Analisis Performa AES Untuk Sekuriti Jaringan Scada Berbasis ATMega16

Eka Puji Widiyanto[1]
[1]AMIK MDP; Jl. Rajawali No.14, Palembang (0711) 376400, Fax: (0711) 376360
JurusanTeknik Komputer, AMIK MDP, Palembang
e-mail:[1]ekapujiw2002@mdp.ac.id

Abstrak

SCADA sebagai tulang punggung sistem kendali modern telah menjadi bagian tak terpisahkan dari berbagai sektor kehidupan, mulai dari sistem industri, ketenagaan, sampai dengan sektor militer dengan cakupan yang bersifat global. Namun hal ini mengundang kekhawatiran tersendiri disebabkan oleh sifat alami sistem SCADA yaitu bahwa semua sistem SCADA konvensional memiliki celah keamanan yang amat besar karena pada dasarnya keamanan bukan menjadi perhatian utama sebuah sistem SCADA. Untuk mengatasi hal tersebut maka pada penelitian ini akan dikaji penerapan metode keamanan berbasis enkripsi untuk menjamin keamanan transaksi data di dalam sebuah sistem SCADA. Penelitian ini akan menerapkan penggunaan enkripsi dan dekripsi AES 128 bit pada mikroprosesor 8 bit yaitu AVR ATMEGA16 dengan clock 11,0592MHz. Pada sistemnya, AES memerlukan waktu 40μs untuk mengenkripsi 16 byte data dan memerlukan waktu 60μs untuk mendekripsinya kembali. Dengan performa ini maka diharapkan penggunaan AES sebagai metode enkripsi data dapat diterapkan secara menyeluruh sampai ke level terendah dari sistem SCADA yaitu pada level instrumen kendali yang berada di lapangan yang pada akhirnya akan meningkatkan reliabilitas sistem secara global.

***Kata kunci*:** SCADA, AES, Mikroprosesor, Enkripsi, AVR.

Abstract

SCADA as the backbone for modern sontrol system has been unseparated part of human daily life, from industrial system, powerline, to military system with its global and vast scope. SCADA by nature is not safe, and because of that reason there is a big security hole in every SCADA system that threatens its functionality. To overcome this, security concept must be applied to existing SCADA system in the form on data encryption. AES 128 bit is used as the encryption method on an 8 bit microprocessor AVR ATMEGA16 clocked at 11.0592MHz. Based on this chip, AES executed with total time of 40μs to encrypt 16 bytes block of data and require 60μs for decryption. With this performance on an 8 bit chip architecture, using AES as encryption for any field object in SCADA system is very advisable to achieve higher security level.

***Keywords*:** SCADA, AES, Microprocessor, Encryption, AVR.

1. PENDAHULUAN

Supervisory control and data acquisition (SCADA) merupakan suatu sistem jaringan kontrol yang terintegrasi baik secara lokal maupun global. Sistem ini pada umumnya memegang peranan penting dalam pengaturan dan manajemen infrastruktur vital suatu organisasi, misalnya perusahaan, perkantoran, gedung, atau bahkan suatu negara [4][5]. SCADA memberikan informasi waktu nyata yang berkaitan dengan proses produksi, pengendalian sistem dengan metode yang lebih aman, ekonomis, namun lebih handal. Keuntungan ini diperoleh sebagai hasil dari kombinasi sistem perangkat keras dan perangkat lunak dengan kemajuan sistem komunikasi. Namun hal ini tidak diimbangi dengan sistem keamanan yang memadai sehingga membuat sistem SCADA pada umumnya rentan terhadap gangguan keamanan, baik dari dalam maupun luar.SCADA didefinisikan sebagai:

1. Suatu teknologi yang memungkinkan pengguna untuk mengumpulkan data dari satu atau lebih tempat yang jauh dan atau mengirimkan perintah ke tempat tersebut. [1]
2. Suatu sistem operasi dengan sinyal komunikasi yang terkode melalui suatu kanal komunikasi untuk memberikan akses kontrol terhadap suatu RTU (*RemoteTerminalUnit*) [2].

Menurut Krutz [3] dan Stouffer [7], sistem SCADA memiliki elemen-elemen yang didefinisikan sebagai berikut:

1. *Operator*
   Operator manusia yang melakukan pengawasan terhadap sistem SCADA dan pengendalian terhadap sistem kendali yang berada di tempat yang jauh.
2. *Human Machine Interface* (HMI)
   Subsistem yang berfungsi untuk merepresentasikan data kepada operator dalam bentuk yang beragam seperti grafik, skematik, jendela informasi, menu, layar sentuh, dan bentuk lainnya.
3. *Master Terminal Unit* (MTU)
   Subsistem yang bertugas mengumpulkan data dari satu atau lebih fasilitas yang jauh dan menampilkan informasi kepada operator. MTU pada umumnya dipergunakan dalam sistem SCADA berbasis *masterslave*.
4. Sistem Komunikasi
   Merupakan metode komunikasi antara MTU dan RTU.
5. *Remote Terminal Unit* (RTU)
   Subsistem yang berfungsi untuk mengirimkan sinyal ke berbagai peralatan yang berada di lapangan, mengumpulkan data, dan mengirimkannya ke MTU melalui sistem komunikasi yang telah ditentukan.

Penelitian mengenai keamanan pada sistem SCADA telah berkembang seiring dengan perkembangan sistem komunikasi yang semakin pesat utamanya dengan perkembangan internet. SANDIA [11] pada tahun 2002 telah mengembangkan sistem keamanan berbasis kunci terdistribusi untuk SCADA. Metode yang dikembangkan menggunakan sistem yang terpisah antara MTU dan RTU di mana kedua sisi ini memiliki kunci yang terpisah juga. MTU memegang kunci semua RTU yang terkoneksi sedangkan semua RTU memiliki kunci yang sama untuk melakukan proses enkripsi dan dekripsi pesan dari dan ke MTU. Pada tahun 2006 dikembangkan sistem SKMA [12]. Sistem ini mengharuskan MTU dan RTU menggunakan dan menyimpan banyak kunci sejumlah RTU dan MTU yang terkoneksi ke dalam sistemnya. Pada tahun 2008 Choi et al. [13] mengembangkan sistem manajemen kunci untuk SCADA berbasis hierarki. Pada sistemnya maka MTU dan RTU dikonfigurasikan dalam konfigurasi bintang sehingga mengakibatkan antara MTU, SUB-MTU, dan RTU tidak dapat saling berkomunikasi satu sama lain secara langsung. Sistemnya mengharuskan MTU, SUB-MTU, dan RTU menyimpan kunci dengan jumlah lebih banyak daripada skema yang telah dikemukakan sebelumnya. Sistem keamanan untuk SCADA berbasis web menggunakan smartphone [8] juga telah dikemukakan pada tahun 2011. Namun sistem ini hanya meliputi keamanan pada bagian HMI saja, bukan pada komunikasi antara MTU dan RTU. Pada penelitian ini akan dirancang

dan diimplementasikan sistem SCADA residensial berbasis mikroprosesor 8 bit dengan protokol komunikasi yang terenkripsi AES. Cakupan penelitian ini akan difokuskan pada level yang paling rendah dari sistem SCADA yaitu level komunikasi antara MTU dan RTU yang berada di lapangan. Hal ini diambil dari fakta bahwa level inilah yang pada umumnya tidak ada proses keamanan apapun, baik otorisasi maupun enkripsi.

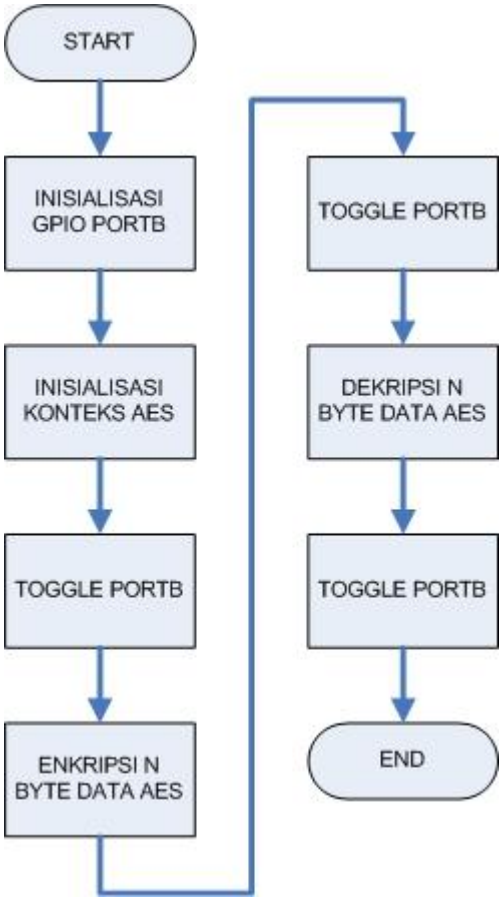
Karena sistem SCADA memegang peranan penting dalam pengendalian objek vital, maka perlu dikembangkan sistem SCADA dengan tingkat keamanan yang tinggi, baik secara perangkat keras, maupun perangkat lunak. Hal ini merupakan suatu spesifikasi yang harus dipenuhi oleh sebuah sistem SCADA konvensional yang umumnya tidak terproteksi dan tidak memiliki sistem *logging* apapun [10]. Selain itu banyaknya kelemahan sistem SCADA konvensional seperti penggunaan *port* standar yang terbuka sebagai *port* perawatan, konfigurasi, dan monitoring, penggunaan satu frekuensi standar dalam sistem komunikasinya, dan tidak adanya sistem otentifikasi dan enkripsi semakin membuat sistemnya mudah sekali untuk diserang. Dalam penelitian ini akan dikembangkan suatu sistem transmisi SCADA dengan memanfaatkan enkripsi data berbasis AES[8]. Sistem SCADA akan diimplementasikan sebagai pengendali peralatan residensial. Kunci untuk sistem ini akan diimplementasikan dalam bentuk perangkat keras berbasis keping silikon dengan panjang kunci sebesar 64 bit. Masing-masing perangkat RTU dalam sistem yang didesain akan memiliki kunci yang berbeda-beda dengan kemungkinan kesamaan yaitu 1 berbanding 2^{64}.

2. METODE PENELITIAN

Dalam melakukan penelitian ini, dipergunakan metode *Prototyping* dengan tahap-tahapan yaitu perencanaan, perancangan, evaluasi desain, pembangunan sistem, pengujian sistem, dan implementasi sistem.

2.1 Perencanaan

Pada tahap ini maka disusun rancangan awal sistem, fitur yang akan dikembangkan, perangkat keras dan lunak yang akan dipergunakan, representasi algoritma AES yang akan diimplementasikan, serta proses evaluasi kinerja sistemnya. Untuk melakukan proses enkripsi dekripsi AES pada sistem yang dirancang, maka dipergunakan flowchart seperti pada Gambar 1. Pada setiap prosesnya maka akan dilakukan proses enkripsi dekripsi n-byte data dengan AES untuk selanjutnya dibandingkan kinerjanya dalam hal waktu komputasi dan validitas datanya.



Gambar 1. *Flowchart* Sistem

2.2 Perancangan

Pada tahap ini penerjemahan dari keperluan atau data yang telah dianalisis ke dalam bentuk yang mudah dimengerti user, prototipe didesain dengan membuat perancangan sementara yang berfokus pada penyajian sistem. Sebagai tahap awal maka disusun simulasi dari sistem yang akan diimplementasikan sehingga didapatkan gambaran awal kelayakan operasional sistemnya, apakah layak diimplementasikan secara riil ataukah tidak dalam sebuah sistem SCADA.

2.3 Evaluasi Desain

Pada tahap ini, dilakukan evaluasi terhadap desain sistemnya. Apakah rancangan sistem yang dibuat sudah sesuai dengan yang diharapkan. Jika tidak, maka desain akan direvisi dengan mengulang langkah sebelumnya.

2.4 Pembangunan Sistem

Dalam penelitian ini dirancang sistem SCADA berukuran kecil dengan mikroprosesor yaitu ATMEGA16 dengan bahasa pemrogramannya yaitu C [6]. Sebagai identifikasinya maka dipergunakan 1-*Wiredevice* yaitu keping silikon DS2401 yang memiliki nomor serial 64 bit yang unik di dalamnya [9]. Guna melindungi datanya maka dipergunakan sistem enkripsi berbasis AES 128 bit dengan kunci yang dibangkitkan dari nomor identifikasinya sendiri yang diduplikasi 2 kali [10]. Sistem ini akan disimulasikan menggunakan ISIS Proteus. Dari simulasi ini akan diukur performa AES 128 bit untuk berbagai ukuran data sehingga dapat diketahui kelayakan AES pada mikroprosesor 8 bit. Enkripsi sebagai jantung dari keamanan datanya tidak boleh menyebabkan terjadinya *overhead* baik dalam komputasi maupun komunikasinya [10].

Penggunaan kunci keamanan juga akan meningkatkan keamanan sistem transmisinya. Kunci dapat mempergunakan sistem *preshared* maupun *publickeyinfrastructure* [10].

2.5 Pengujian Sistem

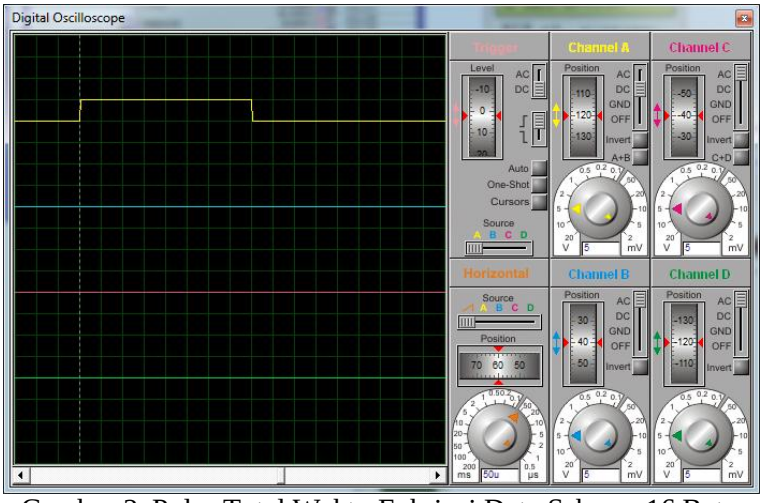
Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibangun. Pengujian yang dilakukan adalah pengujian BlackBox meliputi pengujian algoritma dan kecepatan komputasinya. Jika pada pengujian sesuai kebutuhan maka dilakukan langkah selanjutnya, tetapi jika belum sesuai maka harus diulang kembali dari langkah sebelumnya.

2.6 Implementasi Sistem

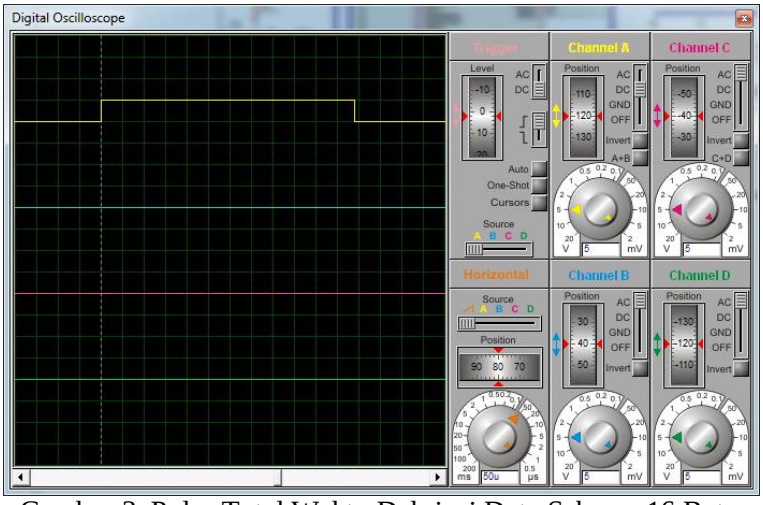
Pada tahap ini telah dibangun sistem yang sesuai dengan kebutuhan melalui proses pengujian yang dianggap telah berhasil dan sesuai. Kemudian dilakukan implementasi system kedalam mikrokontroler yang telah ditentukan agar dapat dipergunakan dan diuji secara riil.

3. HASIL DAN PEMBAHASAN

Pengujian pertama dilakukan untuk mengetahui performa enkripsi AES pada sistem yang dipergunakan yaitu pada ATMEGA16 dengan kecepatan detak 11,0592MHz. Untuk melakukan proses enkripsi data 16 byte menggunakan kunci sepanjang 128 bit memerlukan waktu 400µs seperti pada Gambar 2. Sedangkan untuk mendekripsi kembali datanya maka dibutuhkan waktu sebesar 600µs seperti pada Gambar 3. Pengukuran waktunya dilakukan dengan mengukur lebar pulsa yang dikeluarkan selama prosesnya menggunakan osiloskop yang disediakan pada simulatornya.

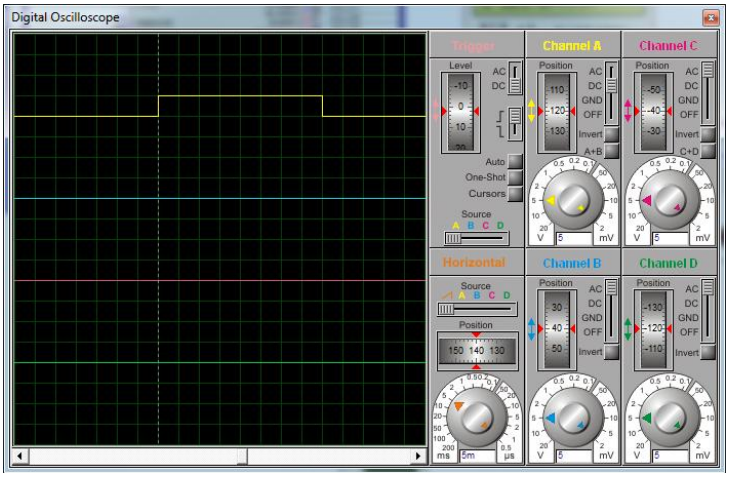


Gambar 2. Pulsa Total Waktu Enkripsi Data Sebesar 16 Byte

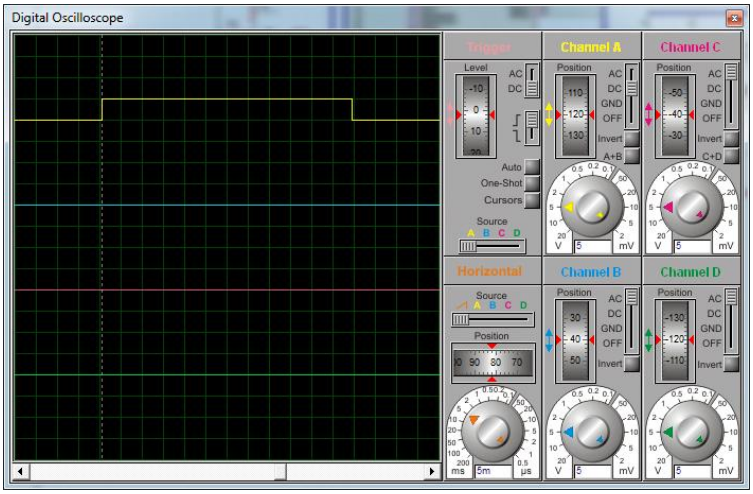


Gambar 3. Pulsa Total Waktu Dekripsi Data Sebesar 16 Byte

Pengujian kedua dilakukan untuk mengetahui konsistensi performa enkripsi AES untuk memproses blok data yang banyak yaitu sebesar 1600 byte. Performa sistemnya tetap konsisten yaitu total waktu enkripsinya sebesar 40ms dan untuk total waktu dekripsinya yaitu sebesar 60ms seperti pada Gambar 4 dan 5. Untuk data hasil dekripsi semuanya memiliki kesamaan dengan data aslinya, sehingga proses enkripsi dekripsi AES telah berhasil dilakukan secara sempurna.



Gambar 4. Pulsa Total Waktu Enkripsi Data Sebesar 1600 Byte



Gambar 5. Pulsa Total Waktu Dekripsi Data Sebesar 1600 Byte

4. KESIMPULAN

AES sebagai salah satu metode enkripsi yang kuat dapat dipergunakan pada pengamanan data sistem SCADA. Dengan waktu eksekusi di bawah 1ms untuk 16 byte data pada mikroprosesor 8 bit dengan *clock* 11,0592 MHz maka penggunaan AES pada sistem SCADA tidak akan memperlambat respon sistem secara umum. Implementasi arsitektur sistem keamanan komputer pada sistem SCADA modern akan meningkatkan reliabilitas sistem, terutama pada bagian sekuritinya, yang mana merupakan suatu hal yang diabaikan dalam arsitektur SCADA tradisional. Dengan adanya sistem SCADA yang memiliki level keamanan yang tinggi, maka akan meminimalkan probabilitas kompromisasi sistem baik dari faktor internal maupun eksternal.

5. SARAN

Untuk meningkatkan pengembangan system ini kedepannya maka dapat ditempuh beberapa langkah berikut ini:

1. Mengimplementasikan system enkripsi dan dekripsi pada proses akuisisi riil berbasis *modbus*.
2. Penggunaan mikroprosesor dengan kemampuan enkripsi dekripsi internal seperti AVR XMEGA atau ARM.
3. Membangun *modbus gateway* berbasis enkripsi dekripsi AES sehingga tidak mengubah secara signifikan terhadap *plant* yang sudah ada.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada

a. Bapak Johannes Petrus, S.Kom., M.T.I, CFP, selaku Direktur AMIK MDP yang telah memberikan kesempatan untuk pelaksanaan penelitian ini.
b. Bapak Abdul Rahman, S.SI., M.T.I, selaku Ketua Program Studi Teknik Komputer yang telah memberikan kesempatan dan persetujuan untuk pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] Beaver et al. 2002, *Key Management for SCADA [Online]*, Available:http://www.sandia.gov/scada/documents/013252.pdf.

[2] B. Linke, 2008, June 19, *Overview of 1-Wire Technology and Its Use[Online]*, Available: http://www.maxim-ic.com/app-notes/index.mvp/id/1796.

[3] Dr. A. Goel and R.S. Mishra, 2009, "*Remote Data Acquisition Using Wireless – SCADA System,*" International Journal of Engineering, Vol. 3, No. 1, pp. 58-64, March 15.

[4] D. Choi et al.,2009, "*Advanced Key Management Architecture for Secure SCADA Communication,*" IEEE Transactions on Power Delivery, Vol. 24,Nno. 3, pp. 1154-1163.

[5] IEEE Standard, 1994, *Definition, Specification, and Analysis of Systems Used for Supervisory Control,* Data Acquisition, and Automatic Control, IEEE.

[6] K. Stouffer et al.,2011, *Guide to Industrial Control System (ICS) Security*, NIST U.S. Department of Commerce, Gaithersburg.

[7] R.L. Krutz, 2005, *Securing SCADA System*, Wiley, Indianapolis.

[8] R.J. Robles et al., 2008, "*Vulnerabilities in SCADA and Critical Infrastructure Systems,*" International Journal of Future Generation Communication and Networking, Vol. 1, No. 1, pp. 99-104.

[9] R.J. Robles and T. Kim, 2011, "*Scheme to Secure Communication of SCADA Master Station and Remote HMI's through Smart Phones,*" Journal of Security Engineering, Vol. 8, No. 3, pp. 349-358.

[10] R. Dawson et al., 2006, *" SKMA A Key Management Architecture for SCADA Systems*," Fourth Australasian Information Security Workshop, Vol. 54, pp. 138-192.

[11] S.F. Barret, 2009, *Embedded System Design with the Atmel AVR Microcontroller*, Morgan & Claypool Publishers, California.

[12] S.A. Boyer, SCADA, 2009, *Supervisory Control and Data Acquisition, The Instrumentation*, Systems, and Automation (ISA) Society, *North Carolina.*

[13] T. Amaio and T. Van, 2011,"*IEEE 1711-2010 Security for Legacy SCADA Protocols*," Presented at The Industrial Control Systems Joint Working Group (ICSJWG), Long Beach, CA.