dalam server. Server menggunakan *phpMyAdmin* untuk menyimpan seluruh nilai *trust* yang dikirim oleh objek.
4. Proses keempat pada sistem ini adalah pengecekan *intruder*. Pengecekan ini dilakukan untuk mendeteksi apakah ada objek yang memiliki dua buah ID. Jika ditemukan adanya objek tersebut, maka sistem akan mengumumkan bahwa objek tersebut adalah objek *intruder*.

Rancangan Sistem



Gambar 3 Rancangan Sistem

Pada gambar 3 ditunjukkan rancangan sistem pada penelitian ini. Raspberry Pi 3b+ digunakan sebagai server, sedangkan tiga buah ESP8266 digunakan sebagai *node* dimana objek 1 bertindak sebagai *node valid*, objek 2 bertindak sebagai penyerang dan objek 3 bertindak sebagai *intruder*. Setiap perangkat akan melakukan proses komunikasi dengan menggunakan protokol MQTT dimana Raspberry Pi 3b+ bekerja sebagai *subscriber* dan ESP8266 bekerja sebagai *publisher*. Pada saat pengujian metode berlangsung, ESP8266 nantinya akan melakukan *publish* topik yang berisi informasi nilai *trust*, lalu Raspberry Pi 3b+ akan melakukan *subscribe* kepada topik yang di *publish* sehingga Raspberry Pi 3b+ akan meyimpan seluruh informasi yang disampaikan oleh ESP8266.

MQTT

MQTT (MQ Telemetry Transport) merupakan sebuah protokol yang biasa digunakan untuk melakukan proses komunikasi *indirect* antar perangkat IoT. Komunikasi *indirect* adalah komunikasi yang dilakukan membutuhkan *middle-man* agar pesan dapat sampai kepada tujuan yang diinginkan. Lalu mekanisme komunikasi yang digunakan pada MQTT adalah *publish* dan *subscribe*. Proses komunikasi dimulai dari *publisher* melakukan *publish* pesan dengan suatu topik tertentu kepada *middle-man*. *Subscriber* nantinya akan melakukan *subscription* pada suatu topik. *Middle-man* nantinya akan melakukan pengecekan terhadap topik yang ada pada *publisher* dan *subscriber*. Jika topik yang dimiliki oleh keduanya sama, maka pesan akan disampaikan menuju *subscriber*, jika topiknya berbeda, maka pesan yang di *publish* oleh *publisher* akan dihapus.

ConTrust

Penelitian [12] menjelaskan bahwa salah satu cara untuk meningkatkan keamanan dari suatu objek adalah dengan meningkatkan privasi dari suatu objek tersebut. Banyak metode yang dapat digunakan untuk

meningkatkan privasi dari suatu objek, salah satunya adalah penggunaan *trust*. *Trust* diperlukan oleh suatu objek di lingkungan IoT untuk mengamankan data komunikasi dengan objek yang dipercaya. Objek dalam IoT memiliki karakteristik yang berbeda-beda dan objek tersebut secara dinamik dapat bergabung dalam suatu komunikasi atau meninggalkan suatu komunikasi, sehingga diperlukan penilaian *trust* untuk menghasilkan rekomendasi objek mana yang dapat dipercaya.

Untuk melakukan penilaian tersebut, digunakan *ConTrust* untuk menilai suatu objek. *ConTrust* adalah *trust model* yang terdiri dari penilaian sekarang dan penilaian sebelumnya, sehingga rumus yang digunakan untuk menghasilkan nilai *trust* sebagai berikut:

$$T(t) = \alpha.T + (1 - \alpha).Ri(t) \quad (1)$$

Keterangan :
T(t) = Total nilai *trust*
T = Nilai *trust* yang diberikan kepada suatu objek
Ri(t) = Nilai reputasi ke - i dari suatu objek
α = Bobot histori [0,1]

Pada rumus (1) terdapat α yang di mana rentang nilainya adalah 0 dan 1. Nilai 0 menunjukan bahwa sistem tidak mempercayai seluruh objek yang masuk ke dalam sistem dan sebaliknya. Pada kondisi awal sistem, seluruh objek yang terhubung ke dalam sistem nantinya tidak dipercaya oleh sistem, sehingga rumus tersebut dapat ditulis sebagai berikut:

$$T(t) = Ri(t) \quad (2)$$

Skenario Pengujian

Pada bagian ini akan disampaikan dua skenario yang akan digunakan. Tujuan dari dibangunnya dua skenario ini adalah untuk mengetahui berapa besar tingkat akurasi yang dapat dihasilkan dari perangkat yang digunakan. Berikut adalah skenario yang akan digunakan :

1. Bukan valid user dan melakukan serangan *sybil*.
   Pada skenario pertama akan berfokus pada pengujian serangan *sybil*, yaitu pada bagian autentikasi. Jika sistem berhasil mendeteksi serangan *sybil*, maka akan dihitung berapa lama waktu yang dibutuhkan untuk mendeteksi serangan tersebut serta akurasi dari sistem tersebut serta menampilkan keluaran berupa objek mana yang melakukan serangan *sybil*.
2. Valid user dan tidak melakukan serangan *sybil*.
   Pada skenario kedua, pengujian dilakukan mulai dari autentikasi hingga objek dapat mengirim nilai *trust*. Jika objek berhasil masuk ke dalam sistem dan dapat mengirimkan nilai *trust*, maka akan dihitung berapa lama waktu yang dibutuhkan mulai dari autentikasi hingga pengiriman nilai *trust* selesai.
3. Valid user dan melakukan serangan *sybil*.
   Pada skenario ketiga akan berfokus kepada objek *intruder*. Objek tersebut memiliki 2 ID sehingga objek tersebut dapat melalui tahap autentikasi. Pengujian nantinya dilakukan mulai dari autentikasi hingga objek dapat mengirim nilai *trust*. Kemudian terakhir, sistem akan melakukan pengecekan ulang terhadap seluruh ID objek. Jika ditemukan adanya suatu objek yang memiliki 2 ID, maka sistem akan mengumumkan bahwa objek tersebut adalah objek *intruder*. Sistem nantinya akan menghitung waktu untuk mendeteksi *intruder* tersebut.

Hasil Pengujian Skenario

Berdasarkan skenario pengujian yang dibuat, pengujian nantinya akan dilakukan 10 kali setiap skenario, sehingga total pengujian untuk seluruh skenario yang dibuat adalah 30 kali. Untuk menghitung akurasi sistem dan waktu, penulis menggunakan rumus yang dapat dilihat dibawah ini.

Untuk menghitung akurasi yang dihasilkan, digunakan rumus sebagai berikut:

$$Akurasi = \frac{N}{Total\ Pengujian} * 100\% \quad (3)$$

Keterangan :
Akurasi = Persentase tingkat keberhasilan (%)
N = Jumlah pengujian berhasil
Total Pengujian = Jumlah total pengujian pada seluruh skenario

Sedangkan untuk menghitung total waktu yang digunakan oleh sistem, digunakan rumus sebagai berikut:

$$Total\ Waktu\ (s) = Waktu\ Autentikasi + Waktu\ Pengiriman\ Nilai\ Trust \quad (4)$$

Pada rumus (4), waktu autentikasi pada sistem ini dimulai saat sistem melakukan pengecekan terhadap ID suatu objek yang akan terhubung ke dalam sistem. Rumus tersebut dapat ditulis sebagai berikut:

$$Waktu\ Autentikasi\ (s) = Waktu\ pengecekan\ ID \quad (5)$$

Jika saat autentikasi sistem menemukan objek yang terdeteksi sebagai penyerang *sybil*, maka rumus (5) berfungsi sebagai waktu deteksi sistem. Rumus tersebut dapat ditulis sebagai berikut:

$$Waktu\ Deteksi\ (s) = Waktu\ deteksi\ serangan\ sybil \quad (6)$$

Sehingga rumus akhir untuk sistem menghitung waktu deteksi adalah:

$$Waktu\ deteksi\ penyerang\ sybil\ (s) = Waktu\ Deteksi \quad (7)$$

Jika pada saat autentikasi seluruh objek mampu masuk ke dalam sistem, namun pada saat pengecekan *intruder* ditemukan adanya objek yang memiliki 2 ID, maka rumus waktu deteksi yang digunakan yaitu:

$$Waktu\ deteksi\ intruder\ (s) = Waktu\ Deteksi + Waktu\ Pengiriman\ Nilai\ Trust \quad (8)$$

4. Evaluasi

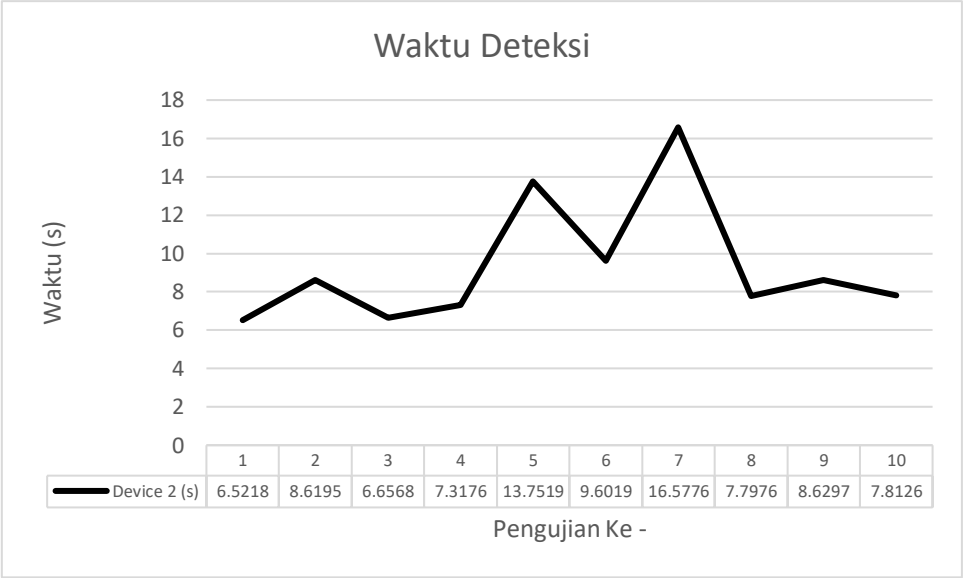
Setelah dilakukan pengujian pada seluruh skenario, pada skenario pertama akurasi yang dihasilkan adalah 100%. Ini disebabkan karena sistem dapat mendeteksi serangan *sybil* dengan baik. Pengujian pada skenario pertama dapat dikatakan berhasil jika sistem dapat mendeteksi objek *sybil* dan mengumumkan bahwa objek tersebut sedang melakukan serangan *sybil.* Lalu pada skenario kedua, sistem juga mampu mendeteksi objek mana saja yang valid sehingga objek tersebut dapat mengirimkan nilai *trust.* Akurasi yang dihasilkan setelah dilakukan pengujian sebanyak 10 kali didapatkan nilai 100%. Pengujian dikatakan berhasil jika sistem dapat mendeteksi objek mana yang valid dan mampu mengirim nilai *trust.* Pada skenario terakhir, akurasi yang dihasilkan oleh sistem adalah 100%. Akurasi tersebut dihasilkan dari sistem yang mampu mendeteksi *intruder*. Pengujian pada skenario ketiga dapat dikatakan berhasil jika sistem mampu mendeteksi objek mana yang merupakan objek *intruder* dan mengumumkan objek tersebut.

Analisis Hasil Pengujian

Penelitian metode manajemen *trustworthiness* yang berdasarkan autentikasi dan *trust value* yang sudah dilakukan pengujian dengan parameter akurasi dan waktu, didapatkan hasil sebagai berikut :

1. Skenario pertama

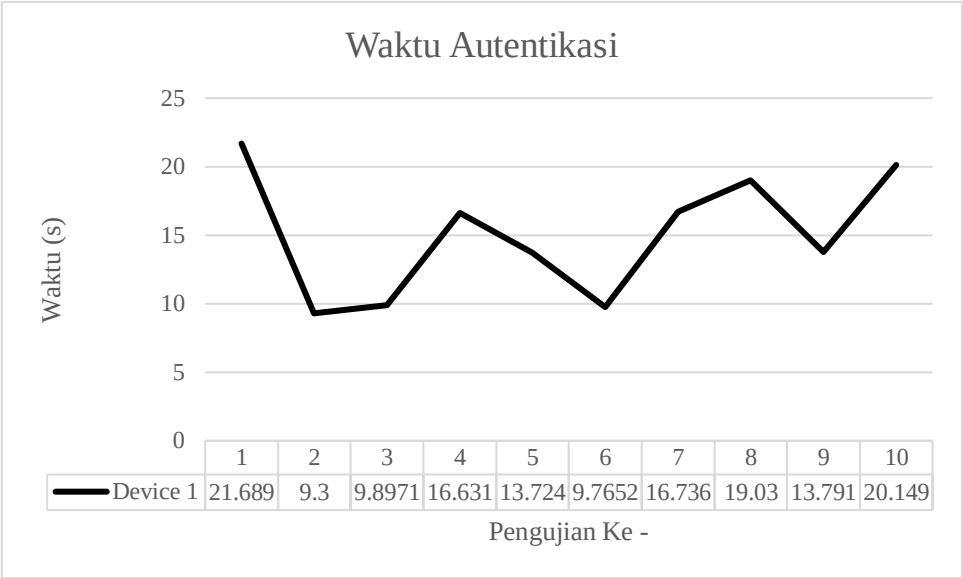
   Pengujian pada skenario pertama berfokus pada autentikasi. Setiap objek yang akan masuk ke dalam sistem akan melalui proses autentikasi. Pada proses autentikasi terdapat 2 fase. Pada fase pertama akan dilakukan pengecekan terhadap *username* dan *password* dari suatu objek. Pada fase ini, seluruh objek belum terdeteksi adanya melakukan serangan. Pada fase kedua, dilakukan pengecekan terhadap ID objek. Pada fase ini, ditemukan objek yang melakukan serangan sehingga objek tersebut tidak dapat masuk kedalam sistem, yaitu objek 2. Sistem akan mengumumkan bahwa objek 2 sedang melakukan serangan *sybil*. Saat sistem mendeteksi objek 2 melakukan serangan *sybil*, sistem mulai menghitung waktu untuk mendeteksi serangan tersebut. Waktu deteksi adalah waktu yang diperoleh dari sistem saat objek terdeteksi oleh sistem sebagai penyerang *sybil*. Pada grafik 1 menampilkan waktu yang didapatkan saat sistem mendeteksi serangan *sybil*. Rata-rata waktu yang dibutuhkan oleh sistem untuk mendeteksi objek yang melakukan serangan *sybil* adalah 9,3287 detik. Pengujian pada skenario ini dikatakan berhasil jika sistem mampu mendeteksi objek *sybil* dan mengumumkan objek tersebut sedang melakukan serangan *sybil*. Akurasi yang dihasilkan pada skenario ini setelah dilakukan pengujian sebanyak 10 kali adalah 100%.



Grafik 1 Waktu Deteksi Serangan *Sybil*

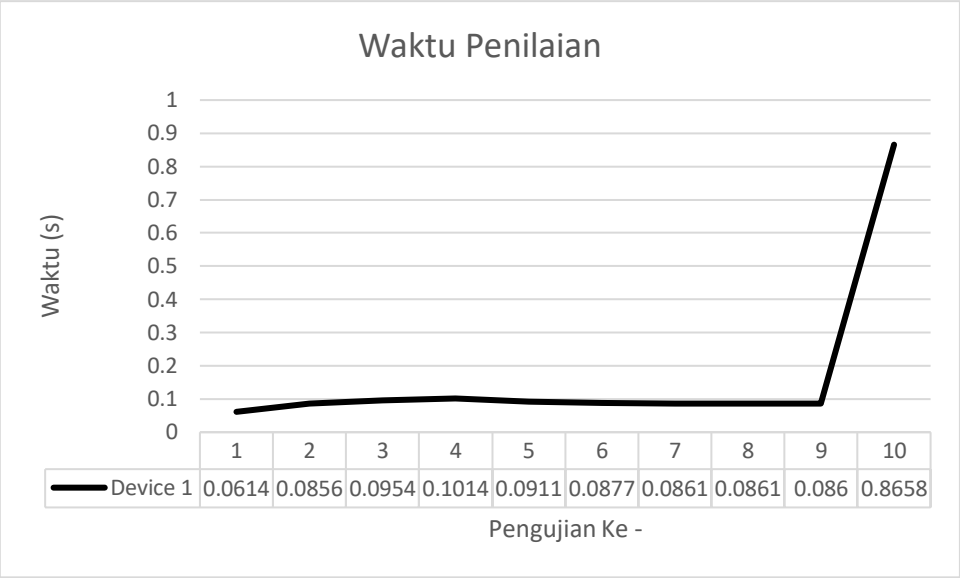
2. Skenario Kedua

Pengujian pada skenario kedua berfokus pada objek yang terautentikasi dan dapat mengirimkan nilai *trust*. Objek yang terautentikasi adalah objek 1. Pada saat objek telah terautentikasi, objek akan mengirimkan nilai *trust* dan nantinya sistem akan meyimpan seluruh data. Selain itu, sistem juga akan menghitung waktu yang dibutuhkan mulai dari autentikasi dan penilaian antar objek. Pada grafik 2 menampilkan waktu autentikasi yang dibutuhkan oleh objek yang valid. Waktu autentikasi adalah waktu yang diperoleh dari sistem saat objek valid berhasil melalui tahap autentikasi dalam sistem. Pada objek 1, rata-rata waktu autentikasi yang dibutuhkan adalah 15,0712 detik.



Grafik 2 Waktu Autentikasi Objek Valid

Selanjutnya, pada grafik 3 menampilkan data waktu yang dibutuhkan oleh objek valid untuk menilai objek valid lainnya. Pada objek 1, rata-rata waktu yang dibutuhkan untuk melakukan penilaian terhadap objek 3 adalah 0,16466 detik.

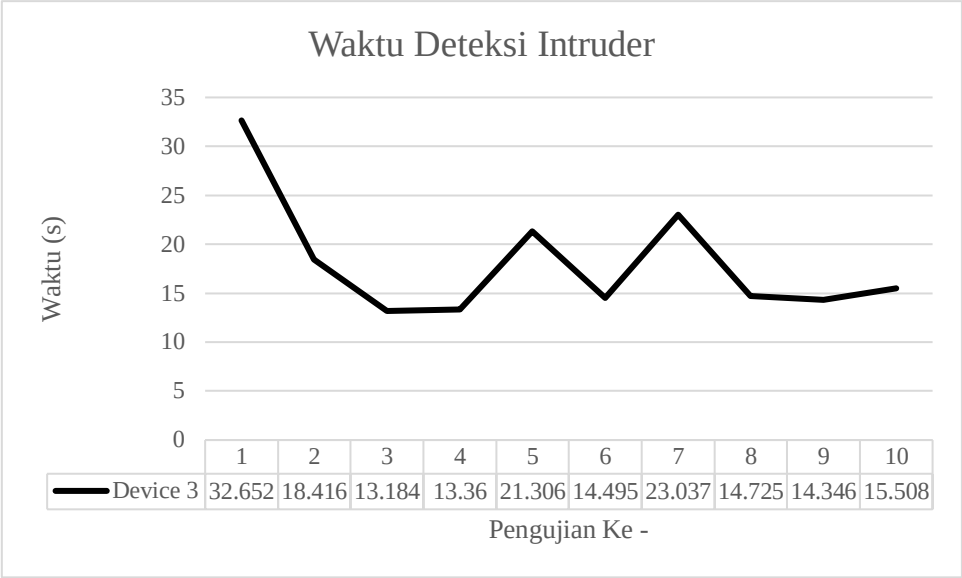


Grafik 3 Waktu Penilaian

Pengujian pada skenario ini dikatakan berhasil jika sistem mampu mendeteksi objek yang valid dan objek tersebut dapat mengirimkan nilai *trust*. Akurasi yang dihasilkan pada skenario ini setelah dilakukan pengujian sebanyak 10 kali adalah 100%.

3. Skenario ketiga

   Pengujian pada skenario ketiga berfokus pada objek *intruder*. Objek *intruder* pada pengujian ini adalah objek 3. Objek tersebut mampu masuk ke dalam sistem namun pada saat pengecekan *intruder*, sistem akan mengumumkan bahwa objek tersebut sedang melakukan serangan. Sistem nantinya akan menghitung seluruh waktu mulai dari waktu autentikasi hingga waktu saat objek tersebut terdeteksi sebagai *intruder*. Pada grafik 4 menampilkan data waktu yang dibutuhkan oleh sistem untuk mendeteksi *intruder*. Waktu deteksi *intruder* adalah waktu yang diperoleh dari sistem saat objek berhasil melalui tahap autentikasi, namun pada tahap pengecekan *intruder*, objek terdeteksi oleh sistem sebagai objek *intruder*. Rata-rata waktu yang dibutuhkan untuk mendeteksi objek *intruder* oleh sistem yaitu 18,1029 detik. Pengujian pada skenario ini dikatakan berhasil jika sistem mampu mendeteksi objek *intruder* dan mengumumkan bahwa objek tersebut sedang melakukan serangan. Akurasi yang dihasilkan pada skenario ini setelah dilakukan pengujian sebanyak 10 kali adalah 100%.



Grafik 4 Waktu Deteksi *Intruder*

5. Kesimpulan

Pada penelitian ini, penulis mengajukan metode manajemen *trustworthiness* berdasarkan autentikasi dan *trust value* untuk mengamankan objek IoT. Berdasarkan hasil pengujian tiga skenario, dengan menggunakan kedua parameter tersebut, sistem mampu mendeteksi serangan *sybil* dengan cepat dan akurat. Rata-rata waktu yang dibutuhkan untuk mendeteksi serangan *sybil* adalah 9,3287 detik. Lalu, rata-rata waktu yang dibutuhkan untuk mendeteksi objek *intruder* pada sistem adalah 18,1029 detik. Akurasi yang dihasilkan pada setiap skenario adalah 100%, sehingga dapat disimpulkan bahwa akurasi yang dihasilkan oleh sistem untuk mendeteksi serangan *sybil* adalah 100%. Selanjutnya, sistem juga mampu memproses nilai *trust* yang telah disimpan di dalam *database* sehingga dapat menentukan objek mana yang memiliki nilai *trust* tertinggi dan terendah.

Penelitian ini tentunya masih terdapat kekurangan dan mampu di eksplorasi lagi lebih lanjut. Oleh karena itu, penulis memberikan saran yaitu :

1. Proses autentikasi dapat dikembangkan dengan menggabungkan autentikasi dan enkripsi sehingga tingkat keamanan lebih baik lagi.
2. Dengan mempertimbangkan hasil implementasi yang telah dilakukan, objek yang digunakan sebagai node dalam penelitian ini tidak dapat menampung data sehingga seluruh proses dilakukan dalam server. Selain itu, protokol komunikasi yang digunakan juga terbatas. Penulis menyarankan agar menggunakan objek yang sama dengan server sehingga node dapat bekerja lebih fleksibel.

Daftar Pustaka

[1] Sarigiannidis, P.. 2015. VisIoT : A Threat Visualisation tool for IoT systems security. IEEE Conference Community Workshop. IEEE
[2] Rajan, A.. Jithish, J.. dan Sankaran, S.. 2017. Sybil Attack in : Modelling and Defenses. IEEE Conferences. IEEE
[3] Putra, G.D.. dan Sulistyo, S.. 2018. Trust Based Approach in Adjacent Vehicles to Mitigate Sybil Attacks in VANET. Hongkong. Association for Computing Machinery.
[4] Yan, Z. Zhang, P. dan Vasilakos, A.S.. 2014. A Survey on Trust Management for Internet of Things. Journal of Network and Computer Applications
[5] Farooq, M.S. Waseem M.M.U. Anjum K.. 2015. A Critical Analysis on the Security Concerns of Internet of Things. International Journal of Computer Applications
[6] Hadjichristofi, G. 2015. Internet of Things: Security Vulnerabilities and Challenges. International Workshop on Smart City and Ubiquitous Computing Applications
[7] Suryani, V. Sulistyo, S. Widyawan, W.. 2018. Two-Phase Security Protection for the Internet of Things Object. Journal of Information Processing Systems
[8] Chae, Y. DiPippo. C.L. Sun, L.Y.. 2013. Trust Management for Defending On-Off Attacks. IEEE Transactions on Parallel and Distributed Systems
[9] Suryani, V. Sulistyo, S. Widyawan, W..Simulation of Trust-based Attacks in Internet of Things. *MATEC Web of Conferences* (Vol. 154, p. 03014). EDP Sciences.
[10] Suryani, V. Sulistyo, S. Widyawan, W.. 2018. The Detection of On-Off Attacks for the Internet of Things Objects. International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)
[11] Hokeun, K. Edward, A.L.. 2017. Authentication and Authorization for the Internet of Things. IEEE Computer Society
[12] Suryani, V. Sulistyo, S. Widyawan, W.. 2016. Contrust: A Trust Model to Enhance the Privacy in Internet of Things. International Journal of Intelligent Engineering and System
[13] Douceur, J. R.. 2002. The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer.

Lampiran

Pengujian Ke -	Waktu Deteksi (s)
1	6.5218
2	8.6195
3	6.6568
4	7.3176
5	13.7519
6	9.6019
7	16.5776
8	7.7976
9	8.6297
10	7.8126
Rata-rata	9.3287

Tabel 1 Waktu Deteksi Serangan *Sybil*

Waktu Autentikasi (s)	
Pengujian Ke -	Device 1
1	21.6888
2	9.3
3	9.8971
4	16.6308
5	13.7241
6	9.7652
7	16.7356
8	19.0303
9	13.7914
10	20.1487
Rata-rata	15.0712

Tabel 2 Waktu Autentikasi Objek Valid

Waktu Penilaian (s)	
Pengujian Ke -	Device 1
1	0.0614
2	0.0856
3	0.0954
4	0.1014
5	0.0911
6	0.0877
7	0.0861
8	0.0861
9	0.086
10	0.8658
Rata-rata	0.16466

Tabel 3 Waktu Penilaian Antar Objek Valid

Waktu Deteksi Intruder	
Pengujian Ke -	Device 3
1	32.652
2	18.416
3	13.184
4	13.36
5	21.306
6	14.495
7	23.037
8	14.725
9	14.346
10	15.508
Rata-Rata	18.1029

Tabel 4 Waktu Deteksi Intruder