e-ISSN 2597-4963 dan p-ISSN 1858-4853

ANALISIS PERBANDINGAN MEKANISME ENKRIPSI DATA PADA TEKNOLOGI LOW POWER WIDE AREA (LPWA) NETWORK : LORA DAN SIGFOX

M. Luqman [1], M. Septama P. [2], Virginia Clara[3] , Trigati WLW [4] , Rusdi Hamidan [5]
[1,2,3,4,5] Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya 60111, Indonesia
E-Mail : : luqman16@mhs.is.its.ac.id [1]; muhamad16@mhs.is.its.ac.id [2]; virginia16@mhs.is.its.ac.id [3]; trigati16@mhs.is.its.ac.id [4]; rusdi16@mhs.is.its.ac.id [5]

ABSTRAK

Komunikasi antar teknologi yang menggunakan Internet of Things (IoT) ini bisa dibagi tergantung dari jarak dari benda/alat yang akan berkomunikasi tersebut. Hingga saat ini kebanyakan bisnis berfokus pada komunikasi yang menggunakan teknologi jarak pendek, seperti WiFi dan Bluetooth. Akan tetapi, kondisi saat ini membutuhkan teknologi untuk komunikasi jarak jauh dan juga munculnya permintaan untuk memonitoring obyek yang tersebar di wilayah yang luas. Obyek tersebut biasanya tidak membutuhkan mengirimkan data yang banyak dan sering digunakan untuk melihat kondisi dari suatu obyek. jaringan tersebut dinamakan Low Power Wide Area (LPWA) Networks. Hal ini juga memiliki resiko keamanan atas data yang dikirim. Pertukaran informasi yang sangat banyak berdampak pada keamanan dan privasi ,hal ini menjadi penting untuk menjamin kerahasiaan informasi yang diberikan. Paper ini bertujuan untuk menyelidiki lebih dalam mengenai keamanan dari sisi enkripsi data pada teknologi LoRa dan SigFox sehingga diharapkan dapat memberikan referensi untuk peneliti selanjutnya dalam melakukan penelitian yang serupa. Hasil dari paper ini adalah dari sisi enkripsi dan autentifikasi data pada kedua teknologi LPWA tersebut, LoRa menjadi lebih efisien dalam penerapan perangkat keras dan perangkat lunak dikarenakan tidak memerlukan perangkat dukungan untuk melakukan enkripsi data sedangkan pada teknologi SigFox mengharuskan adanya dukungan dari perangkat transceiver lain yang kompatibel dan dapat menyediakan standar enkripsi data.

Kata Kunci : autentikasi data, enkripsi, internet of things, keamanan data, lora, low power wide area networks, lora, sigfox

1. PENDAHULUAN

Internet of Things (IoT) merupakan sebuah pandangan dimana internet meluas hingga ke dunia nyata hingga mencapai obyek yang digunakan sehari-hari [1]. Bahkan setiap benda akan tersambung ke dunia maya dan dapat dikendalikan dari jarak jauh dengan menggunakan koneksi internet. Paradigma IoT sendiri bergantung pada jutaan obyek yang memiliki kemampuan untuk mengirimkan informasi tentang keadaan dan lingkungan mereka untuk menciptakan interaksi antara dunia nyata dengan dunia nyata yang aman dan real-time [2].

Komunikasi antar teknologi yang menggunakan IoT ini bisa dibagi tergantung dari jarak dari benda/alat yang akan berkomunikasi tersebut. Hingga sekarang kebanyakan bisnis berfokus pada komunikasi yang menggunakan teknologi jarak pendek, seperti WiFi dan Bluetooth. Teknologi ini bisa diimplementasikan pada barang-barang yang memiliki jarak yang rendah sekitar 10 hingga 100 meter. Implementasi tersebut contohnya seperti Smart Home dan Smart Office, dimana lampu dan AC bisa dikontrol. Akan tetapi sekarang membutuhkan teknologi untuk komunikasi dengan jarak jauh, ditambah lagi dengan munculnya permintaan untuk memonitoring obyek yang bergerak atau obyek yang tersebar di wilayah yang luas. Obyek tersebut biasanya tidak membutuhkan mengirimkan data yang banyak dan sering digunakan untuk melihat kondisi dari suatu obyek. jaringan tersebut dinamakan Low Power Wide Area (LPWA) Networks [3].

Perkembangan ini membuka kesempatan besar dari segi ekonomi suatu negara atau individual. Akan tetapi, hal ini juga berisiko tentang keamanan data yang dikirimkan. Pertukaran informasi yang sangat banyak ini membuat masalah keamanan dan privasi menjadi hal yang harus diperhatikan, karena sifat rahasia dari informasi yang diberikan. Jumlah pelanggaran di tahun 2013 sendiri 62% lebih banyak dari tahun 2012 [4]. Oleh karena itu perhatian lebih diberikan kepada keamanan IoT karena akan mencakup setiap obyek atau perangkat di dalam jaringan tersebut. Obyek sendiri bisa sensor rumah, peralatan medis, mobil, pesawat terbang, bahkan reaktor nuklir, dan hal-hal lain yang bisa menimbulkan risiko bagi kehidupan manusia [5].

Terdapat beberapa teknologi berbeda yang dapat digunakan untuk mengimplementasi LPWA seperti: LoRa, Weightless-N, SigFox, Ingenu dll. Akan tetapi yang akan dibahas pada paper ini adalah teknologi LoRa dan SigFox. Kedua teknologi ini memiliki pengiriman data dan keamanan yang berbeda – beda dan juga terdapat banyak paper yang membahas kelebihan dan kekurangannya baik itu dalam segi teknologi, kemampuan dan cakupan.

Paper ini bertujuan untuk menyelidiki lebih dalam mengenai keamanan dari sisi enkripsi data pada teknologi LoRa dan SigFox sehingga diharapkan dapat memberikan referensi untuk peneliti selanjutnya dalam melakukan penelitian yang serupa.

2. TINJAUAN PUSTAKA

Pada bagian ini akan dijelaskan mengenai teori – teori yang terkait dengan topik yang dibahas yang di paper ini.

A. Internet of Thing

Internet of Things (IoT) dianggap gelombang ketiga teknologi informasi setelah internet dan mobile komunikasi. Konsep IoT resmi diusulkan pada tahun 2005 oleh International Telecommunication Union (ITU). IoT telah menjadi istilah yang mencakup aplikasi baru dan layanan dari wide range yang dibangun pada objek yang dapat berkomputasi dan berkomunikasi. Akibatnya, hal itu menjadi istilah yang memiliki tingkat ketidakjelasan atau tidak dapat didefinisikan dalam hal teknologi tunggal, protokol komunikasi, form factor dan aplikasi atau layanan. Atzori et al. menduga bahwa alasan ketidakjelasan ini karena merupakan konsekuensi dari nama '*Internet of Things*' itu sendiri. Yang pertama mendorong menuju visi yang berorientasi jaringan IoT sedangkan yang kedua fokus pada objek generik untuk diintegrasikan ke dalam framework. Penyebaran IoT dapat memanfaatkan kombinasi protokol komunikasi seperti: *Message Queuing Telemetri Transportasi* (MQTT), *Constrained Application Protocol* (CoAP) dan *Thread* [6].

Perara et al. menguraikan lima karakteristik IoT, yaitu sebagai berikut [6]:

1. *Intelligence*: Transformasi data menjadi pengetahuan.
2. *Architecture*: Event yang heterogen dan infrastuktur berbasis waktu
3. *Complex System*: Sistem granula dari setiap object dengan level yang berbeda sumber
4. *Size Consideration*: Diperkirakan bahwa akan ada 50-100.000.000.000 perangkat yang terhubung ke internet pada tahun 2020
5. *Time Consideration*: Menangani miliaran event yang paralel dan simultan
6. *Space considerations*: Objek dapat digunakan di daerah geografis yang luas
7. *Everything-as-a-service*: Efisien, terukur, aplikasi dan layanan serbaguna

Internet of Thing landscape merupakan broad yang berisi objek – objek dengan kecepatan data dari bps ke Mbps. Rentang kecepatan juga dapat menyebar kurang dari satu meter hingga lebih dari satu kilometer. Komunikasi wireless dapat beroperasi dalam bands yang berlisensi atau tidak berlisensi [7].

B. Organisasi Naskah

Low Power Wide Area (LPWA) *Network* mencakup ruang lingkup wide yang meliputi aplikasi dengan jangka panjang dan daya yang rendah, berarti range melebihi beberapa kilometer dan kecepatan data dari 10bps hingga beberapa kbps. Teknologi jaringan LPWAN digunakan untuk mendukung komunikasi *Machine to Machine* (M2M) dengan tingkat rendah yang menghubungkan antara terminal remote end-point dan server pusat. Kebutuhan utama sistem LPWAN adalah jarak jauh, memperpanjang umur baterai dan biaya end point yang sangat rendah dengan banyak kasus penggunaan yang hanya membutuhkan kecepatan data rendah [7].

Ada dua area utama di mana teknologi LPWA Network adalah yang paling sesuai, yaitu [8]:

1. *Fixed, Medium- To High-Density Connections*.
   Di kota – kota atau bangunan, teknologi LPWAN adalah alternatif yang bagus untuk koneksi seluler M2M. Beberapa contoh termasuk *smart lighting controllers, distribution automation (smart grid),* dan *campusor city-focused GPS asset tracking*.
2. *Long Life, Batterypowered Applications*.
   LPWAN cocok ketika jangkauan jauh lebih dibutuhkan daripada teknologi legacy. Beberapa contoh *termasuk wide-area water metering, gas detectors, smart agriculture* dan *battery-powered door locks & access control points*.

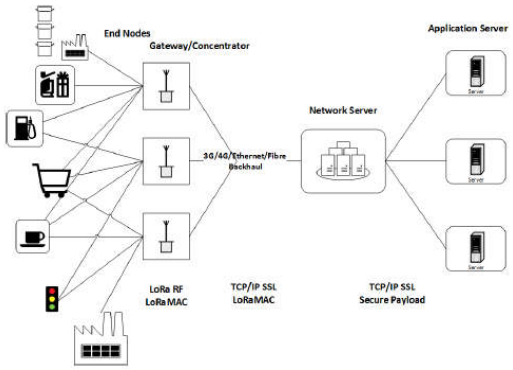
Ada kebutuhan umum yang harus dijadikan panduan untuk merancang jaringan LPWA Network, yaitu sebagai berikut [7]:

1. Transfer data antara objek dan akhir pengguna data harus diamankan sepenuhnya. Jaringan tidak harus bisa mendapatkan akses ke data yang berarti. Sebagai bagian dari keamanan, RF Link juga harus tahan terhadap *jamming*.
2. Dari perspektif aplikasi, objek akan memberikan data yang akan digunakan untuk membangun berbagai macam layanan, baik secara langsung atau melalui proses data fusion and *machine learning*.
3. Tingkat aktivitas dapat bervariasi dari aplikasi ke aplikasi tetapi untuk membatasi konsumsi daya, jaringan seharusnya tidak memerlukan obyek untuk bangkit kecuali ada kebutuhan untuk mengirim atau menerima data.
4. Dalam sebagian besar aplikasi, itu adalah alat penambah yang sangat berguna apabila obyek dapat dengan mudah dilokalisasi dan akan lebih baik tanpa GPS.
5. Obyek umumnya tidak bergerak atau bergerak lambat tapi dapat diposisikan dalam lingkungan yang memiliki karakteristik saluran yang bergerak cepat, seperti berada di samping jalan. Modulasi harus menjadi kuat untuk beberapa kemungkinan pemudaran.

6. Infrastruktur jaringan harus mudah menyebarkan di tingkat nasional dengan cakupan keseluruhan dengan baik dan kemungkinan untuk bergerak ke seluruh negara. Protokol harus menyelaraskan dengan beberapa jenis standar untuk memaksimalkan ketersediaan obyek dan konektivitas tanpa batas. Sebuah downlink yang efisien dipersilahkan untuk memungkinkan manajemen jaringan melalui misalnya *Adaptive Data Rate* (ADR) atau *Transmit Power Control* (TPC).

C. LoRa

LoRa adalah solusi *Low Power Wide-Area* (LPWA) *Network*, menggunakan 868MHz dan 900MHz ISM band dan mampu mengirimkan lebih dari beberapa kilometer dan tergantung pada lingkungan. LoRa adalah solusi *spread spectrum* yang menggunakan *wide bandwidth* untuk membantu melindungi dari gangguan yang disengaja atau kebisingan lingkungan. Protokol jaringan yang digunakan oleh Lora (LoRaWAN), mampu memberikan kecepatan data antara 0.3kbps ke 50Kbps yang bervariasi berdasarkan kebutuhan dan gangguan [9]. LoRa merupakan skema milik Semtech. LoRa mempunyai jenis modulasi *Chirp Spread Spectrum* (CSS) [6].



Gambar 1. LoRaWAN E2E Network Architecture

Perlindungan data yang dikirim melalui jaringan Lora

Setelah Node telah bergabung dengan jaringan Lora, baik melalui OTAA atau ABP, semua pesan akan dienkripsi dan ditandatangani menggunakan kombinasi NwkSKey dan AppSKey. Kunci ini hanya dikenal oleh Jaringan Server dan Node tertentu, seharusnya tidak ada jalan bagi Node lain [9].

Enkripsi pesan dilakukan menggunakan AES128 dalam mode Counter (CTR). Jika FPort diatur ke 0 maka NwkSKey digunakan, jika tidak maka AppSKey digunakan. Sebuah fitur penting dari semua pesan di LoRa adalah bahwa counter untuk mengirim (FCntUp) dan menerima (FCntDown) pesan yang dikelola oleh Node dan Jaringan Server, dan counter ini tidak pernah berulang. Untuk enkripsi dan dekripsi sebuah keystream (S) yaitu sebagai berikut [9]:

```
i = 1..k where
k = ceil(len(FRMPayload) / 16)
Ai = (0x01 | (0x00 * 4) | Dir | DevAddr | FCntUp or FCntDown | 0x00 | i)
Si = aes128_encrypt(K,Ai), for i = 1..k
S = S1|S2|..|Sk
```

Gambar 2. Enkripsi dan Dekripsi Keystream

Keystream termasuk nilai FCntUp atau FCntDown, yang berarti keystream tidak pernah berulang dalam node ini. FRMPayload dan XOR dengan keystream untuk mengenkripsi atau mendekripsi data. Data lain seperti FPort dan FCNTUp dikirim dengan tidak terenkripsi [9].

D. SigFox

SigFox Merupakan salah satu pemimpin dalam LTN (Low Throughput Networks) dan salah satu kontributor utama dalam upaya EFTSI untuk menciptakan standar yang relevan. Pendekatan sigfox merupakan variasi dari jaringan selular yang digunakan oleh ponsel, tapi bukannya menawarkan layanan yang ditargetkan untuk manusia yang membutuhkan bandwith tinggi. Keuntungan dari jaringan selular (jarak jauh, mudah untuk diatur) yang dikombinasikan dengan konsumsi daya yang rendah, dan biaya yang lebih rendah. Transmisi yang digunakan adalah *Ultra Narrow Band* (UNB) dengan setiap sinyal yang dikirim memiliki bandwith 100 Hz [10].

Disisi keamanan sendiri sigfox sebagian besar tertarik pada integritas jaringan. Keamanan payload diserahkan pada sisi pelanggan. Hal ini merupakan tanggung jawab pelanggan untuk menstruktur dan dan mengenkripsi data, SigFox sendiri hanya berfungsi untuk saluran transportasi data ke sistem IT pelanggan. Oleh karena itu keamanan dapat divariasikan tergantung pada implementasi, dan dengan demikian rentan terhadap serangan. Setiap end-point harus didaftarkan online untuk diijinkan menggunakan jaringan. Akan tetapi, faktanya kunci pengaman tetap konstan, bisa menjadi risiko keamanan [10].

Gambar 3. SigFox Security

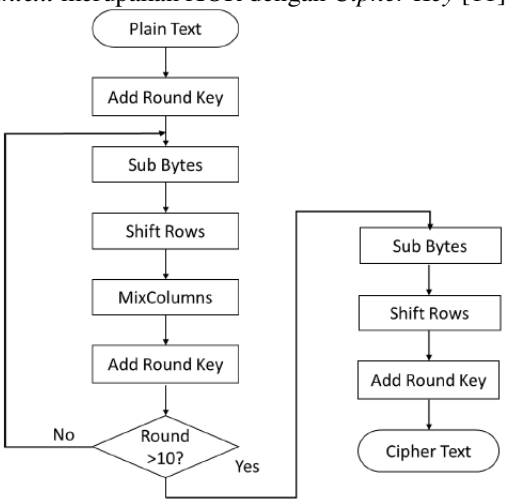
E. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah sebuah spesifikasi untuk enkripsi data elektronik yang ditetapkan oleh National Institute of standards

and Technology (NIST) pada tahun 2001 sebagai *Federal Information Processing Standards* (FIPS) 197. Merupakan algoritma block cipher simetrik yang beroperasi di blok 128-bit, yang digunakan untuk enkripsi dan dekripsi data elektronik. Ukuran kunci yang digunakan untuk enkripsi dan dekripsi AES adalah 128, 192, atau 256 bit, untuk ukuran blok masukan tetap 128 bit.

a. Enkripsi AES-128

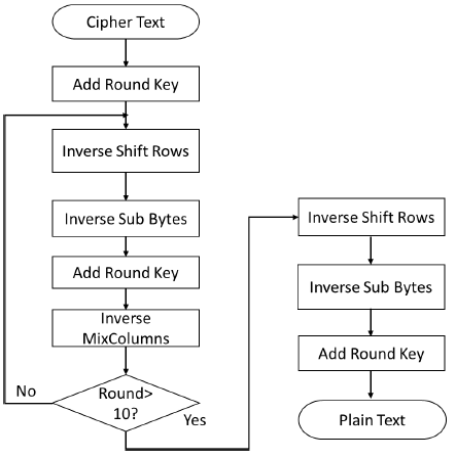
Proses enkripsi AES-128 melibatkan 10 putaran enkripsi bersama dengan putaran awal untuk enkripsi data 128 bit. Untuk memulai, kunci 128-bit diperluas menjadi satu set sebelas putaran kunci 128-bit menggunakan ekspansi rutin kunci. Masing-masing kunci ini digunakan untuk putaran, menghasilkan output *ciphertext*. Putaran awal di enkripsi AES terdiri dari AddRoundKey di mana *plaintext* merupakan XOR dengan *Cipher Key* [11].



Gambar 4. Enkripsi AES-128

b. Deskripsi AES-128

Proses dekripsi AES-128 melibatkan jumlah yang sama putaran seperti proses enkripsi AES-128 sesuai dengan transformasi inverse. Putaran awal hanya mencakup langkah AddRoundKey yang sama seperti pada enkripsi AES-128.



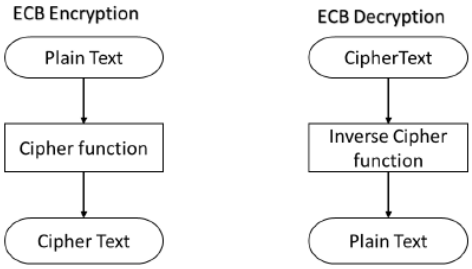
Gambar 5. Dekripsi AES-128

c. Mode Operasi AES yang Ditetapkan Dalam FIPS

Operasi AES mempunyai 5 macam mode, yaitu sebagai berikut [11]:

1. *Electronic Codebook mode* (ECB)

Dalam mode ini, input dibagi dalam blok terpisah dari 128 bit. Setiap blok dienkripsi/didekripsi secara independen. Dalam enkripsi ECB, fungsi cipher langsung diterapkan untuk setiap blok input menghasilkan ciphertext. Dalam dekripsi ECB, fungsi *forward cipher* diterapkan untuk setiap blok untuk mengambil plaintext.

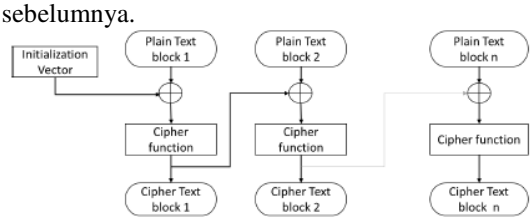


Gambar 6. Enkripsi & Dekripsi ECB

2. *Cipher Block Chaining mode* (CBC)

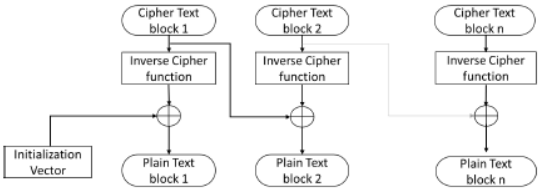
Sesuai namanya, mode ini memiliki chaining dari plain text dengan blok cipher text sebelumnya. Mode ini membutuhkan Initialization Vector (IV) untuk menggabungkan dengan blok pertama. IV tidak rahasia tetapi harus tak terduga.

Di enkripsi CBC, blok pertama dari plain text adalah XOR dengan IV. Ini membentuk blok input untuk fungsi cipher yang menghasilkan blok *ciphertext* pertama. Cipher text ini, XOR dan *plaintext* berikutnya akan membentuk *ciphertext* kedua. Blok *ciphertext* terbentuk dengan menerapkan *forward cipher* setelah XOR dengan masing-masing blok *plaintext* dan *ciphertext* sebelumnya.



Gambar 7. Enkripsi CBC

Pada dekripsi CBC, *forward cipher* diterapkan sebagai input *ciphertext* dan blok output yang dihasilkan adalah XOR dengan IV untuk mendapatkan blok pertama *plaintext*. Blok *ciphertext* yang kedua melewati fungsi cipher terbalik dan hasil dari blok *output* adalah XOR dengan blok *ciphertext* sebelumnya untuk mendapatkan blok *plaintext* kedua. Selanjutnya blok *plaintext* yang diambil dengan menerapkan *forward cipher* atas blok *ciphertext* masing-masing dan kemudian XOR blok *output* yang dihasilkan dengan blok *ciphertext* sebelumnya.

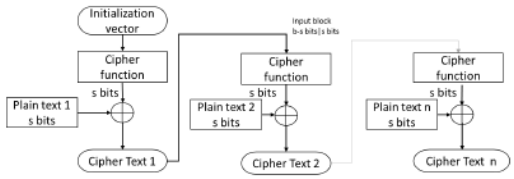


Gambar 8. Dekripsi CBC

F. Cipher Feedback mode (CFB)

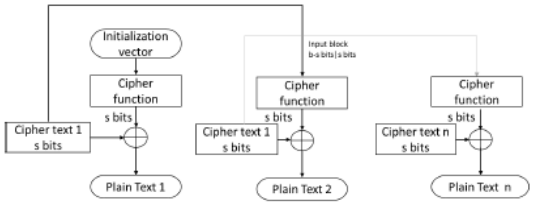
Mode CFB memiliki *feedback* dari elemen *ciphertext* berturut-turut kedalam blok input dari fungsi *forward cipher* untuk menghasilkan blok output, yaitu XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Mode ini membutuhkan IV yang unik selain *plaintext* dan *cipher key*. Mode CFB juga perlu parameter integer s, di mana s harus kurang dari atau sama dengan 128 bit. Dalam mode CFB, setiap blok *plaintext* dan *ciphertext* mengandung s bit.

Untuk enkripsi CFB, IV dilewatkan sebagai blok input pertama ke AES *ciphertext* yang berfungsi untuk menghasilkan blok *output* pertama. Untuk menghasilkan output *ciphertext*, s bit pertama dalam *plaintext* adalah XOR dengan s bit pertama dalam blok output. b-s bit yang tersisa di blok output dibuang (b = 128). Untuk menghasilkan blok *input* kedua, LSB b-s di IV bergabung dengan s bit dari output *ciphertext* dari blok pertama. Proses ini diulang dengan blok input berturut-turut sampai seluruh *plaintext* diubah menjadi output *ciphertext*.



Gambar .9 Enkripsi CFB

Pada dekripsi CFB, IV jika diberikan sebagai blok *input* pertama, dan blok *input* berikutnya dihasilkan dari menggabungkan bit b-s dari IV dengan s bit dari *ciphertext.* Blok *input* diterapkan untuk fungsi *forward cipher* untuk mendapatkan blok *output.* Kemudian s bit *ciphertext* adalah XOR dengan s bit *ciphertext.*

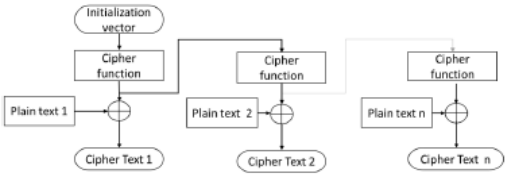


Gambar 10. Dekripsi CFB

G. Output Feedback mode (OFB)

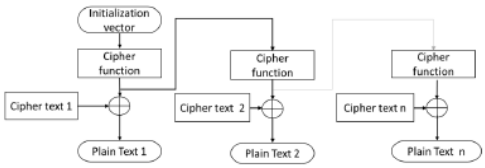
Mode OFB memiliki *feedback* dari blok *output* dari fungsi *forward cipher* di setiap blok ke blok input dari fungsi *forward cipher* dari blok berturut-turut. Mode OFB mengharuskan IV adalah sebuah *nonce*, yang berarti IV harus unik untuk setiap eksekusi dari mode dengan kunci yang diberikan.

Untuk enkripsi OFB, seperti dalam mode CFB, IV diberikan sebagai blok *input* pertama. Ini diterapkan untuk fungsi *forward cipher* untuk menghasilkan blok *output* pertama. Blok output XOR dengan *plaintext* untuk menghasilkan blok pertama output *ciphertext*. Blok *output* pertama kemudian diberikan kepada fungsi *forward cipher* untuk menghasilkan blok *output* kedua, kemudian XOR dengan *plaintext* untuk menghasilkan *ciphertext* blok kedua. Blok *output* kedua kemudian diterapkan pada fungsi *forward cipher* untuk menghasilkan blok *output* ketiga dan seterusnya



Gambar 11. Enkripsi OFB

Dalam dekripsi OFB, IV diberikan sebagai blok input pertama ke fungsi *forward cipher* untuk menghasilkan blok *output* pertama. Blok output pertama adalah XOR dengan *ciphertext* untuk menghasilkan blok *plaintext* pertama. Blok output pertama diberikan kepada fungsi *forward cipher* untuk menghasilkan blok *output* kedua, kemudian XOR dengan *ciphertext* menghasilkan blok kedua dalam *plaintext* dan seterusnya.

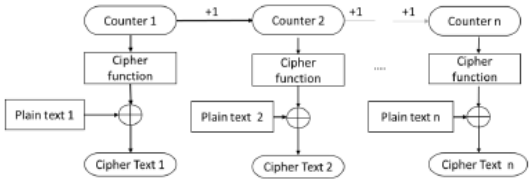


Gambar 12. Dekripsi OFB

H. Counter mode (CTR)

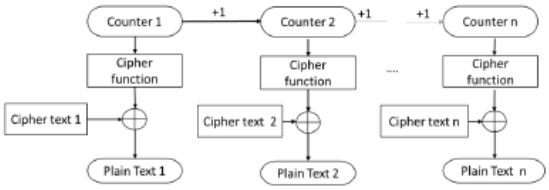
Mode Counter (CTR) adalah mode kerahasiaan yang menampilkan penerapan *forward cipher* untuk satu set blok *input*, yang disebut *counter*, untuk menghasilkan urutan blok output yang eksklusif-ORed dengan *plaintext* untuk menghasilkan *ciphertext*, dan *vice versa*. Dalam enkripsi dan dekripsi CTR, fungsi *forward cipher* dapat dilakukan secara paralel. Urutan *counter* harus memiliki properti yang mana setiap blok dalam urutan berbeda dari setiap blok lainnya.

Enkripsi CTR melibatkan penerapan *forward cipher* atas blok data yang disebut counter kemudian XOR dengan *plaintext* untuk menghasilkan *ciphertext*.



Gambar 13. Enkripsi CTR

Untuk dekripsi, *forward cipher* diaplikasikan di atas counter seperti pada enkripsi. Maka *ciphertext* adalah XOR dengan menghasilkan blok output untuk mengambil *plaintext*.



Gambar 14. Deskripsi CTR

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan hasil mekanisme enkrispi dan deskripsi dari 2 teknologi Low Power Wide Area (LPWA) Network yaitu LoRa dan SigFox.

A. Perbandingan Fitur LoRa dan SigFox

Teknologi LoRa dan Sigfox mempunyai banyak fitur yang dapat dibandingkan, akan tetapi pada sub-bab ini akan difokuskan pada fitur – fitur yang terkait dengan security dari 2 teknologi tersebut. Perbandingannya dapat dilihat pada tabel 1.

Tabel 1. Perbandingan Fitur LoRa dan SigFox

LoRa & SigFox	**LoRa**	**SigFox**
Encryption Standard	AES-128	AES-128
Encryption Mode	Counter (CTR)	Not Supported

B. LoRa

Lora menggunakan standard AES 128 dalam melakukan enkripsi data dengan counter mode (CTR). Mekanisme enkripsi data counter mode pada LoRa diawali dengan merubah teks original menjadi plaintext (P) dengan dapat menggunakan standar kode informasi seperti ASCII. Setelah itu dilakukan penentuan key untuk dienkripsikan dengan plaintext. Operasi yang digunakan enkripsi data plaintext dengan key adalah XOR (Exclusive OR) dimana ketentuan yang digunakan adalah sebagai berikut :

- 1 x 1 = 0
- 1 x 0 = 1
- 0 x 1 = 1
- 0 x 0 = 0

Hasil dari operasi XOR antara plaintext dengan key yang digunakan tersebut akan menjadi chipertext (C) block. Untuk melakukan dekripsi, dilakukan operasi XOR antara chipertext (C) dengan key di urutan counter yang dimaksud untuk menjadi plaintext kembali

a. Enkripsi Teknologi LoRa

Untuk enkripsi, misal original teks yang akan dienkripsi adalah kata hai dengan menggunakan standard kode informasi ASCII sehingga hasil plaintextnya adalah sebagai berikut :

- h : 0110 1000
- a : 0110 0001
- i : 0110 1001

Key yang digunakan adalah misal 7 sehingga bernilai 0011 0111 dan counter 0 yang akan dienkripsi adalah huruf h dengan mekanisme operasi XOR seperti berikut :

- Plaintext (P) : 0110 1000
- Key (K) : 0011 0111

---------- XOR

0101 1111

Sehingga didapatkan nilai Chippertext (C) pada counter 0 adalah 0101 1111 yaitu _

Kemudian pada counter 1, nilai dari key yang digunakan akan ditambah 1 (bersifat incremental) dari key yang digunakan counter 0 sebelumnya sehingga menjadi 0011 1000 yaitu 8. Enkripsi pada huruf kedua yaitu huruf a dilakukan mekanisme operasi XOR seperti berikut :

- Plaintext (P) : 0110 0001
- Key (K) : 0011 1000

---------- XOR

0101 1001

Sehingga didapatkan nilai Chippertext (C) pada counter 1 adalah 0101 1001 yaitu Y

Kemudian pada counter 2, nilai dari key yang digunakan akan ditambah 1 (bersifat incremental) dari key yang digunakan counter 1 sebelumnya sehingga menjadi 0011 1001 yaitu 9. Enkripsi pada huruf ketiga yaitu huruf i dilakukan mekanisme operasi XOR seperti berikut :

- Plaintext (P) : 0110 1001
- Key (K) : 0011 1001

---------- XOR

0101 0000

Sehingga didapatkan nilai Chippertext (C) pada counter 2 adalah 0101 0000 yaitu P

Berdasarkan dari hasil enkripsi dengan menggunakan AES 128b counter mode tersebut, maka didapatkan nilai karakter chippertext dari plaintext hai adalah _YP

b. Deskripsi Teknologi LoRa

Untuk Dekripsi, kata Original text yang telah dienkripsi yaitu _YP akan didekripsi melalui key yang sama pada masing-masing counter dengan menggunakan operasi XOR

Pada counter 0, karakter _ yang menjadi chippertext (C) akan diubah ke dalam bentuk standar kode binary ASCII yaitu 0101 1111 dan akan dioperasikan XOR dengan key yang digunakan ketika melakukan enkripsi sebelumnya yaitu 7 dimana standar kode binary pada ASCII nya

adalah 0011 0111 sehingga operasi XOR yang dilakukan sebagai berikut :

- Chippertext (C) : 0101 1111
- Key (K) : 0011 0111

---------- XOR
0110 1000

Sehingga didapatkan nilai plaintext (P) pada counter 0 adalah 0110 1000 yaitu h.

Pada counter 1, karakter Y yang menjadi chippertext (C) akan diubah ke dalam bentuk standar kode binary ASCII yaitu: 0101 1001 dan akan dioperasikan XOR dengan key yang digunakan ketika melakukan enkripsi sebelumnya yaitu 8 dimana standar kode binary pada ASCII nya adalah 0011 1001 sehingga operasi XOR yang dilakukan sebagai berikut :

- Chippertext (C) : 0101 1001
- Key (K) : 0011 1000

---------- XOR
0110 0001

Sehingga didapatkan nilai plaintext (P) pada counter 1 adalah 0110 0001 yaitu a.

Pada counter 2, karakter P yang menjadi chippertext (C) akan diubah ke dalam bentuk standar kode binary ASCII yaitu 0000 1000 dan akan dioperasikan XOR dengan key yang digunakan ketika melakukan enkripsi sebelumnya yaitu 9 dimana standar kode binary pada ASCII nya adalah 0011 1000 sehingga operasi XOR yang dilakukan sebagai berikut :

- Chippertext (C) : 0101 0000
- Key (K) : 0011 1001

---------- XOR
0110 1001

Sehingga didapatkan nilai plaintext (P) pada counter 2 adalah 0110 1001 yaitu i.

Berdasarkan dari hasil dekripsi dengan menggunakan AES 128b counter mode tersebut, maka didapatkan nilai karakter plaintext dari chippertext _YP adalah hai.

Keuntungan yang didapat teknologi LPWA LoRa dalam menggunakan standar enkripsi data menggunakan counter (CTR) mode adalah efisiensi perangkat keras dan perangkat lunak, tingkat keamanan yang sudah dapat dibuktikan serta sederhana untuk diterapkan. Secara garis besar, teknologi LPWA LoRa tidak memerlukan perangkat dukungan dalam melakukan enkripsi data karena pada dasarnya secara default produk LoRa sudah menyediakan dukungan untuk enkripsi data menggunakan standar AES 128 dengan CTR mode.

C. SigFox

Teknologi LPWA SigFox pada dasarnya tidak memiliki dukungan terhadap enkripsi dan autentifikasi data, tetapi SigFox menawarkan kepada pengguna bila ingin melakukan enkripsi dan autentifikasi data dapat menggunakan perangkat sensor transceiver yang support dengan teknologi SigFox seperti produk teknologi transceiver RF Audenis yang menyediakan enkripsi data untuk teknologi SigFox dengan menggunakan standar AES 128 juga.

4. KESIMPULAN

A. Kesimpulan

Berdasarkan dari hasil analisa komparasi yang dilakukan antara teknologi LPWA yaitu LoRa dan SigFox diperoleh bahwa dalam melakukan enkripsi data kedua teknologi LPWA tersebut memiliki perbedaan dimana produk teknologi LoRa pada dasarnya terdapat standar untuk melakukan enkripsi data yaitu menggunakan standar AES 128b melalui mode counter (CTR) sedangkan pada produk teknologi SigFox pada dasarnya tidak terdapat dukungan dalam melakukan enkripsi data. Tetapi SigFox tetap menyediakan kemungkinan bagi penggunanya dalam melakukan enkripsi data dengan menggunakan perangkat transceiver dukungan yang menyediakan standar konfigurasi untuk melakukan enkripsi data pada teknologi SigFox

Oleh karena itu dapat disimpulkan bahwa dari sisi enkripsi dan autentifikasi data pada kedua teknologi LPWA tersebut, LoRa menjadi lebih efisien dalam penerapan perangkat keras dan perangkat lunak dikarenakan tidak memerlukan perangkat dukungan untuk melakukan enkripsi data sedangkan pada teknologi SigFox mengharuskan adanya dukungan dari perangkat transceiver lain yang kompatibel dan dapat menyediakan standar enkripsi data.

B. Saran

Saran untuk penelitian selanjutnya dapat mengenai perbandingan aspek enkripsi yang dilihat dari tingkat keamanan data dan tingkat kerumitan enkripsi dari kedua teknologi LPWA tersebut dengan melalui tahap pengujian.

5. DAFTAR PUSTAKA

[1]. F. Mattern dan C. Floerkemeier, “From the Internet of Computers to the Internet of Things,” 2010.
[2]. J. M. Gorce dan C. Goursaud, “Dedicated Networks for IoT: PHY/MAC state of the art and challenges,” 2015.
[3]. Samsung, “White Paper : Internet of Things Introducing innumerable opportunities,” 2016.
[4]. Symantec, “Internet Security Threat Report,” 2014.
[5]. F. Olivier, G. Carlos dan N. Florent, “New Security Architecture for IoT Network,” 2015.
[6]. K. E. Nolan, W. Guibene dan M. Y. Kelly, “An Evaluation Of Low Power Wide Area Network Technologies For The Internet Of Things,” IEEE, 2016.
[7]. J.-P. Bardyn, T. Melly, O. Seller dan N. Somin, “IoT : The Era of LPWAN is starting now,” IEEE, 2016.

[8]. LinkLabs Inc, A COMPREHENSIVE LOOK AT Low Power, Wide Area Networks For 'Internet of Things', Annapolis: LinkLabs Inc, 2016.
[9]. R. Miller, "MWR Labs Whitepaper. LoRa Security Building a Secure LoRa Solution," MWR InfoSecurity, 2016.
[10]. G. Margelis, R. Piechocki, D. Kaleshi dan P. Thomas, "Low Throughtput Network for IoT: Lesson Learned From Industrial Impelmentation," IEEE, 2015.
[11]. U. Mehboob, Q. Zaib dan C. Usama, "Low Power Wide Area Networks: A Survey. Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. s.l. : Research Gate, 2016.," xFlow Research Inc, Pakistan, 2016.