Implementasi Algoritma *Advanced Encryption Standard* (AES) pada Jaringan *Internet of Things* (IoT) untuk Mendukung *Smart Healthcare*

Alifina Rachmayanti dan Wirawan
Departemen Teknik Elektro, Institut Teknologi Sepuluh Nopember (ITS)
e-mail: wirawan@ee.its.ac.id

Abstrak*—*Internet of Things* merupakan suatu deskripsi dari jaringan fisik atau "*things*" yang dipasang menggunakan *sensor*, *software* dan teknologi lain dengan tujuan menghubungkan dan menukarkan data antar divisi dan sistem lain menggunakan internet. *Internet of Things* (IoT) memiliki beragam aplikasi yang dapat digunakan untuk kebutuhan manusia yang lebih cerdas, salah satunya adalah *Smart Healthcare*, dimana IoT akan membantu pasien/pengguna untuk memperhatikan kesehatannya. Seiring berkembangnya perangkat, IoT mengakibatkan beberapa tantangan yang harus dihadapi seperti masalah keamanan dan sumberdaya. Serangan yang umum terjadi pada suatu sistem IoT adalah *sniffing*. Salah satu cara mengatasi sniffing adalah enkripsi. Akan tetapi penerapan program enkripsi dapat menimbulkan permasalahan lain terutama pada perangkat IoT berbasis embedded system. Sehingga, dibutuhkan metode keamanan dengan konsumsi daya rendah yang sesuai untuk perangkat IoT yaitu Algoritma *Advanced Encryption Standard* (AES). Setelah seluruh bagian diintegrasikan ke dalam sistem, selanjutnya dilakukan tahap pengujian. Hasil pengujian menunjukkan AES-128 yang diterapkan dapat berjalan baik dengan hasil waktu proses yang lebih lama dibandingkan sistem tanpa menggunakan algoritma AES 128 bit sebesar 0,560 detik untuk enkripsi dan 0,018 detik untuk dekripsi. Proses enkripsi dilakukan pada Raspberry Pi menggunakan bahasa PHP sedangkan proses dekripsi dilakukan pada web menggunakan bahasa PHP. Hasil pengujian konektivitas jaringan wifi menunjukkan jarak maksimum sebesar 54 meter agar dapat terhubung. Pengujian keamanan dengan penetration testing menunjukkan bahwa database pada sistem ini aman dari hacker dan memenuhi unsur *confidentiality* atau kerahasiaan data.

Kata Kunci*—*Advanced Encryption Standard (AES), Internet of Things (IoT),* Keamanan Data*, Raspberry Pi, Smart Healthcare.

I. PENDAHULUAN

INTERNET *of Things* (IoT) merupakan sebuah paradigma di mana sejumlah besar node sensor yang didistribusikan secara acak dapat saling terhubung dan berkomunikasi melalui jaringan internet [1]. Istilah "Things" pada IoT memiliki pengertian bahwa manusia dapat mengumpulkan serta mengubah informasi kapan saja dan di mana saja [2]. *Internet of Things* (IoT) bertujuan untuk menyediakan teknologi canggih dan layanan cerdas [3] serta dapat diterapkan untuk kontrol, pemantauan lingkungan, pariwisata, pendidikan, dan keamanan [4]. Di sisi lain, *Internet of Things* (IoT) merupakan sekumpulan perangkat yang memiliki sumber daya rendah dan daya komputasi yang rendah.

Penelitian oleh Gurunath, Agarwal, Nandi, Samanta [5] menyatakan bahwa desainer IoT sering mengabaikan aspek keamanan. Banyak perusahaan juga telah menganalisis IoT yang tersedia di pasaran dan menyimpulkan bahwa keamanan adalah hal yang harus menjadi perhatian utama seiring meningkatnya jumlah perangkat IoT dan serangan siber [3].

Seiring berkembangnya kasus COVID-19 di Indonesia, *smart healthcare* menjadi salah satu pengaplikasian perangkat IoT pada smart city yang mendapat banyak perhatian [6]. *Smart healthcare* menggunakan node sensor untuk menyimpan data pasien seperti profil pasien, detail demografis, hasil diagnosis, *sensitive levels*, dan sebagainya [7]. Berdasarkan hasil riset Zion, sekitar 7,1 juta pasien terdaftar dalam pemantauan pasien secara real-time pada tahun 2016. Selain itu, Pasar Global IoT healthcare memperkirakan terjadi keuntungan sebesar 403% pada 5 tahun kedepan. Hal tersebut tentu dapat menjadi target yang menguntungkan bagi penjahat siber. Sehingga, keamanan menjadi hal penting untuk melindungi data pasien dari serangan siber. Keamanan data pada healthcare dapat diklasifikasikan menjadi 2, yaitu: keamanan jaringan dan keamanan data. Keamanan jaringan berkaitan dengan keberhasilan pengiriman data melalui jaringan sedangkan keamanan data berkaitan dengan integritas dan keaslian data pasien tersebut [4].

Dalam penelitian tugas akhir ini, penulis melakukan proses keamanan menggunakan teknik kriptografi dengan konsumsi daya rendah yang cocok untuk perangkat IoT yaitu Algoritma *Advanced Encryption Standard (AES)*. Mikrokontroller yang digunakan penulis adalah *Raspberry Pi*. Terdapat tiga pengujian untuk memastikan keberhasilan sistem yakni pengujian konektivitas jaringan, pengujian dan kalibrasi sensor suhu DS18B20, serta pengujian waktu komputasi. Proses enkripsi dan dekripsi dalam penelitian ini dilakukan menggunakan bahasa pemrograman PHP.

II. TINJAUAN PUSTAKA

A. *Internet of Things (IoT)*

Internet of Things (IoT) adalah sebuah konsep yang menghubungkan semua perangkat ke internet dan memungkinkan perangkat IoT berkomunikasi satu sama lain melalui internet. "Things" dalam konteks IoT adalah sekumpulan perangkat apa saja dengan pemancar internal yang dapat mengumpulkan dan mengirim data melalui jaringan tanpa intervensi manual. Teknologi yang tertanam dalam objek membantu perangkat IoT berinteraksi dengan keadaan internal dan lingkungan eksternal sehingga dapat membantu dalam hal pengambilan keputusan [8]. Contoh beberapa aplikasi IoT adalah bahan makanan, elektronik, barang koleksi, peralatan apa pun, termasuk benda hidup melalui sensor yang disematkan dan selalu aktif.

Tabel 1.
Tiga Versi AES

Versi AES	Panjang Kunci (Nk words)	Ukuran Blok (Nb words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

B. Ancaman Keamanan IoT

Salah satu tantangan yang harus diatasi untuk mendorong implementasi IoT secara luas adalah faktor keamanan. IoT adalah sistem kompleks yang melibatkan banyak komponen. Kompleksitas tersebut tidak hanya karena keterlibatan berbagai entitas seperti data, perangkat, jalur komunikasi, sensor, dll, tetapi juga karena melibatkan berbagai perangkat dengan berbagai kemampuan komunikasi dan pemrosesan data. Banyaknya entitas dan data yang terlibat membuat IoT menghadapi risiko keamanan yang dapat mengancam dan merugikan konsumen. Ancaman ini dapat berupa akses oleh orang yang tidak berwenang untuk mengakses data dan penyalahgunaan informasi pribadi, memfasilitasi serangan terhadap sistem lain, dan mengancam keselamatan pribadi pengguna. Ancaman yang dapat memengaruhi entitas IoT sangat bervariasi, tergantung pada target serangan.

C. Smart Healthcare

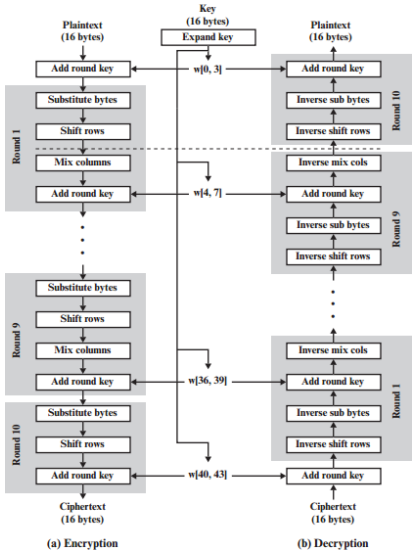
Smart healthcare lahir dari konsep "*Smart Planet*" yang dikemukakan oleh IBM pada tahun 2009 [9]. Smart Planet merupakan konsep infrastruktur cerdas yang memanfaatkan sensor untuk mengirimkan dan menerima informasi melalui *Internet of Things* (IoT), serta mengolah dan memproses informasi menggunakan superkomputer dan komputasi awan agar dapat mengintegrasikannya pada sebuah sistem untuk mewujudkan masyarakat manusia yang dinamis. *Smart healthcare* didefinisikan sebagai sistem pelayanan kesehatan yang mengimplementasikan teknologi seperti perangkat IoT, dan internet seluler untuk mengakses informasi secara dinamis, menghubungkan antar individu, material, dan institusi yang terkait dengan perawatan kesehatan, dan secara aktif dapat mengelola dan menanggapi kebutuhan medis dengan sistem yang cerdas [9].

Penerapan *smart healthcare* berdasarkan jenis kebutuhannya dapat diklasifikasikan sebagai berikut [9] :

a. Diagnosis dan pengobatan
b. Manajemen kesehatan
c. Pencegahan penyakit dan pemantauan risiko
d. Smart hospitals

D. Advanced Encryption Standard (AES)

Advanched Encryption Standard (AES) merupakan cipher blok kunci simetris. AES diterbitkan pada tahun 2001 oleh National Institute of Standards and Technology. AES diperkenalkan untuk menggantikan DES karena DES menggunakan kunci sandi yang sangat kecil dan algoritmenya lebih lambat. Rijndael dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, dan diajukan oleh mereka untuk proses seleksi AES [10]. Algoritma AES memiliki ukuran blok 128 bit atau 16 byte. Tiga versi AES beserta spesifikasi yang mengikuti tercantum pada Tabel 1. AES terdiri dari tiga penyandian blok, yaitu AES-128, AES-192, dan AES-256. Proses enkripsi dan deskripsi AES ditunjukkan oleh Gambar 1.



Gambar 1. Proses Enkripsi dan Dekripsi AES.

1) Proses Enkripsi AES

Tidak seperti DES yang berorientasi bit, Algoritma Rijndael beroperasi dalam orientasi byte (untuk memangkuskan implementasi algoritma ke dalam software dan hardware). Garis besar Algoritma Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan *round key*) [10]:

a. *Addroundkey*

Proses untuk melakukan XOR antara *state* awal (plainteks) dengan cipher key. Tahap ini disebut juga *initial round.*

b. Blok

Blok yang didapat dari proses XOR antara state awal (plainteks) dengan cipher key akan masuk ke tahap selanjutnya dan mengalami putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran antara lain: SubBytes, yaitu substitusi byte dengan menggunakan tabel substitusi (S-box), ShiftRows yaitu pergeseran baris-baris *array state* secara *wrapping*, kemudian MixColumns untuk mengacak data di masing-masing kolom *array state*, dan AddRoundKey untuk melakukan XOR antara state sekarang *round key.*

c. *Final round*

Proses untuk putaran terakhir yang terdiri dari *SubBytes*, *ShiftRows*, dan *AddRoundKey.*

2) Proses Deskripsi AES

Proses dekripsi algoritma AES berbeda dengan proses enkripsi, transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey [10]. Adapun langkah – langkah dekripsi AES adalah:

a. *Addroundkey*

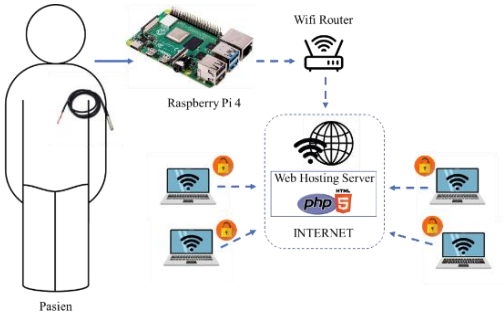
Pada tahap ini pesan yang diterima *(plain text)* akan di XOR kan dengan cipher key. Tahap ini disebut juga dengan *Initial round.*

b. Round

Selanjutnya akan dilakukan putaran sebanyak Nr-1 kali. Proses yang dilakukan terdiri dari: *InvShiftrows* yaitu hasil dari Subbytes digeser secara wrapping, kemudian pada proses

Gambar 2. Spesifikasi Raspberry Pi.

Gambar 3. Sensor Suhu DS18B20.



Gambar 4. Skema Sistem Jaringan Smart Healthcare.

InvSubbytes, hasil dari addroundkey akan dikonversikan menggunakan nilai Inverse sbox, dilanjutkan dengan *InvMixcolumns* yaitu proses mengacak data dengan melakukan perkalian antara matriks publik keys dengan matriks hasil Shiftrows, dan *Addroundkey* dimana state yang dihasilkan sebelumnya di XOR kan dengan *Round key*.

c. *Final Round*

Untuk putaran ke Nr, dilakukan tahap-tahap yang sama dengan round namun tidak melalui proses Mixcolumns. Adapun prosesnya yaitu *InvShiftrows*, *InvSubbytes*, dan *Addroundkey*.

E. Rasberry Pi

Raspberry Pi 4 Model B (Pi4B) adalah produk generasi terbaru dari serangkaian komputer *Raspberry Pi* yang popular di kalangan masyarakat. Produk ini memiliki beberapa keunggulan dibandingkan generasi sebelumnya *Raspberry Pi* 3 Model B+ dalam hal kecepatan prosesor, kinerja multimedia, memori, dan konektivitas dengan konsumsi daya yang serupa. Bentuk *Rasberry Pi* ditunjukkan oleh Gambar 2 dan spesifikasinya terdapat pada Tabel 2.

F. Sensor Suhu DS18B20

Sensor suhu DS18B20 dipilih sebagai salah satu sensor dalam implementasi *smart healthcare* dikarenakan memiliki beberapa keunggulan, seperti: stabil, aman, handal, serta *user friendly* dalam hal pemasangan, juga dapat digunakan untuk pengukuran dengan range 55 – 125^0 C tanpa kalibrasi. Bentuk sensor suhu ditunjukkan oleh Gambar 3. Spesifikasi teknis sensor suhu DS18B20:

a. DC supply voltage: 3 – 5,5 Volt.
b. Tegangan dapat diambilkan dari jalur data (VDD).
c. Tingkat keakuratan: 0,50C dari -100C sampai 850C.
d. Batas temperatur: -550C s/d >1250C
e. *Output*: Digital 1-wire.

Tabel 2.
Spesifikasi Rasberry Pi.

No	Spesifikasi	Keterangan
1	Prosesor	Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) SoC 64-bit @1.5GHz
2	Memori	LPDDR4 1GB, 2GB, 4GB or 8GB (tergantung model) dengan ECC on-die
3	Konektivitas	▪ LAN nirkabel 2.4 GHz dan 5.0 GHz IEEE 802.11b/g/n/ac, Bluetooth 5.0, BLE ▪ Gigabit Ethernet ▪ 2 × USB 3.0 ports ▪ 2 × USB 2.0 ports
4	GPIO	Header GPIO 40-pin standar (kompatibel sepenuhnya dengan papan sebelumnya)
5	Video & suara	▪ 2 × micro HDMI ports (up to 4Kp60 supported) ▪ Port tampilan MIPI DSI 2 jalur ▪ Port kamera MIPI CSI 2 jalur ▪ Audio stereo 4-tiang dan port video komposit
6	Multimedia	▪ H.265 (4Kp60 decode); ▪ H.264 (1080p60 decode, 1080p30 encode); ▪ OpenGL ES, 3.0 graphics
7	SD card support	Slot kartu Micro SD untuk memuat sistem operasi dan penyimpanan data
8	Daya input	▪ 5V DC melalui konektor USB-C (minimal 3A1) ▪ 5V DC melalui header GPIO (minimal 3A1) ▪ *Power over Ethernet* (PoE)–*enabled* (*requires separate* PoE HAT)
9	Environment	Suhu pengoperasian 0-50ºC

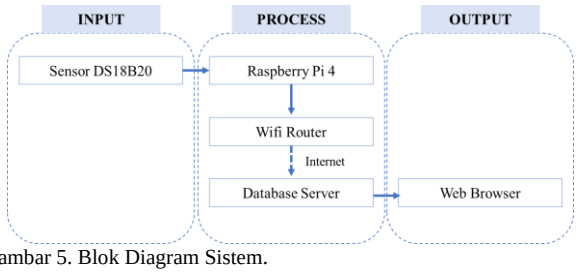
f. Resolusi: 9 – 12 bit.
g. Waktu konversi maks: 750 ms.
h. Tidak membutuhkan komponen lain untuk melakukan pembacaan suhu.

III. METODOLOGI

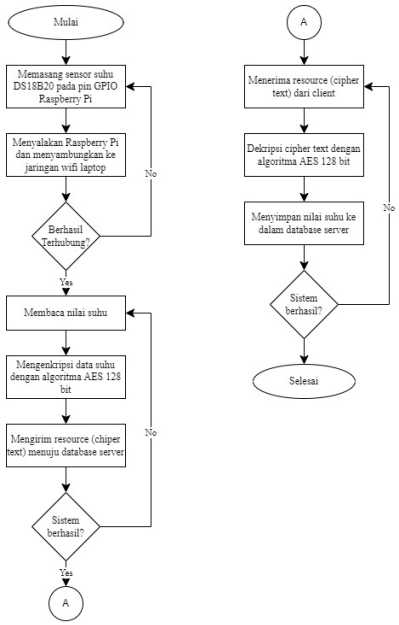
A. Perancangan Sistem

Implementasi *smart healthcare* yang dilakukan pada penelitian ini adalah rawat jalan pasien dimana pengukuran yang dilakukan adalah pengukuran tanda vital pasien. Salah satu parameter penting tanda vital pasien adalah suhu tubuh. Pembacaan pengukuran suhu tubuh pasien dari perangkat sensor suhu DS18B20 oleh *Raspberry Pi* melalui pin GPIO akan dikirim dan disimpan pada database webserver. Pengiriman data dari *Raspberry Pi* ke server tujuan dalam bentuk http request melalui jaringan seluler. Server tujuan yang berisi basis data dan web terhubung dengan node sensor. Di sisi lain pengguna yang tehubung ke internet dapat mengakses data hasil pembacaan node sensor ini melalui web. Data yang dikirimkan oleh *Raspberry Pi* menuju database server merupakan data suhu yang telah dienkripsi menggunakan algoritma AES 128 sehingga bentuk data tersebut bukan lagi plain teks teks melainkan cipher teks. Adapun blok diagram yang akan dirancang seperti dicantumkan pada Gambar 5.

Pada bagian pertama merupakan bagian sensor, yaitu sensor suhu DS18B20 yang dihubungkan oleh pin GPIO *Raspberry Pi*.



Gambar 5. Blok Diagram Sistem.



Gambar 6. Rancangan Alur Kerja Client dan Server.

Pada bagian kedua merupakan gambaran proses enkripsi data sensor yang dilakukan oleh *Raspberry Pi*, data yang diterima pada *Raspberry Pi* akan dikirimkan secara wireless dengan menggunakan wifi yang nantinya diterima oleh komputer.

Proses penerimaan data pada *Raspberry Pi* dengan komputer menggunakan IP address untuk menyambungkan konektivitas jaringan. Setelah itu masuk pada bagian ketiga, pada bagian ketiga menjelaskan mengenai fungsi dari web browser yang dibangun untuk *monitoring* ini yaitu display dan database.

B. *Perancangan Perangkat Lunak*

Pada perancangan perangkat lunak meliputi proses perancangan program – program yang mendukung kinerja sistem. Terdapat 3 tahap dalam perancangan program, yaitu diawali perancangan program sensor suhu DS18B20, server dan database, web browser, algoritme, kemudian dilakukan pengujian waktu komputasi. Gambar 6 menggambarkan rancangan alur kerja dari *client* dan *server* yang digunakan pada penelitian ini.

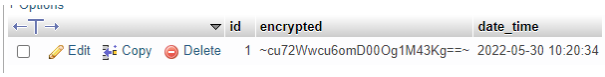
IV. IMPLEMENTASI DAN PENGUJIAN

A. *Implementasi Perangkat Keras*

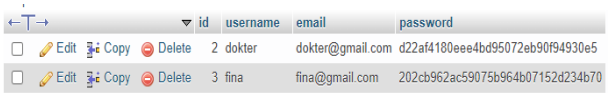
Implementasi perangkat keras seperti pada Gambar 7 merupakan perangkat keras yang digunakan untuk mengimplementasikan sistem keamanan data pasien menggunakan algoritma AES 128 berupa perangkat keras laptop, *Raspberry Pi* 4, dan sensor suhu DS18B20.

Gambar 7. Implementasi Pernagkat Keras.

Gambar 8. Tabel Database Sistem.



Gambar 9. Struktur Tabel Enkripsi Suhu.



Gambar 10. Struktur Tabel *User*.

Implementasi alat monitoring suhu pasien digunakan pada salah satu ruang di rumah sakit untuk pasien rawat jalan. Pada implementasi ini *Raspberry Pi* akan dihubungkan dengan laptop menggunakan wifi. Perancangan tersebut dilakukan dengan setting IP *Raspberry Pi* dan IP laptop dalam satu network sehingga *Raspberry Pi* dapat diakses menggunakan aplikasi remote desktop connection. Daya yang digunakan oleh *Raspberry Pi* berasal dari power adaptor dengan daya minimal 5V / 3A DC agar *Raspberry Pi* dapat bekerja dengan optimal.

B. *Implementasi Basis Data*

Implementasi basis data (*database*) merupakan tahapan dalam pembuatan database pada MySQL yang berfungsi untuk mendukung penyimpanan data. Tampilan basis data web terdiri dari: database sistem yang ditunjukkan Gambar 8, struktur tabel enkripsi suhu pada Gambar 9, dan struktur tabel *user* ditunjukkan oleh Gambar 10.

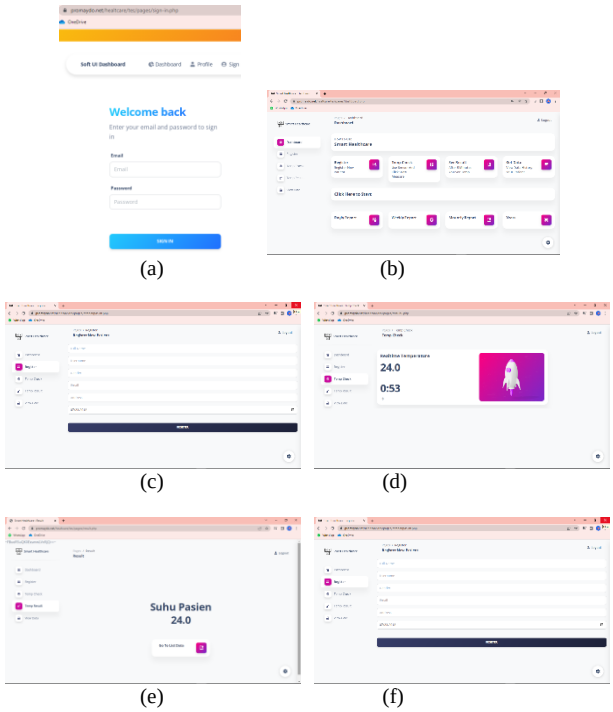
C. *Implementasi Antarmuka*

Tahap implementasi antarmuka merupakan hasil dari perancangan antarmuka sebelumnya, yang akan dioperasikan oleh pengguna. Implementasi ini menggunakan web server untuk mengakses data pasien. Implementasi antarmuka sistem pada penelitian dapat dilihat pada Gambar 11.

D. *Pengujian Konektivitas Jaringan*

Penelitian ini menggunakan jaringan Wifi sebagai media transmisinya, oleh karena itu dilakukan pengukuran kekuatan level sinyal terhadap jarak. Hal ini untuk mengetahui kemampuan maksimal pancaran Wi-Fi pada perangkat *Raspberry Pi*. Pengujian koneksi wifi antara laptop dengan *Raspberry Pi* dilakukan di depan rumah Penulis tanpa ada penghalang yaitu Kota Malang menggunakan aplikasi wifi analyzer. Proses pengujian konektivitas disajikan pada Gambar 12.

Berdasarkan data pada Tabel 3 didapatkan kekuatan sinyal dari berbagai jarak mulai dari 10 meter hingga 54 meter. Pada jarak terdekat, didapatkan kekuatan sinyal sebesar -44 dBm,



(a) (b) (c) (d) (e) (f)

Gambar 2. (a) Tampilan Menu Login. (b) Tampilan Halaman Dashboard. (c) Tampilan Halaman Register Pasien. (d) Tampilan Halaman Cek Suhu. (e) Tampilan Hasil Suhu, (f) Tampilan Data Pasien.

Gambar 3. Pengujian Kekuatan Sinyal Wifi terhadap Jarak.

semakin jauh jarak maka semakin rendah kualitas sinyal yang dikirimkan laptop kepada *Raspberry Pi*.

Adapun jarak maksimal yang didapatkan agar laptop dapat tetap terhubung dengan *Raspberry Pi* adalah 54 meter, dimana pada saat jarak 55 meter koneksi *Raspberry Pi* dengan laptop terputus seperti yang ditunjukkan Gambar 13.

E. Pengujian Keamanan

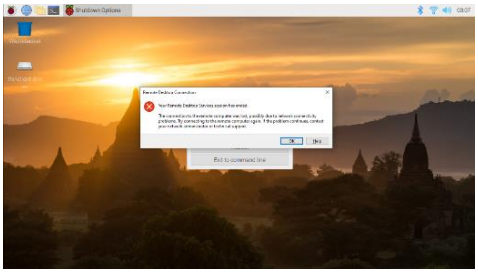
Pengujian keamanan dilakukan untuk memastikan sistem telah memenuhi mekanisme keamanan CIA (*Confidentiality, Integrity, Availability*). Pengujian ini berfokus pada unsur *confidentiality* atau kerahasiaan data yang dikirim melalui jaringan wifi. Parameter yang dilihat pada pengujian ini adalah keamanan database pasien dengan melakukan *penetration test* terhadap celah *SQL Injection* menggunakan *tools* sqlmap versi 1.3.11 yang dijalankan di *command prompt*.

Gambar 14 merupakan langkah *penetration testing* ke dalam database sql.promaydo.net menggunakan *tools* sqlmap. Perintah yang dimasukkan adalah sebagai berikut "sqlmap-uhttps://promaydo.net/healtcare/tes/pages/tables.php?id=40 –dbs –level=3 --risk=3". Ketika perintah tersebut dijalankan, sqlmap akan melakukan proses *scanning* untuk menemukan celah pada website sql.promaydo.net.

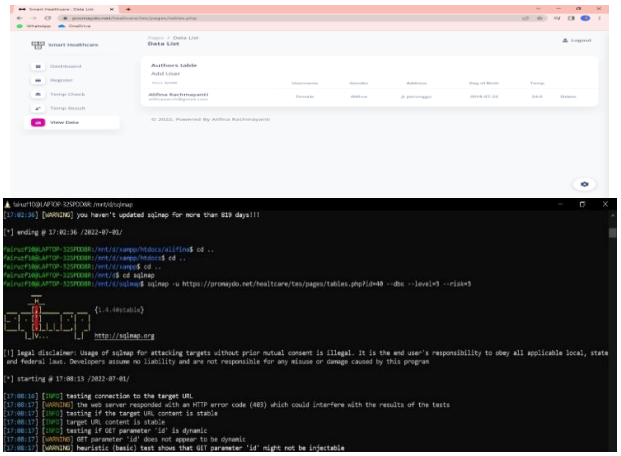
Berdasarkan **Gambar 15** merupakan hasil dari *penetration testing* yang menggunakan *sqlmap* dan didapatkan hasil yaitu

Tabel 3.
Hasil Pengujian Kualitas Sinyal Wifi Terhadap Jarak

Jarak (m)	Kekuatan Sinyal (dBm)	Kualitas Sinyal	Konektivitas
10	-44	Sangat Baik	Aktif
20	-57	Sangat Baik	Aktif
30	-63	Baik	Aktif
40	-77	Cukup Buruk	Aktif
50	-89	Buruk	Aktif
55	-108	Sangat Buruk	Tidak Aktif



Gambar 13. Koneksi Wifi raspberry Terputus dengan Laptop.



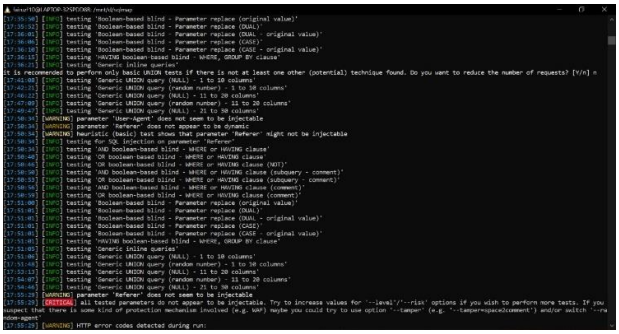
Gambar 14. Perintah Sqlman.

"*parameter 'Referer' does not seem to be injectable*".Output dari sqlmap menunjukkan bahwa database pada sistem ini aman dari *hacker*. Apabila terdapat *hacker* yang ingin menyerang sistem dan berusaha untuk membuka database pasien menggunakan teknik *SQL Injection*, maka secara otomatis *hacker* tidak dapat mengaksesnya. Dapat disimpulkan bahwa implementasi algoritma AES untuk keamanan database pasien pada jaringan *smart healthcare* memenuhi unsur *confidentiality* atau kerahasiaan data.

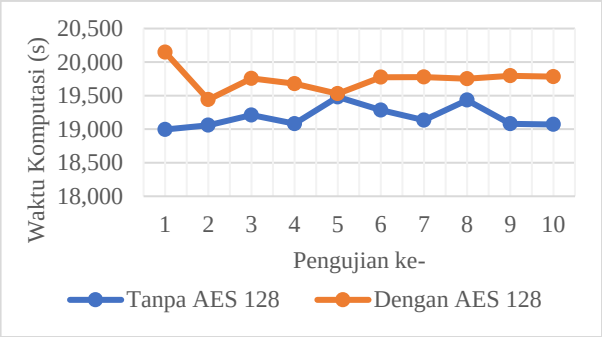
F. Pengujian Waktu Komputasi

Setelah dilakukan pengukuran waktu komputasi sistem menggunakan algoritma AES 128 dan tanpa menggunakan algoritma AES 128, selanjutnya adalah membandingkan kedua hasil pengujian tersebut. Hasil pengujian tersebut ditunjukkan pada Gambar 16 untuk proses enkripsi data dan Gambar 17 untuk proses dekripsi data.

Gambar 16 menampilkan grafik dari hasil perbandingan proses pengiriman data tanpa enkripsi dan setelah dienkripsi. Pengujian dilakukan sebanyak 10 kali pembacaan program dengan looping 100 kali. Sumbu x pada grafik menunjukkan berapa kali waktu pengujian dan sumbu y menunjukkan waktu komputasi sistem dalam satuan detik. Dapat dilihat pada Gambar 4 bahwa waktu enkripsi memakan waktu selama 0,560 detik. Hasil perbandingan membuktikan bahwa implementasi sistem menggunakan algoritma AES memiliki



Gambar 15. Hasil *Penetration Testing* dengan Sqlmap.



Gambar 16. Perbandingan Waktu Komputasi Pengiriman Data.

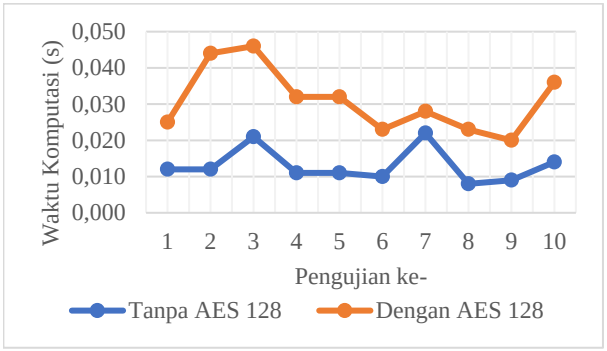
hasil waktu proses yang lebih lama dibandingkan sistem tanpa menggunakan algoritma AES.

Pada Gambar 17 terlihat grafik perbandingan proses penerimaan data menggunakan algoritma AES dan tanpa menggunakan algoritma AES. Dapat dilihat pada Gambar 17 bahwa waktu dekripsi memiliki waktu selama 0,018 detik. Hasil perbandingan ini membuktikan bahwa implementasi sistem menggunakan algoritma AES memiliki hasil waktu proses yang lebih lama dibandingkan sistem tanpa menggunakan algoritma AES. Penggunaan AES 128 bit pada sistem ini memiliki hasil waktu proses yang lebih lama dibandingkan sistem tanpa menggunakan algoritma AES 128 bit. Hal ini dikarenakan adanya pemakaian resource komputer.

V. KESIMPULAN

Pada penelitian ini telah dilakukan implementasi algoritma AES 128 pada jaringan *Internet of Things (IoT)* untuk mendukung *smart healthcare*. Implementasi *smart healthcare* yang dilakukan pada penelitian ini diterapkan untuk pasien rawat jalan untuk mengukur salah satu tanda vital pasien yaitu suhu. Pembacaan pengukuran suhu tubuh pasien menggunakan perangkat sensor suhu DS18B20 oleh *Raspberry Pi* melalui pin GPIO akan dikirim dan disimpan pada database webserver. Apabila *user* ingin mengakses data yang dikirim oleh *Raspberry Pi* menggunakan antarmuka web. Setelah dilakukan implementasi sistem, kemudian dilakukan uji konektivitas wifi dan waktu komputasi sistem enkripsi pada *Raspberry Pi* serta dekripsi pada web menggunakan bahasa pemrograman PHP.

Kesimpulan yang dapat diambil setelah penelitian telah selesai dilakukan adalah sebagai berikut: (1) Konektivitas Raspberry Pi dengan laptop memiliki jarak jangkauan maksimal 54 meter. (2) *Penetration testing* menggunakan sqlmap didapatkan hasil "*parameter 'Referer' does not seem to be injectable*" yang menunjukkan bahwa database pada sistem ini aman dari *hacker* dan memenuhi unsur kerahasiaan data atau *confidentiality*. (3) Proses pengiriman data menggunakan algoritma AES 128 memakan waktu enkripsi selama 0,560 detik untuk ukuran data 16 bit. (4) Proses penerimaan data menggunakan algoritma AES 128 memakan waktu dekripsi selama 0,018 detik untuk ukuran data 16 bit. (5) Hasil penelitian menunjukan bahwa metode enkripsi AES dapat memberikan hasil yang maksimal sehingga metode AES dapat diterapkan pada *smart healthcare* untuk melindungi data pasien yang dikirimkan menggunakan jaringan IoT.



Gambar 17. Perbandingan Waktu Komputasi Penerimaan Data.

DAFTAR PUSTAKA

[1] F. Alshehri and G. Muhammad, "A comprehensive survey of the internet of things (IoT) and AI-based smart healthcare," IEEE Access, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[2] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (IoT)," IEEE Internet Initiat., vol. 1, no. 1, pp. 1–86, 2015.

[3] O. Georgiana Dorobantu and S. Halunga, "Security Threats In IoT," in 2020 International Symposium on Electronics and Telecommunications (ISETC), Nov. 2020, pp. 1–4, doi: 10.1109/ISETC50328.2020.9301127.

[4] M. Khader, M. Alian, R. Hraiz, and S. Almajali, "Simplified AES Algorithm For Healthcare Applications On Internet Of Thing," in 2017 8th International Conference on Information Technology (ICIT), May 2017, pp. 543–547, doi: 10.1109/ICITECH.2017.8080056.

[5] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An Overview: Security Issue In IoT Network," in 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Aug. 2018, pp. 104–107, doi: 10.1109/I-SMAC.2018.8653728.

[6] W. Mercy Kiruba and M. Vijayalakshmi, "Implementation And Analysis Of Data Security In A Real Time IoT Based Healthcare Application," in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), May 2018, no. Icoei, pp. 1460–1465, doi: 10.1109/ICOEI.2018.8553908.

[7] S. K. S. Raja, A. Sathya, and L. Priya, "A Hybrid Data Access Control Using AES And RSA For Ensuring Privacy In Electronic Healthcare Records," in 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Dec. 2020, pp. 1–5, doi: 10.1109/ICPECTS49113.2020.9337051.

[8] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, and F. S. Aliee, "IoT fundamentals: Definitions, architectures, challenges, and promises," in Intelligent Internet of Things, Cham: Springer International Publishing, 2020, pp. 3–50.

[9] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: Making medical care more intelligent," J. Glob. Health, vol. 3, no. 3, pp. 62–65, 2019, doi: 10.1016/j.glohj.2019.07.001.

[10] W. Stallings, Cryptography and Network Security Principles and Practice 7th Edition Global Edition British Library Cataloguing-in-Publication Data, 7th ed. England: Pearson Education, 2017.