ABSTRACT

Internet of Things, also called IoT enables smart object become active participant in communication process among objects in the network. Since IoT services utilize the Internet connection, then it require some solutions to such important issues: security and privacy. Smart object communication and machine-to-machine or thing-to-things are important research areas in IoT, especially those related to security. The security aspects in IoT can be implemented by the means of encryption algorithms, limiting access to data or users, or applying certain rules or policies.

Access restrictions on data or users are important process to be done, so that objects can only commmunicate to reliable objects. Choosing a trustworthy object is one way to improve the security aspect, specially the privacy aspect. The process of selecting a reliable object can be resolved by investigating the history of the assessed object, or by calculating a value that is used as the threshold of an object to be considered "trusted" or not.

This research focused on the selecting process of a reliable object by calculating the threshold value of the trust of an object. The process begins by describing the position and connectivity of the object in the form of a two-way graph. Then the position and connectivity of each object is described in the form of a matrix. This matrix is an input for the next process which dealing with mathematical calculations to generate the trust value. The output of the calculation process is a value in the range of zero to one. Determining the threshold of trust value is the important process which aimed to determine the object' trust level. Objects in IoT have dynamic characteristics, which mean the objects can join or leave to any network as long as connected to the Internet. Objects are also expected to be resistance to some attacks, such as trust-based attack, Sybill attack, and On-off attack. The contribution of this research is the security framewok consisting a mathematical model of calculating the trust value of an object to improve the privacy aspect in IoT area.

In this research, we developed a security model for objects in IoT. The security model is chosen to ensure that the security mechanisms used are more structured. The proposed model, called ConTrust contains a model for calculating the trust level of an object, the election of an object coordinator in a network that manages reputation values, and statistical models to prevent objects from trust-based attacks. The ConTrust

model can be used for the trust assessment among IoT objects, as well as for detecting trust-based attacks and on-off attacks. The simulation results depicted that the ConTrust model can be used to detect trusted objects or not through a trust assessment, and be able to identify the existence of trust-based attacks on IoT objects. The trust assessments result from ConTrust model compared to the TC-BAC model with a variation of the α value resulting a trust value increasing of 0.02 for the ConTrust model. While the variation of the β value produced a more stable of reputation value in ConTrust model compared to TC-BAC model.

The contribution of this research is to provide an alternative solution for securing IoT objects, in addition to improving the privacy aspect of those objects.

Keyword: Internet of Things, objects, security model, ConTrust, trust, trust-based attack

INTISARI

Internet of Things, disebut juga IoT membuat *smart object* menjadi partisipan aktif dalam proses komunikasi antar sesama objek maupun dengan lingkungan. Layanan yang memanfaatkan koneksi Internet ini membutuhkan solusi untuk persoalan baru, yaitu keamanan dan privasi. Komunikasi *smart object* dan *machine-to-machine* atau *thing-to-thing* merupakan area penelitian yang cukup penting di IoT, terutama yang terkait dengan keamanan. Aspek keamanan di IoT dapat diimplementasikan dengan cara menggunakan pelbagai algoritme enkripsi, pembatasan akses terhadap data atau pengguna, maupun menerapkan aturan-aturan atau *policy* tertentu.

Pembatasan akses terhadap data atau pengguna penting dilakukan agar objek hanya dapat melakukan proses komunikasi dengan objek yang dapat dipercaya saja. Memilih objek yang dapat dipercaya merupakan salah satu cara untuk meningkatkan aspek privasi, dibandingkan tanpa *filter* sama sekali. Proses pemilihan objek yang dapat dipercaya dapat dilakukan dengan berbagai metode, mulai dari autentikasi, penggunaan sertifikat digital, atau menggunakan algoritme tertentu yang saat ini sudah digunakan untuk mengamankan jaringan Internet. Salah satunya adalah penggunaan model matematika, dengan cara menilai histori atau perilaku sebelumnya dari objek tujuan, atau dengan menghitung suatu nilai yang dijadikan sebagai ambang batas suatu objek dianggap "dipercaya" atau tidak.

Pada penelitian ini dilakukan proses pemilihan objek yang dapat dipercaya dengan cara menghitung nilai ambang batas *trust* dari suatu objek. Proses yang dilakukan dimulai dengan menggambarkan posisi dan konektivitas objek dalam bentuk graf dua arah. Kemudian posisi dan konektivitas setiap objek tersebut digambarkan dalam bentuk matrik, dari matrik tersebut dilakukan proses perhitungan matematis guna perhitungan nilai *trust*. Keluaran dari proses perhitungan tersebut merupakan suatu nilai yang berada pada kisaran nol sampai dengan satu. Penetapan nilai ambang batas atau *threshold* untuk nilai keluaran tersebut merupakan proses selanjutnya untuk menentukan apakah objek tersebut termasuk objek yang *trustable* atau tidak. Penelitian dikembangkan untuk objek di IoT yang memiliki karakteristik dinamis, yaitu bisa berpindah ke jaringan manapun selama terhubung dengan Internet. Objek diharapkan

juga tahan terhadap serangan, semisal yang memalsukan reputasi suatu objek *(trust-based attack)*.

Penelitian ini menyajikan model keamanan untuk objek-objek di IoT. Model keamanan yang telah dibuat bertujuan membuat mekanisme pengamanan agar lebih terstruktur. Model yang diajukan, disebut dengan *ConTrust* berisi model untuk menghitung tingkat kepercayaan suatu objek, pemilihan koordinator objek dalam satu jaringan yang bertugas menangani nilai reputasi. Keunggulan dari model ConTrust adalah selain dapat digunakan untuk proses *trust assessment,* ConTrust juga dapat dipakai untuk mendeteksi serangan *trust-based attack* dan *on-off attack.* Hasil pengujian yang dilakukan menunjukkan bahwa model *ConTrust* dapat digunakan untuk melakukan deteksi objek yang terpercaya atau tidak melalui *trust assessment,* serta mampu mengidentifikasi adanya serangan *trust-based attacks* pada objek IoT. Hasil *trust assessment* dari ConTrust dibandingkan dengan metode *TC-BAC* dengan variasi nilai α yang sama menghasilkan peningkatan nilai *trust* sebesar 0.02 pada model ConTrust. Sedangkan variasi nilai β menghasilkan nilai reputasi yang lebih stabil dibandingkan algoritme *TC-BAC.*

Kontribusi dari penelitian ini adalah menyediakan alternatif pilihan untuk pengamanan objek IoT, dengan cara meningkatkan aspek privasi dari objek tersebut.

Kata kunci : *Internet of Things*, objek, model keamanan, *ConTrust, trust, trust-based attack*