ANALISIS KEAMANAN PADA SISTEM INTERNET OF THINGS UNTUK PENGENDALIAN PERANGKAT ELEKTRONIK RUMAH TANGGA

Oleh :
Eko Mutiha Patrio Siagian[1] Jeremia Siregar[2] Rikardo H. Siahaan[3]
Mahasiswa Teknik Informatika, Fakultas Teknologi Industri
Dosen Teknik Informatika, Fakultas Teknologi Industri([23])
Institut Sains dan Teknologi T.D Pardede([123])

Email :
ekosiagian19@gmail.com[1], jeremiasiregar@istp.ac.id[2], ricardosiahaan@istp.ac.id[3]

ABSTRAK

Sistem Internet of Things (IoT) telah menjadi bagian integral dari kehidupan sehari-hari kita, terutama dalam pengendalian perangkat elektronik di rumah tangga. Namun, pertumbuhan pesat dalam implementasi IoT juga telah membawa berbagai tantangan keamanan yang perlu ditangani secara serius. Skripsi ini bertujuan untuk melakukan analisis mendalam terhadap keamanan pada sistem IoT yang digunakan untuk pengendalian perangkat elektronik rumah tangga. Penelitian ini menggali berbagai risiko keamanan yang mungkin terjadi pada sistem IoT rumah tangga, termasuk serangan siber, pencurian data, dan pelanggaran privasi. Penulis melakukan tinjauan terhadap kerentanan umum yang ada dalam perangkat IoT dan protokol komunikasi yang digunakan. Selain itu, penelitian ini juga membahas praktik terbaik dalam mengamankan sistem IoT, termasuk penggunaan otentikasi yang kuat, enkripsi data, pemantauan keamanan, dan pembaruan perangkat lunak berkala. Metodologi penelitian ini mencakup analisis literatur, studi kasus, dan eksperimen terkait keamanan pada sistem IoT rumah tangga. Hasil penelitian ini akan memberikan pemahaman yang lebih baik tentang risiko keamanan yang terkait dengan IoT dan memberikan panduan praktis untuk meningkatkan keamanan sistem pengendalian perangkat elektronik rumah tangga. Keamanan IoT sangat penting untuk melindungi privasi pengguna dan mencegah potensi kerugian yang dapat disebabkan oleh serangan siber. Dengan peningkatan kesadaran dan pemahaman tentang masalah keamanan pada sistem IoT, diharapkan dapat menghasilkan solusi yang lebih andal dan aman untuk pengendalian perangkat elektronik rumah tangga. Penelitian ini menjadi langkah awal dalam upaya untuk menciptakan ekosistem IoT yang lebih aman dan andal di masa depan.

Kata Kunci: Interne of Things, Kemanan IoT, Pengendalian Alat Elektronik Rumah Tangga, Privasi Pengguna, Protokol Keamanan

ABSTRACT

Internet of Things (IoT) systems have become an integral part of our daily lives, especially in controlling electronic devices in the household. However, the rapid growth in IoT implementation has also brought various security challenges that need to be taken seriously. This thesis aims to carry out an in-depth analysis of the

security of IoT systems used to control household electronic devices. This research explores various security risks that may occur in household IoT systems, including cyberattacks, data theft, and privacy violations. The author reviews the common vulnerabilities that exist in IoT devices and the communication protocols used. Additionally, this research also discusses best practices in securing IoT systems, including the use of strong authentication, data encryption, security monitoring, and regular software updates. This research methodology includes literature analysis, case studies, and experiments related to security in household IoT systems. The results of this research will provide a better understanding of the security risks associated with IoT and provide practical guidance for improving the security of home electronic device control systems. IoT security is critical to protecting user privacy and preventing potential harm that could be caused by cyberattacks. By increasing awareness and understanding of security issues in IoT systems, it is hoped that more reliable and safe solutions for controlling household electronic devices can be produced. This research is the first step in efforts to create a safer and more reliable IoT ecosystem in the future.

Keywords: *Internet of Things, IoT Security, Control of Household Electronic Devices, User Privacy, Security Protocols.*

1. PENDAHULUAN

Internet of Things (IoT) adalah teknologi yang semakin berkembang dan mulai banyak digunakan dalam kehidupan sehari-hari, terutama dalam hal pengendalian perangkat elektronik rumah tangga. Sistem IoT memungkinkan perangkat-perangkat tersebut dapat terhubung ke internet dan saling berkomunikasi, sehingga memudahkan pengguna untuk mengendalikan dan memantau perangkat tersebut dari jarak jauh.

Namun, semakin banyaknya perangkat yang terhubung ke internet melalui IoT juga meningkatkan risiko keamanan. Penyusupan ke dalam sistem IoT dapat mengancam privasi dan keamanan pengguna, serta mengakibatkan kerugian finansial. Oleh karena itu, perlu dilakukan analisis keamanan pada sistem IoT untuk mencegah serangan dari pihak yang tidak bertanggung jawab.

(IoT) merupakan segala aktifitas yang pelakunya saling berinteraksi dan dilakukan dengan memanfaatkan internet. Sistem penggunaan internet secara keseluruhan untuk memenuhi aktifitas kampus akan sangat banyak mendapat manfaat terlebih jika sistem (IoT) ini mempunyai kehandalan jika berintegrasi dengan *cloud computing.* Untuk itu penelitian memanfaatkan (IoT) untuk membuat pengendalian perangkat elektronik rumah (Muhammad Rifaldi 2017).

Dalam penelitian ini, juga menggunakan NodeMCU dan Arduino UNO yang sudah dilengkapi dengan modul WiFi dan beberapa sensor. Sensor IR sebagai pendeteksi jika ada orang tidak dikenal yang masuk melalui jendela dan kamera sebagai pengambil gambar ketika sensor IR mendeteksi

sesuatu yang melewatinya. Ketika kamera sudah mengambil gambar, maka gambar akan disimpan di *SD Card* dan pesan akan dikirimkan kepada pemilik rumah (Fandi Ahmad 2019).

Oleh karena itu, saya mengambil judul ini untuk melakukan analisis keamanan pada sistem IoT untuk pengendalian perangkat elektronik rumah tangga, dan juga diharapkan dapat meningkatkan keamanan dan mencegah serangan dari pihak yang tidak bertanggung jawab, sehingga pengguna dapat merasa lebih aman.

2. TINJAUAN PUSTAKA

Internet of things (IoT) adalah sebuah konsep dimana objek tertentu memiliki kemampuan untuk mentransfer data melalui jaringan wifi, sehingga proses ini tidak memerlukan interaksi dari manusia ke manusia ataupun manusia ke komputer dan semua sudah dijalankan secara otomatis dengan program. Istilah Internet of tings sendiri diperkenalkan oleh Kevin Ashton pada presentasi Proctor & Gamble pada tahun 1999. Kevin Ashton mengoptimalkan RFID (yang digunakan pada barcode detector) untuk supply-chain management domain. Dia juga telah memulai Zensi, sebuah perusahaan yang membuat energi untuk teknologi penginderaan dan monitoring. Internet of things menurut rekomendasi dari ITU-T Y2060 yang didefinisikan sebagai sebuah penemuan yang mampu menyelesaikan permasalahan yang ada melalui penggabungan teknologi. IoT dapat digambarkan sebagai infrastruktur global untuk memenuhi kebutuhan informasi masyarakat yang memungkinkan 6 layanan canggih dengan interkoneksi baik secara fisik dan virtual berdasarkan pada perkembangan informasi serta teknologi komunikasi (ICT). Selain itu, Kevin Ashton sebagai pencetus IoT menyampaikan definisi sensor-sensor yang terhubung ke internet dan berprilaku seperti internet dengan membuat koneksi-koneksi terbuka setiap saat, serta berbagi data secara bebas dan memungkinkan aplikasi-aplikasi yang tidak terduga, sehingga komputer-komputer dapat memahami dunia di sekitar mereka menjadi bagian dari kehidupan manusia (Yudhanto Yudo, 2019).

Asal usul Internet of Things (IoT) dapat ditelusuri kembali ke perkembangan teknologi komputer dan jaringan yang telah berlangsung selama beberapa dekade. Konsep dasar IoT muncul ketika orang-orang mulai menyadari potensi menghubungkan perangkat elektronik dan objek-objek fisik secara bersamaan melalui jaringan.

Pada awalnya, komputer dan perangkat elektronik beroperasi secara terpisah dan memiliki keterbatasan dalam berbagi informasi satu sama lain. Namun, dengan perkembangan teknologi seperti sensor, mikrokontroler, dan jaringan komputer, ide untuk menghubungkan dan mengendalikan berbagai perangkat elektronik mulai muncul.

Istilah "Internet of Things" pertama kali digunakan oleh Kevin Ashton, seorang ahli teknologi dari Massachusetts Institute of

Technology (MIT), pada tahun 1999. Ashton menyadari bahwa dengan memberi objek-objek fisik alat Radio Frequency Identification (RFID) yang mampu mengirimkan dan menerima data melalui jaringan, objek-objek tersebut dapat berkomunikasi dengan infrastruktur komputer tanpa interaksi manusia.

3. METODE PENELITIAN

Internet of things (IoT) adalah sebuah konsep dimana objek tertentu memiliki kemampuan untuk mentransfer data melalui jaringan wifi, sehingga proses ini tidak memerlukan interaksi dari manusia ke manusia ataupun manusia ke komputer dan semua sudah dijalankan secara otomatis dengan program. Istilah Internet of tings sendiri diperkenalkan oleh Kevin Ashton pada presentasi Proctor & Gamble pada tahun 1999. Kevin Ashton mengoptimalkan RFID (yang digunakan pada barcode detector) untuk supply-chain management domain.

3.1 Arduino

Arduino adalah sebuah platform perangkat keras (hardware) dan perangkat lunak (software) yang dirancang untuk memudahkan pengembangan dan prototyping proyek elektronik. Arduino sangat populer di kalangan penggemar elektronika, mahasiswa, dan hobiis karena kemudahan penggunaannya, fleksibilitas, serta biayanya yang relatif terjangkau.

3.2 Metode Analisis Data

Ada beberapa metode analisis data yang dapat digunakan untuk menganalisis keamanan pada sistem IoT tersebut. Beberapa metode analisis data yang relevan meliputi:

1. **Analisis Keamanan Jaringan**: Metode ini mencakup pemeriksaan keamanan pada jaringan yang digunakan untuk menghubungkan perangkat IoT dengan sistem pengendalian. Analisis dilakukan untuk mengidentifikasi kerentanan, potensi serangan, dan celah keamanan pada infrastruktur jaringan. Beberapa teknik yang digunakan dalam analisis keamanan jaringan termasuk *penetration testing*, *vulnerability assessment*, dan *network traffic analysis*.
2. **Analisis Keamanan Perangkat**: Fokus analisis ini adalah pada masing-masing perangkat IoT yang terhubung. Tujuannya adalah untuk mengidentifikasi kerentanan, potensi *firmware* atau *software* yang rentan, dan celah keamanan pada perangkat. Metode ini dapat melibatkan *reverse engineering* untuk menganalisis *firmware* perangkat dan *source code* perangkat lunak yang digunakan.

3.3 Pengumpulan Data

Untuk melengkapi data yang sudah ada diperlukan metode pengumpulan data. Tahap pengumpulan data yang digunakan sebagai berikut:

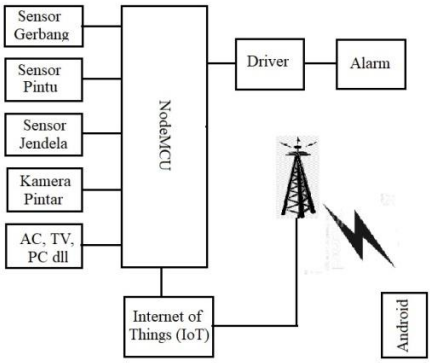
1. **Pengujian Aplikasi:** Jika ada aplikasi pengendalian yang terhubung dengan sistem IoT, pengumpulan data melalui

pengujian aplikasi akan membantu dalam mengidentifikasi kerentanan keamanan pada aplikasi tersebut. Ini melibatkan pengujian aplikasi menggunakan teknik penetration testing dan analisis source code untuk menemukan potensi kerentanan yang dapat dimanfaatkan oleh penyerang.

2. **Pengujian Jaringan:** Pengumpulan data melalui pengujian jaringan akan membantu dalam mengidentifikasi kerentanan dan celah keamanan pada infrastruktur jaringan yang menghubungkan perangkat IoT dengan sistem pengendalian.

3.5 Perancangan Alat

Sebelum melakukan perakitan, peneliti melakukan perancangan desain skematik alat yang akan peneliti buat, dibawah adalah gambar skematik alat yang akan dibuat. Berdasarkan skematik pada Gambar 3.2, cara kerja blok diagram perancangan tersebut. Ketika alat diberi masukan daya dari power, maka alat tersebut akan berada pada kondisi *standby.* Jika sensor mendeteksi NodeMCU dan Arduino UNO akan memproses data, menyalakan *buzzer* dan LED, kemudian kamera akan mengambil gambar dan disimpan dimemori flash NodeMCU kemudian dikirim ke android melalui jaringan Mesos Telegram.



Gambar 1. Skematik Alat

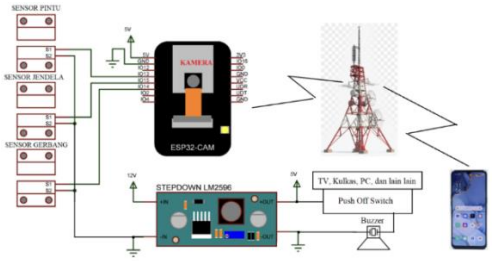
3.6 Prinsip Cara Kerja Alat

Prinsip kerja blok diagram alat yang akan dirancang bangun sebagai berikut:

a. Sensor gerbang, sensor pintu, sensor jendela berfungsi untuk mendeteksi apakah gerbang, pintu, jendela terbuka atau tertutup, jika terbuka maka diinformasikan ke HP android bahwa gerbang, pintu, jendela terbuka dan alarm berbunyi ditempat alat yang dirancang bangun ditempatkan.
b. Kamera pintar berfungsi untuk dapat memantau setiap sudut ruangan yang hasil sorotannya ditampilkan di HP android secara jarak jauh
c. Bila AC, TV, PC dan peralatan lain dicuri maka alarm berbunyi secara otomatis.

3.7 Rangkaian Lengkap

Rangkaian lengkap alat yang dirancang bangun ditunjukkan pada Gambar 3.14. Rangkaian dirancang bangun dengan menggunakan modul sensor pintu, NodeMCU ESP32 Cam, dan PCB matrix.



Gambar 2. Rangkaian Lengkap

Prinsip kerja rangkaian lengkap sebagai berikut:

Sensor pintu gerbang, sensor pintu dan jendela berfungsi untuk mendeteksi apakah pintu dan jedela terbuka atau tidak. Kalau terbuka maka dikirim sinyal informasi ke HP android pemilik rumah bahwa pintu gerbang, pintu dan jendela rumah dibuka maling melalui telegram. Begitu pintu gerbang, pintu dan jendela rumah terbuka maka kamera aktif memphoto dan hasilnya dikirim ke HP android sipemilik rumah. Setelah sipemilik rumah mengetahui bahwa rumahnya dimasuki maling maka tinggal menghubung kantor polisi terdekat supaya datang untuk mengamankan atau menangkap malingnya.

Push off switch (DPDT) berfungsi untuk mendeteksi bahwa peralatan listrik/ elektronika dirumah itu mau diangkat maling sehingga secara otomatis alarm (buzzer) berbunyi. Alarm berbunyi maka malingnya mejadi ketakutan karena orang lain disekitar rumah mendengar suara alarm.

4. HASIL DAN PEMBAHASAN

4.1 Algoritma dari NodeMCU ESP32-CAM

NodeMCU ESP32-CAM adalah modul pengembangan yang menggabungkan mikrokontroler ESP32 dan modul kamera. Algoritma yang ada dalam NodeMCU ESP32-CAM tergantung pada tujuan penggunaannya. Berikut adalah gambaran umum tentang algoritma yang dapat ada dalam alat NodeMCU ESP32-CAM:

1. **Inisialisasi Perangkat:**
   - Menginisialisasi mikrokontroler ESP32 dan mengaktifkan modul kamera.
   - Mengkonfigurasi koneksi Wi-Fi untuk menghubungkan NodeMCU ke jaringan Wi-Fi.
2. **Capture Gambar:**
   - Memulai kamera untuk menangkap gambar.
   - Mengambil data gambar dari sensor kamera.
3. **Praproses Gambar:**
   - Jika diperlukan, melakukan praproses pada gambar seperti pemrosesan warna, penyesuaian kontras, dan pengurangan noise.
4. **Kompresi dan Pengiriman:**
   - Melakukan kompresi gambar untuk mengurangi ukuran file.
   - Mengirim gambar yang telah dikompresi melalui jaringan Wi-Fi ke server atau penyimpanan cloud.
5. **Pemrosesan pada Server (Opsional):**
   - Jika gambar dikirim ke server, server dapat melakukan analisis lebih lanjut, penyimpanan, atau

berbagi gambar dengan pengguna.

6. **Kendali Jarak Jauh (Opsional):**
   - Jika ada fitur kendali jarak jauh, NodeMCU dapat menerima instruksi dari pengguna melalui jaringan Wi-Fi untuk melakukan tindakan tertentu seperti mengambil gambar atau mengaktifkan perangkat terkait.
7. **Manajemen Koneksi:**
   - Mengelola koneksi Wi-Fi untuk memastikan konektivitas yang andal.
   - Menangani situasi koneksi putus atau gangguan sinyal.
8. **Penanganan Error:**
   - Mengelola kondisi error yang mungkin terjadi selama proses, seperti kesalahan kamera, kesalahan jaringan, atau kapasitas memori yang terlampaui.
9. **Manajemen Daya:**
   - Mengelola konsumsi daya dengan bijaksana, seperti mematikan komponen yang tidak digunakan untuk menghemat daya.
10. **Keamanan (Opsional):**
    - Jika diperlukan, menerapkan langkah-langkah keamanan seperti enkripsi data atau otorisasi akses.

4.2 Pengujian Alarm Security

TV, kulkas, komputer, dan peralatan listrik lainnya diangkat sipencuri maka push buttom off switch aktif on sehingga buzzer dan lampu sebagai alarm security berbunyi dan hidup maka sipencuri menjadi takut dan sipemilik rumah atau orang sekitar rumah menjadi mendengar suara alarm dan lampu merah hidup mati pertanda ada pencuri mengambil peralatan listrik. Peralatan listrik (TV, kulkas, komputer dan lain-lain) posisinya dibuat menimpah/ menindih push buttom switch sehingga menjadi aktif off (memutus sambungan listrik ke buzzer). Bila peralatan listrik yang menimpah push buttom switch diangkat maka sensor ini menjadi aktif on untuk menyambungkan arus listrik ke buzzer dan lampu alarm.

4.3 Pengujian IoT

Pengujian IoT Umum:

1. **Koneksi Cloud:** Jika Anda berencana untuk mengirimkan data dari perangkat ke cloud (seperti AWS, Google Cloud, atau platform IoT lainnya), uji koneksi dan transfer data ke cloud tersebut.
2. **Remote Control**: Pastikan Anda dapat mengontrol perangkat secara remote melalui platform cloud atau aplikasi seluler.
3. **Ketahanan:** Uji bagaimana perangkat Anda menangani situasi yang tidak biasa, seperti putusnya koneksi Wi-Fi atau listrik yang mati, dan bagaimana perangkat ini memulihkan diri setelah situasi semacam itu.

4. **Keamanan:** Pertimbangkan aspek keamanan, termasuk mengamankan koneksi dan data yang dikirimkan antara perangkat dan cloud.

4.4 Pembahasan

Alat yang dirancang bangun dapat berkomunikasi dengan HP android melalui jaringan medsos telegram:

1. Nama hotspot dan password tempat alat yang dirancang bangun telah didaftarkan ke dalam program, list programnya yaitu: const char* ssid = "Going to go"; const char* password = "qwerty123";
2. Pin NodeMCU ESP32 CAM yang disambungkan ke sensor magnetic switch didaftarkan pada program, dimana ada tiga buah magnetic switch yang dipakai (satu untuk pintu gerbang, satu untuk pintu rumah, dan satu lagi untuk jendela), list programmnya yaitu:
   const int pinSen1 = 13;
   const int pinSen2 = 15;
   const int pinSen3 = 14;
3. Token "6551109047:AAFJGcaIkhRrR85om9NoV9AujvlU_7tIFBg" ; "6551109047:AAFJGcaIkhRrR85om9NoV9AujvlU_7tIFBg" ; dan ID "1424125601"; akun telegram sipemilik rumah telah didaftarkan pada program. Hasil potret kamera berupa photo dikirim ke HP android sipemilik rumah melalui jaringan medsos, list programnya yaitu:
   String BOTtoken = "6551109047:AAFJGcaIkhRrR85om9NoV9AujvlU_7tIFBg" ;String CHAT_ID = "1424125601";

5. SIMPULAN

5.1 KESIMPULAN

Dari hasil pengujian dan pembahasan penelitian perancangan sistem kendali kamera dan alarm pintar berbasis IoT maka penulis membuat kesimpulan sebagai beriku:

1. Alat sistem keamanan elektronik rumah tangga berbasis *Internet of Things* (IoT) dapat mengendalikan kamera dan buzzer sebagai sumber suara alarm.
2. Sistem kendali alarm bekerja secara otomatis mengaktifkan buzzer untuk mengeluarkan suara alarm bila peralatan rumah tangga dicuri.
3. Medsos telegram yang sudah disetting melalui BotFather sudah membuat jaringan pengiriman photo ke android yang dihasilkan kamera pantau.
4. Bahasa program Arduino IDE dan dikolaborasi dengan program Lau bawahan NodeMCU dapat digunakan menjadi *softdriver* alat yang dibuat.
5. Program aplikasi arduino dapat digunakan untuk memprogram NodeMCU.

5.2 SARAN

Supaya alat yang dirancang bangun ini dapat beroperasi dengan baik dan penelitia pengembagan

berikut maka penulis menyarankan sebagai berikut:

1. Menggunakan kecepatan transmisi dan kapasitas kecepatan pengiriman data internet yang lebih besar dan kencang.
2. Kamera pantau bekerja secara otomatis bila sipencuri/ sipenjahat membuka pintu dan jendela. Kalau sipencuri/ sipenjahat lewat tembok masuk ke pekarangan rumah belum bisa mengaktifkan kamera pantau secara otomatis.
3. Alarm berbunyi bila peralatan rumah tangga sudah diangkat sipencuri maka dikembangkan supaya alarm berbunyi jika peralatan rumah mau diangkat. Karena bila peralatan diangkat dan alarm berbunyi bisa membuat kerusakan sebab pencurinya terkejut.

6. DAFTAR PUSTAKA

1. Alaba, F. A., & Adetunmbi, A. O. (2018). Internet of Things (IoT) in industries: A survey. Future Generation Computer Systems, 82, 480-502.
2. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.
3. Fandi Ahmad. (2019). Sistem Keamanan Rumah berbasis *Internet of Things* (IoT), 4-26
4. Ray, P. P. (2017). A survey of Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences.
5. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266-2279.
6. Vlajic, N., & Dhillon, G. (2019). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 85, 82-105.
7. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261-274.