SIMULASI DAN ANALISIS TOPOLOGI JARINGAN IOT UNTUK SMART HOME MENGGUNAKAN CISCO PACKET TRACER

Ahmad Yusuf Al-Hafiz[1], Gerhard Hasangapon Parapat[2], Musa Dwi Cahyo Nababan[3], Dedy Kiswanto[4]
nur23aisyah11@gmail.com[1], parapatgerhard@gmail.com[2], musadwicahyo995@gmail.com[3], dedykiswanto@unimed.ac.id[4]
Universitas Negeri Medan

ABSTRAK

Penelitian ini membahas simulasi dan analisis topologi jaringan Internet of Things (IoT) untuk implementasi sistem smart home menggunakan Cisco Packet Tracer. Tujuan dari penelitian ini adalah merancang sebuah sistem keamanan rumah berbasis IoT yang dapat dikendalikan secara otomatis dan dipantau dari jarak jauh melalui jaringan. Topologi yang dibangun melibatkan router, server IoT, serta beberapa perangkat client seperti laptop dan smartphone yang terhubung dengan perangkat-perangkat IoT berupa kamera, alarm, pintu otomatis, dan jendela. Berdasarkan hasil simulasi, sistem ini mampu merespons skenario keamanan secara otomatis sesuai perintah dari IoT Monitor, seperti mengaktifkan alarm saat pintu terbuka atau saat sistem diakses secara tidak sah. Implementasi ini menunjukkan bahwa topologi jaringan yang dirancang cukup efisien untuk mendukung fungsionalitas smart home. Sistem dapat bekerja secara optimal meskipun tanpa penggunaan switch, karena setiap perangkat telah terhubung melalui jaringan nirkabel. Hasil ini menunjukkan bahwa sistem ini layak digunakan sebagai model awal untuk pengembangan sistem keamanan rumah pintar berbasis IoT.

Kata Kunci: Cisco Packet Tracer, Internet of Things, Sistem Keamanan Rumah, Smart Home, Topologi Jaringan.

ABSTRACT

This study presents a simulation and analysis of an Internet of Things (IoT) network topology for smart home implementation using Cisco Packet Tracer. The primary objective is to design a home security system based on IoT that can be monitored remotely and operates automatically through network control. The proposed topology consists of a router, IoT server, and several client devices such as laptops and smartphones connected to IoT-based security devices including cameras, alarms, automatic doors, and windows. Simulation results show that the system can effectively respond to security scenarios through automation triggered by the IoT Monitor, such as activating an alarm when a door is opened or unauthorized access occurs. The implemented network topology demonstrates efficient performance in supporting smart home functions. Even without switches, the system operates effectively as all devices communicate via wireless connections. These findings indicate that the designed model can serve as a reliable foundation for further development of IoT-based smart home security systems.

Keywords: *Cisco Packet Tracer, Internet of Things, Smart Home, Network Topology, Home Security System.*

PENDAHULUAN

Perkembangan Internet of Things (IoT) telah membawa perubahan besar dalam berbagai aspek kehidupan, terutama dalam bidang sistem keamanan rumah pintar (Smart Home Security System). IoT memungkinkan perangkat-perangkat seperti kamera pengawas, alarm, kipas, lampu, pintu otomatis, dan jendela pintar untuk saling terhubung dalam satu jaringan dan dapat dikendalikan dari jarak jauh menggunakan jaringan internet (Atzori et al., 2010).

Dalam implementasi sistem keamanan rumah berbasis IoT, diperlukan topologi

jaringan yang mendukung komunikasi nirkabel maupun kabel untuk memastikan konektivitas yang stabil dan respons cepat terhadap perintah pengguna. Cisco Packet Tracer menjadi alat simulasi yang tepat untuk memodelkan serta menganalisis perancangan dan performa jaringan IoT dalam Smart Home.

Pada penelitian ini, topologi jaringan IoT dirancang dengan Wireless Router sebagai pusat konektivitas utama yang menghubungkan berbagai perangkat seperti kamera pengawas, alarm, lampu, jendela, pintu otomatis, kipas, dan perangkat rumah tangga lainnya. Selain itu, digunakan juga server IoT untuk mengelola komunikasi antar perangkat dan menyimpan konfigurasi sistem. Penggunaan switch dan laptop sebagai client dalam jaringan juga membantu dalam monitoring dan pengelolaan sistem keamanan rumah. Tujuan dari penelitian ini adalah merancang sebuah sistem keamanan rumah berbasis IoT yang dapat dikendalikan secara otomatis dan dipantau dari jarak jauh melalui jaringan.

Berdasarkan studi yang dilakukan oleh Gubbi et al. (2013), kinerja jaringan IoT sangat bergantung pada efisiensi komunikasi data antar perangkat. Oleh karena itu, penelitian ini berfokus pada simulasi dan analisis topologi jaringan IoT menggunakan Cisco Packet Tracer untuk mengamati stabilitas koneksi, efektivitas sistem keamanan, serta peran perangkat dalam mendukung keamanan rumah pintar.

METODE PENELITIAN

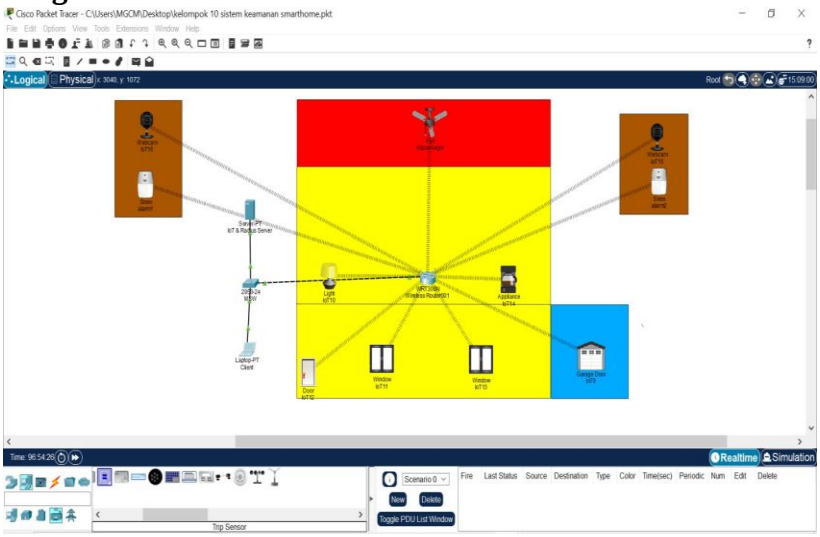
Penelitian ini menggunakan metode simulasi eksperimental dengan pendekatan studi kasus. Simulasi dilakukan melalui perangkat lunak Cisco Packet Tracer untuk merancang dan menganalisis topologi jaringan IoT dalam sistem keamanan rumah pintar (Smart Home).

HASIL DAN PEMBAHASAN

Hasil Simulasi Sistem Keamanan Rumah Pintar

Dalam simulasi menggunakan Cisco Packet Tracer, sistem keamanan rumah pintar berbasis IoT telah berhasil diimplementasikan dengan berbagai perangkat yang saling terhubung dalam satu topologi jaringan. Sistem ini memungkinkan pemilik rumah untuk melakukan pemantauan dan pengendalian perangkat secara otomatis melalui IoT Server yang berperan sebagai pusat kendali utama. Sistem keamanan rumah berbasis IoT yang telah dikembangkan menggunakan Cisco Packet Tracer memanfaatkan perangkat-perangkat IoT yang dikonfigurasi melalui IoT Server. Sistem ini bekerja secara otomatis untuk mendeteksi dan merespons ancaman berdasarkan kondisi tertentu. Dalam implementasinya, sistem keamanan ini didasarkan pada aturan kondisi (device conditions) yang ditetapkan pada IoT Server. Dari gambar kedua yang diberikan, terlihat bahwa aturan ini mengandalkan status perangkat IoT16 dan IoT15 (kamera pengawas) sebagai pemicu utama. Jika kedua kamera tersebut aktif, maka sistem akan menjalankan serangkaian tindakan keamanan secara otomatis. Topologi jaringan yang digunakan dalam simulasi ini termasuk jenis topologi star (bintang), di mana perangkat-perangkat IoT seperti kamera pengawas, sensor, dan lampu terhubung ke pusat kendali utama, yaitu IoT Server. Penggunaan topologi star ini memudahkan pengelolaan dan kontrol dari satu titik pusat, sehingga cocok untuk implementasi sistem keamanan pada rumah pintar.

Arsitektur Jaringan IoT untuk Keamanan Rumah



Berdasarkan hasil implementasi, topologi jaringan terdiri dari beberapa komponen utama yang berperan dalam sistem keamanan, antara lain:

1. Router Nirkabel (WRT300N)
   a. Berfungsi sebagai penghubung utama perangkat IoT melalui koneksi Wi- Fi.
   b. Memungkinkan komunikasi antar perangkat tanpa perlu koneksi kabel.
2. IoT Server & Radius Server
   a. Mengontrol dan mengelola perangkat IoT berdasarkan kondisi yang telah dikonfigurasi.
   b. Berfungsi sebagai pusat pemrosesan data dan eksekusi otomatisasi.
3. Perangkat Keamanan IoT
   a. Kamera CCTV (IoT15 & IoT16): Bertugas melakukan pemantauan visual terhadap lingkungan rumah.
   b. Siren Alarm (alarm1 & alarm2): Digunakan sebagai sistem peringatan jika terdeteksi kondisi mencurigakan.
   c. Pintu Otomatis (IoT12 - Door): Memungkinkan penguncian otomatis saat sistem mendeteksi ancaman.
   d. Jendela (IoT11 & IoT13): Dapat dikendalikan melalui sistem otomatisasi untuk menutup atau membuka berdasarkan kondisi tertentu.
   e. Pintu Garasi (IoT9 - Garage Door): Dapat dikontrol secara otomatis melalui sistem.
4. Perangkat Otomasi Rumah
   a. Lampu Pintar (IoT10): Menyala atau mati berdasarkan kondisi yang telah ditentukan dalam sistem.
   b. Peralatan Rumah Tangga (IoT14 - Appliance): Menunjukkan integrasi perangkat elektronik dalam ekosistem IoT.
   c. Kipas Angin (IoT8 - Fan): Dikendalikan secara otomatis untuk meningkatkan kenyamanan pengguna.

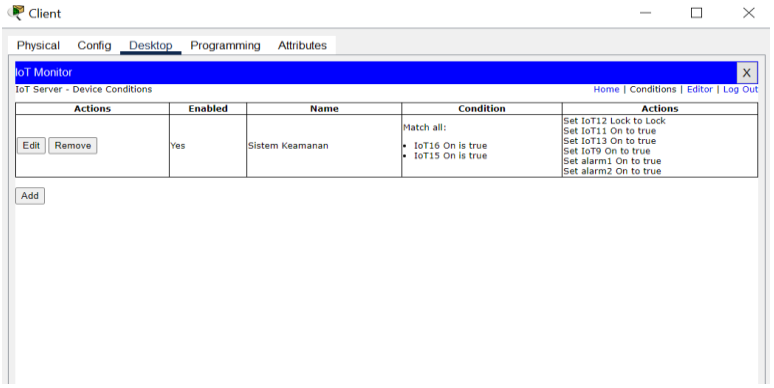
Konfigurasi Sistem Keamanan pada IoT Server

1. Pengertian IoT Monitor dalam Sistem Keamanan

IoT Monitor adalah fitur yang memungkinkan pengguna untuk memantau, mengontrol, dan mengotomatisasi perangkat IoT dalam suatu jaringan. Dalam sistem keamanan berbasis IoT, IoT Monitor berfungsi sebagai pusat kendali utama yang dapat digunakan untuk melihat status perangkat keamanan secara real-time serta mengatur kondisi dan respons otomatis terhadap berbagai peristiwa yang terjadi di lingkungan

rumah pintar.

IoT Monitor bekerja dengan menghubungkan berbagai perangkat seperti kamera pengawas (CCTV), alarm, sensor, lampu, dan pintu otomatis ke dalam satu sistem terintegrasi. Dengan demikian, pemilik rumah dapat melakukan pengawasan dan pengendalian jarak jauh menggunakan antarmuka yang disediakan oleh server IoT.

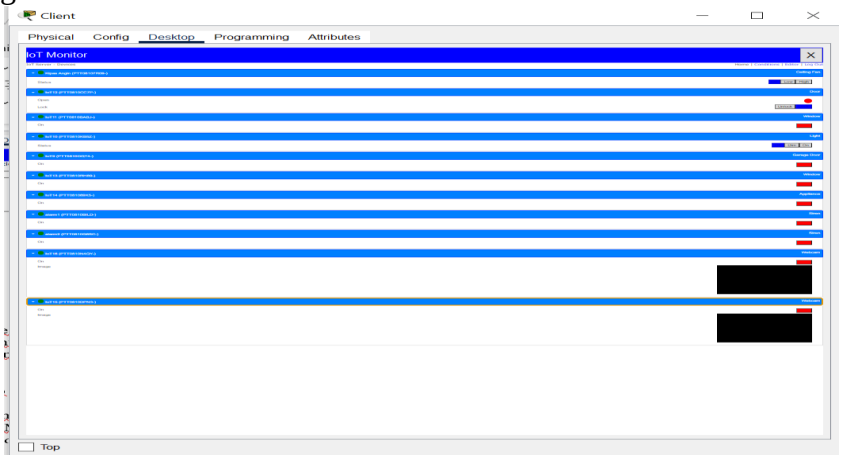


Dari gambar kedua, tampak bahwa IoT Server telah dikonfigurasi menggunakan fitur IoT Monitor untuk mengelola kondisi keamanan rumah. Beberapa aturan otomatisasi yang diterapkan adalah sebagai berikut:

2. Skenario Aktivasi Keamanan
   1) Jika kamera pengawas (IoT15 dan IoT16) menyala, sistem akan secara otomatis:
      a. Mengunci pintu utama (IoT12) untuk mencegah akses yang tidak diinginkan.
      b. Menyalakan jendela pintar (IoT11 dan IoT13) untuk memberikan indikasi visual.
      c. Membuka pintu garasi (IoT9) sebagai alternatif akses darurat.
      d. Mengaktifkan alarm sirine (alarm1 dan alarm2) sebagai peringatan suara terhadap ancaman.
3. Evaluasi Keefektifan Konfigurasi
   a. Konfigurasi ini memastikan bahwa ketika sistem keamanan aktif, tidak ada akses masuk tanpa izin karena pintu utama dikunci secara otomatis.
   b. Kamera CCTV yang menyala menjadi pemicu utama dalam mengaktifkan sistem, yang berarti sistem akan selalu merespons ketika ada aktivitas yang terdeteksi di dalam area rumah.

Monitoring dan Kontrol Perangkat melalui IoT Monitor

1. Keterangan IoT Monitor dalam Simulasi Cisco Packet Tracer



Berdasarkan gambar yang ditampilkan, IoT Monitor dalam sistem keamanan rumah pintar ini memiliki fungsi sebagai berikut:

1) Pemantauan Status Perangkat Keamanan
   a. IoT Monitor menampilkan daftar perangkat yang terhubung, seperti kamera pengawas (webcam), alarm keamanan, jendela otomatis, pintu garasi, lampu, dan kipas angin.
   b. Setiap perangkat memiliki indikator status (On/Off) yang menunjukkan apakah perangkat sedang aktif atau tidak.
2. Pengendalian Perangkat IoT
   a. IoT Monitor memungkinkan pengguna untuk mengaktifkan atau menonaktifkan perangkat keamanan secara manual.
   b. Dalam simulasi ini, perangkat yang dapat dikendalikan antara lain pintu garasi, jendela otomatis, alarm, dan lampu.
3. Otomatisasi Keamanan Berbasis IoT
   a. IoT Monitor dapat digunakan untuk mengatur kondisi otomatis, misalnya jika kamera mendeteksi gerakan, maka alarm akan berbunyi dan jendela serta pintu akan terkunci secara otomatis.
   b. Hal ini meningkatkan efisiensi sistem keamanan dan mengurangi keterlambatan dalam merespons ancaman keamanan.
4. Analisis Visual Status Keamanan Rumah
   a. Dari tampilan IoT Monitor yang diperlihatkan, sebagian besar perangkat keamanan dalam kondisi terkunci dan nonaktif, kecuali kamera pengawas yang tetap aktif sebagai sensor utama dalam sistem keamanan.
   b. Jika terjadi gangguan atau kondisi darurat, sistem dapat langsung memberikan respons sesuai dengan skenario yang telah ditetapkan.

KESIMPULAN

Berdasarkan hasil pengujian dan analisis sistem keamanan rumah berbasis IoT menggunakan IoT Monitor, dapat disimpulkan bahwa teknologi ini mampu meningkatkan efektivitas pengawasan dan pengendalian perangkat keamanan secara real-time. Sistem ini memungkinkan otomatisasi berbagai perangkat, seperti alarm, kamera pengawas, sensor gerak, dan kunci pintu, yang dapat diatur sesuai dengan kondisi tertentu. Dengan adanya fitur otomatisasi ini, respons terhadap ancaman keamanan dapat dilakukan lebih cepat dan efisien dibandingkan dengan metode konvensional. Selain itu, integrasi berbagai perangkat keamanan dalam satu platform terpusat memberikan kemudahan dalam pengelolaan dan memastikan bahwa semua sistem dapat bekerja secara sinergis.Selain kemudahan dalam pengendalian perangkat, sistem ini juga memungkinkan pengguna untuk melakukan pemantauan dan kontrol jarak jauh melalui jaringan internet. Dengan demikian, pemilik rumah dapat dengan mudah mengakses dan mengontrol perangkat keamanan mereka kapan saja dan dari mana saja, memberikan fleksibilitas serta kenyamanan lebih dalam menjaga keamanan rumah. Implementasi teknologi IoT dalam sistem keamanan rumah ini terbukti memberikan solusi yang lebih responsif, efisien, dan aman dibandingkan dengan metode keamanan tradisional.Namun, agar sistem ini dapat berfungsi secara optimal, diperlukan beberapa langkah peningkatan.

Salah satu aspek penting yang perlu diperhatikan adalah keamanan jaringan, mengingat sistem ini terhubung dengan internet dan rentan terhadap serangan siber. Oleh karena itu, penerapan enkripsi data, firewall, serta autentikasi dua faktor sangat disarankan untuk mencegah akses tidak sah. Selain itu, integrasi teknologi kecerdasan buatan (AI) dapat menjadi solusi tambahan dalam meningkatkan keamanan, misalnya dengan mendeteksi pola gerakan mencurigakan dan mengenali wajah secara otomatis.Fleksibilitas dalam pengaturan sistem juga perlu ditingkatkan agar pengguna dapat lebih mudah

menyesuaikan konfigurasi keamanan sesuai kebutuhan mereka. Selain itu, untuk mengantisipasi kemungkinan terputusnya daya listrik yang dapat mengganggu kinerja sistem, penggunaan sumber daya cadangan seperti UPS atau baterai darurat sangat dianjurkan. Tidak kalah penting, pengujian dan pemeliharaan sistem secara berkala perlu dilakukan untuk memastikan bahwa semua perangkat berfungsi dengan baik dan tetap responsif terhadap kondisi darurat.Dengan adanya berbagai perbaikan dan optimalisasi ini, sistem keamanan rumah berbasis IoT dapat semakin andal dan memberikan perlindungan maksimal bagi penghuninya. Penerapan teknologi ini diharapkan tidak hanya meningkatkan keamanan rumah secara signifikan, tetapi juga memberikan kenyamanan serta kemudahan dalam pengelolaan keamanan properti secara modern dan efisien.

DAFTAR PUSTAKA

A. N. D. Nugroho and R. Hidayat, "Perancangan dan Simulasi Smart Home dengan Sistem Keamanan Berbasis IoT Menggunakan Cisco Packet Tracer," Jurnal Infra, vol. 8, no. 1, pp. 34–41, 2020.

A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, Feb. 2014.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805.

D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT Security (IoTSec) Considerations, Requirements, and Architectures," in 2017 IEEE 14th International Conference on Smart City (SmartCity), 2017, pp. 1–8.

I. Nurcahyani and G. Wibisono, "Simulasi Keamanan Jaringan Smart Home Menggunakan Cisco Packet Tracer," Jurnal Teknologi Informasi dan Komputer, vol. 7, no. 2, pp. 45–51, 2021.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

pp. 80–86, 2020

R. Kurniawan and I. Widiatmika, "Implementasi Sistem Keamanan Rumah Berbasis IoT Menggunakan NodeMCU dan Sensor PIR," Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), vol. 6, no. 1,

Z. Mahmood and R. Hill, Smart Home Devices and the Internet of Things: The Essential Guide. Cham: Springer, 2018.