INTISARI

Dengan meningkatnya implementasi ekosistem *Internet of Things* (IoT) menyebabkan meningkat pula risiko serangan terhadap ekosistem IoT tersebut. Namun perangkat IoT memiliki kekhasan seperti karakteristik jaringan, keterbatasan kemampuan komputasi misalnya CPU, RAM, dan sumber tenaga misalnya baterai yang terbatas. Oleh karena itu diperlukan solusi keamanan yang dapat mengakomodasi karakteristik dan keterbatasan sumber daya yang dimiliki ekosistem IoT. Solusi yang ditawarkan untuk menjawab permasalahan tersebut berupa pendekatan keamanan berbasis nilai kepercayaan. Pendekatan keamanan berbasis kepercayaan melakukan kuantifikasi interaksi dari entitas atau objek di dalam ekosistem IoT sebagai dasar nilai kepercayaan. Pada pengerjaan dokumentasi C501 ini telah menghasilkan solusi berupa paket program kontrak pintar berbasis *Ethereum* dan hasil pengujian terhadap serangan yang ditujukan pada paket program. Paket program kontrak pintar ini bekerja secara independen untuk melayani proses autentikasi dan otorisasi objek IoT yang meminta sumber daya, sehingga mengurangi beban komputasi perangkat IoT yang berdampak pada penggunaan energi yang lebih sedikit. Paket solusi dapat berjalan dengan baik dan dapat menangkal sebagian besar rangkaian serangan yang diujikan. Pada iterasi pengembangan selanjutnya diperlukan improvisasi terutama pada uji coba lapangan dan pengembangan perlu didampingi oleh ahli dalam bidang IoT dan *Ethereum* untuk dapat menghasilkan solusi secara menyeluruh.

Kata Kunci: Internet of Things, Trust Based Security, Blockchain, Smart Contract, Solidity

ABSTRACT

With the increasing implementation of the Internet of Things (IoT) ecosystem, the risk of attacks against the IoT ecosystem also increases. However, IoT devices have characteristics such as network characteristics, limited computing capabilities, such as CPU, RAM, and limited power sources, such as batteries. Therefore, a security solution is needed that can accommodate the characteristics and resource limitations of the IoT ecosystem. The solution offered to answer these problems is in the form of a security approach based on trust values. The trust-based security approach quantifies the interactions of entities or objects within the IoT ecosystem as a basis for the value of trust. The work on the C501 documentation has produced a solution in the form of an Ethereum-based smart contract program package and the results of testing against attacks aimed at the program package. This smart contract program package works independently to serve the authentication and authorization processes of IoT objects that request resources, thereby reducing the computational burden of IoT devices which results in less energy usage. The solution package works well and can counteract most of the attacks tested. In the next development iteration, improvisation is needed, especially in field trials and development needs to be accompanied by experts in the field of IoT and Ethereum to be able to produce a comprehensive solution.

Keyword : Internet of Things, Trust Based Security, Blockchain, Smart Contract, Solidity

RINGKASAN EKSEKUTIF

Dengan semakin meningkatnya implementasi ekosistem *Internet of Things* (IoT). Pemanfaatan sumber daya komputasi menjadi semakin mudah dan murah untuk dapat memenuhi kebutuhan bisnis dan peningkatan kualitas layanan yang diberikan. Peningkatan pemanfaatan IoT juga menyebabkan peningkatan faktor risiko serangan siber yang mengarah pada ekosistem IoT. Dengan demikian, peningkatan keamanan pada ekosistem IoT menjadi keperluan kritis.

Dengan karakteristik ekosistem dan peranti IoT yang terbatas CPU, RAM, perilaku jaringan, dan kapasitas penyimpanan, pendekatan keamanan tradisional berbasis perimeter tidak dapat mengakomodasi keterbatasan dan syarat layanan yang diterapkan. Oleh karena itu diperlukan pendekatan keamanan yang dapat memenuhi kebutuhan yang diminta oleh ekosistem IoT. Pada dokumen C501 Skripsi *Capstone Project* ini menawarkan solusi keamanan berbasis *trust* yang dapat diterapkan pada ekosistem IoT. Dari pengerjaan *Capstone Project* ini memberikan paket solusi keamanan dan hasil uji program terhadap serangkaian uji yang dibuat. Dengan demikian, ekosistem dan perangkat IoT dapat berkomunikasi dengan aman dan menjamin bahwa perangkat yang terhubung di dalamnya adalah perangkat yang dapat dipercaya.

Paket solusi terdiri dari program untuk komputasi nilai kepercayaan perangkat, mekanisme pendaftaran perangkat, dan manajemen izin sumber daya. Program komputasi nilai kepercayaan digunakan untuk kuantifikasi perilaku perangkat di dalam jaringan dan sebagai basis informasi tingkat kepercayaan perangkat IoT. Program manajemen izin perangkat digunakan untuk mengelola dan memproses permintaan izin akses sumber daya yang diminta perangkat IoT. Dan program pendaftaran perangkat untuk mengelola informasi registrasi perangkat IoT. Ketiga solusi pengembangan ini memanfaatkan teknologi kontrak pintar berbasis *ethereum*. Sehingga memberikan transparansi layanan dan mempermudah untuk melakukan pengembangan lanjutan pada solusi yang diberikan. Dengan demikian, pada perangkat IoT beban komputasi untuk memproses autentikasi dan otorisasi akses sumber daya berkurang karena ditangani secara independen oleh paket solusi. Solusi yang dikembangkan telah diuji dengan rangkaian tes yang ditetapkan dalam *capstone* ini.

Solusi yang dikembangkan dapat menangkal sebagian besar bentuk serangan siber yang ditujukan pada solusi keamanan yang dikembangkan berdasarkan batasan masalah yang telah ditetapkan. Namun, solusi yang dikembangkan masih dalam bentuk kontrak pintar yang perlu integrasi lanjutan dengan layanan IoT yang akan memanfaatkan solusi keamanan ini. Batasan utama yang dihadapi oleh pengujian solusi adalah mekanisme pengujian masih dalam skala laboratorium, sehingga keandalan layanan perlu diujikan kembali pada iterasi pengembangan selanjutnya. Kemudian, solusi keamanan yang dikembangkan perlu peningkatan lebih lanjut pada proses iterasi selanjutnya hingga menghasilkan solusi yang menyeluruh.

Untuk merangkum ringkasan eksekutif ini, pengerjaan *Capstone Project* dengan judul *Capstone* “Implementasi Keamanan IoT Berbasis *Trust* dengan Teknologi *Blockchain*” telah dilaksanakan. Hasil yang diberikan berupa paket solusi keamanan serta hasil pengujian yang dilakukan.