Implementasi hardware dari algoritma enkripsi RC4 (Rivest Chiper IV) untuk keamanan data pengguna/pelanggan pada smart grid berbasis IoT (Internet of Things) dengan menggunakan NIOS processor.

Surya Ramadhan

23215093

Rivest Chiper 4 (RC4) merupakan stream chiper yang cukup populer dikarenakan implementasi algoritmanya yang tergolong sederhana. Algoritma RC4 sendiri banyak diterapkan dalam bidang keamanan data seperti pada WEP (Wireless equivalent privacy), WPA (Wi-Fi protected access), SSL (Secure socket layer) dan keamanan database. Algoritma RC4 terdiri dari Plain text dan Pseudo Random Generator yang keduanya digabung menjadi stream chiper. Experiment yang akan dilakukan yaitu mengiplementasikan algoritma RC4 pada processor NIOS pada FPGA ALTERA Cyclone IV, dengan menggunakan sampling USERNAME (Plaintext) dan PASSWORD (Key Chiper).

Implementasi pada hardware memiliki keunggulan yaitu kecepatan proses data yang jauh lebih cepat dibandingkan implementasi dengan software, data throughput yang dihasilkan dari implementasi hardware hingga 62.09 MB/sec (E.Taqieddin, O.A. Rjei, K. Mhaidat, R.B Hani, 2015). Oleh karena itu, pengimplementasian hardware pada keamanan dan dan informasi digital akan semakin dibutuhkan seiring bertumbuhnya data dan informasi digital.

Smart Grid mulai dikembangkan dalam dekade terakhir seiring dengan kebutuhan energi listrik meningkat setiap tahunnya, para peneliti mulai memikirkan langkah untuk membuat sebuah terobosan untuk menciptakan efisiensi dalam penggunaan tenaga listrik. Istilah smart grid tidak hanya berputar pada monitoring dua arah, efisiensi, namun juga termasuk didalamnya terdapat smart metering, smart appliance, dan renewable energy. Dan juga diterapkannya smart grid yang berbasis IOT, dimana penggunaan listrik dapat dimonitoring dan dilaporkan secara online, sehingga baik pengguna energy listrik maupun pihak yang terkait untuk memproduksi pasokan listrik dapat mengevaluasi langsung. Seperti penerapan billing/pembayaran listrik secara online. Hal ini akan terintegrasi dengan Internet (IOT) dimana pengguna listrik dapat membayar tagihan listriknya secara online, melakukan evaluasi bulanan sehingga para pelanggan dapat menentukan jumlah kebutuhan dan melakukan penghematan.

Dengan ditanamkannya system online pada smart grid, maka akan muncul permasalahan dalam keamanan data pengguna. Sehingga dengan penerapan algoritma RC4 untuk melindungi data dari pengguna diharapkan dapat memberikan solusi keamanan dari data data yang dimiliki oleh pengguna.

References:

[1] E.Taqieddin, O.A. Rjei, K. Mhaidat, R.B Hani," *Efficient FPGA Implementation of the RC4 Stream Cipher using Block RAM and Pipelining*", EUSPN 2015, Elsevier, 2015.

[2] P. Jindal, B. Singh,"*RC4 Encryption-A Literature Survey*", ICICT 2014, Elsevier, Published in 2015.

[3] S. C. Wagaj, C. Bagul, R. Chaudhari,"*Implementation of RC4 Stream Cipher Using FPGA*", International Journal of Advanced Computer Research, 2013.

[4] P. Hämäläinen, M. Hännikäinen, T. Hämäläinen, J. Saarinen," *Hardware Implementation of The Improved WEP and RC4 Encryption Algorithms for Wireless Terminals*" Digital and Computer Systems Laboratory, Tampere University of Technology.

[5] T.H. Tran, L. Lanante, Y. Nagao, M. Kurosaki, H. Ochi," *Hardware Implementation of High Throughput RC4 Algorithm*", IEEE, 2012.

[6] S.S. Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, B.P. Sinha," *High-Performance Hardware Implementation for RC4 Stream Cipher*", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 4, 2013.

[7] R. Prabu," *Design Of High Performance Rc4 Stream Cipher For Secured Communication*" International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, 2014.

[8] W. Wang, Z. Lu,"*Cyber security in the Smart Grid: Survey and challenges",*Computer Network, Elsevier, 2013.