# ABSTRAK

Metode *Nitti-Trust* memiliki kelemahan utama terkait *scalability* dan arsitektur jaringan yang terpusat (*centralized*). Kompleksitas komputasi meningkat secara signifikan dengan bertambahnya jumlah *node*, karena proses penghitungan *trust* membutuhkan iterasi melalui seluruh jaringan untuk mengumpulkan opini langsung dan tidak langsung. Arsitektur jaringan terpusat juga menyebabkan efisiensi menurun, dengan risiko *bottleneck* dalam pengumpulan opini dan kurangnya optimasi lokal. Kelemahan-kelemahan ini membatasi penerapan metode dalam jaringan besar, yang merupakan karakteristik utama dari ekosistem IoT modern. Tujuan utama dari penelitian ini adalah untuk merancang model keamanan berbasis *trust* pada jaringan dan ekosistem IoT yang terpercaya sehingga akan terbentuk suatu lingkungan yang aman untuk menjalankan layanan sistem IoT.

Secara garis besar penelitian ini terbagi menjadi dua bagian yaitu perancangan model keamanan pada IoT berbasis *trust* dan tahap pengujian. Termasuk dalam perancangan model adalah model arsitektur, model matematika, model interaksi, penentuan parameter *trust*, penyusunan algoritma kalkulasi *trust*, dan manajemen *trust*. Penelitian ini menggunakan metode eksperimental untuk menguji dan memverifikasi model keamanan yang diusulkan.

Hasil dari penelitian ini adalah terbentuknya suatu model keamanan berbasis *trust, QS-Trust*, untuk sistem IoT. Model tersebut menjamin tersedianya mekanisme bagi setiap objek IoT untuk memutuskan bahwa sebuah objek IoT lain yang menjadi partner interaksi merupakan objek yang dapat dipercaya (*trusted*). Pengujian waktu eksekusi algoritma *QS-Trust* pada komunitas IoT dengan 10 objek menghasilkan waktu eksekusi berkisar pada rentang 21 – 128 milidetik pada berbagai jenis perangkat IoT. Model yang diusulkan menyediakan mekanisme untuk mendeteksi serangan *bad mouthing attack* dan *good mouthing attack* yang sering dialami sistem IoT. Selain itu, *QS-Trust* menawarkan skalabilitas yang lebih baik dan waktu eksekusi yang lebih rendah dalam jaringan IoT yang lebih besar dibandingkan dengan *Nitti-Trust*. Pada pengujian dengan 1000 *nodes*, *QS-Trust*

hanya membutuhkan waktu 179 milidetik untuk eksekusi, sedangkan *Nitti-Trust* membutuhkan lebih dari 543 milidetik.

**Kata Kunci** : IoT, *internet of things*, keamanan IoT, keamanan berbasis *trust*, model keamanan IoT

# *ABSTRACT*

*The previously developed IoT security model (Nitti-Trust) has several weaknesses related to its centralised network architecture and scalability aspects. Computational complexity increases significantly as the number of nodes grows, because the trust calculation process requires iteration through the entire network to gather direct and indirect opinions. The centralised network architecture also reduces efficiency, with risks of bottlenecks in opinion collection and a lack of local optimisation. These weaknesses limit the application of the method in large networks, which are a defining characteristic of modern IoT ecosystems.*

*The main objective of this research is to design a trust-based security model for networks and IoT ecosystems, creating a secure environment for operating IoT system services. The research is divided into two parts: the design of a trust-based security model for IoT and the testing phase. The design includes architectural modelling, mathematical modelling, interaction modelling, determining trust parameters, developing trust calculation algorithms, and trust management. This research employs experimental methods to test and verify the proposed security model.*

*The outcome of this study is the development of a trust-based security model, QS-Trust, for IoT systems. This model ensures a mechanism for each IoT object to determine whether another IoT object in an interaction partnership is trustworthy. Testing the execution time of the QS-Trust algorithm on an IoT community with 10 objects yielded execution times ranging from 21 to 128 milliseconds across various types of IoT devices. The proposed model provides mechanisms to detect bad mouthing attacks and good mouthing attacks, which are common in IoT systems. Additionally, QS-Trust offers better scalability and lower execution times in larger IoT networks compared to Nitti-Trust. In the execution time testing with 1000 nodes, QS-Trust only took 179 milliseconds to execute, while Nitti-Trust needed more than 543 milliseconds.*

***Keywords**: IoT, internet of things, IoT security, trust-based security, IoT security model*