Rancang Bangun Pengaman Rumah dan Kontrol Pada Kunci Pintu dengan Metode Kriptogafi Hill Cipher Berbasis IoT

Nasron
Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi,
Politeknik Negeri Sriwijaya
Palembang, Indonesia
nasronrahman19@gmail.com

Suroso
Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi,
Politeknik Negeri Sriwijaya
Palembang, Indonesia
osorus11@gmail.com

Chandra Buana
Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi,
Politeknik Negeri Sriwijaya
Palembang, Indonesia
chandrabuana886@gmail.com

Abstract— Various kinds of problems are threatening homeowners from the danger of fire to the danger of theft. To reduce the crime rate that occurs in the community, especially the crime of theft and fire hazard, we need an Internet-based home security tool that can be used to access and obtain reports on the condition of the house directly. In this study the design of a unit of home security equipment was carried out using Arduino as a microprocessor to connect software and hardware by combining several sensors to monitor the home security. Sensors used include Passive Infra Red (PIR) to detect moving objects, MQ-2 sensors to detect smoke and solenoid door lock to lock doors that can be controlled and monitored through the android application as an interface used by its users. The research method used is the cryptographic method with the hill cipher algorithm as a safety data command given to the sensor device and door lock. The results of this study in the form of a home security system that is useful for monitoring the state of the house through an android mobile phone when detecting people or smoke that can endanger the situation when the house is empty, and can control the door lock and sensors remotely.

Keywords— home security, IoT, Android, Arduino, kriptografi hill cipher

I. PENDAHULUAN

Ada beberapa penyebab yang mengakibatkan masalah pada keamanan rumah, misalnya tidak menggunakan kunci pintu dan juga masalah seperti kebakaran dan pencurian. Sebagian besar malah timbul karena belum terpenuhi kriteria standar keamanan seperti sensor pendeteksi api, sensor pendeteksi penyusup dan lain-lain.

Perkembangan teknologi telah merambah di dalam berbagai aspek kehidupan. Dimana teknologi memberikan kemudahan bagi penggunanya. Karena itulah berbagai macam pengembangan dalam bidang teknologi dirancang untuk memberikan keamanan, bahkan melindungi aset dan barang yang dimiliki [1].

Dalam situasi maraknya bahaya kebakaran dan pencurian maka dibutuhkan suatu sistem keamanan dan pengawasan yang baik pada sebuah rumah yang dtinggalkan agar tindak pencurian atau bencana kebakaran bisa dihindari. Perkembangan industri elektronik pada saat ini ikut meningkatkan teknologi sistem keamanan rumah. Salah satu teknologi sistem keamanan rumah tersebut adalah teknologi yang diaplikasikan kedalam sistem keamanan rumah dengan basis Internet of Things. Sehingga kita dapat mengakses dan mendapatkan laporan tentang kondisi rumah secara langsung melalui handphone android meskipun dari jarak jauh dengan memanfaatkan jaringan internet yang tersedia.

Tujuan penelitian ini adalah merancang perangkat sistem kemanan rumah yang berguna untuk memonitor dan mengendalikan perangkat yang terkoneksi pada sistem Keamanan Rumah Berbasis Internet of Things (IoT). Diamana Internet of Things (IoT) adalah suatu pengembangan internet yang sedang berjalan dimana benda-benda memiliki kemampuan komunikasi yang membuat mereka dapat mengirim dan menerima data [2].

Pada alat keamanan rumah ini menggunakan metode kriptografi dengan algoritma hill cipher supaya keamanan data kontrol yang dikirimkan bisa terjaga kerahasiannya. Baik berupa kontrol kunci pintu maupun on/ off pada sensor menggunakan kode acak yang berbeda-beda dengan kunci matriks rahasia untuk dapat mengakses printah tersebut, sehingga lebih sulit dibajak oleh orang lain.

II. TEORI DASAR

A. Internet of Things (IoT)

Internet of Things (IoT) adalah sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus-menerus [3]. Konsep dari Iot yaitu bagaimana setiap objek ataupun benda dalam kehidupan sehari – hari dapat terhubung ke jaringan internet untuk mempermudah penggunanya.

B. Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan

aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Hill Cipher juga termasuk dari ilmu Kriptografi yang diciptakan oleh Lester S. Hill pada tahun 1929. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya [4].

C. Arduino Uno

Mikrokontroler Arduino Uno adalah sebuah board mikrokontroler yang memiliki basis ATmega328 [5]. Arduino sendiri termasuk mikrokontroler dimana dapat digunakan untuk mengontrol satu atau berbagai fungsi, proses dan sebagainya dari suatu alat.

Gambar 1. Arduino Uno

D. Sensor MQ-2

Sensor gas asap MQ-2 ini mendeteksi konsentrasi gas dan asap yang mudah terbakar di udara dan outputnya berupa tegangan analog [6]. Berikut gas yang dapat terdeteksi oleh sensor MQ-2: LPG, smoke, i-butane, propane, methane, alcohol, Hydrogen.

Gambar 2. Sensor MQ-2

E. Sensor PIR

Sensor PIR (Passive Infra Red) adalah sensor yang digunakan untuk mendeteksi adanya pancaran sinar infra merah [6]. Mudul Sensor PIR cukup efektif untuk mendektsi gerakan dari objek hingga jarak 6 meter.

Gambar 3. Sensor PIR

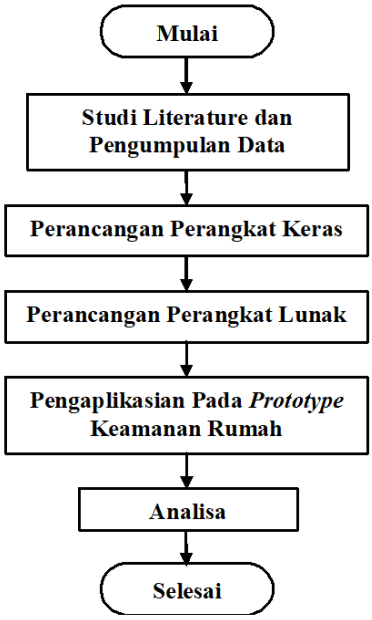
F. Solenoid Door Lock

Solenoid door lock adalah perangkat elektronik kunci pintu dengan menggunakan tegangan 12V sebagai pengendalinya [7]. Dalam kondisi normal atau tanpa diberi tegangan tuas pada solenoid dalam kondisi memanjang atau terkunci, jika diberi tegangan tuas akan memendek atau terbuka.

Gambar 4. Modul Solenoid door lock

III. METODE PENELITIAN

Pada tahap penelitian yang akan dilakukan mengikuti kerangka penelitian sebagai acuan supaya memudahkan proses perancangan dan menghasilkan suatu sistem.



Gambar 5. Kerangka Penelitian

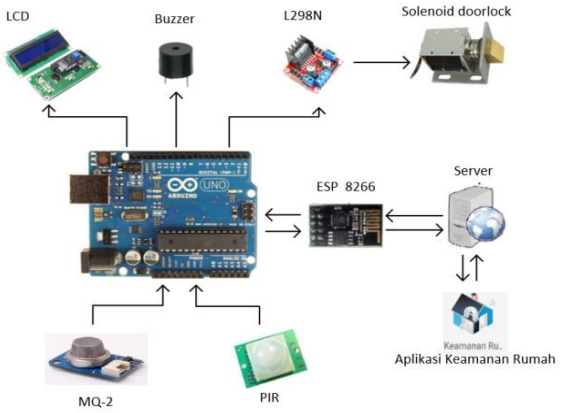
A. Perancangan Perangkat

Perancangan dan pembuatan alat dalam penelitian ini dibagi menjadi dua tahapan, yaitu tahap pertama perancangan perangkat keras (hardware) dan tahap kedua perancangan perangkat lunak (software).

B. Perancangan Perangkat Keras (Hardware)

Perancangan perangkat keras diawali dengan pembuatan blok diagram rangkaian. Pada penelitian ini komponen dan peralatan yang dibutuhkan berupa Arduino Uno, esp8266 sebagai modul wifi untuk mengirim dan menerima data sensor dan kontrol ke alat maupun aplikasi, sensor asap MQ-2 sebagai pendeteksi asap, sensor PIR sebagai pendeteksi pergerakan, buzzer sebagai output apabila sensor

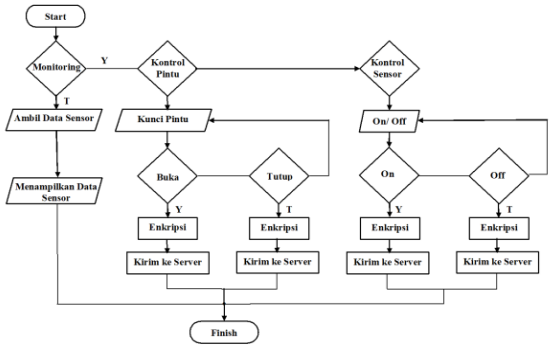
mendeteksi bahaya, LCD untuk melihat setatus secara langsung, L298 digunakan sebagai pengambil keputusan untuk memberikan tegangan atau tidaknya kepada solenoid door lock, solenoid door lock sebagai buka/ tutup kunci pintu serta aplikasi keamanan rumah sebagai media untuk memonitor dan kendali perangkat.



Gambar 6. Blok Diagram Rangkaian

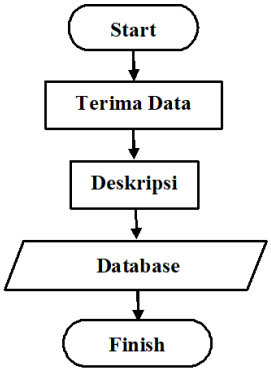
C. Perancangan Perangkat Lunak (Software)

Setelah tahap perancangan perangkat keras yang telah dirakit dirakit, tentunya tidak terlepas dari perancangan perangkat lunak yaitu menggunakan aplikasi android untuk memonitoring dan mengontrol sistem keamanan rumah.



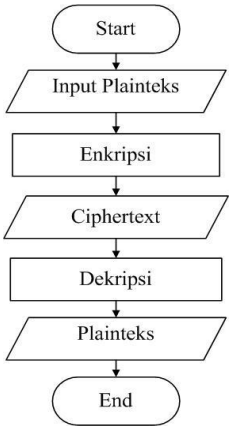
Gambar 7. Flow Chart Sistem pada Android

Pada gambar flow chart sistem pada android terdapat 2 menu yaitu monitoring dan kontrol. Jika memilih monitoring maka akan menuju pengambilan data sensor yang selanjutnya akan menampilkan data sensor. Jika memilih kontrol maka akan menuju ke menu kontrol kunci pintu dan On/Off sensor. Didalam kontrol kunci pintu terdapat 2 pilihan Buka dan Tutup. Jika di pilih Buka maka data perintah akan di enkripsi dan dikirim ke server, jika dipilih perintah Tutup maka data tersebut di enkripsi dan dikirim ke server, jika tidak memilih keduanya maka data akan tetap menampilkan menu kontrol. Ketika memilih On/Off sensor maka terdapat menu On/Off, jika memilih On maka maka perintah akan di enkripsi dan dikirim keserver, jika memilih Off maka perintah akan dienkripsi lalu kirim ke server dan jika tidak memilih keduanya maka akan tetap di menu On/ Off.



Gambar 8. Flow Chart Data di Server

Pada gambar flow chart tersebut menunjukan bahwa alur penerimaan data. Dimana saat data deterima di server maka selanjutnya akan di deskripsi terlebih dahulu baik perintah Buka/ Tutup kunci pintu maupun On/ Off pada sensor yang telah di kirim dari android. Selanjutnya setelah dilakukan deskripsi maka akan disimpan di database berupa text aslinya.



Gambar 9. Diagram Alir Hill Cipher

Proses dimulai dari memberikan input palinteks (data asli) kemudian plainteks tersebut akan di enkripsi menggunakan kunci dengan matriks ordo 2x2 sehingga akan menghasilkan ciphertext (data yang telah tersandi). Untuk mengetahui isi pesan asli tersebut maka dilakukan lagi proses dekripsi yaitu dengan cara mengalikan ciphertext dengan matriks invers kunci dan akan mengubah ciphertext menjadi plaintext kembali. Algoritma *hill cipher* ini diimplementasikan pada kode ASCII.

Berikut proses enkripsi pada *Hill Cipher* adalah:

$$C = K \,.\, P \bmod 256 \qquad (1)$$

Keterangan:
C = Ciphertext
K = Matriks Kunci
P = Matriks Plaintext

Proses dekripsi pada *Hill Cipher* dapat dilakukan dengan cara berikut ini :
Mencari nilai determinan matriks K :

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$|K| = ad - bc$$

Mencari nilai X dengan persamaan :

$$|K| \,.\, X \mod 128 = 1$$

Menentukan matriks invers dari K :

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Proses dekripsi dilakukan dengan persamaan :

$$P = X.\ K\text{-}1.\ C \qquad (2)$$

Keterangan:
P = Plainteks
X = Invers Multiplikasi
K^{-1} = Matriks Kunci Invers
C = Matriks Cipherteks

IV. HASIL DAN PEMBAHASAN

A. Hasil Perancangan Perangkat Keras (Hardware)

Perancangan hardware pada alat keamanan rumah berbasis IoT telah dibuat bedasarkan rancangan alat. Berikut merupakan hasil perancangan perangkat keras (hardware) yang berupa prototype rumah.

Gambar 10. Prototipe Simulasi tampak depan

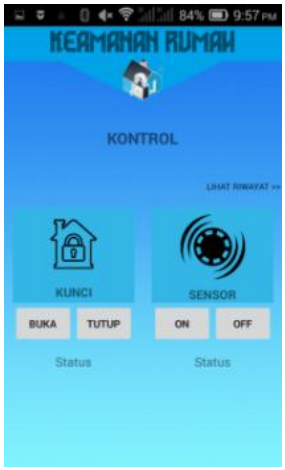
Gambar 11. Prototipe Simulasi tampak atas

Gambar 12. Rangkaian elektronik di dalam *box*

B. Hasil Perancangan Perangkat Lunak (Software)

Data yang di terima dari sensor-sensor pada alat (*hardware*) akan dikirim dalam bentuk informasi ke server. Sistem ini dapat mengirim informasi terus-menerus ke server. Dimana server digunakan sebagai tempat penyimpanan data atau yang disebut dengan database yang nantinya data yang tersimpan dapat kita lihat melalui aplikasi android. Berikut merupakan tampilan hasil dari perancangan *softwere*.

Gambar 13. Tampilan Awal Pada Aplikasi Kemanan Rumah



Gambar 14. Tampil Menu Kontrol

Gambar 15. Tampilan Pada Menu Riwayat Kontrol

Gambar 16. Tampilan Pada Menu Riwayat Sensor

C. Hasil Pengujian

1. Uji Sensor MQ-2

TABEL 1 HASIL PENGUJIAN SENSOR MQ-2

No	Jarak uji (cm)	Likmit Maksimal Asap (ppm)	Asap Terdata (ppm)	Buzzer	Notifikasi
1	5	600	859	Berbunyi	√
2	15	600	719	Berbunyi	√
3	30	600	614	Berbunyi	√
4	50	600	581	TIDAK Berbunyi	×
5	70	600	583	TIDAK Berbunyi	×

Dimana pengujian ini dilakukan terhadap asap yang dihasilkan oleh pembakaran kertas dengan jarak beberapa senti meter dari sensor. Pada pengujian tersebut asap yang dihasilkan tidak terlalu banyak atau pekat dikarenenakan melakukan pengujian dengan cara membakar kertas, jadi semakin pekatnya asap yang terdeteksi maka semakin besar pula asap terdata pada sensor MQ-2 sehingga melewati limit maksimal yang telah di atur.

2. Uji Sensor PIR

TABEL 2 HASIL PENGUJIAN SENSOR PIR

No	Jarak Uji (Meter)	Buzzer	Notifikasi	Status pada LCD
1	1	Berbunyi	√	Ada
2	3	Berbunyi	√	Ada
3	6	Berbunyi	√	Ada
4	7	Tidak Berbunyi	×	No
5	8	Tidak Berbunyi	×	No

Pada tabel tersebut merupakan proses pengujian sensor PIR dengan jarak- jarak tertentu yang telah diukur dengan melalukan pengujian pendeteksian terhadap manusia. Pada jarak 1-6 meter sensor PIR tersebut masih dapat mendeteksi adanya gerakan manusia dan menghidupkan buzzer serta mengirim notifikasi kepemilik rumah, tetapi pada jarak 7 meter dan seterusnya sensor tersebut tidak dapat mendeteksi adanya orang. Pada pengujian sensor PIR dapat diketahui bahwa sensor PIR memiliki sensitivitas tinggi terhadap objek yang melewatinya hingga jarak maksimal 5 meter. Namun, pada jarak 4-6 meter terkadang sensor sulit untuk mendeteksi objek. Sehingga jarak maksimum deteksi yang objektif adalah 3 meter. Ketika tidak adanya gerakan manusia maka otomatis sensor pir tidak akan mengirimkan informasi, walaupun terdapat orang disana. Tetapi ketika ada gerakan lagi maka sensor PIR akan mendeteksi adanya gerakan tersebut.

3. Uji Kontrol Kunci

TABLE 3 UJI KONTROL KUNCI

No	Perintah Yang Dikirim	Waktu Delay (Detik)	Status Pada LCD	Status App
1	BUKA	5,83	Buka	
	TUTUP	6,35	Tutup	
2	BUKA	6,82	Buka	
	TUTUP	8,25	Tutup	
3	BUKA	6,61	Buka	
	TUTUP	6,29	Tutup	
4	BUKA	7,01	Buka	
	TUTUP	7,77	Tutup	
5	BUKA	9,13	Buka	
	TUTUP	9,02	Tutup	

Tabel uji kontrol kunci pintu yang dilakukan sebanyak 5 kali pengujian. Dimana saat diberi perintah BUKA maka solenoid door lock akan merespon dan tuas pada solenoid door lock akan memendek sehingga pintu dapat dibuka dan sebalik nya saat di beri perintah TUTUP maka tuas pada solenoid door lock akan memanjang. Pada saat melakukan pengujian kontrol pada kunci dari aplikasi ke kunci atau solenoid door lock terdapat delay dengan rata-rata delay 7,3 detik, dimana delay tersebut disebabkan oleh kondisi lingkungan dan jaringan internet yang digunakan saat melakukan pengujian.

4. Uji Kontrol Sensor

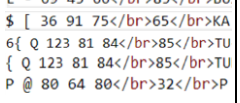
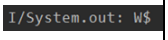
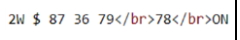
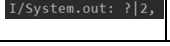
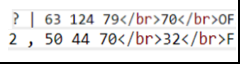
TABEL 4 UJI KONTROL SENSOR

No	Perintah Yang Dikirim	Waktu Delay (Detik)	Status Pada LCD	Status App
1	ON	5,34	On	
	OFF	8,04	Off	
2	ON	7,23	On	
	OFF	5,5	Off	
3	ON	6	On	
	OFF	8,48	Off	
4	ON	9,31	On	
	OFF	11,57	Off	
5	ON	7,51	On	
	OFF	4,86	Off	

Pada uji kontrol sensor dimana pada aplikasi apabila diberi perintah ON maka semua sensor dapat mengirim respon bahaya terhadap pemilik rumah dan sebalik nya apabila di beri perintah OFF maka semua sensor tidak mendeteksi bahaya atau dalam keadaan mati. Pada saat melakukan pengujian kontrol pada sensor dari aplikasi ke sensor terdapat delay dengan rata-rata delay 7,3 detik, dimana delay tersebut disebabkan oleh kondisi lingkungan dan jaringan internet yang digunakan saat melakukan pengujian.

5. Uji Kriptografi Hill Chiper

TABEL 5 UJI KRIPTOGRAFI HILL CHIPER

No	Perintah Yang Dikirim	ENKRIPSI	DESKRIPSI
1	BUKA		
	TUTUP		
2	ON		
	OFF		

Pada tabel uji penerapan kriptografi hill chipper untuk perintah yang dikirim melalui aplikasi android. Dimana saat perintah yang dikirim dari aplikasi adalah perintah ON maka akan di enkripsi dengan menggunakan kunci matrik (K) = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ menjadi karakter W$ dimana nomor asciinya 87 36 akan dikirim ke server terlebih dahulu. selanjutnya pada server akan di deskripsi yang hasil nya akan kembali ke bentuk plain text atau text aslinya ON dengan nomor ascii nya 79 78. Dan untuk perintah-perintah yang lainnya juga di enkripsi terlebih dahulu di aplikasi android, selanjutnya akan di kirim ke server. Didalam server akan dilakukan deskripsi atau pengembalian text yang terenkripsi ke dalam bentuk aslinya agar perintah yang diberikan tersebut dapat membaca oleh alat.

V. KESIMPULAN

Berdasarkan hasil rancang bangun keamanan rumah dengan metode kriptografi hill chipper dapat disimpulkan bahwa Sitem keamanan dengan metode kriptografi hill chipper berbasis IoT (Internet of Things) ini menggunakan mikrokontroler arduino yang di kombinasikan dengan sensor PIR, sensor MQ2 serta Buzzer dan interface nya menggunakan aplikasi android ini telah berfungsi sesuai dengan spesifikasi dan tujuan yang diinginkan. Untuk smua respon baik respons dari pembacaan sensor dan respon dari pengontrolan solenoid door lock meupun kontrol pada sensor bekerja dengan baik sesuai dengan perintah yang dikirimkan. Serta pada Hasil penerapan metode kriptografi hill chipper pada aplikasi keamanan rumah dimana enkripsi dan deskripsi bekerja dengan baik sehingga perintah yang dikirim kan dapat terbaca oleh alat.

DAFTAR PUSTAKA

[1] Tempongbuka, Haribu, dkk. 2015. "Rancang Bangun Sistem Keamanan Rumah Menggunakan Sensor PIR (Passive Infrared) dan SMS Sebagai Notifikasi", E-Journal Teknik Elektro dan Komputer Vol. 4 No. 6, ISSN : 2301-8402.

[2] Marvin, Arie & Eka Puji Widiyanto. 2016. "Sistem Keamanan Rumah Berbasis Internet of Things (IoT) dengan Raspberry Pi. Program Studi Teknik Informatika", STMIK GI MDP Palembang.

[3] Sujadi, Harun & dkk. 2018, "Pengembangan Sistem Monitoring Keamanan Sepeda Motor Berbasis *Internet Of Things* ". Jurnal J-Ensitec: Vol.05 No. 01

[4] Hasugian, Abdul Halim. 2013. "Implementasi Algoritma Hill Cipher dalam Penyandian Data", Pelita Informatika Budi Darma, 4(2), 115–122.

[5] Khana, Rajes, & Uus Usnul. 2018. "Rancang Bangun Sistem Keamanan Rumah Berbasis *Internet Of Things* Dengan Platform Android". Ejournal Kajian Teknik Elektro Vol.3 No.1 Universitas 17 Agustus 1945 Jakarta.

[6] Purnomo, Sigit, & Rozeff Pramana. 2015. "Perancangan Sistem Keamanan Rumah Berbasis SMS Gateway Menggunakan Mikrokontroller Arduino Atmega 2560". jurnal Teknik Elektro, FT UMRAH.

[7] Dharma, Gede Widya, dkk. 2018. "Kontrol Kunci Pintu Rumah Menggunakan Raspberry Pi Berbasis Android". MERPATI VOL. 6, NO. 3.