ISSN 2278-3091

Volume 6, No.3, May - June 2017

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse02632017.pdf

A Smart Grid Security Solution Model Using RC6 Cryptographic Algorithm

Philemon Uten Emmoh[1], Ahmadu Ally Dauda[2], Prof. Mohammed B. Hammawa[3] and Asabe Sandra Ahmadu[4]

[1, 2] ICT Centre, Federal University, Wukari, Taraba State, Nigeria. [1]philiemmoh@yahoo.com, [2]italtd2000@yahoo.com

[3]Department of Mathematics and Computer Science, University of Abuja, Nigeria, mbhammawa@gmail.com

[4]Department of Computer Science, Modibbo Adama University of Technology, Yola, Nigeria.,
ahmaduasabe@mautech.edu.ng

ABSTRACT

A smart grid security solution protects smart grid power systems from attacks from various sources and ensures continuous service and availability. RC6 cryptographic algorithm is a compact, secure and efficient cryptographic system that meets the security demands of smart grid power systems. This paper uses the RC6 cryptographic algorithm to design a model for a secure smart grid security system. We also look at the structure and form of Smart Grid Power systems, devices and interconnection and memory/resource requirements. We then make use of UML tools to design the model and show how the RC6 low memory demand capacity, lack of lookup table and robust/unbreakable security can be used to protect smart grid powers systems in an efficient and effective manner. Finally, we look at the implementation of the RC6 cryptographic algorithm in Java Netbeans 8.2 and how the size of the code can be accommodated in memory hungry devices that are prevalent in smart grid power systems.

Keywords : Cryptography, Java, Security, Smart Grid,

1. INTRODUCTION

The world has seen the emergence of different and wide-ranging types of computer systems and technology networked to provide quality service to mankind. These technologies range from simple smart phones that enable people to stay connected with our loved ones to high technology medical equipment that help to connect doctors, and other specialist in medical service to remote locations to provide quality medical service that may have been available only in big cities and developed nations. A smart power grid system is a sophisticated electrical network, that uses computer systems to deliver electrical energy from power generating firms through smart transmission and distribution networks to consumers' smart meters. These networks utilizes the enormous computing capabilities available today to offer enormous benefits to all stakeholders; government, power firms, transmission and distribution firm, consumers and the environment. It is currently being adopted and promoted by governments and power firms in the United States, Europe and South Africa.

Key benefits of smart grid power systems include providing power consumers the ability to pursue smart energy demand using accurate, time-of-use pricing rates. This means users of smart power systems may schedule heavy power usage services at off peak periods when rates are lower thus saving them money and thus helping in the distribution of power demand evenly across the day, month or year [1]. The other benefits of Smart Grid Power systems include improved reliability, efficiency, economy and protection of national security due to the fact that it is easier to control and monitor. Smart meters are physical systems that are becoming more and more complex. These systems now have more computing capacity, have more dynamic capabilities, and are connected to communication networks, such as the Internet. These improvements have allowed for much greater risk of vulnerabilities. Since smart power systems cover large geographical space, security vulnerabilities increase and [12] enumerated the following; malicious control from an adversary connected over the Internet, malicious code, such as a virus might infect the system, and also threats from internal staff. Modern computers, tablets, mobile phones and smart meters come with increased processing power and more generalized computing resources thus viruses and malware would have a greater attack surface and more opportunities to compromise smart grid infrastructure.

The communication infrastructure in smart grid power system must support the expected smart grid functionalities and meet the performance requirements [9]. This is because the infrastructure connects an enormous number of electric devices and manages the complicated device communications and security protocols; it may be constructed in a hierarchical architecture with interconnected individual sub-networks and with each taking responsibility for separate geographical regions. In general, the communication networks can be categorized into three classes: wide area networks, field area networks, and home area networks. Since smart grid power systems are tightly interconnected using communication channels, they are prone to threats from sophisticated cyber criminals that imperils power users, producers, society and government. These threats could target the generation, transmission, distribution, and market domains. This means all domain not only has a set of core operational assets to defend, they need to build defenses to help protect their critical business and corporate environments from exposure [4] using cryptographic protective schemes that uses less memory, tis fast to meet the demands of the smart infrastructure and secure [3]..

Security Needs

To address the above cyber security threats, the general requirements for Advanced Metering Infrastructure (AMI) security are mainly include Device authentication, Data confidentiality, Message integrity, maintaining, secrecy, preventing potential cyber-attacks. Security as a major requirement covers all aspects of the SG, from physical devices to routing protocol operations to ensure the availability and reliability of the whole network.[10], [2] Many end-point devices in power transmission and distribution networks, and power generation networks are located in an open, potentially insecure environment which makes them prone to malicious physical attacks. These devices must be protected properly against unauthorized access such as modifying the routing table or some network information stored in the compromised device. These actions as well as spoofing, altering or replaying routing information during information exchange between nodes are examples of attacks against routing protocols. Another major concern in the routing would be the privacy of the power data [11].

2. STRUCTURE AND FORM OF SMART GRID POWER SYSTEM

[7] In Figure 1 below developed a high level model of a Smart Grid Power system to be made up of the Bulk Power Generators, Transmission Firms, Distribution Firms and Consumers as shown below.

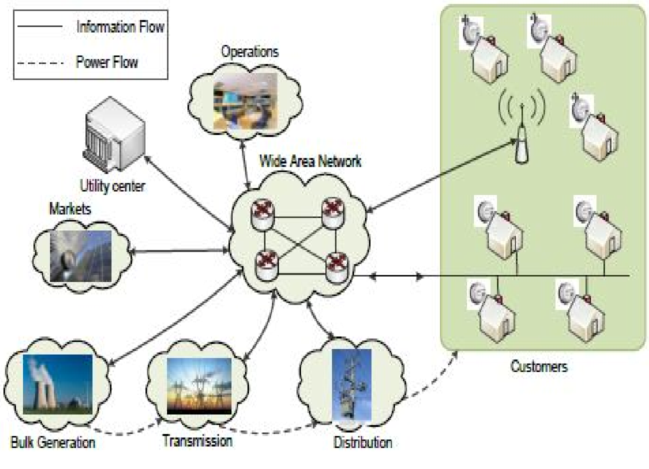


Figure 1: A High-Level Model of Smart Grid [7]

It is important to note that in figure 1above we have the following key actors:-

A. **Bulk Generators:** Power generators feed the smart grid network and therefore need to be paid to enable them recoup their investments with profits. They need smart meters to accurately measure and bill the power delivered to transmission firms.

B. **Transmission Firms:** Transmission firms receive power from Generation firms and need to deliver same quantity to Distribution firms and bill them after adding their transmissions charges. A smart meter is needed to bill this service.

C. **Distribution Firms:** These firms add their distribution cost and the profits needed to deliver power to customers or retail users. They need smart to bill customers for power delivered to them and enable them monitor and control usage.

D. **Infrastructure Control Devices:** Smart grid power systems use smart generation, transmission and distribution facilities to operate. Smart control devices are needed to protect the infrastructure from attacks.

E. **Bulk Buyer/Markets:** In most power markets to ensure the availability of liquidity, bulk buyers or markets exist. There is therefore the need for them to have smart meters for billing, monitoring and control between them and generators and transmission firms.

It is important to note that in figure 1above we have the following key actors:-

A. **Bulk Generators:** Power generators feed the smart grid network and therefore need to be paid to enable them recoup their investments with profits. They need smart meters to accurately measure and bill the power delivered to transmission firms.

B. **Transmission Firms:** Transmission firms receive power from Generation firms and need to deliver same quantity to Distribution firms and bill them after adding their transmissions charges. A smart meter is needed to bill this service.

C. **Distribution Firms:** These firms add their distribution cost and the profits needed to deliver power to customers or retail users. They need smart to bill customers for power delivered to them and enable them monitor and control usage.

D. **Infrastructure Control Devices:** Smart grid power systems use smart generation, transmission and distribution facilities to operate. Smart control devices are needed to protect the infrastructure from attacks.

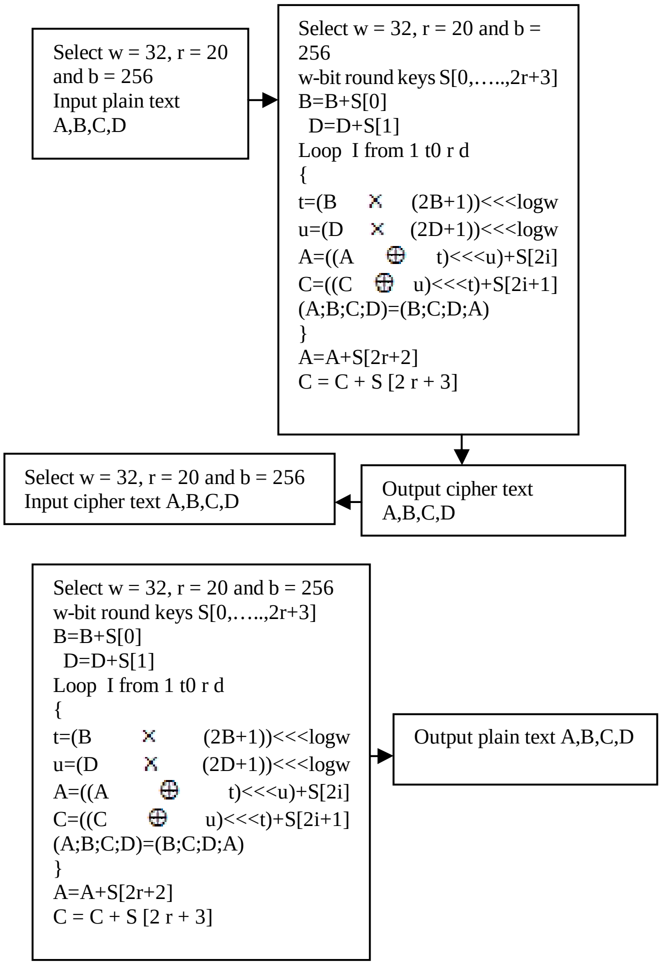
E. **Bulk Buyer/Markets:** In most power markets to ensure the availability of liquidity, bulk buyers or markets exist. There is therefore the need for them to have smart meters for billing, monitoring and control between them and generators and transmission firms.

3. RC6 CRYPTOGRAPHIC ALGORITHM

RC6 is a block cipher submitted to NIST for consideration as the new Advanced Encryption Standard (AES). The design of RC6 began with a consideration of RC5 [5] as a potential candidate for an AES submission. Modifications were then made to meet the AES requirements, to increase security, and to improve performance. The inner loop, however, is based around the same half-round" found in RC5. Like RC5, RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6- w / r / b where the word size is w bits, encryption consists of a nonnegative number of rounds r , and b denotes the length of the encryption key in bytes [6]. Since the AES submission is targeted at w = 32 and r = 20, we shall use RC6 as shorthand to refer to such versions. In this algorithm first we have to select the word size which in our implementation is w = 32 , the non-negative number of rounds r = 20 and the byte size of the key b = 256 bytes. The encryption key shall be provided for each smart device from the key schedule service with length of 256 byte (255) will be loaded in array S[0,….,2r+3].

4. PROPOSED RC6 ALGORITHMIC MODEL

RC6 uses four registers A,B,C,D and the plain text will be loaded into four eighth bit registers A, B, C, and D from the least significant to the most significant bits. The RC6 operations of addition, subtraction, duplication, rotation and exclusive – or is then applied to generate the cipher text. During the process of decryption, the cipher text is placed in the same registers A, B, C, D and the process of generating the plain text is similarly done as shown in the model below.


Select w = 32, r = 20
and b = 256
Input plain text
A,B,C,D

```
Select w = 32, r = 20 and b =
256
w-bit round keys S[0,…..,2r+3]
B=B+S[0]
  D=D+S[1]
Loop  I from 1 t0 r d
{
t=(B    ×    (2B+1))<<<logw
u=(D    ×    (2D+1))<<<logw
A=((A    ⊕    t)<<<u)+S[2i]
C=((C    ⊕    u)<<<t)+S[2i+1]
(A;B;C;D)=(B;C;D;A)
}
A=A+S[2r+2]
C = C + S [2 r + 3]
```

Output cipher text
A,B,C,D
Select w = 32, r = 20 and b = 256
Input cipher text A,B,C,D

```
Select w = 32, r = 20 and b = 256
w-bit round keys S[0,…..,2r+3]
B=B+S[0]
  D=D+S[1]
Loop  I from 1 t0 r d
{
t=(B    ×    (2B+1))<<<logw
u=(D    ×    (2D+1))<<<logw
A=((A    ⊕    t)<<<u)+S[2i]
C=((C    ⊕    u)<<<t)+S[2i+1]
(A;B;C;D)=(B;C;D;A)
}
A=A+S[2r+2]
C = C + S [2 r + 3]
```

Output plain text A,B,C,D

Figure 2: Model for the poposed RC6 Cryptographic

RC6 Algorithm Security Flow Chart

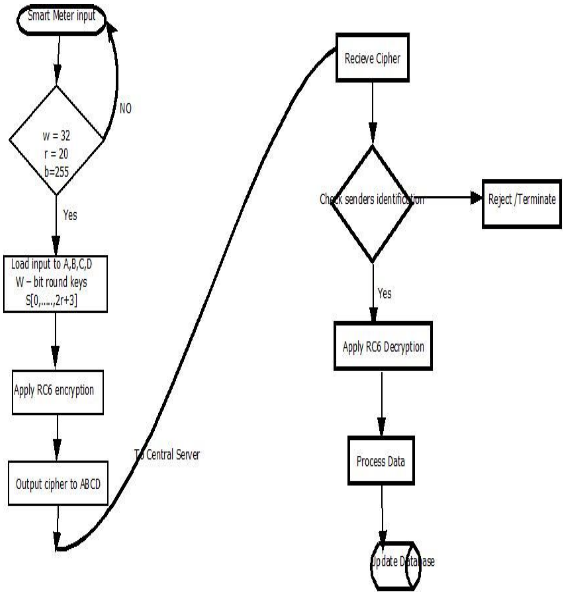


Figure 3: Model for the poposed RC6 Cryptographic

RC6 Java Netbeans 8.2 Implementation

This solution will be implemented using Netbeans Java 8.2 and is have a server control back-end at a separate location. Each customer will have smart meters with the front app that will be tightly linked to provide security for the smart grid power system.

5. CONCLUSION

Smart grid power systems offer interesting performance advantages but are bedeviled with several challenges that can be very costly materially and to human lives. To be able to overcome these challenges, a robust, low memory, fast and break-proof security solution is needed. RC6 cryptographic algorithm is a good candidate for this type of solution because, it uses little memory, is compact, does not require look up tables, and is very fast. A java implementation allows it to run all operating platforms and the low code side reduces memory demand. It is our expectation that this and other new developments in Smart Grid security systems will not only improve operational service but save human lives and boost the adaption of smart grid power in our country and globally.

REFERENCES

1. R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, Z. Huang, M. Joung, J. Kim, D. Kirschen, S. Lee, F. Li, J. Li, Z. Li, C.C. Liu, X. Luo, Mili, L., Miller, S., Nakayama, M., Papic, M., Podmore, R., Rossmaier, J., Schneider, K., Sun, H., Sun, K., Wang, D., Wu, Z., Yao, L., Zhang, P., Zhang, W. and Zhang, Z. **Vulnerability assessment for cascading failures in electric power systems**, *in Power Systems Conference and Exposition, PSCE '09. IEEE/PES*, pp. 1–9, 2009.

2. K.C. Ravindra. **Design of a new Security Protocol,** *IEEE International Conference on Computational Intelligence and Multimedia Applications*, pp 132 – 134, 2007.
3. M.J.B. Robshaw and Y.L. Yin. **Elliptic Curve Cryptosystems,** Technical Note. Dublin: RSA Laboratories, 1997.
4. K. Rivest. **The Secret Hidden Key for Encryption Development and Generation**. *Vancouver: Brooklyn Books.* 123-156, 2009.
5. R.L. Rivest. **The RC5 encryption algorithm**. In B. Preneel, editor, Fast Software Encryption, volume 1008 of Lecture Notes in Computer Science, pages 86=96, Springer Verlag, 1995.
6. R.L. Rivest, M.J.B. Robshaw, R. Sidney and Y.L. Yin. (1998) The RC6 Block Cipher. v1.1,. Available at www.rsa.com/rsal abs /aes / , 1998.
7. B.M. Nasim. **An Intrusion Detection System for Smart Grid Neighborhood Area Network**. A Master's thesis presented to the department of Computer Science Ryerson University. Toronto, Ontario, Canada, 2013.
8. National Energy Technology Laboratory. **A compendium of smartgrid technologies**. Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, 2009.
9. S. Pahwa, A. Hodges, C. Scoglio and S. Wood. **Topological analysis of the power grid and mitigation strategies against cascading failures, in Systems Conference**, *IEEE. IEEE*, pp. 272–276, 2010.
10. E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi.***Communication Security for Smart Grid Distribution Networks,*** IEEE Communications Magazine, pp.42-49, 2012
11. P. Shuva, M. S. Rabbani, R. K. Kundu, and S. M. R. Zaman. ***A Review of Smart Technology (Smart Grid) and Its Features.****IEEE Proceedings,* (ICONCE 2014).
12. L. Sankar, S. Kar, R. Tandom and H.V. Poor. **Competitive privacy in the smart grid**: **An information theoretic approach, in smart grid communication, smart grid com,** *IEEE International Conference*, pp220-225, 2011.