

Sistem Deteksi Penyusupan Gedung Berbasis IoT

Rawan Djunaedy Sakam¹⁾, Muhammad Tirta Mulia²⁾, Muhammad Sudarsono³⁾

Universitas Pasundan

Jl. Dr. Setiabudhi No. 193 Bandung, (022) 2019371

sakam@unpas.ac.id¹⁾, tirta.mulia@unpas.ac.id²⁾, sudarsono@mail.unpas.ac.id³⁾

Abstrak

Salah satu komponen gedung cerdas adalah keamanan. Dalam hal keamanan, kemampuan untuk mendeteksi penyusupan secara otomatis merupakan fitur yang harus ada pada gedung cerdas. Selain perangkat lunak, sistem deteksi ini membutuhkan perangkat keras yang perlu disesuaikan dengan kondisi fisik dari area yang diobservasi seperti ruangan tertutup, ruangan terbuka, pagar dengan permukaan yang rata dan pagar tidak rata. Artikel ini menganalisis kebutuhan pengembangan dan implementasi sistem deteksi penyusupan yang meliputi perangkat keras (*sensor, platform microcontroller, single board computer*), perangkat lunak (*pengembangan dan automation framework*) serta protokol komunikasi yang berbasis IoT. Tipe area observasi meliputi ruangan dan pagar. Dari hasil implementasi disimpulkan bahwa dengan perangkat keras yang tersedia di pasar saat ini dan dengan *framework home automation* terbuka dapat digunakan untuk mengembangkan sistem deteksi penyusupan di gedung dan dengan konsep IoT pemantauan bisa dilakukan secara *realtime* dan berbasis web yang bisa diakses dimana saja.

Kata kunci: deteksi, penyusupan, sensor, microcontroller, IoT

1. Pendahuluan

Keamanan merupakan salah satu faktor yang penting dalam manajemen perumahan maupun gedung. Tindak kejahatan yang terjadi pada lingkungan gedung rumah dan perkantoran semakin meningkat. Berdasarkan data yang didapat dari Badan Pusat Statistic (BPS) Pada tahun 2010 terjadi 332.490 kasus dan meningkat pada tahun 2015 mencapai 352.936 kasus. Modus yang paling banyak adalah pencurian. Dibutuhkan pemantauan area gedung maupun pemukiman secara terus menerus untuk menghindari terjadinya penyusupan. Pemantauan secara konvensional yaitu yang dilakukan petugas keamanan tidak dapat memenuhi kebutuhan dikarenakan luasnya area yang perlu dipantau dibandingkan dengan personil yang tersedia. Sehingga besarnya usaha untuk memperkecil area *blank spot* sebanding dengan jumlah dari petugas keamanan.

Metode pengamanan tambahan yang paling banyak diterapkan adalah dengan memasang sistem *closed circuit television* atau yang dikenal dengan CCTV. Walaupun dapat beroperasi secara *realtime*, sistem CCTV konvensional secara teknis tidak memberikan dukungan langsung dalam mendeteksi penyusupan, dikarenakan sistem ini memerlukan peran dari manusia (petugas keamanan) untuk melihat layar dari sistem CCTV secara terus menerus. Hal ini memberikan peluang terhadap faktor *human error* dalam pencegahan penyusupan [1]. Penerapan *building automation system* (BAS) yang *highend* pada gedung-gedung lama sangat mungkin dari sisi ekonomi tidak terjangkau. Oleh karena itu dibutuhkan solusi yang bisa berdiri sendiri agar bisa diterapkan pada gedung-gedung tanpa BAS. Solusi ini berupa sistem deteksi pergerakan/penyusupan yang bisa bekerja secara *realtime* dan otomatis serta terjangkau secara ekonomi.

Pada artikel ini, pendekatan *embedded system* dan *internet of thing* (IoT) digunakan untuk mengembangkan sistem tersebut. Konsep *Embedded system* yang dibahas meliputi *platform* perangkat keras (*microcontroller*) dan sensor-sensor yang bisa digunakan untuk deteksi penyusupan dan disesuaikan dengan area observasi. Dari sisi konsep IoT, beberapa metode komunikasi dipertimbangkan agar sesuai dengan kebutuhan dan hemat. Selain itu, *framework* sistem otomasi rumah yang bersifat *open source* juga dipilih dan diaplikasikan untuk kebutuhan gedung. Hal ini mempercepat waktu pengembangan sistem deteksi penyusupan yang diinginkan.

Artikel ini berkontribusi pada (1) penentuan tipe sensor yang paling tepat untuk deteksi pergerakan/penyusupan pada area observasi tertentu, (2) *proof of concept* IoT pada komponen keamanan

gedung cerdas dan (3) pengujian realibilitas *home automation framework* yang bersifat *opensource* pada gedung. Lokasi penelitian dilakukan di Kampus IV Universitas Pasundan, Bandung.

2. Metode Penelitian

2.1. Studi Literatur

Home/Building Automation

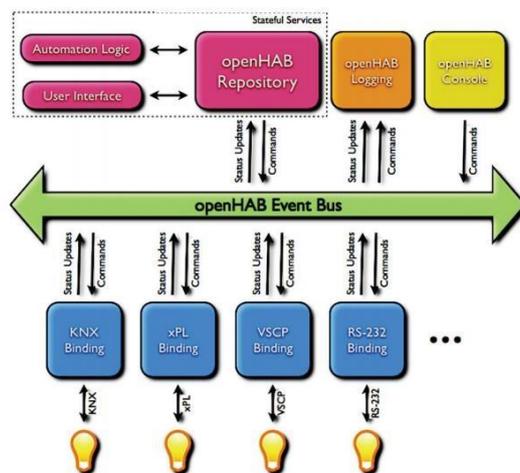
Home automation dapat diartikan sebagai sebuah mekanisme untuk menghilangkan proses kontrol alat-alat elektronik secara teknis atau manual, dan menggantikannya dengan sistem elektronik terprogram [2]. *Home Automation* atau biasa juga disebut *smart home*, untuk skala gedung disebut *building automation* atau *smart building*. Otomasi yang dimaksud adalah pengintegrasian dan pengendalian dari perangkat elektronik yang ada di gedung/rumah misalnya Lampu, TV, Home Theater, CCTV, Alarm, Kipas angin, Door Lock, Motion Sensor, dan masih banyak lagi. Tujuan dari sistem Home Automation mencakup kemudahan, efisiensi energi, keamanan, dan kenyamanan. Pada artikel ini akan dibahas terkait faktor keamanan yang menggunakan perangkat *motion sensor* untuk tujuan deteksi penyusupan. Dari hasil penelusuran literatur, terdapat 5 (lima) *open source home automation framework* yang dapat digunakan pada saat ini, diantaranya yaitu Calaos, Domoticz, Home Assistant, OpenHAB, dan OpenMotics. Pada artikel ini framework yang akan digunakan adalah OpenHAB.

Internet of Things (IoT)

Jika membangun *Home/Building Automation* pada saat ini tentunya Home Automation memiliki hubungan erat dengan konsep IoT. Tidak seperti penelitian tentang Home Automation terdahulu yang mengontrol rumahnya melalui SMS (Short Message Service), sekarang rumah dapat dikontrol secara langsung melalui internet. Internet of Things adalah sebuah sistem yang mengizinkan berbagai perangkat untuk berkomunikasi satu sama lain tanpa campur tangan manusia [3]. Secara singkat Internet of Things dapat didefinisikan sebagai semua benda-benda di sekitar kita dapat berkomunikasi antara satu sama lain melalui sebuah jaringan seperti internet. Perangkat - perangkat ini dapat berkomunikasi dan biasanya memiliki kemampuan sensing parameter lingkungan dengan bantuan microcontroller dan perangkat komunikasi berbasis IP.

Home Automation Framework

Jika berbicara kerangka kerja Home Automation, dari sudut pandang teknologi ada dua platform yaitu *Universal Resource Control (URC)* dan *Eclipse Smart Home (ESH)*. Kerangka kerja URC dan kerangka kerja ESH memiliki banyak kesamaan. Namun, mereka tidak benar-benar tumpang tindih dengan konsep mereka dan karenanya bisa saling melengkapi. Kesamaan yang paling penting adalah kedua platform tersebut mencoba mengintegrasikan teknologi backend yang berbeda dan memberikan deskripsi abstrak tentang perangkat dan layanan yang terhubung. Perbedaan besar antara sistem ada dalam jumlah teknologi backend yang didukung. Berkat dukungan masyarakat yang kuat, implementasi referensi ESH - openHAB - lebih maju dalam aspek ini daripada infrastruktur URC. Di sisi lain, kerangka kerja URC dengan implementasi resource server memiliki konsep yang lebih maju untuk menyediakan user interface yang dipersonalisasi kepada pengguna. Gambar 1 memberikan gambaran umum tentang arsitektur openHAB yang menjadi dasar ESH [4].



Gambar 1 ARsitektur openHAB (dasar dari ESH)

OpenHAB

OpenHAB atau “Open Home Automation BUS” adalah software untuk menggabungkan teknologi atau standard dari Home automation sistem yang berbeda menjadi satu kesatuan, dan menawarkan User Interface yang seragam. Karena sistem yang bersifat opensource dan dapat digunakan untuk pengembangan pemrograman *Home Automation* maka OpenHAB dapat disebut sebuah *framework* untuk *Home Automation*. OpenHAB tidak mencoba untuk menggantikan solusi dari home automation yang sudah ada, tetapi lebih kepada meningkatkannya.

2.2. Analisis

Analisis Kebutuhan Fungsional

Telah diketahui bahwa ada kelemahan pada metode pemantauan gedung/rumah secara konvensional dengan petugas yang berpatroli bahkan yang dibantu dengan alat pemantau menggunakan CCTV. Kelemahan ini berupa *coverage* pemantauan yang berdasarkan mobilitas petugas keamanan dan juga sifat CCTV yang pasif dan masih membutuhkan personil untuk memantau melalui monitor. Untuk itu dibutuhkan sistem deteksi penyusupan yang memiliki fungsi sebagai berikut:

- a. Mampu mendeteksi pergerakan pada area observasi (space atau ruangan, pagar dengan permukaan rata maupun tidak rata)
- b. Mampu melakukan poin a secara realtime
- c. Informasi hasil deteksi dapat diakses secara mobile via internet

Analisis Kebutuhan Perangkat Keras

Untuk memenuhi kebutuhan fungsional pada bagian sebelumnya, dibutuhkan perangkat keras tertentu. Perangkat keras yang dibutuhkan diturunkan dari fungsional dicantumkan pada tabel 1

Tabel 1 Kebutuhan Perangkat Keras

Kebutuhan Fungsional	Perangkat Keras		
	Sensor	Microcontroller	Server
Mendeteksi gerakan pada area observasi	V	V	
Pendeteksian secara realtime	V	V	
Akses informasi dari perangkat mobile via internet			V

Dari tabel satu diketahui bahwa dibutuhkan tiga jenis perangkat keras mulai dari sensor, microcontroller dan server. Platform microcontroller yang dinilai paling ekonomis dan kompatibilitas tinggi adalah platform Arduino. Versi yang digunakan adalah versi 3 dan ESP. Untuk sensor digunakan beragam tipe *motion sensor* yang disesuaikan dengan karakteristik area observasi. Tabel 2 menunjukkan hasil analisis tipe sensor yang sesuai terhadap area observasi.

Tabel 2 Tipe Sensor Untuk Area Observasi

Area Observasi	Tipe sensor	Keterangan
Open space Room	Passive Infrared	
Pagar rata	LDR – Laser beam atau IRBeam	
Pagar tidak rata	IRBeam	

Selain perangkat tersebut, ada juga perangkat keras pendukung yaitu untuk infrastruktur jaringan. Keseluruhan perangkat keras yang dibutuhkan ditunjukkan tabel 3.

Tabel 3 Kebutuhan Perangkat Keras Keseluruhan

No	Kebutuhan	Nama	Jumlah
1.	Server/Gateway	Raspberry Pi 3 model B	1 unit

No	Kebutuhan	Nama	Jumlah
2.	Microcontroller Unit (MCU)	Arduino Uno, Wemos D1 R2	4 unit, 1 unit
3.	Sensor dan Actuator	PIR Sensor, LDR Sensor, Laser Sensor, Relay (1 channel)	1 unit, 8 unit, 8 unit 5 unit
4.	Communication Shield	Ethernet Wiznet W5100	4 unit
5.	Kabel	Kabel Jumper, Kabel UTP, Kabel USB type B,	5 pack, 120 meter, 3 buah
6.	LED indicator	LED 5v	20 buah
7.	Router	TP-Link 65A8	1 unit
8.	Power Supply Unit	USB Power Adaptor (~5V, 1.5 Ampere)	6 buah
9.	Client Devices	Smartphone Android, PC dengan Web browser	1 unit, 1 unit

Analisis Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak dapat dibagi menjadi dua yaitu perangkat lunak untuk pengembangan dan perangkat lunak untuk implementasi. Tabel 4 menunjukkan kebutuhan perangkat lunak untuk sistem deteksi penyusupan ini.

Tabel 4 Kebutuhan Perangkat Lunak

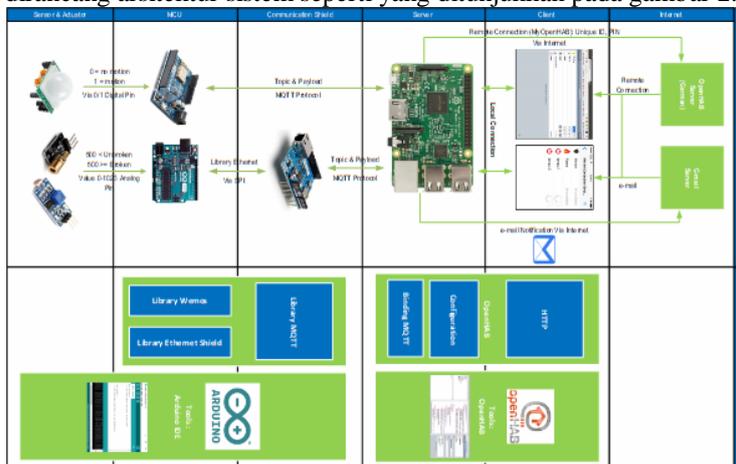
No	Kebutuhan	Nama
1.	IDE/Developer Tool	Arduino IDE v1.8.2, OpenHAB Designer v1.8.3
2.	Framework/Building Automation System	OpenHAB Runtime v1.8.3, OpenHAB Addons v1.8.3
3.	Text Editor	Sublime Text v3
4.	Message Broker (Protokol Komunikasi)	Mosquitto
5.	Operating System Raspberry Pi	Raspbian Jessie
6.	Terminal	MobaXterm
7.	VNC Connection	RealVNC Server dan Viewer
8.	Client side application	Browser Mozilla Firefox, Openhab iOS

Analisis Kebutuhan Komunikasi

Pertukaran data pada sistem berbasis IoT pada dasarnya berjalan di atas protokol TCP/IP. Metode yang paling banyak digunakan sebelumnya adalah berbasis *http request-response*, dimana menggunakan standar pertukaran data pada form aplikasi berbasis web. Namun metode memiliki kekurangan yaitu besarnya ukuran pesan karena banyak sekali header dari pesan. Sedangkan untuk pengiriman data realtime dan kontinyu, hal tersebut dapat membebani jalur komunikasi maupun pemrosesan. Untuk menanggulangi ini digunakanlah protokol MQTT. MQTT (*MQ Telemetry Transport* atau *Message Queuing Telemetry Transport*) adalah protocol konektivitas *machine-to-machine* (M2M)/Internet of Things (IoT) yang berbasis *open source* (Eclipse) dengan standard terbuka (OASIS) yang sangat sederhana dan ringan, yang dirancang untuk perangkat terbatas dan bandwidth rendah, dengan latency tinggi atau dapat berjalan pada jaringan yang tidak dapat diandalkan. Untuk menjalankan protokol ini dibutuhkan *message broker*, salah satunya adalah Mosquitto. Mosquito adalah aplikasi pesan yang mengimplementasikan protocol mqtt, pada penelitian ini agar node(Arduino) dan gateway(raspberry) dapat berkomunikasi satu sama lain dengan menggunakan protocol MQTT, maka mosquito akan ditanamkan pada Raspberry Pi.

2.3 Perancangan Sistem

Dari hasil analisis dirancang arsitektur sistem seperti yang ditunjukkan pada gambar 2.



Gambar 2 Arsitektur Sistem

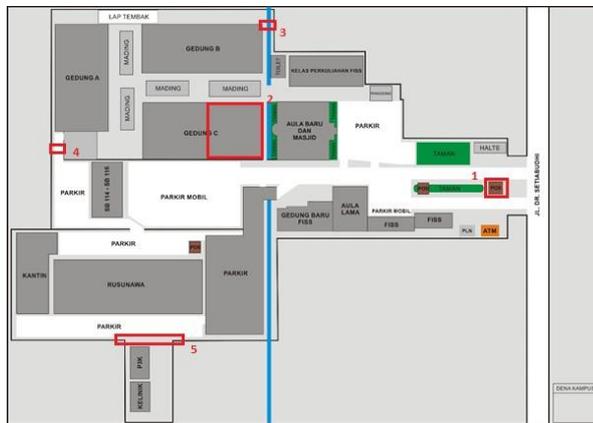
3. Hasil dan Pembahasan

Gambar 3 menunjukkan implementasi komponen sistem dalam hal ini perangkat keras.



Gambar 3 Pengujian Komponen Sistem (A) Server, (B) Node Deteksi Penyusupan Untuk Pagar, (C) Node Deteksi Untuk Ruang/Open Space

Sistem diuji coba di Kampus IV Unpas pada area observasi yang ditunjukkan gambar 4. Gambar 5.a menunjukkan proses yang terjadi pada node, dalam hal ini adalah node untuk deteksi penyusupan di tipe area observasi ruangan, dan gambar 5.b ada screenshot notifikasi email jika deteksi positif.



Gambar 4 (a) Denah Lokasi Observasi (Area Merah); (b) Screenshot Proses Pada Node

Hasil uji coba untuk pendeteksian penyusupan melalui pagar ditunjukkan pada tabel 5 dan hasil pendeteksian pada tipe ruangan ditunjukkan tabel 6. Terlihat pada tabel 5-6 bahwa node dapat mendeteksi adanya pergerakan di area observasi yang mana untuk keadaan tertentu memicu notifikasi berupa email. Email notifikasi ini dapat dilakukan jika server terkoneksi ke internet. Demikian sebaliknya jika node-server hanya terkoneksi ke LAN, maka email notifikasi tidak dapat dikirimkan.

Tabel 5 Hasil Deteksi Di Tipe Area Pagar

Device	Koneksi	Notifikasi Email	Sensor	Tanggal Pengujian
iOS	Internet	Ada	Terdeteksi	11 Agustus 2017
Chrome	Internet	Ada	Terdeteksi	
iOS	LAN	Tidak	Terdeteksi	15 Agustus 2017
Chrome	LAN	Tidak	Terdeteksi	

Tabel 6 Hasil Deteksi Pada Tipe Area Ruangan/Space

Device	Koneksi	Notifikasi Email	Sensor	Tanggal Pengujian
iOS	Internet	Ada	Terdeteksi	11 Agustus 2017
Chrome	Internet	Ada	Terdeteksi	
iOS	LAN	Tidak	Terdeteksi	15 Agustus 2017
Chrome	LAN	Tidak	Terdeteksi	



Gambar 5 (a) Proses pada node; (b) Notifikasi email jika deteksi positif

4. Simpulan

Sistem deteksi yang dibangun baik dari sisi komponen perangkat keras maupun perangkat lunak telah memenuhi kebutuhan fungsional. Penerapan tipe sensor pada node berdasarkan karakteristik area observasi berjalan sesuai perancangan. Dapat dibuktikan bahwa *framework home automation* yang bersifat *open source* dalam hal ini OpenHAB dapat dimanfaatkan untuk mendeteksi pergerakan/penyusupan pada skala gedung. Implementasi konsep IoT memberikan kemudahan dalam memonitor maupun mendapatkan informasi bahkan yang bersifat *push notification* seperti email. Untuk implementasi node, disarankan menggunakan model komunikasi wireless sehingga memudahkan instalasi di area observasi. Selain itu, perlu untuk mengemas node yang berisi microcontroller dan sensor secara tertutup untuk menjaga kerjanya. Serta perlu untuk menyertakan personil di bidang infrastruktur jaringan saat implementasi.

Daftar Pustaka

- [1] N. O. Negara and A. Rahman, "Perancangan Active Surveillance Camera dalam Otomasi Pengawasan Gedung," Institut Teknologi Sepuluh November, Surabaya, 2011.
- [2] A. K. Dennis, *Raspberry Pi Home Automation with Arduino*, Birmingham: Packt Publishing, 2015.
- [3] B. Underdahl, *The Internet of Things for Dummies*, KORE Wireless Edition, Hoboken New Jersey: John Wiley & Sons, Inc, 2014.
- [4] G. Z. M. B. Lukas Smirek, "Just a Smart Home or Your Smart Home – A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console," in *Procedia Computer Science*, London, 2016.