UNIVERSITAS
GADJAH MADA
Pengembangan Model Keamanan Internet of Things Berbasis Trust pada Sistem Transportasi Cerdas
Latifah Dewi Purwitasari, Dr. Warsun Najib, S.T., M.Sc.; Ir. Sujoko Sumaryono, M.T.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Sistem transportasi cerdas atau *Intelligent Transportation System* (ITS) berbasis *Internet of Things* (IoT) sangat rentan terhadap serangan akibat karakteristik perangkat IoT yang dinamis, heterogen, dan memiliki keterbatasan sumber daya. Analisis menunjukkan bahwa sistem keamanan konvensional tidak cukup adaptif untuk menangani interaksi perangkat yang beragam, sehingga diperlukan sebuah model keamanan yang dinamis untuk mengevaluasi kepercayaan setiap entitas di dalam jaringan dan mencegah *insider threats*. Untuk menjawab permasalahan tersebut, dikembangkan sebuah model keamanan berbasis *trust* yang diimplementasikan dalam bentuk prototipe dengan arsitektur *microservices*. Sistem ini mengadopsi konsep komunitas dari model ekosistem IoT. ITS dibangun sebagai sebuah komunitas IoT dengan satu entitas yang berperan sebagai koordinator komunitas untuk mengelola layanan dan manajemen *trust* dalam jaringan. Sistem terdiri atas *Trust Service* independen untuk perhitungan *trust*, *backend* ITS, dan *frontend* berupa *dashboard* pemantauan keamanan. Model keamanan yang digunakan merupakan adaptasi dari kerangka QS-Trust yang mengevaluasi nilai *trust* perangkat berdasarkan *direct observation, indirect observation,* dan *centrality*. Hasil pengujian melalui berbagai simulasi menunjukkan bahwa sistem dapat mendeteksi serangan *bad mouthing* dan *flooding*, serta mampu menjaga stabilitas jaringan melalui rotasi koordinator otomatis. Secara kuantitatif, sistem berhasil mencapai tiga dari empat target spesifikasi luaran, termasuk akurasi deteksi rata-rata 90,00%. Meskipun demikian, analisis menyimpulkan bahwa kestabilan nilai *trust* masih menjadi tantangan akibat adanya *cold start problem* dan mekanisme *indirect observation* yang kurang adaptif terhadap perilaku perangkat yang variatif.

Kata kunci: keamanan berbasis *trust*, internet of things, sistem transportasi cerdas, QS-Trust, *microservices*, *insider threats*

UNIVERSITAS
GADJAH MADA

Pengembangan Model Keamanan Internet of Things Berbasis Trust pada Sistem Transportasi Cerdas
Latifah Dewi Purwitasari, Dr. Warsun Najib, S.T., M.Sc.; Ir. Sujoko Sumaryono, M.T.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

Intelligent Transportation Systems (ITS) based on the Internet of Things (IoT) are highly vulnerable to attacks due to the dynamic, heterogeneous, and resource-limited nature of IoT devices. Conventional security systems are not adaptive enough for varied device interactions, requiring a dynamic security model to continuously evaluate the trustworthiness of each entity in the network and mitigate insider threats. To solve this problem, a trust-based security model was developed and implemented as a prototype using a microservices architecture. The system is built as an IoT community with a coordinator to manage services and trust. It consists of an independent Trust Service for trust calculations, an ITS backend, and a security monitoring dashboard as its frontend. The security model is an adaptation of the QS-Trust framework, which evaluates a device's trust score based on direct observation, indirect observation, and centrality. Simulations show the system can detect bad mouthing and flooding attacks and maintain network stability through automatic coordinator rotation. Quantitatively, the system achieved three out of four of its target specifications, including an average detection accuracy of 90.00%. However, trust score stability remains a challenge due to the cold-start problem and an indirect observation mechanism that is not fully adaptive to varied device behaviors.

Keywords: *trust-based security, internet of things, intelligent transportation systems, QS-Trust, microservices, insider threats*