Rancang Bangun CRYPTOBLE (Cryptography Portable) Sebagai Alat Pengaman Data Plaintext 16 Bytes pada Jaringan Komunikasi WiFi

Oktario, Swadexi Istiqphara

Program Studi Teknik Elektro, Jurusan Teknologi Produksi, Industri dan Informasi, Institut Teknologi Sumatera
Email : oktario.13116072@student.itera.ac.id, swadexi.istiqphara@el.itera.ac.id

***Abstract*—Semakin maju perkembangan teknologi maka semakin berpengaruh pada perilaku manusia sebagai penggunanya khususnya di era Revolusi Industri 4.0 seperti sekarang ini. Era digital sangat berpengaruh pada perkembangan tekonologi komunikasi khususnya pada jaringan yang semakin cepat dan perangkat elektronik yang semakin cerdas. Salah satu implementasi teknologi komunikasi tersebut adalah telemetry yakni pengukuran jarak jauh yang dapat mempermudah kerja manusia. IoT merupakan integrasi perangkat cerdas yang dapat berkomunikasi untuk mengirimkan data dari jarak yang jauh menggunakan teknologi jaringan internet, oleh karena itu IoT merupakan salah satu bentuk aplikasi telemetry. Proses pengiriman paket data dari perangkat yang satu ke perangkat pusat atau server dengan jaringan wifi merupakan salah satu bentuk IoT. Alhasil data yang dikirikmkan bisa dengan mudah dan cepat. Akan tetapi tidak menjamin suatu keamanan. Karena data yang dikirim melalui suatu jaringan bisa dibaca oleh orang yang tidak berwenang dengan cara *sniffing*. Untuk menghindari terjadinya *sniffing* data solusinya adalah enkripsi dari plaintext menjadi ciphertext. Untuk membuat dan mengimplementasikan algoritma enkripsi tersebut bukanlah hal yang mudah khususnya bagi orang pengguna IoT sekalipun, karena harus mempelajari algoritma yang cukup sulit yaitu kriptografi. Oleh karena itu, penelitian ini bertujuan untuk membuat produk kriptografi portable yang dapat mengamankan data dari prilakui *sniffing*. Produk ini bernama CRYPTOBLE yang dapat mengamankan data sebesar 16 bytes pada komunikasi wifi dengan algoritma yang handal yaitu AES-128-CBC. Hasil penelitian menunjukkan bahwa penggunaan CRYPTOBLE pada jarak 4m, 10, dan 20m. waktu pengiriman data dari perangkat elektronik masing membutuhkan waktu 118.067 µs, 119.467 µs, 123.533 µs.**

***Index Terms*—LPG, PPM, *smartbox*, LITECTOR, MQ-6, *load cell*.**

I. PENDAHULUAN

TELEMETRY merupakan suatu proses pengukuran parameter obyek (benda, ruang, kondisi alam) dengan jarak tertentu yang hasil dari pengukuran tersebut akan dikirimkan baik melalui media kabel maupun nirkabel (wireless) [1]. Penggunaan sistem komunikasi nirkabel (wireless) semakin populer sekarang ini, karena aplikasi teknologi nirkabel memberikan informasi dan komunikasi yang cepat dan mudah dibandingkan dengan komunikasi dengan kabel [2]. Pada kemajuan era digital seperti sekarang ini pengguna lebih banyak menggunakan Internet of Things (IoT) untuk mengirimkan data atau informasi melalui media komunikasi nirkabel [2]. Secara umum, IoT adalah sistem yang digunakan untuk menghubungkan objek-objek cerdas dengan objek yang lainnya, serta lingkungan dengan komputasi awan melalui jaringan internet [3].

Pengiriman data dari sensor yang satu dengan yang lainnya ke komponen penerima biasanya dikenal dengan istilah node, dimana node-node tersebut saling terhubung antara yang satu dengan yang lainnya dalam suatu topologi jaringan atau dikenal dengan istilah wireless sensor network (WSN). WSN merupakan suatu sistem komunikasi yang dapat menghubungkan node-node sensor. Komunikasi yang digunakan dapat bermacam-macam seperti Bluetooth, IR, Wi-Fi, dan Radio. Jaringan komunikasi yang digunakan pada arsitektur IoT biasanya menggunakan Wi-Fi untuk terhubung ke internet. Dengan adanya sistem komunikasi yang benar, maka informasi analog dari lingkungan dapat dikirimkan dalam bentuk data atau digital melalui sensor. Informasi tersebut diambil secara real-time, kemudian diubah kedalam format yang sesuai untuk ditransmisikan melalui jaringan. Selanjutnya, data akan diolah oleh pengolah cerdas dengan teknologi komputasi cerdas tertentu, untuk mencapai tujuan IoT [3].

Data sensor yang terkirim dari sebuah node biasanya mengandung makna atau informasi yang penting bahkan privasi pengguna. Sedangkan, salah satu isu yang menjadi kelemahan pada masalah penggunaan IoT yaitu keamanan dan privasi data [3]. Permasalahannya terletak pada kerentanan suatu jaringan pada sistem komunikasi yang dapat disadap. Hal ini bukan menjadi tidak mungkin dan bisa saja berbahaya jika privasi pengguna dapat diketahui oleh orang lain selain user melalui data yang didapat tersebut. Penyadapan data ini termasuk tindakan kejahatan atau dikenal dengan istilah Cybercrime, dimana orang yang berperan dalam tindakan Cybercrime ini

disebut sniffer. Menurut Kominfo, dalam menghadapi perkembangan teknologi yang memasuki era internet of thing (IoT), keterhubungan menurut Menteri rudiantara menjadi hal yang sangat penting." Era IoT dan big data memungkinkan semua terhubung dengan cyberspace atau jaringan siber" [4]. Selain itu, menurut avast "IoT membawa risiko yang signifikan bagi seluruh ekosistem digital, hal ini karena sebagian besar

perangkat yang terlibat tidak mempunyai sistem keamanan bawaan yang melindunginya dari serangan peretas. Selanjutnya menurut peneliti keamanan di kapersky "ketika orang menjadi semakin dikelilingi oleh perangkat pintar, kami menyaksikan bagaimana serangan IoT juga kian meningkat" [5].

Pengiriman suatu data pada jalur transmisi yang bukan non-https bisa disadap atau sniff dengan menggunakan tool network analyser seperti *wireshark*. Adapun solusi yang dapat digunakan untuk mengatasi sniffing data tersebut supaya tidak dapat dibaca oleh orang lain. Caranya yaitu dengan menerapkan enkripsi data. Enkripsi merupakan suatu proses yang digunakan untuk mengubah data plaintext atau pesan asli menjadi pesan yang tidak dapat terbaca karena sudah disandikan dengan kunci tertentu. Pada tugas akhir ini, peneliti akan merancang alat yang bernama CRYPTOBLE. CRYPTOBLE merupakan alat yang dapat mengenkripsi pesan atau plaintext menjadi ciphertext melalui jaringan wifi, dengan tujuan supaya pesan tidak dapat terbaca. Selain itu pesan yang telah terubah menjadi ciphertext akan diubah kembali menjadi plaintext. Algoritma yang akan digunakan untuk proses enkripsi dan dekripsi yaitu AES-128-CBC.

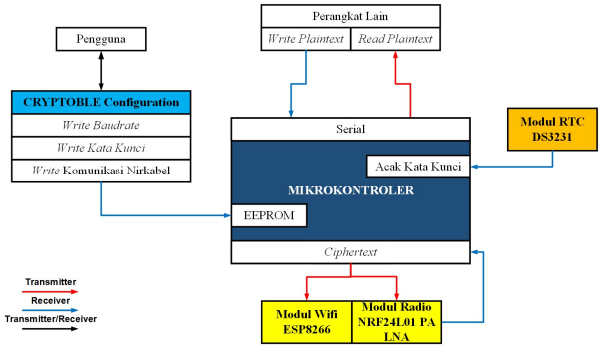
II. METODE PENELITIAN

Metode penelitian yang digunakan memiliki lima alur berikut adalah alurnya.

Gambar 1. Metode Penelitian yang digunakan

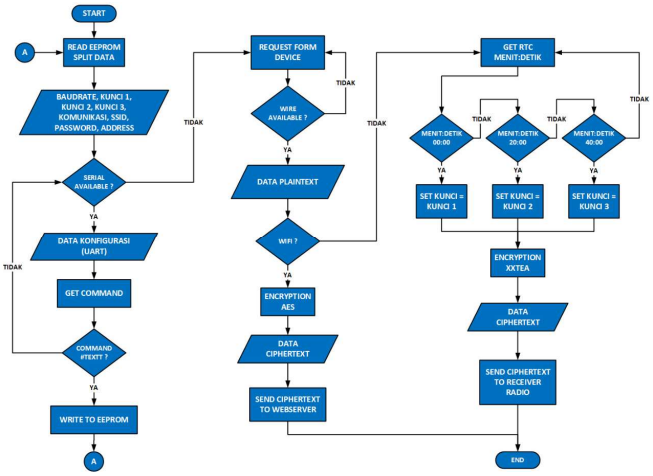
III. PERANCANGAN DAN IMPLEMENTASI

A. *Diagram Blok*



Gambar 2. Diagram Blok Sistem

B. *Flowchart Alat*



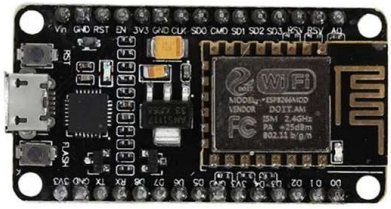
Gambar 3. *Flowchart* Alat

Ketika dijalankan CRYPTOBLE Configuration akan mendeteksi komunikasi serial yang terhubung dengan PC/laptop. Jika komunikasi serial tersedia maka muncul pada kolom PORT nama dari komunikasi serial tersebut, seperti "COM 3". Pengguna memilih komunikasi serial dari CRYPTOBLE dan menekan tombol Connect sehingga membuka jalur serial antara PC/laptop dengan CRYPTOBLE untuk mengirimkan data. Selanjutnya pengguna memasukkan data-data konfigurasi yang diperlukan seperti baudrate, PASSWORD dan SSID. Kemudian menekan tombol OK untuk mengirimkan data-data konfigurasi tersebut ke CRYPTOBLE. Terakhir pengguna menekan tombol *Disconnect* untuk menutup jalur komunikasi serial.

C. KEBUTUHAN KOMPONEN

1. NodeMCU
   Modul nirkabel ESP NodeMCU merupakan modul low-cost wifi dengan dukungan penuh untuk penggunaan TCP/IP. Modul ESP NodeMCU merupakan salah satu modul yang digunakan untuk

komunikasi wifi antar platform. Platform ini dimaksudkan sebagai penghubung antara PC dan mikrokontroler yang dibuat dalam bentuk webclient untuk transmitter dan receiver data yang mempunyai bentuk fisik seperti chip. Modul ESP NodeMCU ini sudah dilengkapi dengan processor, memori, dan juga akses ke General-Purpose Input/Ouput (GPIO) sehingga hal ini menyebabkan modul ESP8266 dapat secara langsung menggantikan Arduino dan keunggulannya telah mendukung koneksi wifi secara langsung [6].



Gambar 4. Modul Wifi NodeMCU

Categories	Items	Parameters
Wi-Fi	Protocol	802.11 b/g/n/3/i
	Frequency Range	2.4 GHz ~ 2.5 GHz
Hardware	CPU	Tensilica L106 32-bit processor
	Peripheral Interface	UART/SDIO/SPI/I2C/I2S/IR Remote Control
		GPIO/PWM
	Operating Voltage	2.5 V ~ 3.6 V
	Operating Current	80 mA
	Operating Temperature Range	−40 ℃ ~ 125 ℃
Software	Wi-Fi Mode	Station/SoftAP/SoftAP+Station
	Security	WPA/WPA2
	Encryption	WEP/TKIP/AES
	Network Protocols	IPv4, TCP/UDP/HTTP/FTP
Harga	Rp 40.000	

2. Arduino Nano
   Arduino merupakan mikrokontroler open-source yang sudah dirangkai lengkap dengan sistem minimum. Salah satu mikrokontroler Arduino yang di produksi adalah Arduino Nano. Menggunakan chip mikrokontroler ATmega328 dan dikemas dalam ukuran yang kecil mikrokontroler ini sangat cocok untuk project berskala kecil. Arduino Nano dibekali dengan 32 KB flash memory (2 KB digunakan untuk bootloader), 16 Mhz clock speed, dan memiliki 20 pin I/O.

Microcontroller	ATmega328
Operating Voltage	5 V
Input Voltage	7 – 12 V
Flash Memory	32 KB (2 KB *bootloader*)
SRAM	2 KB
Clock Speed	16 MHz
EEPROM	1 KB
DC Current per* I/O *pins	40 mA
Analog IN pins	8
Digital* I/O *pins	22 (6 PWM)
Input Voltage	7 – 12 V
Harga	Rp 37.000

D. *Kebutuhan software*

1. Arduino IDE
   Software ini merupakan *software* pengembangan dari produk Arduino untuk *mengompile* dan mengunggah *source code* yang telah dibuat menggunakan Bahasa Arduino ke mikrokontroler Arduino.
2. Wireshark untuk pengujian sniffing data yang sedang dalam jalur transmisi atau sedang berjalan dari perangkat pemancar menuju webserver.
3. MySQL + XAMPP
   Sebuah perangkat lunak *Relational Database Management System* (DBMS) yang didistribusikan secara gratis dibawah Graphic Public Lisence (GPL).

E. Hasil Implementasi

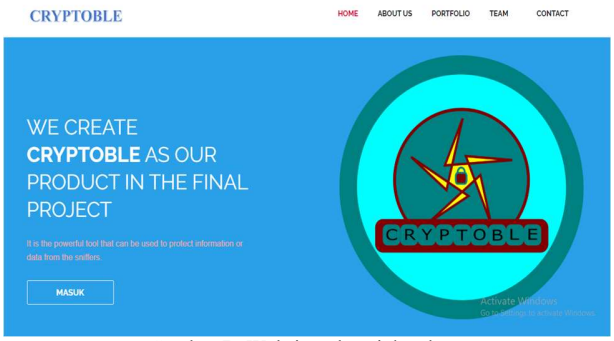
Hasil implementasi alat berdimensi kotak dan berwarna hitam serta diberi nama *CRYPTOBLE.*

Gambar 5. CRYPTOBLE

Pada CRYPTOBLE terdapat beberapa konektor, yaitu konektor masukkan VCC, RX, TX, GND untuk menghubungkan CRYPTOBLE denhgan perangkat lain atau untuk menerima data serial yang dikirim ke pemancar dan juga ada konektor untuk menghubungkan modul wifi sehingga data bisa terhubung ke webserver.

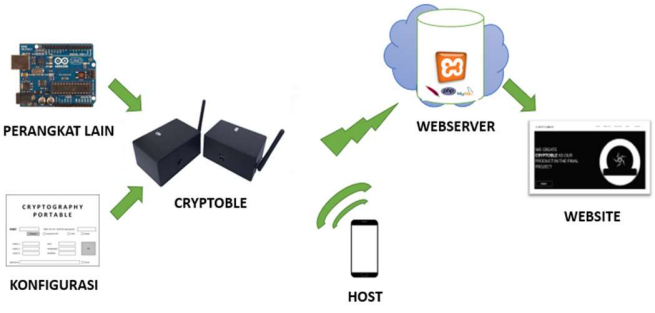
Gambar 6. CRYPTOBLE Configuration

CRYPTOBLE Configuration dibuat dengan spesifikasi yang dicapai, yaitu terdapat fitur konfigurasi perangkat, fitur konfigurasi kata kunci, dan fitur konfigurasi komunikasi nirkabel. Terdapat kolom *SSID* dan *PASSWORD*, sebagai fitur konfigurasi komunikasi nirkabel untuk memasukan data konfigurasi komunikasi nirkabel yang digunakan pada CRYPTOBLE. Setelah konfigurasi dilakukan oleh pengguna maka pengaturan konfigurasi tersebut dikirim melalui komunikasi serial.



Gambar 7. Website sebagai data logger

Kemudian telah dirancang sebuah website yang bertujuan untuk memberikan beberapa informasi mengenai produk CRYPTOBLE khususnya pada *front-end*. Selain itu, pengguna dapat masuk pada halaman *back-end* untuk melihat aktivitas datasensor yang telah terkirim dari pemancar. Untuk masuk ke halaman *back-end* pengguna dapat melakukan klik pada opsi masuk.



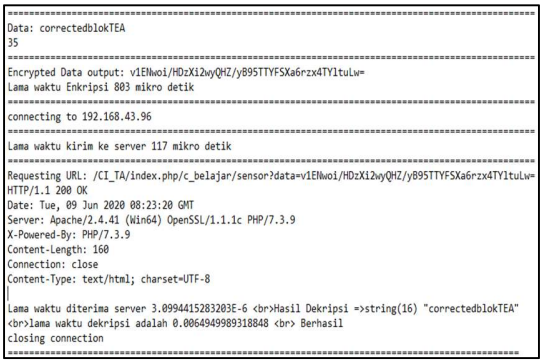
Gambar 8. Diagram Komunikasi Wifi

Diagram dari subsistem komunikasi nirkabel *wifi* yang menerima input berupa *plaintext* dari sensor kemudian data itu dienkripsi pada mikrokontroler sebagai pengolah atau Arduino Nano. Kemudian hasil enkripsi tersebut akan dikirim pada webserver untuk ditampilkan. Data yang telah dienkripsi tersebut tidak akan bisa dilihat oleh orang yang tidak mempunyai kewenangan atau tidak memiliki sandi untuk membuka pesan tersebut. Sebagai penerima yang mempunyai kewenangan untuk menerima pesan tersebut, maka seorang penerima dapat membuka pesan tersebut dengan cara mendekripsi melalui sebuah kunci yang telah ada pada proses enkripsi. Sehubungan dengan algoritma yang dipakai merupakan algoritma yang simetris maka kunci yang bersifat privat pada proses enkripsi maupun dekripsi haruslah sama. Proses dekripsi ini terjadi pada mikrokontroler sebagai pengolah atau Arduino Nano

IV. PENGUJIAN

1. Komunikasi *wifi*

Pengujian perangkat CRYPTOBLE menggunakan komunikasi radio dilakukan di alam ruangan dengan memasang perangkat pemancar dan penerima pada titik berbeda sesuai dengan jarak komunikasi yang ditentukan, yaitu 1 meter dan 4 meter. Pengiriman data berupa teks dilakukan dengan panjang teks dari 2 bytes sampai 16 bytes secara berurut. Pengujian pengiriman data teks ditunjukkan pada Gambar 2.4



Gambar 9. Hasil Pengujian Perangkat Pemancar dan Penerima Webserver

1812	correctedblokTEA
1813	correctedblokTEA
1814	correctedblokTEA
1815	correctedblokTEA
1816	correctedblokTEA
1817	correctedblokTEA
1818	correctedblokTEA
1819	correctedblokTEA
1820	correctedblokTEA
1821	correctedblokTEA
1822	correctedblokTEA
1823	correctedblokTEA
1824	correctedblokTEA
1825	correctedblokTEA
1826	correctedblokTEA

Gambar 10. Penampilan Data Logger pada Website

V. HASIL DAN PEMBAHASAN

A. Pengujian Hasil Enkripsi Jarak 1 Meter

No	Plaintext	Panjang Data (Bytes)	Ciphertext	Waktu Enkripsi (µs)	Waktu Pengiriman (µs)
1	Hi	2	zzngHuhHjXC0E8bi/jo4qg==	557	115
2	INA	3	Hy2Tarx4PL7K0Sohg5kw9A==	646	128
3	2020	4	AErIEOI80HcvivEHIdA8sA==	647	129
4	ITERA	5	tzY48tUq4qF6AlGs4I4Hlg==	647	115
5	TEKNIK	6	x50fWeNqj5yJD7S/DqMa9Q==	648	115
6	Listrik	7	lUT9CWubeR5Suq9B2lX/gw==	648	115
7	Humidity	8	MDfW73xUqBnHeO2AEfaaSg==	649	115
8	TEKNOLOGI	9	iYoKVB1RUiXUl71wVI3O0A==	657	115
9	datasensor	10	UF3m1J9xUVNHrxcDX2115A==	658	114
10	datasuhu=32	11	jwcC2D3bRKbOle07kLb3Y3vlKJPvE+3cHs7agiFVsvc=	802	115
11	nodemcuesp01	12	wwvYiaFPUsPejfPn1ZN5i8RRK4ffbG1yFD5qmizfgPl=	804	117
12	xampp mysql 1	13	iHClkuniVp1UNxV/KDUkfYYHGyMAnYtG3BuOl/tImdl=	802	121
13	Teknik Elektro	14	5zyqCnN8cz9MMTbO3Sz6VaAUh4/yv52qbqTQDpGGTB8=	804	117
14	lampung selatan	15	7bj1z4Elz4yYLfBsS/YX6iZwV2X0WlSW9eQk4tmWEQc=	804	120
15	correctedblokTEA	16	v1ENwoi/HDzXi2wyQHZ/yB95TTYFSXa6rzx4TYltuLw=	806	120

Gambar 11. *Hasil Enkripsi Pengujian Komunikasi Wifi pada Cryptoble Jarak 1m.*

Berdasarkan hasil pengujian pada table 11 diatas mengenai hasil dekripsi pada jarak 1m, didapati bahwa data berhasil dikirim dengan baudrate sebesar 115200 bps. Hasil menunjukkan bahwa data berhasil dienkripsi dari plaintext menjadi ciphertext. Selain itu waktu enkripsi menunjukkan semakin besar bytes suatu plaintext yang dipakai untuk proses enkripsi maka semakin besar waktu yang dibutuhkan.

B. Pengujian Hasil Dekripsi Jarak 1 Meter

No	CipherText	Panjang Data (Bytes)	Baudrate (115200)	Waktu Dekripsi (µs)	Waktu diterima webserver (µs)
1	zzngHuhHjXC0E8bi/jo4qg==	2	Hi	0.007655143737791	28610229,49
2	Hy2Tarx4PL7K0Sohg5kw9A==	3	INA	0.007071018218994	28610229,49
3	AErIEOI80HcvivEHIdA8sA==	4	2020	0.006965160369873	30994415,28
4	tzY48tUq4qF6AlGs4I4Hlg==	5	ITERA	0.006515979676684	30994415,28
5	x50fWeNqj5yJD7S/DqMa9Q==	6	TEKNIK	0.006784915924072	30994415,28
6	lUT9CWubeR5Suq9B2lX/gw==	7	Listrik	0.006763935089113	40531158,45
7	MDfW73xUqBnHeO2AEfaaSg==	8	Humidity	0.006666898727417	28610229,49
8	iYoKVB1RUiXUl71wVI3O0A==	9	TEKNOLOGI	0.007148981094360	28610229,49
9	UF3m1J9xUVNHrxcDX2115A==	10	datasensor	0.007776021957397	30994415,28
10	jwcC2D3bRKbOle07kLb3Y3vlKJPvE+3cHs7agiFVsvc=	11	datasuhu=32	0.007506132125854	30994415,28
11	wwvYiaFPUsPejfPn1ZN5i8RRK4ffbG1yFD5qmizfgPl=	12	nodemcuesp01	0.007674932479858	40531158,45
12	iHClkuniVp1UNxV/KDUkfYYHGyMAnYtG3BuOl/tImdl=	13	xampp mysql 1	0.007728150787354	28610229,49
13	5zyqCnN8cz9MMTbO3Sz6VaAUh4/yv52qbqTQDpGGTB8=	14	Teknik Elektro	0.007956981658935	40531158,45
14	7bj1z4Elz4yYLfBsS/YX6iZwV2X0WlSW9eQk4tmWEQc=	15	lampung selatan	0.007756948470169	21457672,12
15	v1ENwoi/HDzXi2wyQHZ/yB95TTYFSXa6rzx4TYltuLw=	16	correctedblokTEA	0.006354808807373	28610229,49

Gambar 12. *Hasil Dekripsi Pengujian Komunikasi Wifi pada Cryptoble Jarak 1m*

Berdasarkan hasil pengujian pada table 12 diatas mengenai hasil dekripsi pada jarak 1m, didapati bahwa data berhasil dikirim dengan baudrate sebesar 115200 bps. Hasil menunjukkan bahwa data berhasil dienkripsi dari plaintext menjadi ciphertext. Selain itu waktu enkripsi menunjukkan semakin besar bytes suatu plaintext yang dipakai untuk proses enkripsi maka semakin besar waktu yang dibutuhkan.

C. Pengujian Hasil Enkripsi Jarak 4 Meter

No	Plaintext	Panjang Data (Bytes)	Ciphertext	Waktu Enkripsi (µs)	Waktu Pengiriman (µs)
1	Hi	2	zzngHuhHjXC0E8bi/jo4qg==	557	115
2	INA	3	Hy2Tarx4PL7K0Sohg5kw9A==	646	128
3	2020	4	AErIEOI80HcvivEHIdA8sA==	647	129
4	ITERA	5	tzY48tUq4qF6AlGs4I4Hlg==	647	115
5	TEKNIK	6	x50fWeNqj5yJD7S/DqMa9Q==	648	115
6	Listrik	7	lUT9CWubeR5Suq9B2lX/gw==	648	115
7	Humidity	8	MDfW73xUqBnHeO2AEfaaSg==	649	115
8	TEKNOLOGI	9	iYoKVB1RUiXUl71wVI3O0A==	657	115
9	datasensor	10	UF3m1J9xUVNHrxcDX2115A==	658	114
10	datasuhu=32	11	jwcC2D3bRKbOle07kLb3Y3vlKJPvE+3cHs7agiFVsvc=	802	115
11	nodemcuesp01	12	wwvYiaFPUsPejfPn1ZN5i8RRK4ffbG1yFD5qmizfgPl=	804	117
12	xampp mysql 1	13	iHClkuniVp1UNxV/KDUkfYYHGyMAnYtG3BuOl/tImdl=	802	121
13	Teknik Elektro	14	5zyqCnN8cz9MMTbO3Sz6VaAUh4/yv52qbqTQDpGGTB8=	804	117
14	lampung selatan	15	7bj1z4Elz4yYLfBsS/YX6iZwV2X0WlSW9eQk4tmWEQc=	804	120
15	correctedblokTEA	16	v1ENwoi/HDzXi2wyQHZ/yB95TTYFSXa6rzx4TYltuLw=	806	120

Gambar 13. Hasil Enkripsi Pengujian Komunikasi Wifi pada Cryptoble Jarak 4m

Berdasarkan hasil pengujian pada table 2.8 diatas mengenai hasil dekripsi pada jarak 4m, didapati bahwa data berhasil dikirim dengan baudrate sebesar 115200 bps. Hasil menunjukkan bahwa data berhasil dienkripsi dari plaintext menjadi ciphertext. Selain itu waktu enkripsi menunjukkan semakin besar bytes suatu plaintext yang dipakai untuk proses enkripsi maka semakin besar waktu yang dibutuhkan.

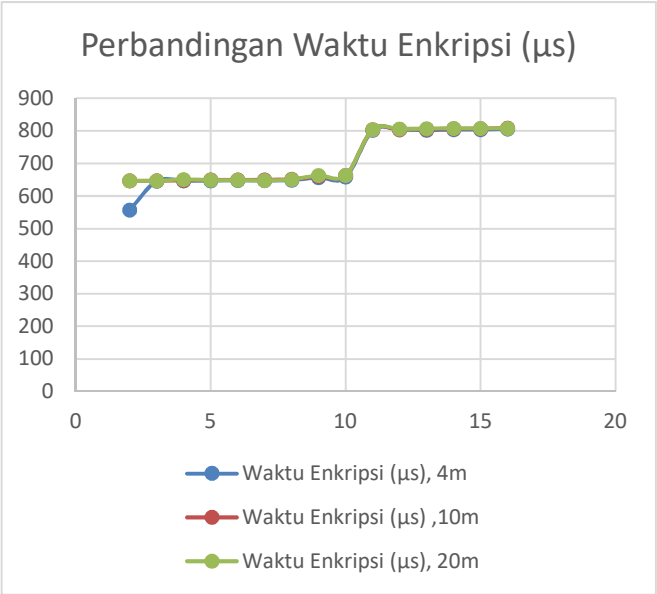
D. Pengujian Hasil Dekripsi Jarak 4 Meter

No	CipherText	Panjang Data (Bytes)	Baudrate (115200)	Waktu Dekripsi (µs)	Waktu diterima webserver (µs)
1	zzngHuhHjXC0E8bi/jo4qg==	2	Hi	0.008695143737792	29261024,49
2	Hy2Tarx4PL7K0Sohg5kw9A==	3	INA	0.008812182189941	29310549,49
3	AErIEOI80HcvivEHIdA8sA==	4	2020	0.007965160369884	31974715,28
4	tzY48tUq4qF6AlGs4I4Hlg==	5	ITERA	0.009515979676842	32984416,28
5	x50fWeNqj5yJD7S/DqMa9Q==	6	TEKNIK	0.007784915994082	32984425,28
6	lUT9CWubeR5Suq9B2lX/gw==	7	Listrik	0.007763935091433	40536159,48
7	MDfW73xUqBnHeO2AEfaaSg==	8	Humidity	0.008666898727488	29610235,49
8	iYoKVB1RUiXUl71wVI3O0A==	9	TEKNOLOGI	0.007155981094363	30610245,42
9	UF3m1J9xUVNHrxcDX2115A==	10	datasensor	0.008776551957398	31294415,28
10	jwcC2D3bRKbOle07kLb3Y3vlKJPvE+3cHs7agiFVsvc=	11	datasuhu=32	0.007901322278545	32394415,27
11	wwvYiaFPUsPejfPn1ZN5i8RRK4ffbG1yFD5qmizfgPl=	12	nodemcuesp01	0.008674932479859	46731158,45
12	iHClkuniVp1UNxV/KDUkfYYHGyMAnYtG3BuOl/tImdl=	13	xampp mysql 1	0.008128815078721	29210229,49
13	5zyqCnN8cz9MMTbO3Sz6VaAUh4/yv52qbqTQDpGGTB8=	14	Teknik Elektro	0.008956981658936	46731158,45
14	7bj1z4Elz4yYLfBsS/YX6iZwV2X0WlSW9eQk4tmWEQc=	15	lampung selatan	0.008756948470678	22657672,19
15	v1ENwoi/HDzXi2wyQHZ/yB95TTYFSXa6rzx4TYltuLw=	16	correctedblokTEA	0.007354868807384	28656229,52

Gambar 14. Hasil Dekripsi Pengujian Komunikasi Wifi pada Cryptoble Jarak 4m

Berdasarkan hasil pengujian pada table 2.9 diatas mengenai hasil dekripsi pada jarak 4m, didapati bahwa data berhasil diterima dengan baudrate sebesar 115200 bps. Hasil menunjukkan bahwa data tidak ada yang berubah atau sama dengan pesan aslinya atau plaintext sehingga bisa dikatakan bahwa pengujian ini berhasil didekripsi dari ciphertext menjadi plaintext. Selain itu , waktu dekripsi menunjukkan semakin besar bytes suatu ciphertext yang dibutuhkan untuk proses dekripsi maka waktu akan semakin lama untuk menjadi hasil plaintext atau pesan asli.

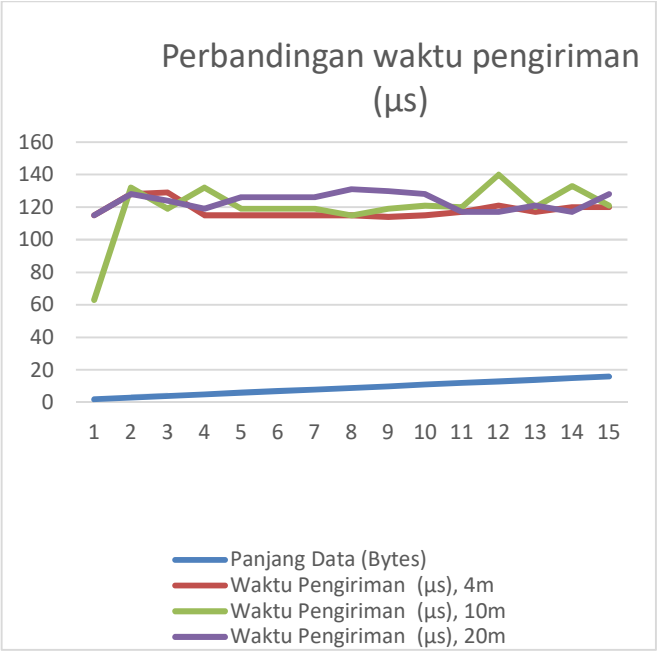
E. Hasil Perbandingan



Gambar 15. Grafik Hasil Perbandingan Waktu Enkripsi

Hasil Analisa pada grafik perbandingan waktu enkripsi diatas menunjukkan bahwa pada data 2 bytes menghasilkan waktu 557 µs pada jarak 4m, 3-10 bytes menghasilkan waktu pengiriman berkisar 600 µs, kenudian terjadi lonjakan pada pengiriman data 11-16 bytes berkisar 800 µs. Kenaikan lama waktu pengiriman ini juga terjadi pada data dengan jarak 10m dan 20m. Adapun data yang terdegradasi yaitu pada data 12 ke 13 bytes penurunan dengan waktu 804-802 µs.

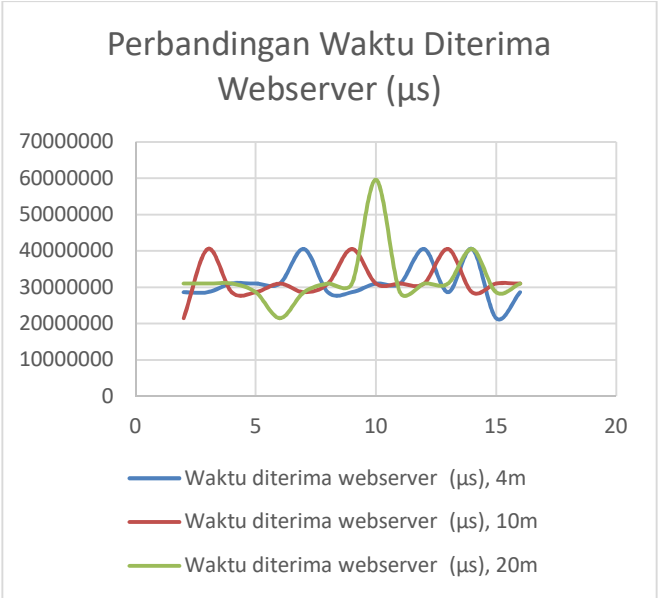
F. Hasil Perbandingan



Gambar 16. Grafik Hasil Perbandingan Waktu Pengiriman

Berdasarkan grafik pada gambar diatas menunjukkan bahwa ketidakteraturan bentuk kurva dikarenakan seringkali terjadi degradasi atau penurunan dan kenaikan yang signifikan waktu pengiriman seperti pada data 11, 12 ke 13 bytes yaitu terjadi penurunan 121 µs ke 120 µs dan naik menjadi 140 µs pada jarak 10 meter. Akan tertapi rata- rata waktu menunjukkan kenaikan yaitu pada jarak 4m total waktu pengiriman rata-rata sebesar 118.067 µs, 119.467 µs pada jarak 10m, 123.533 µs pada jarak 20m.

G. Hasil Perbandingan



Gambar 17. Grafik Hasil perbandingan Data yang diterima pada Weberver

Berdasarkan gambar grafik diatas menunjukkan bahwa ketidakteraturan waktu penerimaan data pada webserver, namun setelah di hitung nilai rata-rata lama waktu pengirimannya untuk setiap jarak 4 meter, 10 meter, dan 20 meter, masing-masing 31.3 ps, 31.6 ps, dan 32,.2 ps. Jadi semakin jauh jarak yang digunakan untuk mengirimkan data dari pemancar ke server waktu yang dibutuhkan untuk penerimaan pada webserver pun semakin meningkat.

VI. KESIMPULAN

Pada pengujian CRYPTOBLE pada jarak 4 meter, 10 meter maupun 20 meter, hasil enkripsi pada baudrate 115200 dapat mengirimkan pesan berupa ciphertext pada webserver dengan waktu pengiriman yang dipengaruhi oleh besar suatu data akan tetapi dipengaruhi oleh jarak. Akan tertapi, besar suatu data plaintext akan mempengaruhi lama waktu yang dibuthkan pada proses enkripsi. Lama waktu yang dibutukan pada proses enkripsi berkisar ratusan mikro detik.

Pada pengujian CRYPTOBLE baik pada jarak 4, 10 meter maupun 20 meter, hasil dekripsi pada baudrate 115200 dapat menerima pesan berupa ciphertext dari perangkat pemancar

(encryptor) dengan waktu penerimaan yang dipengaruhi oleh besar suatu data ciphertext dan jarak. Akan tertapi, besar suatu data ciphertext akan mempengaruhi lama waktu yang dibutuhkan pada proses dekripsi.

Semakin jauh suatu jarak yang digunakan untuk mengirimakan data dari perangkat pemancar dan server penerima, maka akan semakin besar total rata-rata waktu yang dibutuhkan.

REFERENSI

[1] S. C. Umam and B. Sumanto, "PERANGKAT SISTEM TELEMETRI PENGUKURAN SUHU MENGGUNAKAN RF MODUL XBEE ZIGBEE BERBASIS MIKROKONTROLLER ATMEGA 8535," *ELEKTRONIKA DAN INSTRUMENTASI,* 2013.

[2] C. I. jonathan patrick, "cnnindonesia.com," cnn, 31 10 2019. [Online]. Available: cnnindonesia.com/teknologi/20191031115151-185-444432/serangan-ke-iot-meningkat-sembilan-kali-lipat. [Accessed 05 06 2020].

[3] D. I. Af'idah, A. F. Rohim and E. D. Widianto, "Perancangan Jaringan Sensor Nirkabel (JSN) untuk Memantau Suhu dan Kelembapan Menggunakan nRF24L01+," *Jurnal Teknologi dan Sistem Komputer,* vol. II, no. 4, pp. 267-276, 2014.

[4] daon001, "www.kominfo.go.id," kominfo, 39 07 2018. [Online]. Available: kominfo.go.id/content/detail/13656/big-data-dan-iot-harus-perhatikan-isu-keamanan-siber/0/sorotan_media. [Accessed 05 06 2020].

[5] I. Rahmayani, "KOMINFO," 2 OCtober 2015. [Online]. Available: https://kominfo.go.id/content/detail/6095/indonesia-raksasa-teknologi-digital-asia/0/sorotan_media. [Accessed 4 April 2020].

[6] A. Satriadi and Y. Christiyono, “PERANCANGAN HOME AUTOMATION BERBASIS NodeMCU,” vol. 8, no. 1, pp. 64–71, 2019.