IMPLEMENTASI TEKNIK ENKRIPSI TRANSAKSI DATA PERANGKAT IOT

The Implementation of Data Encryption in IoT Device

Hendro FJ Lami[1)], Kalvein Rantelobo[2)], Jani FM Mandala[3)], Agustinus S. Sampeallo[4)]
[1, 2,3,4)] Prodi Teknik Elektro Universitas Nusa Cendana
Jl. A. Sucipto Penfui
[1)]e-mail: h.lami@staf.undana.ac.id

ABSTRAK

Penelitian ini bertujuan mengimplementasi sistem keamanan data antar sensor node menggunakan teknik enkripsi pada perankat IoT. Pada pengujian ini data transaksi dimodelkan dalam dua keadaan tidak terenkripsi dan dalam keadaan terenkripsi. Data tersebut ditransmisikan pada kanal radio menggunakan sistem multiple input single output(*MISO)* dan proses monitoring data transaksi melalui packet sniffing. Berdasarkan hasil pengujian pada level daya minimal perangkat sebesar -72dBm dalam jarak maksimum 60m seluruh data berhasil terkirim dan terenkripsi di sisi penerima.
Kata Kunci: *IoT*, *MISO, esp8266, encrypt, packet, sniffing*.

ABSTRACT

This research aims to stipulate the data encryption of IoT devices. The data transaction models in non-encrypted and encrypted. The data also transmit over a multi-input single-output(MISO) wireless channel and will be analized by a packet sniffing tool. The result shows the encryption of data transactions has successfully delivered to the receiver at a maximum distance of 60m with the receiver sensitivity of esp8266 is -72dBm.

Keywords*: IoT, MISO, esp8266, encrypt, packet, sniffing.*

PENDAHULUAN (Arial 11, Bold, spasi 1,5, spacing before 12 pt, after 6 pt)

Pertanian merupakan salah satu sektor yang menjadi fokus implementasi wireless sensor network(*WSN*). Teknologi tersebut memberikan kontribusi dalam hal sitem monitoring dan kontrol. Beberapa penerapan sistem monitoring dan kontrol WSN dalam sektor pertanian antara lain monitoring dampak pertanian kualitas air (Zia dkk, 2013), monitoring pengaturan distribusi pengairan pada lahan pertanian (Li et al, 2006)(Bouleau et al, 2015), monitoring pertanian lahan kering berbasis multimedia (rantelobo et al,2021)

Selain berfokus pada monitoring data dan kontrol perangkat elektronik, saat ini beberapa riset WSN memberikan kontribusi dalam hal otentikasi data. Beberapa riset mulai mempertimbangkan perangkat IoT pabrikan dengan memiliki keterbatasan memori dan media penyimpanan serta akses konektifitas jaringan. Perkembangan penelitian mengenai otentikasi keamanan data pada perangkat IoT terlihat pada tabel 1. Terlihat pada tabel penggunaan perangkat IoT pabrikan arduino, espressif, serta raspberry pi menjadi pilihan objek perangkat pengujian untuk masing-masing topik.

Tabel 1 Beberapa Penelitian Mengenai Otentikasi dan Keamanan Data Perangkat IoT

No	Topik	Kontribusi	Perangkat IoT	Tahun
1	*Authentication of IoT device and IoT server using secure vaults(Sha et al, 2018)*	Mekanisme Otentikasi Multi Key/ Multi Password	Arduino	2018
2	Design and Implementation of IoT Based Smart Laboratory(Poongothai et al, 2018)	Data Publish-subscribe MQTT	Espressif esp8266 Raspberry pi	2018
3	Investigation of the IoT Device Lifetime with Secure Data Transmission(Kuzminykh et al, 2019)	Efek Kriptografi pada konsumsi daya	Arduino Mega 2560	2019
4	Implementasi Challenge Response Authentication Mechanism (Cram) Untuk Keamanan Transaksi Perangkat Iot(Lami et al, 2021)	Client-Server Otentikasi AES	Esp8266 Esp32	2021

Perangkat esp8266 maupun esp32 pabrikan espressif memiliki kelebihan dibanding arduino yaitu menyediakan fasilitas interkoneksi pada jaringan dalam satu modul yaitu wlan dan bluetooth(A. Kurniawan, 2019). Karakteristik Perangkat wifi esp8266 terlihat pada tabel 2.

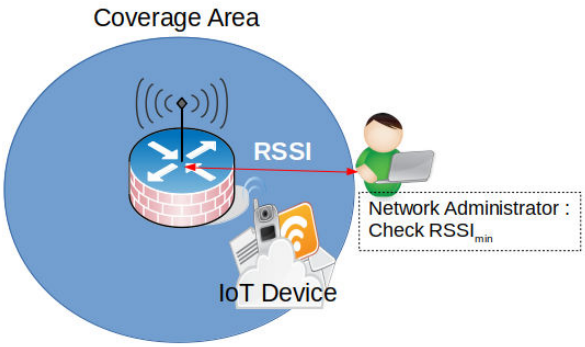
Tabel 2. Parameter Esp8266 (ESP8266EX Datasheet , 2021)

Kategori	Item	Parameter
Wifi	Certification	Wi-Fi Alliance
	Protocols	802.11 b/g/n (HT20)
	Frequency Range	2.4 GHz ~ 2.5 GHz (2400 MHz ~ 2483.5 MHz)
	Channel	1-14
	TX Power	802.11 b: +20 dBm 802.11 g: +17 dBm 802.11 n: +14 dBm
	Rx Sensitivity	802.11 b: –91 dbm (11 Mbps) 802.11 g: –75 dbm (54 Mbps) 802.11 n: –72 dbm (MCS7)
	Antenna	PCB Trace, External, IPEX Connector, Ceramic Chip 2dBi
Software	Software Development	Supports Cloud Server Development / Firmware and SDK for fast on-chip programming

Berdasarkan trend perkembangan penelitian IoT pada tabel 1 dan ketersediaan perangkat pendukung IoT maka pada penelitian ini akan memodelkan implementasi data terenkipsi perangkat IoT multi terminal.

METODOLOGI PENELITIAN

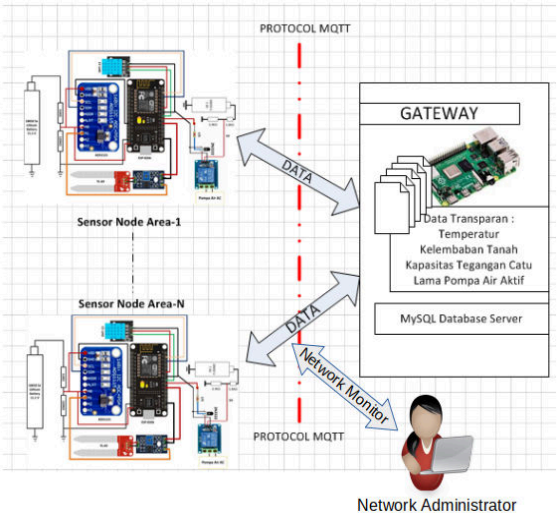
Penelitian ini memiliki memiliki dua fokus penelitian yaitu mendisaian sistem embeded untuk melakukan pengukuruan kualitas sinyal RSSI antara sensor node (gambar 1.) dan mendisain sistem untuk mengamankan data transaksi antara sensor node (gambar 2).



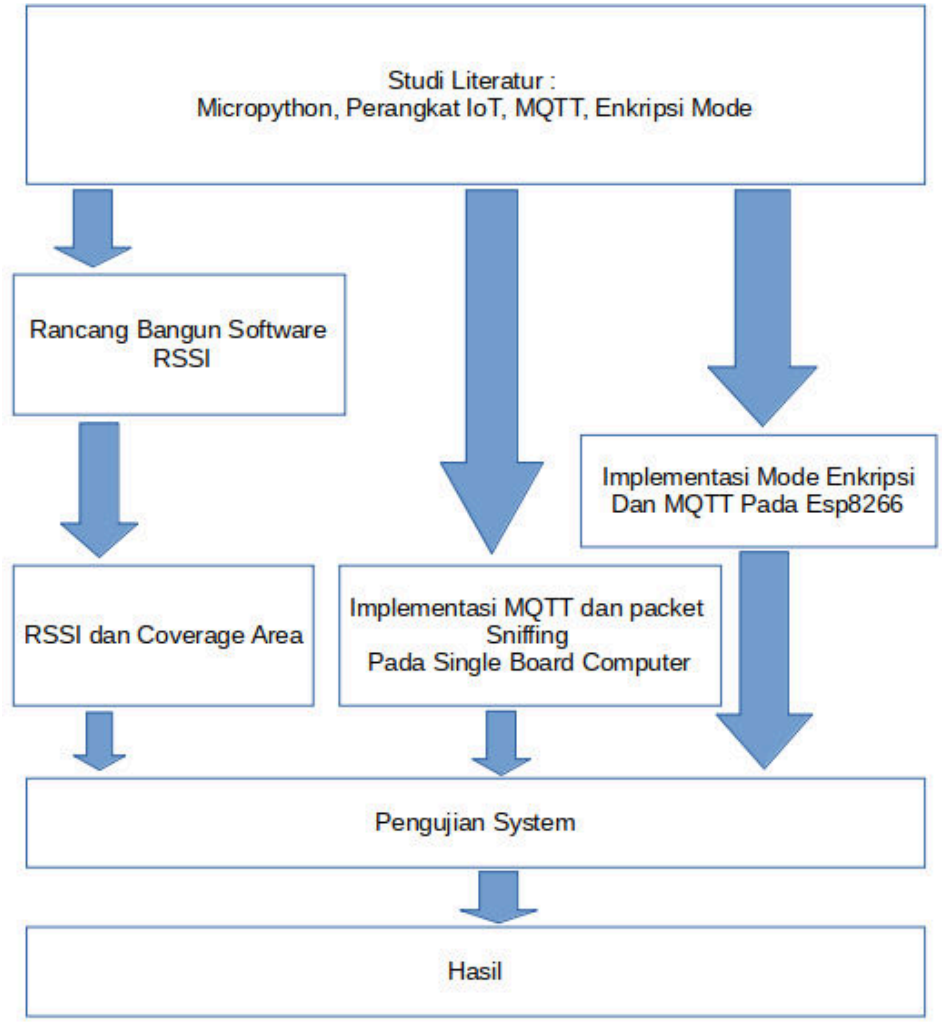
Gambar 1 Jarak maksimum Gateway dan Node Client

Berdasarkan gambar 1 dan 2, sebuah akses point berfungsi untuk menhubungkan antara sensor node esp8266 dan gateway. Akses point memiliki spesifikasi (2x2, MIMO) yang bekerja pada mode 802.11b/g/n dengan sensitifitas penerimaan sebesar -28dBm(Zte.com.cn. 2021). Pada sisi sensor node esp8266 hanya memiliki sebuah antena dengan gain sebesar 2dBi. Oleh karena jumlah antena pada pemancar dan penerima yang berbeda maka model sistem ini merupakan sebuah model multi input single output yang bekerja pada frekuensi 2.4GHz.

Gambar 2 menginformasikan penggunaan MQTT sebagai protokol komunikasi antar sensor node seperti yang dilakukan pada penelitian ke-2 pada tabel 1. Penelitian ini mencoba mengembangkan model transaksi data MQTT terenkripsi dengan menempatkan sebuah single board computer sebagai pusat data aktifitas sensor node. Aktifitas penelitian dapat dilihat pada gambar 3.



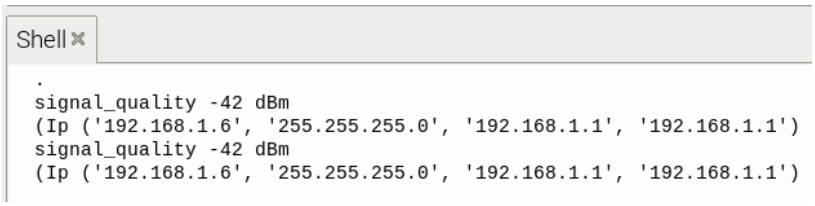
Gambar 2: Model Komunikasi antar Sensor Node



Gambar 3: Alur Penelitian

HASIL DAN PEMBAHASAN

Berdasarkan metodologi penelitian maka penelitian ini diawali dengan mengembangkan sebuah perangkat lunak untuk mengukur kualitas sinyal antara sensor node dan gateway. Skenario pengujian tersebut terlihat pada gambar 2. Jarak referensi pengukuran antar sensor nodes dan akses point adalah 1 m. Gambar 4 merupakan perangkat lunak pada esp8266 sedangkan tabel 3 merupakan hasil pengukuran pada beberapa titik yang terpilih secara acak.



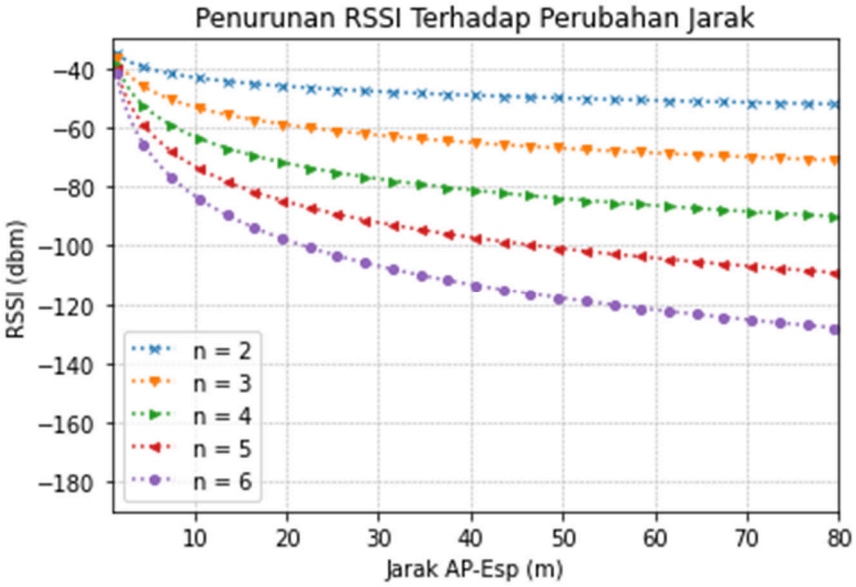
Gambar 4 Tampilan Shell Perangkat Lunak

Tabel 3. Hasil Pengukuran RSSI

Jarak Link Esp-client dan Gateway (m)	RSSI (dBm)
0.6	$-33 \leqslant RSS \leqslant -31$
1	-33
3	$-35 \leqslant RSSI \leqslant -33$
6	$-64 \leqslant RSSI \leqslant -62$
9	$-53 \leqslant RSSI \leqslant -50$
15	$-56 \ll -59$
30	$-64 \leqslant RSSI \leqslant -62$
$Jarak \gg 31$	$RSSI \ll -65$

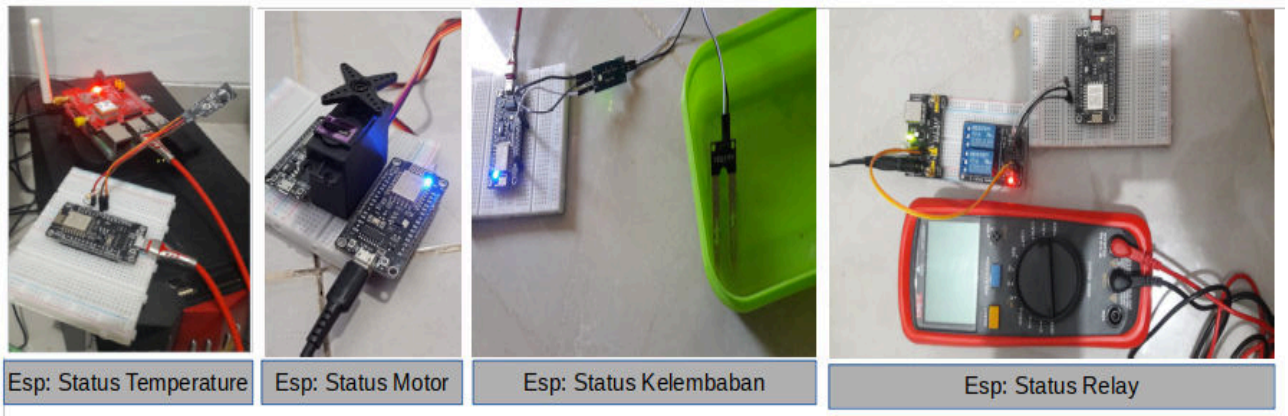
Terlihat pada tabel pada jarak referensi d_0 sebesar 1 m diperoleh hasil pengukuran rssi sebesar 33 dBm. Nilai ini akan dipakai sebagai inputan persamaan untuk mengetahui nilai RSSI dengan beberapa eksponensial rugi lintasan sebesar 2,3,4,5, dan 6. Nilai eksponensian rugi lintasan tersebut sebagai referensi nilai rssi pada propagasi simyal dalam keadaan lingkungan transmisi yang berbeda. Hasil plot sinyal terlihat pada gambar 5 untuk nilai eksponensial rugi lintasan yang berbeda. Menurut tabel datasheet esp8266, komunikasi antara perangkat ini dan gateway dapat berlangsung maksimal pada daerah lahan pertanian dalam jarak hingga 60 meter

(n=2) dengan rssi sebesar -72dbm. Untuk luasan melebihi jarak 60 meter maka dibutuhkan penambahan AP sebagai transceiver agar antara server dan client dapat saling menerima data.



Gambar 5. Dampak Pertambahan Jarak AP-Esp Terhadap RSSI

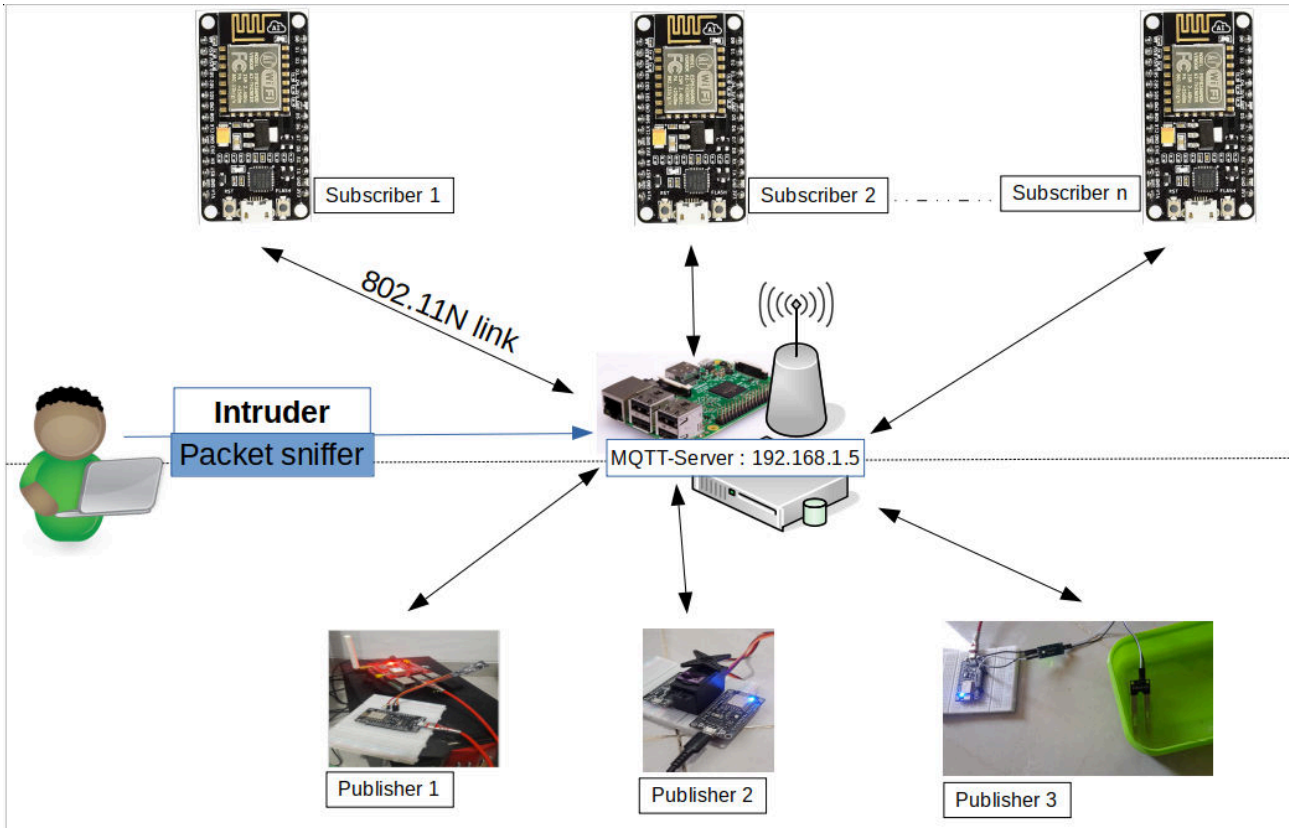
Setelah memodelkan penurunan kualitas sinyal RSSI maka langkah selanjutnya adalah memodelkan enkripsi dan dekripsi data antara esp-client dan gateway. Data yang dikirimkan antara lain data kelembaban, data temperatur, data status motor, dan data status relay.



Gambar 6 Konfigurasi Perangkat IoT

Pengujian mekanisme transaksi data diawali dengan melakukan monitoring data yang dikirim oleh setiap sensor node dalam keadaan tidak terekripsi. Sebuah single board computer bertugas sebagai network administrator untuk melihat dan menganalisis setiap paket data yang melintasi jaringan nirkabel dari model sistem ini. Selain network administrator, terdapat sebuah server yang bertugas sebagai data center tiap hasil penginderaan tiap sensor. Server tersebut merupakan MQTT server yang bertugas mempublikasi data tiap sensor node yang terdaftar pada jaringan.

Terlihat pada gambar 7 sebuah server MQTT dengan IP 192.168.1.5 bertugasi sebagai broker untuk melayani transaksi data antara subscriber dan publisher. Pada kondisi tersebut melalui packet sniffer, intruder berhasil melihat data publisher 1 yang terlihat pada gambar 8 dan 9. Protokol MQTT dan TCP merupakan protokol komunikasi yang digunakan antara publisher 1 dan server. Protokol mqtt mensyaratkan topik dalam melakukan komunikasi sesama client dalam satu broker. Namun skenario pada gambar 10 membuktikan bahwa ketika data transaksi tidak terenkripsi maka intruder pada jaringan dapat mengetahui seluruh data yang ditransmisikan menuju broker dalam hal ini topic maupun message.



Gambar 7. Konfigurasi Multi Client IoT antar Sensor Node dan MQTT-Server

ip.addr==192.168.1.6

No.	Time	Source	Destination	Protocol	Lengtl	Info
4	0.756901885	192.168.1.6	192.168.1.5	MQTT	91	Publish Message [no_encrypt]
5	0.756994717	192.168.1.5	192.168.1.6	TCP	54	1883 → 16706 [ACK] Seq=1 Ack=38 Win=64113 Len=0
40	22.636654101	192.168.1.6	192.168.1.5	MQTT	91	Publish Message [no_encrypt]
41	22.636703434	192.168.1.5	192.168.1.6	TCP	54	1883 → 16706 [ACK] Seq=1 Ack=75 Win=64076 Len=0

Gambar 8. Data Record antar Sensor Node dan MQTT-Server

```
⊞ Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 35
  Topic Length: 10
  Topic: no_encrypt
  Message: Temperatur terukur 25^c
```

Gambar 9. Data Topic dan Message Tidak Terenkripsi

Pengujian delanjutnya adalah mekanisme data terenkripsi antara client dan gateway. Prosesnya terlihat pada gambar 10 dengan protokol komunikasi mqtt dan enkripsi messagenya

adalah advanced encription standard (AES). Plain text pada pengujian ini adalah informasi yang dikirimkan oleh tiap esp-client subscriber dengan topic “notification”. Berikut ini adalah hasil pengujian yang ditampilkan oleh gambar 11 dan 12.

```
Plain Text: b'Motor aktif'
Connection successful
('192.168.1.6', '255.255.255.0', '192.168.1.1', '192.168.1.1')
Connected to 192.168.1.5 MQTT broker, subscribed to b'notification' topic
```

Gambar 10. Informasi Terkirim pada Shell esp-client subscriber

ip.addr==192.168.1.6

No.	Time	Source	Destination	Protocol	Lengtl	Info
19	17.338798706	192.168.1.6	192.168.1.5	MQTT	81	Publish Message [encrypt]
20	17.338898427	192.168.1.5	192.168.1.6	TCP	54	1883 → 2961 [ACK] Seq=1 Ack=28 Win=64133 Len=0
53	37.835105438	192.168.1.6	192.168.1.5	MQTT	81	Publish Message [encrypt]
54	37.835203067	192.168.1.5	192.168.1.6	TCP	54	1883 → 2961 [ACK] Seq=1 Ack=55 Win=64106 Len=0
88	58.563030662	192.168.1.6	192.168.1.5	MQTT	81	Publish Message [encrypt]
89	58.563091662	192.168.1.5	192.168.1.6	TCP	54	1883 → 2961 [ACK] Seq=1 Ack=82 Win=64079 Len=0
94	63.305638039	192.168.1.6	192.168.1.5	TCP	54	2961 → 1883 [FIN, ACK] Seq=82 Ack=1 Win=2135 Len=0
95	63.305803094	192.168.1.5	192.168.1.6	TCP	54	1883 → 2961 [FIN, ACK] Seq=1 Ack=83 Win=64078 Len=0
96	63.314130657	192.168.1.6	192.168.1.5	TCP	54	2961 → 1883 [ACK] Seq=83 Ack=2 Win=2134 Len=0

Gambar 11. Data Record Protokol Komunikasi MQTT Subscriber dan Broker

```
[PDU Size: 27]
MQ Telemetry Transport Protocol, Publish Message
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 25
  Topic Length: 7
  Topic: encrypt
  Message: \360u\bP\017\300\327\364\220\257W\356y\232\b
```

Gambar 12. Data Topic dan Message Terenkripsi

KESIMPULAN

Penelitian ini berhasil menentukan coverage area berdasarkan perubahan RSSI terhadap pertambahan jarak dan sensitivitas penerimaan minimum perangkat esp8266. Pada nilai eksponentsial pathloss sebesar 2 diperoleh jarak jangkauan maksimum antara perangkat esp8266 dan aksespoint sebesar 60m.

Implementasi data terenkripsi antar sensor node IoT berhasil dimodelkan dimana data yang terkirim menggunakan standar AES tidak terbaca sebagai karakter data asli pada sisi intruder. Untuk itu data hanya bisa terbaca pada penerima yang memiliki key yang sama dengan pemancar.

DAFTAR PUSTAKA

Bouleau, C. R., Baracchini, T., Barrenetxea, G., Repetti, A., & Bolay, J. C. (2015). Low-cost wireless sensor networks for dryland irrigation agriculture in Burkina Faso. In *Technologies for Development* (pp. 19-31). Springer, Cham.

“ESP8266EX Datasheet Espressif.com, 2021.” [Online]. Available: https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf. [Accessed: 12 October 2021].

"ESP8266EX Datasheet Espressif.com. 2021." [online] Available at: <https://www.espressif.com/sites/default/files/documentation/esp8266_wi-fi_channel_selection_guidelines_en.pdf> [Accessed 12 October 2021].

Kurniawan, A. (2019). *Internet of Things Projects with ESP32: Build exciting and powerful IoT projects using the all-new Espressif ESP32*. Packt Publishing Ltd.

Kuzminykh, I., Carlsson, A., Yevdokymenko, M., & Sokolov, V. (2019). Investigation of the IoT device lifetime with secure data transmission. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* (pp. 16-27). Springer, Cham.

Lami, H. F., & Pella, S. I. (2021). IMPLEMENTASI CHALLENGE RESPONSE AUTHENTICATION MECHANISM (CRAM) UNTUK KEAMANAN TRANSAKSI PERANGKAT IoT. *Jurnal Media Elektro*, 15-21.

Li, Y., Wang, Z., & Song, Y. (2006, June). Wireless sensor network design for wildfire monitoring. In *2006 6th World Congress on Intelligent Control and Automation* (Vol. 1, pp. 109-113). IEEE.

Poongothai, M., Subramanian, P. M., & Rajeswari, A. (2018, April). Design and implementation of IoT based smart laboratory. In *2018 5th International Conference on Industrial Engineering and Applications (ICIEA)* (pp. 169-173). IEEE.

Rantelobo, K., Lami, H. F. J., Louk, A. C., Bernandus, B., & Olviana, T. (2021, September). Design implementation of wireless multimedia sensor networks for dryland agriculture. In *Journal of Physics: Conference Series* (Vol. 2017, No. 1, p. 012013). IOP Publishing.

Shah, T., & Venkatesan, S. (2018, August). Authentication of IoT device and IoT server using secure vaults. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 819-824). IEEE.

Zia, H., Harris, N. R., Merrett, G. V., Rivers, M., & Coles, N. (2013). The impact of agricultural activities on water quality: A case for collaborative catchment-scale management using integrated wireless sensor networks. *Computers and electronics in agriculture*, *96*, 126-138.

Zte.com.cn. 2021. *ZXHN F660 : N300 Gigabit GPON Gateway - ONT - ZTE Product*. [online] Available at: <https://www.zte.com.cn/global/products/access/Smarthome/ONT/ZXHN-F660> [Accessed 12 October 2021].