IMPLEMENTASI MEKANISME *END-TO-END ENCRYPTION* PADA IoT MENGGUNAKAN METODE *RIVEST CIPHER 4* (RC4)

TUGAS AKHIR

OLEH:

STEVANUS CHRISTIVAN PANJAITAN

09011181520030

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

IMPLEMENTASI MEKANISME *END-TO-END ENCRYPTION* PADA IoT MENGGUNAKAN METODE *RIVEST CIPHER 4* (RC4)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memeroleh Gelar Sarjana Komputer

OLEH:

STEVANUS CHRISTIVAN PANJAITAN

09011181520030

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

IMPLEMENTASI MEKANISME *END-TO-END ENCRYPTION* PADA IoT MENGGUNAKAN METODE *RIVEST CIPHER 4* (RC4)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

STEVANUS CHRISTIVAN PANJAITAN

09011181520030

Palembang, Desember 2020

Mengetahui,

Pembimbing Tugas Akhir	**Ketua Jurusan Sistem Komputer**
Ahmad Heryanto, S.Kom., M.T.	**Dr. Ir. H. Sukemi, M.T.**
NIP. 197806172006041002	**NIP. 196612032006041001**

Scanned with CamScanner

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 31 Desember 2020

Tim Penguji:

1. **Ketua : Rahmat Fadli Isnanto, M.Sc.**
2. **Anggota I : Huda Ubaya, M.T.**
3. **Anggota II : Ahmad Heryanto, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

Scanned with CamScanner

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Stevanus Christivan Panjaitan

NIM : 09011181520030

Judul : Implementasi Mekanisme *End-to-End Ecnryption* Pada IoT Menggunakan Metode *Rivest Cipher* 4 (RC4)

Hasil Pengecekan *Software iThenticate/Turnitin* : 5 %

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 06 Januari 2021

METERAI TEMPEL 6000 ENAM RIBU RUPIAH

Stevanus Christivan Panjaitan

NIM. 09011181520030

HALAMAN PERSEMBAHAN

“Serahkanlah Hidupmu Kepada Tuhan dan Percayalah Kepada-Nya, Dan Ia Akan Bertindak; Ia Akan Memunculkan Kebenaranmu Seperti Terang, Dan Hakmu Seperti Siang”

Mazmur 37:5-6

Kupersembahkan khusus untuk keluarga serta sahabatku

Bukan mengenai apa yang kita inginkan, apa yang ingin kita capai, dan juga bukan mengenai apa yang ingin kita tuju

Melainkan, ini semua mengenai apa yang Tuhan inginkan, apa yang ingin Tuhan capai dari kita, dan juga mengenai tujuan apa yang telah Tuhan sediakan buat kita.

Terimakasih untuk kalian yang telah menjadi Mata dalam Hatiku.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa karena berkat karunia dan rahmat-Nya penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "Implementasi Mekanisme *End-to-End Encryption* Pada *Internet of Things* (IoT) Menggunakan Metode *Rivest Cipher* 4 (RC4)*."*

Pada penyusunan tugas akhir ini, tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terimakasih kepada:

1. Tuhan Yesus Kristus, yang telah memberikan berkat dan karunia-Nya sehingga penulisan tugas akhir ini dapat berjalan dengan lancar.
2. Bapak, Mamak, serta abang-abangku yang selalu memberikan semangat dan doa.
3. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Dr. Erwin, S.Si., M.Si. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer.
6. Bapak Ahmad Heryanto,S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir si penulis.
7. Sahabat Karib ku Talking Zero (Alex, Bobi, Habel, Maraden, Okik, Obok, Lawrencius, Tius, Jo, Dwik, Hengki, Indra, Brehan, Renol), Given, Cindy, Apri, Econ, dan Yosafat sebagai penyemangat dan pendoa bagi ku.
8. Teman Hidupku Ade Indriani Siagian yang selalu setia menjadi teman debat, tempat bertukar pikiran dan menjadi sistem penyemangat terbaik disetiap waktu dan kondisi.

1. Jurusan Sistem Komputer Reguler kelas A angkatan 2015 yang tidak dapat saya sebutkan satu persatu.

Penulis juga berterima kasih kepada semua pihak yang terlibat, baik secara langsung ataupun tidak langsung dalam penyelesaian tugas akhir ini. Tentunya dalam pembuatan tugas akhir ini masih terdapat beberapa kekurangan dan kesalahan yang mungkin terjadi. Oleh karena itu, sebagai bahan perbaikan ke depan penulis tentunya mengharapkan koreksi, saran, serta masukan terhadap isi dari tugas akhir ini.

Akhir kata, semoga dengan pembuatan tugas akhir ini akan menjadi tambahan ilmu dan pengembangan wawasan kita terhadap pengolahan citra digital dan dapat menjadi bahan referensi terhadap mahasiswa yang memerlukan.

Indralaya, Oktober 2020

Penulis,

Stevanus Christivan Panjaitan

IMPLEMENTASI MEKANISME *END-TO-END ENCRYPTION* PADA IoT MENGGUNAKAN METODE *RIVEST CIPHER 4* (RC4)

Stevanus Christivan Panjaitan (09011181520030)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: ivanpanjaitan97@gmail.com

ABSTRAK

Judul penelitian ini adalah Implementasi Mekanisme *End-To-End Encryption* Pada IoT Menggunakan Metode *Rivest Cipher* 4 (RC4). Penelitian ini bertujuan untuk mengimplementasikan kriptografi RC4 dalam proses pengamanan pengiriman data pada perangkat IoT. Metode yang digunakan adalah metode *Rivest Cipher* 4. Tahapan penelitian dimulai dengan studi pustaka, perancangan IoT dan topologi, instalasi dan konfigurasi *server*, merangkai dan membuat pengkodean perangkat IoT, melakukan *sniffing*, analisa sementara, implementasi RC4 dan *sniffing* kembali, hingga terakhir analisa akhir dan penarikan kesimpulan. Hasil penelitian menunjukkan bahwa perangkat IoT telah dapat mengirimkan data melalui jaringan *wireless* yang telah dirancnag. Data berhasil tersimpan dalam tabel yang tersedia dan hasil *sniffing* memperlihatkan bahwa data yang dikirimkan tidak lagi terlihat nilainya setelah dienkripsi. Dengan demikian, RC4 berhasil mengantisipasi *Eavesdrop* dengan baik.

Kata Kunci: *End-to-end Encryption*, Perangkat IoT, *Rivest Cipher* 4.

IMPLEMENTATION OF END-TO-END ENCRYPTION MECHANISM ON IoT USING THE RIVEST CIPHER 4 (RC4) METHOD

Stevanus Christivan Panjaitan (09011181520030)

Department of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email: ivanpanjaitan97@gmail.com

ABSTRACT

The title of this research is the Implementation of the End-To-End Encryption Mechanism on IoT Using the Rivest Cipher 4 (RC4) Method. This study aims to implement RC4 cryptography in the process of securing data transmission on IoT devices. The method used is the Rivest Cipher 4 method. The stages of the research begin with literature study, IoT and topology design, server installation and configuration, assembling and coding IoT devices, performing sniffing, temporary analysis, implementing RC4 and sniffing again, until the final analysis and drawing conclusions. The results showed that the IoT device was able to send data via a wireless network that had been designed. The data was successfully stored in the available table and the sniffing results showed that the value of the data sent was no longer visible after encryption Thus, RC4 managed to anticipate the Eavesdrop well.

Keywords: *End-to-end Encryption, IoT Device, Rivest Cipher 4.*

DAFTAR ISI

Halaman

Halaman Judul i

Halaman Pengesahan ii

Halaman Persetujuan iii

Halaman Pernyataan iv

Halaman Persembahan v

Kata Pengantar vi

Abstrak viii

Abstract ix

Daftar Isi x

Daftar Gambar xii

Daftar Tabel xiv

Daftar Lampiran xiv

BAB I PENDAHULUAN

1.1 Latar Belakang 1
1.2 Tujuan 2
1.3 Manfaat 2
1.4 Perumusan Masalah 3
1.5 Batasan Masalah 3
1.6 Metode Penelitian 3
1.7 Sistematika Penulisan 4

BAB II TINJAUAN PUSTAKA

2.1 *Internet of Things*.....6
2.2 Kriptografi 9
2.3 NodeMCU 12
2.4 Arduino IDE 15
2.5 Algoritma RC4 16

BAB III METODE PENELITIAN

3.1 Pendahuluan.....29
3.2 Kerangka Kerja Penelitian.....29
3.3 Perancangan Sistem.....31
3.4 Metode RC4.....36
3.5 Simulasi Pengujian 38

BAB IV HASIL DAN PEMBAHASAN

4.1 Pendahuluan.....39
4.2 Konfigurasi *Application Programming Interface* (API) 39
4.3 Proses Pemanggilan Data ke Server 41
4.4 Proses Upload Program ke NodeMCU.....43
4.5 Respon dari Server Menuju Database.....44
4.6 Proses *Sniffing* Menggunakan *Wireshark*.....45
4.7 Proses Enkripsi Data pada Perangkat 46
4.8 Hasil *Sniffing* Setelah di Enkripsi.....48

BAB V KESIMPULAN

5.1 Kesimpulan.....50

DAFTAR PUSTAKA 51
LAMPIRAN

DAFTAR GAMBAR

Halaman

2.1 NodeMCU 13
2.2 Komponen NodeMCU 14
2.3 Konsep Kerja RC4 17
2.4 Kode Rumus KAS 20
2.5 Iterasi 1 KAS 20
2.6 Iterasi 2 KAS 21
2.7 Iterasi 3 KAS 21
2.8 Iterasi 4 KAS 22
2.9 Rumus PRGA 23
2.10 Iterasi 1 PRGA 23
2.11 Iterasi 2 PRGA 24
2.12 Iterasi 3 PRGA 24
2.13 Iterasi 4 PRGA 25
2.14 Arsitektur Enkripsi RC4 26
2.15 Arsitektur Dekripsi RC4 27
3.1 Kerangka Kerja Penelitian 30
3.2 Perangkat Keras IoT 32
3.3 Perancangan Topologi 33
3.4 Perancangan Device 34
3.5 Flowchart Perancangan Alat 35
3.6 Proses Enkripsi Dengan Metode RC4 37
3.7 Proses Dekripsi Dengan Metode RC4 38
4.1 Proses Konfigurasi Api Menangkap Data dari Perangkat IoT 39
4.2 Kolom Tabel Database yang Digunakan 40
4.3 Proses Pemanggilan Subrutin yang Ada di Library Pada Halaman Sketch 41
4.4 Proses Pembacaan Sensor 42

4.5 Proses Pengiriman Data 42
4.6 Proses Upload Program Ke NodeMCU 43
4.7 Respon Dari Server Data.....44
4.8 Data yang Masuk ke Database 44
4.9 Pengiriman Paket dari IoT Menuju Server.....45
4.10 Data Paket IoT 46
4.11 Proses Sniffing Data Pada Perangkat.....47
4.12 Hasil Sniffing (Dapat terlihat suhu
dan lembap tidak terpublish nilainya).....49

DAFTAR TABEL

Halaman

3.1 Perangkat Keras IoT.....31
3.2 Pin Perancangan Device.....34
3.3 Spesifikasi Software.....36
4.1 Dekripsi Database yang digunakan.....40

DAFTAR LAMPIRAN

Lampiran 1. Surat Keterangan Tugas Akhir

Lampiran 2. Form Revisi Tugas Akhir II

Lampiran 3. Hasil Uji Plagiarisme

BAB I
PENDAHULUAN

1.1 Latar Belakang

Akhir-akhir ini kita perhatikan dan ikuti berita tentang teknologi terbaru seputar *embedded systems*, lebih spesifik lagi teknologi yang sering diaplikasikan untuk pekerjaan sehari-hari. Tren ramalan kedepan, mayoritas perangkat di sekeliling kita akan terhubung ke internet atau biasa disebut dengan *The Internet of Things*."*A Things*" pada *Internet of Things* dapat didefinisikan sebagai subjek misalkan orang dengan monitor implant jantung, hewan peternakan dengan *transponder biochip*, sebuah mobil yang telah dilengkapi *built-in* sensor untuk memperingatkan pengemudi ketika tekanan ban rendah. Sejauh ini, IoT paling erat hubungannya dengan komunikasi *machine-to-machine* (M2M) di bidang manufaktur dan listrik, perminyakan, dan gas. Produk dibangun dengan kemampuan komunikasi M2M yang sering disebut dengan sistem cerdas atau "smart". (contoh: smart label, smart meter, smart grid sensor).[1]

IoT pada dasarnya merupakan perluasan dari internet, sehingga masalah dan tantangan yang dihadapi juga serupa terutama dalam hal privasi dan perlindungan data.[2] Salah satu cara untuk mengambil data adalah pada saat proses transmisi data, dan ini disebut dengan *eavesdropping*. *Eavesdropping* merupakan serangan yang dilakukan dengan cara mendengarkan semua paket-paket yang ditransmisikan oleh user yang berada dalam jaringan komputer yang tidak terenkripsi menggunakan teknik enkripsi apapun.[3]

Pada penelitian [4] penerapan algoritma kriptografi AES-CBC 128 pada komunikasi node sensor ke *middleware* dan mekanisme TLS pada komunikasi middleware dengan aplikasi berbasis IoT. Hasil yang didapat *end-to-end security* berbasis kriptografi pada pub/sub dapat menjamin kerahasiaan data dengan enkripsi *payload* akan tetapi topik masih terlihat, sedangkan TLS/SSL menjamin kerahasiaan seluruh data yang dikirim. Penggunaan mekanisme ini tidak berdampak signifikan pada penundaan pengiriman data, yaitu masih dibawah 1 detik.

Pada penelitian [5] menggunakan algoritma kriptografi Vigenere Chiper. Algoritma ini menggunakan proses enkripsi dan dekripsi untuk menjaga kerahasiaan pesan. Pengamanan data teks dengan menggunakan metode vigenere cipher sangat berguna dalam menjaga keamanan pesan teks dari serangan-serangan yang lain, seperti serangan *eavesdropping*.

Pada umumnya, mayoritas komunikasi jaringan terjadi dalam bentuk *cleartext* atau format yang tidak aman, sehingga mengizinkan *attacker* atau *hacker* yang telah mempunyai akses ke data di dalam jaringan untuk mendengarkan atau membaca lalu lintas jaringan.

Network eavesdropping atau yang juga biasa disebut *network sniffing* merupakan proses memeriksa atau menangkap paket ketika sedang transit diantara *source* dan *destination device* untuk mencari informasi yang sensitif seperti *password*, *session*, atau informasi rahasia lainnya. Kemampuan *eavesdropper* untuk memonitor jaringan merupakan masalah keamanan paling besar yang dihadapi oleh seorang administrator di dalam sebuah perusahaan. Tanpa enkripsi yang kuat, data bisa dibaca oleh orang lain yang melewati jaringan.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Ada berbagai metode kriptografi saat ini, seperti RC4 dan RSA. Dalam Penelitian Akinyele A., menyatakan bahwa RC4 memiliki kelemahan di sisi keamanan kunci, namun memiliki kelebihan di sisi kecepatan, demikian sebaliknya untuk RSA sangat aman, namun prosesnya sangat lamban. [6]

Berdasarkan uraian diatas penulis bermaksud untuk melakukan sebuah penelitian yang bertujuan untuk mengembangkan sebuah pendekatan baru untuk mengamankan komunikasi perangkat IoT dari *eavesdropping* dengan menggunakan algoritma RC4 (*Rivest Chiper* 4).

1.2 Tujuan

Adapun tujuan dari penelitian ini adalah:

Mengimplementasikan Kriptografi RC4 dalam proses pengamanan pengiriman data pada perangkat IoT.

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Mampu membuat sistem pengiriman data yang aman dan dapat menghindari *eavesdropper.*
2. Masalah keamanan pada distribusi kunci dapat ditangani.
3. Algoritma ini dapat digunakan pada sistem secara *real time* misalkan pada saluran telepon karena proses enkripsi dan dekripsinya cepat.

1.4 Perumusan Masalah

Bagaimana implementasi Metode kriptografi RC4 pada pengamanan komunikasi perangkat IoT dengan Server?

1.5 Batasan Masalah

1. Data atau informasi yang dikirim berupa text
2. Metode yang digunakan adalah RC4
3. Perangkat IoT dibuat berbasis NodeMCU
4. Server menggunakan laptop/pc dengan sistem operasi windows
5. Pengujian Eavesdropper menggunakan aplikasi Wireshark atau sejenis.
6. Bahasa pemograman yang digunakan adalah python.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam tugas akhir ini akan melewati beberapa tahapan sebagai berikut:

1. Studi Pustaka/Literatur

   Tahap ini dilakukan dengan cara mempelajari jurnal dan buku tentang algoritma *Kriptografi RC4* sehingga dapat menunjang penulisan laporan tugas akhir ini.

2. Perancangan Sistem

   Tahap ini dilakukan dengan melakukan perancangan dan pembuatan perangkat IoT dan server, kemudian menerapkan kriptografi RC4 didalamnya.

3. Pengujian

   Tahap ini dilakukan dengan cara menyadap paket pengiriman data dari perangkat IoT ke Server dan kemudian juga mengukur waktu proses enkripsi dan dekripsi dari algoritma yang digunakan.

4. Analisis

   Tahap ini dilakukan dengan menganalisis hasil pengujian untuk mengetahui keberhasilan dan kegagalan serta faktor penyebabnya sehingga dapat diperbaiki dan dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Kesimpulan dan Saran

   Tahap ini dilakukan dengan menarik kesimpulan dari analisa dan studi literature serta saran untuk penulis selanjutnya jika akan dijadikan bahan referensi.

1.7 Sistematika Penelitian

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari tiap bab, maka dibuat suatu sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah dan Batasan Masalah kemudian Metodologi Penelitian, dan yang terakhir mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian terkait dengan *Internet of Things*, Kriptografi Algoritma *Rivest Chipper* 4, dan yang berkaitan langsung dengan penelitian.

BAB III. METODE PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISISA

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang penelitian yang dilakukan, serta menjawab setiap tujuan yang hendak dicapai sesuai yang tercantum pada BAB I (Pendahuluan).

DAFTAR PUSTAKA

[1] Yudha Yudhanto, E.2015. IOT (Internet Of Things). IlmuKomputer.com (Google Scholar)

[2] Ernita Dewi Meutia, E2017. Dampak Sosial Internet of Things. ISSN. 2088-9984

[3] Ida Bagus Verry Hendrawan Manuaba Risanuri Hidayat, Sri Suning Kusumawardani, Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada) , JNTETI, Vol. 1, No. 1, Mei 2012.

[4] Deny H. Eko S. Fariz A. Lutfi A. 2019. Implementasi Mekanisme End-to-End Security pada IOT Middleware. Universitas Brawijaya.

[5] Benyamin S. Dina P. Eko A. Indra G. 2020. Pengamanan Pesan Teks Menggunakan Kriptografi Algoritma Vigenere Chiper dari Serangan Eavesdropping. STIKOM Tunas Bangsa Pematangsiantar. Vol. 4, No. 1.

[6] Akinyele A. Okedola, Yekini N. Asafe, — RSA and RC4 Cryptosystem Performance Evaluation Using Image and Text File,2015, ISSN 2229-5518.

[7] Apri Junaidi, E.2015. INTERNET OF THINGS, SEJARAH, TEKNOLOGI DAN PENERAPANNYA: REVIEW ISSN: 2407 - 3911

[8] Ronal W. 2015. Perbandingan Teknik Kriptografi Metode Sapphire II dan RC4. AMIK Labuhanbatu. Vol.3 No.2.