JT : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 12 No. 01 Th. 2023
Halaman : 20 - 25
17 Januari 2023

Model Keamanan Ubiquitous Dalam Mendukung Keamanan Data Pada Smart Agriculture Berbasis Autentikasi Token

Ubiquitous Security Model in Support of Data Security on Smart Agriculture Based on Token Authentication

[1]Sopian Alviana, [2]Sri Wahjuni, [3]Heru Sukoco, [4]Hendra Rahmawan, [5]Shelvie Nidya Neyman
[1,2,3,4,5]Institut Pertanian Bogor, Jl. Meranti Kampus IPB
e-mail: sopianalviana@apps.ipb.ac.id

Receive: 7 Desember 2021 Accepted: 17 Januari 2023

Abstract

The purpose of the study was to propose a ubiquitous system security model using token authentication on Smart Agriculture. The need for an ever-connected network is needed for data delivery in Smart Agriculture, especially those based on the internet of things. However, because it is always connected, data security is needed in every data transmission process. Data security models with authentication are needed to maintain and ensure that communicating is a permitted device. Methods used in the development of this model include literature studies, data collection, analysis of data security needs, as well as creating data security models. The results showed that the Smart Agriculture system model with security support using token authentication has the opportunity to be implemented directly to support security in the data delivery process.

Keywords*: Security, Ubiquitous, Agriculture, Authentication, Token*

Abstrak

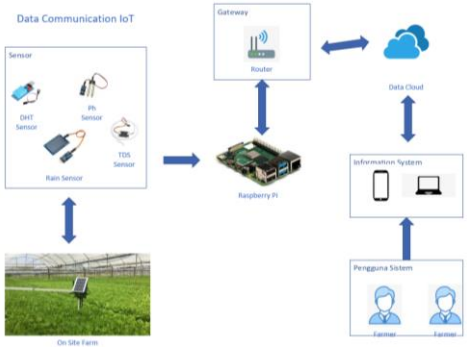
Tujuan dari penelitian ini adalah untuk mengusulkan model keamanan sistem ubiquitous menggunakan autentikasi token pada Smart Agriculture. Kebutuhan jaringan yang selalu terkoneksi dibutuhkan untuk pengiriman data dalam Smart Agriculture, khususnya yang berbasis pada internet of things. Tetapi, karena selalu terkoneksi maka dibutuhkan keamanan data pada setiap proses pengiriman data. Model keamanan data dengan autentikasi dibutuhkan untuk menjaga dan memastikan bahwa yang berkomunikasi adalah perangkat yang diizinkan. Metode yang digunakan dalam pengembangan model ini meliputi studi literatur, pengumpulan data, analisis kebutuhan keamanan data, serta membuat model keamanan data. Hasil penelitian menunjukan bahwa model sistem Smart Agriculture dengan dukungan keamanan menggunakan autentikasi token memiliki peluang untuk diimplementasikan secara langsung untuk mendukung keamanan dalam proses pengiriman data.

Kata Kunci: Keamanan, Ubiquitous, Pertanian, Autentikasi, Token

PENDAHULUAN

Keamanan merupakan Kerahasiaan, Integritas, dan Keaslian informasi [1]. Perkembangan teknologi yang pesat seperti komputasi awan, analisis data, jaringan berbasis Protokol Internet, komputasi dimana – mana, dan lainnya. Telah menjadikan internet of things menjadi sebuah perantara dalam mengendalikan perangkat [2]. Dalam beberapa decade terakhir penggunaan internet of things telah banyak digunakan seperti pada perangkat pintar yang saat ini dikembangkan diantaranya Kota Pintar, Rumah Pintar, Mobil Pintar, Pertanian Pintar dan peangkat pintar lainnya. Meningkatnya jumlah

keterhubungan antar perangkat di internet sudah mencapai beberapa miliar [3]. Perkembangan komputasi ke arah komputasi cerdas ini perlu diimbangi dengan ketersediaan koneksi antar perangkat dengan media penyimpanan data. Ketersediaan koneksi pada system berbasis internet of things dapat mengkonsumsi daya yang sangat besar [4]. Selain itu pentingnya keamanan pada saat berkomunikasi antar perangkat perlu menjadi perhatian saat proses pengiriman data terutama dengan menggunakan internet of things. Sebagian perangkat internet of things bekerja tanpa adanya pengawasan. Penyusup dapat secara mudah masuk ke perangkat tersebut melalui mekanisme jaringan [5]. Keamanan dan privasi merupakan factor yang paling penting dalam sebuah koneksi internet of things [6]. Model koneksi internet of things saat ini seperti pada gambar 1.

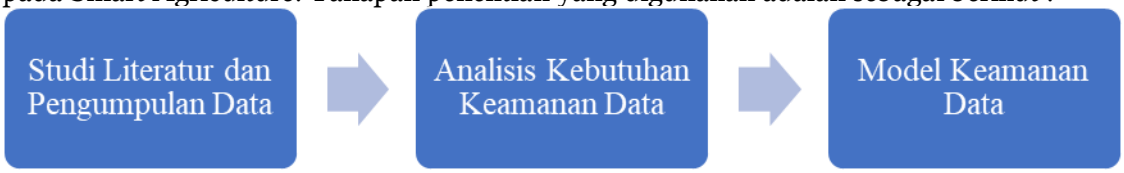


Gambar 1 Data Komunikasi IOT

Model dengan koneksi data pada Smart agriculture pada gambar 1 memiliki beberapa kelemahan diantaranya pertambahan perangkat pada jaringan tersebut seperti penambahan perangkat node sensor atau raspberry perlu dipastikan keamanannya. Karena semakin bertambahnya perangkat, maka tingkat kerentanan data semakin meningkat. Pengambilan keputusan dalam monitoring perangkat dapat meningkatkan implementasi internet of things yang aman [7]. Mekanisme ketersediaan jaringan dalam pengiriman data perlu diperhatikan serta mekanisme keamanan perangkat, agar tercipta penerapan internet of things pada smart agriculture yang memiliki koneksi pengiriman data yang lancar dan aman.

METODE PENELITIAN

Penelitian ini merupakan awal dari pengkajian untuk menghasilkan model system keamanan data yang dapat diterapkan dalam proses pengiriman data untuk penerapan pada Smart Agriculture. Tahapan penelitian yang digunakan adalah sebagai berikut :



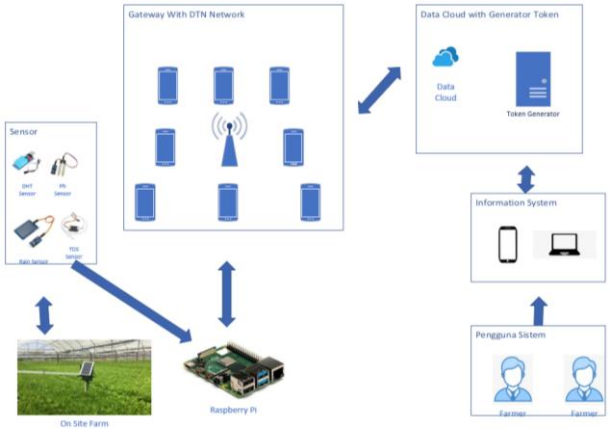
Gambar 2 Metode Penelitian

a. Pengumpulan data dan studi literature, merupakan tahapan awal yang digunakan dalam penelitian ini. Tahapan ini meliputi pengumpulan data penelitian terkait kebutuhan data yang akan digunakan untuk penelitian melalui studi literature terhadap artikel ilmiah yang berkaitan.
b. Analisis Kebutuhan, merupakan inisialisasi dan penelusuran terkait kebutuhan data dan system yang akan digunakan untuk mendukung keaman data pada Smart Agriculture.

c. Model keamanan data yang diusulkan merupakan studi literature terhadap pengumpulan data yang dilakukan pada tahapan awal.

HASIL DAN PEMBAHASAN

Model keamanan data pada Smart Agriculture merupakan upaya dalam melindungi keamanan data pada saat proses pengiriman data sensor ke tempat penyimpanan. Untuk menghasilkan koneksi yang baik dan komunikasi yang berjalan dengan baik dibutuhkan juga proses keamanan data yang dapat mendukung proses tersebut. Smart Agriculture yang berbasis menggunakan internet of things merupakan sebuah awal ide pengembangan ini. Proses pengiriman data yang membutuhkan konektifitas yang baik, agar keamanan data dapat didukung. Model system yang diusulkan adalah dengan memodifikasi arsitektur internet of thing dalam proses pengiriman data. Modifikasi tersebut adalah dengan menambahkan jaringan Delay Tolerant Network, sebagai media perantara yang dapat memberikan kemudahan dalam jaringan yang memiliki konektifitas yang tidak baik [8]. Mekanisme jaringan DTN dapat digunakan untuk melakukan proses pengiriman data dengan mekanisme delay yang diizinkan untuk mempermudah konektifitas dengan kondisi daerah yang tidak terlalu mendukung jaringan yang baik [9]. Gambar 2 merupakan komunikasi data yang digunakan dengan berbasis menggunakan jaringan DTN yang terletak diantara controller node sensor (Raspberry) dengan media penyimpanan data. Hal ini dilakukan, agar pengiriman data dapat diatur dengan mekanisme jaringan delay.



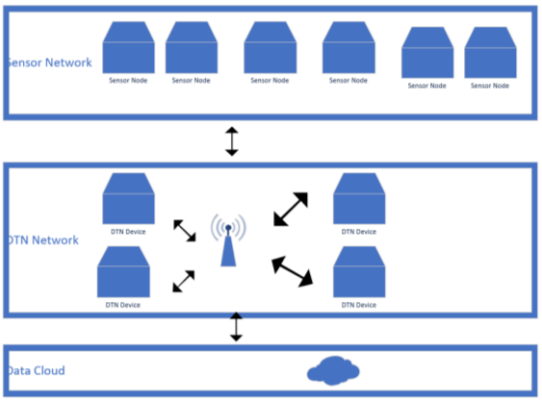
Gambar 3 Komunikasi Data IOT dengan DTN dan Autentikasi Token

Sehingga, dengan gambaran pada gambar 2, menunjukan bahwa penggunaan jaringan DTN dapat dimanfaatkan untuk mekanisme pengiriman data dari node sensor. Sedangkan, mekanisme DTN menggunakan mode store carry setiap bertemu node pada jaringan tersebut. Hal ini memberikan keuntungan bahwa dengan memanfaatkan mekanisme DTN, dapat memberikan kemudahan dalam pengiriman data dengan node yang bersifat mobile [10]. Dengan adanya node tersebut, data akan sering berpindah dan melalui beberapa node. Maka, untuk menjamin keamanan data pada tulisan ini mengusulkan penggunaan mekanisme autentikasi token. Autentikasi token digunakan untuk menjamin bahwa perangkat yang berkomunikasi dan melalui jaringan DTN tersebut adalah merupakan perangkat yang diizinkan. Sehingga, sisi konektifitas yang rendah pada mekanisme Smart Agriculture dapat ditangani dengan menerapkan jaringan

DTN, dan untuk keamanan data menggunakan mekanisme autentikasi token agar dapat menjamin konektifitas perangkat yang melalui jaringan tersebut. Penggunaan DTN juga memungkinkan untuk menghindari kegagalan pada satu titik serta menghindari kegagalan transmisi secara keseluruhan [11].

Delay Tolerant Network (DTN) Untuk Smart Agriculture

Penerapan smart agriculture digunakan hampir di berbagai jenis daerah. Daerah dengan koneksi yang memadai dan tidak memadai telah bergerak kepada penerapan smart agriculture. Jika berada pada daerah dengan koneksi yang baik, maka pengiriman data tidak menjadi kendala. Tetapi dengan kondisi daerah yang minim pada konektifitas, diperlukan sebuah mekanisme dalam pengiriman data sensor yang dibutuhkan pada smart agriculture. Data tersebut sangat berpengaruh karena dibutuhkan untuk proses identifikasi lebih lanjut. Model mekanisme DTN yang diusulkan untuk smart agriculture dalam mendukung mekanisme pengiriman data ditunjukan pada gambar 3.



Gambar 4 Mekanisme DTN

Modifikasi jaringan DTN untuk smart agriculture merupakan perantara antara jaringan node sensor dengan media penyimpanan data. Node sensor akan mengirimkan data dengan mekanisme dibaca oleh konsentrator yaitu Raspberry. Jika menggunakan mekanisme jaringan internet of things konvensional, kebutuhan konektifitas sangat tinggi antara raspberry pi dengan media penyimpanan data di internet. Maka, untuk mengatasi hal tersebut, jaringan DTN menjadi perantara antara data yang dikirimkan oleh raspberry dengan media penyimpanan. Sehingga, dengan koneksi node yang terus berjalan dapat mengoptimalkan waktu transmisi data [12].

Model Autentikasi Token Untuk Perangkat Smart Agriculture

Pada makalah ini, perangkat Raspberry akan meminta layanan kepada server yang telah disiapkan dengan layanan autentikasi token. Raspberry sebagai perangkat node, akan meminta token kemudian layanan pada server membuat token untuk proses autentikasi kemudian hasil token tersebut akan disimpan pada database mysql sebagai data pencatatan awal. Data yang disimpan merupakan data token perangkat, tanggal meminta token, serta id token. Hal ini dipergunakan untuk mekanisme autentikasi pada jaringan Smar Atgriculture yang aman [13]. Layanan autentikasi dapat memastikan keamanan data pada setiap layer yang dilalui [14]. Mekanisme penggunaan autentikasi token tersebut terlihat pada gambar 5.

Gambar 5 Model Autentikasi

Model mekanisme autentikasi, Raspberry akan memintar permintaan kode pada layanan autentikasi. Layanan autentikasi akan mengecek data perangkat yang meinta layanan. Jika perangkat tersebut valid, maka layanan akan melakukan random kode yang menjadi autentikasi kemudian menyimpan kode beserta informasi perangkat kedalam database untuk disimpan. Kode yang telah dibuat akan dikirimkan Kembali ke Raspberry sebagai balasan atas layanan yang diminta. Sehingga, raspberry menjadi perangkat yang sah dan diizinkan untuk mengirimkan data pada jaringan tersebut. Sehingga, dengan mekanisme seperti ini keamanan data akan lebih terjamin dan lebih aman.

UCAPAN TERIMAKASIH

Terima kasih kepada para dosen di Ilmu Komputer IPB untuk semua ilmu yang telah diberikan terutama dalam proses pembuatan jurnal ini.

SIMPULAN DAN SARAN

Hasil penelitian menunjukan bahwa, model usulan keamanan data dengan melakukan modifikasi pada jaringan DTN berbasis pada autentikasi token memberikan ketersediaan jaringan dalam pengiriman data secara aman. Daerah dengan konektifitas rendah dapat memanfaatkan jaringan DTN untuk skema pengiriman data. Teknologi jaringan internet of things dikombinasikan dengan keamanan menggunakan autentikasi token dapat membantu system Smart Agriculture agar tetap terkoneksi dengan keamanan data yang aman dan rahasia

DAFTAR PUSTAKA

Krumm, J. (Ed.). (2018). *Ubiquitous computing fundamentals*. CRC Press.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), 10250-10276.

Roukounaki, A., Efremidis, S., Soldatos, J., Neises, J., Walloschke, T., & Kefalakis, N. (2019, June). Scalable and configurable end-to-end collection and analysis of IoT security data: Towards end-to-end security in IoT systems. In *2019 Global IoT Summit (GIoTS)* (pp. 1-6). IEEE.

Sennan, S., Balasubramaniyam, S., Luhach, A. K., Ramasubbareddy, S., Chilamkurti, N., & Nam, Y. (2019). Energy and delay aware data aggregation in routing protocol for Internet of Things. Sensors, 19(24), 5486.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.

Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., ... & Bhattacharyya, S. (2019). Review on security of Internet of Things authentication mechanism. *IEEE Access*, *7*, 151054-151089.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.

Bounsiar, S., Benhamida, F. Z., Henni, A., Ipiña, D. L. D., & Mansilla, D. C. (2019). How to enable delay tolerant network solutions for internet of things: from taxonomy to open challenges. In *Multidisciplinary Digital Publishing Institute Proceedings* (Vol. 31, No. 1, p. 24).

Singh, V. J., & Bansal, K. L. (2017). Delay Tolerant Networking: Basics for Efficient Communication in Disaster Management. *International Journal of Computer Science & Engineering Technology*, *8*(4), 157-162.

Deng, Q., Huang, S., Tian, S., Liu, H., Cao, J., & Jia, S. (2020, August). A Security Trust Mechanism for Data Collection with Mobile Vehicles in Smart City. In *2020 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 512-517). IEEE.

Yaacoub, E., Abualsaud, K., Khattab, T., & Chehab, A. (2020). Secure transmission of IoT mHealth patient monitoring data from remote areas using DTN. *IEEE Network*, *34*(5), 226-231.

Hansen, M. T., & Biagioni, E. (2010, October). BTP: A Block Transfer Protocol for delay tolerant wireless sensor networks. In *IEEE Local Computer Network Conference* (pp. 897-904). IEEE.

Yang, Y. S., Lee, S. H., Chen, W. C., Yang, C. S., Huang, Y. M., & Hou, T. W. (2021). TTAS: Trusted Token Authentication Service of Securing SCADA Network in Energy Management System for Industrial Internet of Things. *Sensors*, *21*(8), 2685.

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, *19*(5), 1141.