Secured Smart Grid Network for Advanced Metering Infrastructure (AMI)

Philani Khumalo[1]
Department of Electronic Engineering
DUT
Durban, KZN
philanipk@gmail.com

Bakhe Nleya[2]
Department of Electronic Engineering
DUT
Durban, KZN
bakhen@dut.ac.za

***Abstract* — Smart Grids are generally modern electric power network technology systems used by power utility to optimise the efficiency of power supply. While it is good practice to introduce Smart Grid technology, the use of digital technology introduces security threats on Smart Grid systems. Smart Grids mostly have a sophisticated network arrangement which may be exploited to access private information and private sensitive data therefore there is a need to secure it. Energy theft and the metering information are amongst the biggest fears related to the Smart Grid application. This paper will discuss Smart Grid security technology challenges and possible effective solutions. Particularly overcoming Smart Grid security challenges, a robust communications protocol that will implement security functionalities is required. The solution aspect should include but not be limited to encryption of messages, minimizing delays due to cryptographic processes and guaranteeing integrity of these messages with negligible latency. Smart Grid is a part of Advanced Metering Infrastructure (AMI) and the whole network need to be secured. Advanced Encryption Standard (AES) will be implemented to enhance security of this network. Using OPNET and Java NetBeans 8.2 complier it will be proven that the AES or modified AES will best serve the Power Line Communications (PLC) Smart Grid security challenges.**

***Key words* — Power Line Communications, Smart Metering, Smart Grid, Advanced Encryption Standard, Advance Metering Infrastructure, and Security.**

I. INTRODUCTION

Power Line Communication (PLC) Smart Grid uses the existing power lines to transmit information or data. The information is transferred on a conductor that is simultaneously used for carrying Alternative Current (AC) power to consumers. Diversity of PLC technologies are required for diverse applications, ranging from home automation to internet access. Different data rates and frequencies are used in various PLC applications and there are a number of technical problems that are common on this technology. The major concern on Advanced Metering Infrastructure (AMI) is the security of data. Since PLC uses existing electrical power grid infrastructure it is less costly and most popular. The security of information over PLC network has become a focus of many organizations. Challenges of PLC network protocols used will be discussed and various levels of data protection schemes with the intention to address PLC Smart Grid security challenges. The data must be safeguarded by robust encryption and authentication. The protocols, bandwidth, reliability, and accessibility are important aspects because these are the core components of the robust network. PLC would be a perfect last mile candidate since it is comparatively inexpensive as compared to fibre and the infrastructure already exists. The PLC network advantage is that the medium also carries power which makes these medium resistant to cable tapping attacks [1], [2], [3].

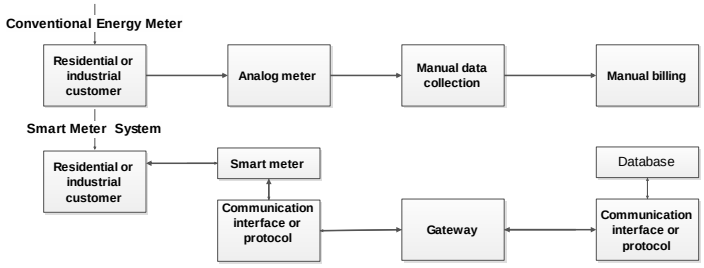

Fig. 1. Architecture of Analog and Smart Meter [4].

II. ADVANCED METERING INFRASTRUCTURE

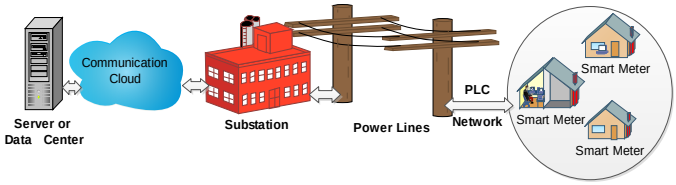

Fig. 2. Typical AMI Network

Fig. 2 above shows a typical AMI network configuration. The smart meters are connected at the customer houses and they communicate via PLC using the existing power lines. The connection goes from Smart meter to PLC network through to the nearest substation, from the substation to the data management center, it uses a different communication medium which can be fibre or wireless.

III. LITERATURE REVIEW

Recently Smart Grid technology attracted a huge attention worldwide. Many researchers have executed tremendous work to implement protocols that will secure the Smart Grid. The introduction of digital data management in Smart Grid brought about data security concern. Robust protocols are required to safeguard the data. Some protocols used in Smart Grid networks are propriety and others are open. In Smart Grid utility can use any protocol but it is important to select the best to secure the sensitive information.

In [1] the author has discussed Smart Grid challenges, few PLC protocols and standards that can be used such as IEEE 1901.2. The author also discussed the presence of noise in PLC Channel and the use of OFDM on PLC for noise mitigation. The frequency band available for PLC CENELEC was also discussed. It became clear that PLC will attract many business opportunities and is the technology of the future. In [2] the authors discussed the self-healing Smart Grid system. In [3] the author introduced PRIME Physical layer protocol that uses OFDM in physical layer for communications. The author also mentioned the standardisation of PLC e.g. IEEE 1901.2. In [4] the author have introduced the advantages and challenges of Smart Grid. Session Initiation Protocol (SIP) is an open standard based technology for robust communication in Smart Grid applications, peer to peer, DNP3, ZigBee were also discussed in this paper. The authors in [5] have focused on enhancing Smart Grid technologies and they proposed an end to end communication infrastructure and NIST framework for Smart Grid. The challenges introduced were interoperability efficiency and performance. In [6] all PLC standards are listed e.g. IEEE P1901 for high speed PLC communications. In [10] the author introduced various levels of Smart Grid security. In [19] a comparison study was executed on DES AES and RSA and it was concluded that AES was best for securing data.

Looking at the above research a lot was done concerning Smart Grid but there is less attention to secure Smart Grid using robust and fast algorithms. The robust algorithm research was conducted on this paper for a robust encryption to run on Smart Grid. It was concluded that AES is a possible secure algorithm that offers better security for implementation on PLC Smart Grid. There are a vast of protocols, data encryption and decryption algorithm available namely: RSA, Mars, ABE but AES which is a symmetric key encryption proved to be more efficient in hardware, speed and price. Public key encryption is not a solution due to computational requirement, it is slow, and costly [22], [23].

A. Advanced Metering

Smart metering is a solution for the utility and consumers due to the intelligence it provides. Smart metering provides two way communications, the utility can use the meter to send the message to the customer and the message can be displayed on the meter display. The smart meter on the customer side will provide information about consumption behavior. Information can be sent by the utility to the smart meter for the customer to access it i.e. monthly consumption therefore eliminating the need for sending billing letters [5].

On the other hand the supplier will have information on meters when being tampered with by customers. The smart meter can be both prepaid or credit meter depending on the customer plan. Smart meter will give the customers real time consumption. If the customers can see how much they consume in real time it will be up to them to monitor, save and change their consumption behavior by reducing non-essential appliances. Smart meter will reduce the cost of personnel to be sent to all house hold to manually read meters. Billing can be executed remotely, by downloading the usage and bill the customers. The restrictions commands can also be sent remotely when the customers have not paid their utility bill [6].

B. Advantages of Smart Metering

- The smart meters reports when it is tampered with
- The smart meters reports power outage
- The household power can be restricted via smart meter
- Load shedding can be executed remotely
- The smart meter helps in real time consumption
- The smart meter can help in power saving
- The smart meter can reduce energy theft

C. Disadvantages of Smart Meters

- Expensive.
- Security issues.
- Less jobs.

D. PLC standards consideration

Table I below shows the PLC standard as part of AMI. The table shows the standards of different PLC bands, technology frequency and data rate [6].

TABLE I. PLC STANDARDS [6]

Bandwidth	Standards used	Technology	Frequency	Data Rate
Narrow band	PRIME	OFDM	42-90kHZ	21-128kbps
Narrow band	PLC G3	OFDM	35-90kHz	2.4-34 kbps
Broad band	P1901	OFDM	2-3MHz	100 Mbps
Narrow band	Home plug	OFDM	2-30MHz	3.8 Mbps
Narrow band	IEC	SFSK	60-76 kHz	1.2-2.4kbps

The protocols used on PLC are: X10, CE Bus Lon works etc. Some of these protocols are outdated and they have inadequate security features on them. The bandwidth and speed is also a limiting factor on the communications network and needs to be addressed. Most PLC's currently make use of Orthogonal Frequency-Division Multiplexing (OFDM) coding schemes. OFDM is a method of encoding digital information on multiple carrier frequencies [7].

OFDM has industrialised into a popular structure for wideband digital communication, whether wireless or over copper wires. OFDM is used in applications such as digital television audio broadcasting, Internet access, wireless networks and power line networks etc. [6]. IEEE P1901 is a standard for high speed devices via AC power line [6]. IEEE P1675 is a standard for connecting Broadband Power Line (BPL) devices underground and overhead power line distribution lines [7].

IV. PLC CHANNEL

A. Power Line Channel Noise

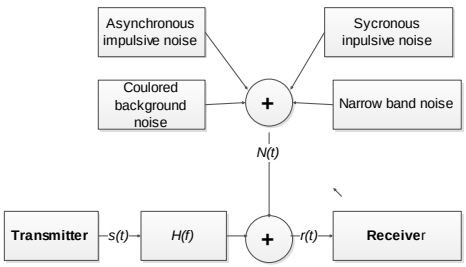

Fig. 3. Channel noise introduced on PLC network [8].

The Power Line Communications channel problem is that the channel is mostly exposed to severe noise interference; unlike other transmission channels it does not represent an Additive White Gaussian Noise (AWGN) channel [8]. The noise interference situation is much more compound because it does not only work with broadband noise, but also with narrow band interference and diverse types of impulsive disturbance also occur as portrayed in Fig. 3. When dealing with PLC Smart Grid all types of noise needs to be accounted for and select a proper signal modulation scheme to suppress or cancel the noise available on the channel [8].

B. The Transfer Function of PLC Multipath Signal

When designing a PLC Smart Grid network the PLC channel and PLC transfer function need to be understood. Understanding the channel will enable easy design and security protocol implementation on the channel. Zimmerman developed an echo model that has an extra signal attenuation factor on his equation. The model proves and represents the superposition of signals from *N* unlike paths, a weighting factor g_i and length d_i characterising each different path individually. Additionally, the values a_0 ,a_1, and k are utilised to model frequency dependent attenuation. Equation (1) defines a general transfer function of the power line channel [9].

$$H(f) = \sum_{i=0}^{N} g_i \; e^{-(a_0 + a_1 f^k) d_i} \; e^{-j2\pi f \frac{d_i}{v_p}} \qquad (1)$$

V. AMI SECURITY

A. PLC Security

In the design of AMI and PLC system security, important security features needs to be considered as well as protocol used channel capacity and data transmission speed. Deficiency of security in AMI system can make electrical distribution untrustworthy [4]. To define attacks on the AMI there are four components that need to be looked at which are: Smart meter, AMI Head End, Communication Network and Meter Data Management System (MDMS). To identify the attack at a specific node, it is important to understand what kind of security service is running on that precise node. The attacker will manipulate or alter a specific controlled data to gain admission to a forbidden area in order to perform malicious operation and destroy the network or steal information [11], [10].

B. The Security Rules and Design Considerations

- **AMI Authentication:**

  An AMI data requires to be protected against the eavesdropping and tampering.

- **Authentication and Coupling:**

  The AMI devices should be able to authenticate themselves right after they are installed in order not to allow meter spoofing. The smart meters shall constantly re-authenticate in the back ground.

- **Key Management:**

  There should be an enhanced cryptosystem to secure data and the establishment of encryption keys e.g. Advanced Encryption Standard (AES).

- **Flexibility and Extensibility:**

  The AMI should be open for future expansion without any difficulty of hardware change.

- **Security Strength:**

  The security algorithms should ensure high security strength.

- **Forward Secrecy:**

  Different keys should be used in each session, and they must not be able to be derived from the exposed key.

C. Threats Modeling

To define the threat model we need to identify the intruder and define counter measures to mitigate the dangerous threats [9]. The following are the identified threats:

- Tampering application on AMI nodes.
- Authentication bypass in smart meters
- Firmware manipulation.
- Masquerade the control center.
- Man in the middle attacks
- Buffer overflow through AMI firmware.

D. The Threats of Security Domain

- Privacy of data must not be compromised or bridged.
- Tampering of data or messages must be discouraged during transmission.
- Unverified equipment on the network is undesirable
- Availability of data when it is required by an authorized person should be constant.

E. The Intruder Motives

- Disruption of services.
- Stealing of electricity.

TABLE II. PLC SECURITY THREATS VULNERABILITY AND IMPACT SUMMARY TABLE [10]

Treats	Vulnerabilities	Impact
Tamper	Management applications	Distribution of communication
Masquerade	Lack of authentications and encryption	Impersonate the control centre and send unauthorized commands
Authentication bypass	Poor proper metering protocol	Manipulate the parameters of the meter
Buffer overflow	Firmware assumption	System not stable
Firmware manipulation	Firmware poor access control	Attacker shut down the meter

F. Security recommendations

- **Control for Buffer Overflow**.

  Use stack canaries to sense for buffer overflow if the canary value is altered, attack can be detected before execution.

- **Control for Firmware**

  Encrypt firmware, validate firmware integrity and authenticate before it gets located to the boot loader [12].

- **Control for Authentication**.

  Metering protocols like AES must be used to support authentication. Depending on the requirement, the modified AES can be used since it provides fast encryption and authentication scheme.

G. PLC Physical Security

PLCs are naturally more secure than wireless due to its physical medium. PLC network is a danger due to the presence of AC voltage on them. The differences in the Signal to Noise Ratio (SNR) and Channel frequency response between different

nodes in the network makes it more difficult to retrieve information from intercepted signal [12].

H. PLC Semantic Security

Cryptography - denies intruders access to data exchange on the network, the information is encoded using Encryption key before transmission and this makes data useless to the intruder or someone who eavesdrop it [15],[16].

Authentication - access to the network gained after identifying the user.

Integrity control - the data sent will be identified if it was changed or not.

Confidentiality - Data travelling across a network should not be viewed by an intruder.

Two cryptography techniques:

- Asymmetric – key cryptography or public key cryptography where two different pair of keys is used to encrypt and decrypt data
- Symmetric – key cryptography single key is used to encrypt and decrypt information. The key must be available on both ends (transmitter and receiver).

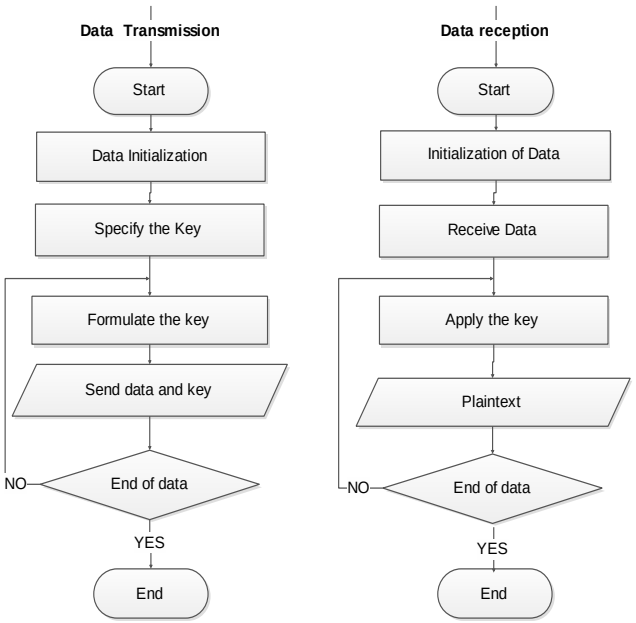

Fig. 4. Security Algorithm Flow Chart.

Fig 4 shows the flow chart of the security algorithm.

I. Cryptology

Cryptology is the scientific study of cryptosystems, and it is divided into two categories.

- Cryptography - which is the design of cryptosystems.
- Cryptanalysis - is the study of how to crack or deciphering coded data without a key.

These two features of cryptology are closely linked when setting up a cryptosystem. The study of its security plays a significant role. There are numerous reasons for this, for example the privacy of data. When conveying data, we do not want an eavesdropper to comprehend the information conveyed. The same is true for kept data that should have privacy against unapproved access, for example by hackers. Authentication is the equivalent of a signature whereby the receiver of data wants proof that the data comes from a certain party and not from someone else. Integrity means that the receiver of certain message or data has indication that no alterations that have been made on the data received. The safety of the data will be performed by means of cryptographic techniques [13], [14].

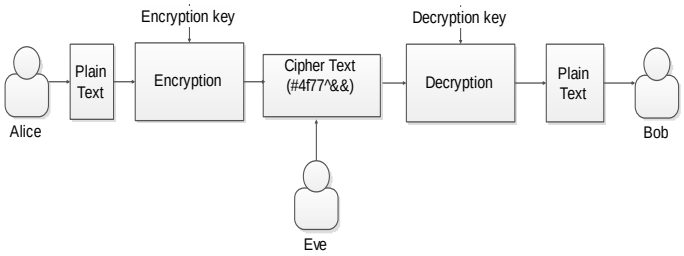

Fig. 5. Encryption block diagram [13].

Fig. 5 above shows how the encryption process is executed when Alice sends plain text to Bob and there is an Eavesdropper listening to the conversation.

VI. AES CRYPTOSYSTEM

The challenge of data transmission on the PLC network is securing the network from the adversary [17]. The data encryption for security can be implemented using Advance Encryption Standard (AES) to encrypt and decrypt information. The data have to be authenticated to verify if the data received comes from the trusted source and the data is not tampered with during the transmission.

Lost packets that are retransmitted and repeated data are authenticated [17]. The smart meters are authenticated before they are requested for data by utility, to prevent the meter spoofing and impersonation. There is less security on the smart meter built-in software that is why there is a need to secure data on the transmission network [18].

The study has been conducted on few encryption protocols like RSA, 3DES and AES. AES has proven to be the best with respect to data block size against data execution time. AES has been proven to be the fastest and efficient encryption method [19]. AES provides low-cost and low frequency encryption. It is essential and appropriate for security and low resource applications.

The AES algorithm is a part of the Rijndael algorithm scheme. The AES algorithm utilises 128 bit block and other three different sizes of keys which are: 128, 192 and 256 data bits. AES uses symmetric key algorithm that means that the key that is utilized for encryption and decryption of data is the same. The cipher text created by AES encryption is of the same size as the plain text [19]. AES also makes use of multiplication state matrix called GF (2^8) the equations 3 and 4 below depicts this algorithm formulae [20], [21].

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{3}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,2} & s_{2,3} & s_{2,3} \\ s_{3,0} & s_{3,2} & s_{3,3} & s_{3,3} \end{bmatrix}$$

$$= \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,2} & s'_{2,3} & s'_{2,3} \\ s'_{3,0} & s'_{3,2} & s'_{3,3} & s'_{3,3} \end{bmatrix} \tag{4}$$

The key and input data are referred to as state and are structured in a 4x4 matrix of bytes [21]. Fig. 6 shows how 128 bit key is distributed into byte matrix.

State

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

Key

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

Fig. 6. Structure of the Key and the State [20].

A. AES Encryption and Decryption.

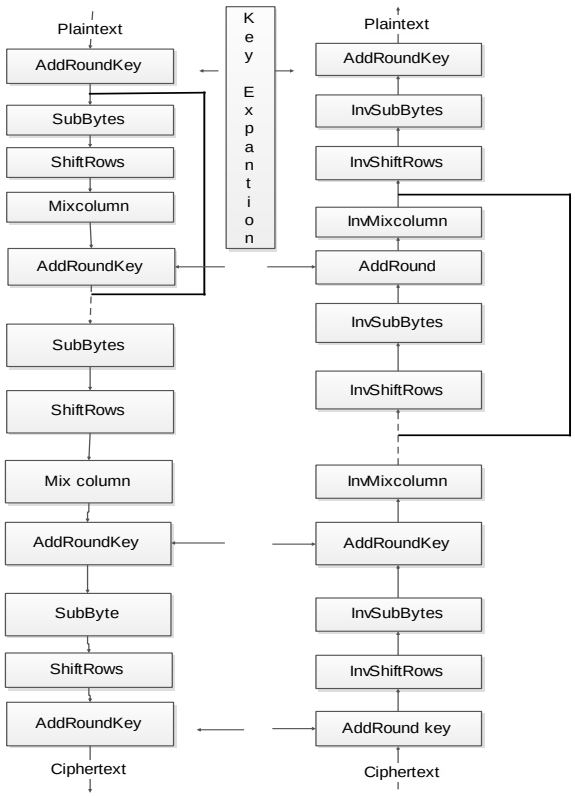

Fig. 7. Flowchart of AES Algorithm [18].

Table III below shows us the key length number of rounds and the required number of keys.

TABLE III. SUMMARY TABLE FOR KEYSAND ROUND

Key length	No. of rounds	No. of keys
128	10	11
192	12	13
256	14	14

The AES encryption consist of ten rounds. After the first key is added at round key 0.The initial 9 rounds are similar the only difference is on the final round. The first 9 rounds are made up of four changes. The last round does not have MixColumns change [20]. There are four straightforward steps named layers that are executed on the incoming data while performing the encryption process these are:

- ByteSub,
- ShiftRow.
- MixColumn and
- AddRoundKey.

B. AES Decryption

The four steps that are executed on encryption are reversed in a decryption structure. The decryption process is a follows:

- The InvShiftRow
- The InvByteSub
- Add RoundKey
- The InvMixColumn

C. AES Modification to Enhance Speed

AES is one of the fastest encryption scheme but it can be a bit slower when processing big data files. To minimise more calculation an AES was investigated and modified to lessen the calculation time of encryption and decryption. Lessening the calculation of the algorithm will improve the encryption performance. This led to development of a modified AES. The aim to modify AES is to lessen computation time but not compromising security of data. Modified AES algorithm provides improved encryption speed. AES has the block length data and the key length. The three alternatives are 128, 192, or 256 bits. We selected 128 bits key since it is the most applied in encryption of PLC. To defeat big calculation on encryption process the Mixcolumn step is skipped and the permutation is used. Other three junctures remain unchanged [17], [18].

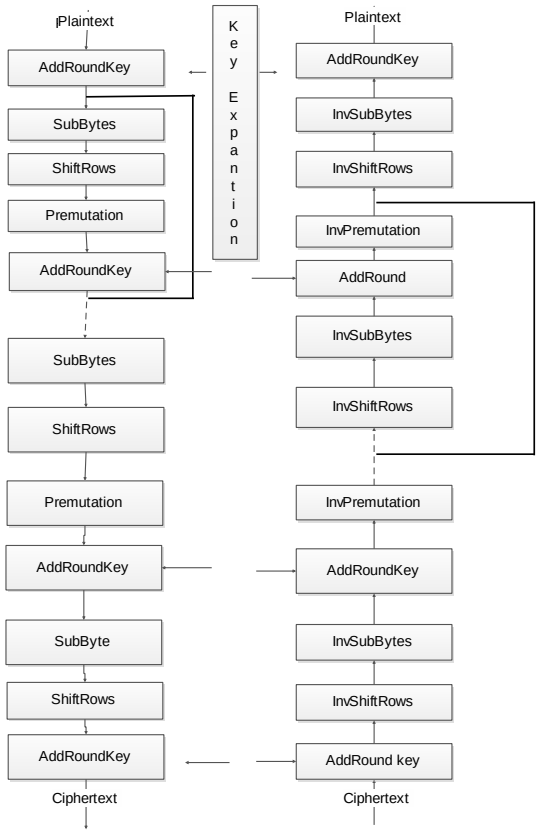

Fig. 8. Flowchart of Modified AES Algorithm [18].

D. AES Results and Analysis

We used OPNET and NetBeans 8.0.2 Java compiler to verify the efficiency of the modified AES encryption and decryption. Using this test analysis it shows that the modified AES is faster than the original AES. A few data sizes were simulated using AES and Modified AES and the results were compared.

The program was run on the Java compiler and the results are depicted below.

Start program

==Java==

Plain: test text ABC

Cipher: -104 48 9 29 -121 21 47 -114 -118 44 -25 25 -86 -109 -112 109

Decrypt: test text ABC

TABLE IV. ENCRYPTION AND DECRYPTION TIME

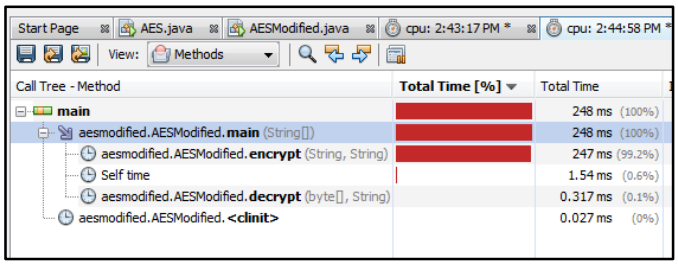

TABLE V. ENCRYPTION ANALYSIS TIME

file size	AES (ms)	Modified (ms)	Efficiency (ms)
16 bit	290	247	43

VII. COMPARISON OF AES CRYPTOSYSTEM WITH DES

Both AES and DES use block cipher scheme. The AES and DES use symmetric cryptosystems. Both encryption schemes make use of substitution tables called S-boxes. AES and DES encryption and decryption process are similar. Despite these resemblances of AES and DES, there are essential and important differences between their algorithms. The DES algorithm is based on the Feistel cipher arrangement. DES'uses 64-bit block size and 56-bit key length and it is attacked a lot as its key is too short to provide robust security. The AES algorithm on the other hand does not use Feistel cipher. AES has three layers, each with its own function. The AES also is 128-bit block twice the length used by DES and is represented by 4 x 4 array of bytes. Another difference between these two is rounds required. DES needs 16 rounds and the AES needs 9, 11 or 13 rounds. For a 128-bit block and a 128-bit key, no attacks were found for more than six rounds. Three additional rounds, and final round, were added for security enhancement on AES [22].

VIII. CONCLUSION

The AES algorithm is an enhancement security over the DES and other cryptosystem. The AES offers a very high level of security efficiency. Though AES will need improvements to keep up with current threats AES will still be strong for decades to come. Due to AES flexibility and variable length block of 128, 192 or 256 bits it is possible that in future, the AES block size be stretched beyond 128, 192 and 256 bit length. AES is a modern block cipher and it provides excellent long term security against brutal force attacks. AES is efficient in software and hardware. Concluding AES is the best solution for PLC security [22], [23].

References

[1] S. Galli, A. Scaglione, and Z. Wang, "For the grid and through the grid: The role of power line communications in the smart grid," *Proceedings of the IEEE*, vol. 99, pp. 998-1027, 2011.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 5-20, 2013.

[3] A. A. Atayero, A. Alatishe, and Y. A. Ivanov, "Power line communication technologies: modeling and simulation of PRIME physical layer," in *World Congress on Engineering and Computer Science*, 2012, pp. 931-936.

[4] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews*, vol. 15, pp. 2736-2742, 2011.

[5] S. Elyengui, R. Bouhouchi, and T. Ezzedine, "The Enhancement of Communication Technologies and Networks for Smart Grid Applications," *arXiv preprint arXiv:1403.0530*, 2014.

[6] V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, *et al.*, "Smart grid technologies: communication technologies and standards," *Industrial informatics, IEEE transactions on*, vol. 7, pp. 529-539, 2011.

[7] G. Ren, S. Qiao, H. Zhao, C. Li, and Y. Hei, "Mitigation of periodic impulsive noise in OFDM-based power-line communications," *Power Delivery, IEEE Transactions on*, vol. 28, pp. 825-834, 2013.

[8] M. Götz, M. Rapp, and K. Dostert, "Power line channel characteristics and their effect on communication system design," Communications Magazine, IEEE, vol. 42, pp. 78-86, 2004.

[9] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," Communications, IEEE Transactions on, vol. 50, pp. 553-559, 2002.

[10] K. Adak, J. Mohamed, and S. H. Darapuneni, "Advanced Metering Infrastructure Security," ed: Technical report, University of Colorado, Boulder, 2009.

[11] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473-484, 2014.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *Communications Surveys & Tutorials, IEEE*, vol. 14, pp. 998-1010, 2012.

[13] J. Benoit, "An Introduction to Cryptography as Applied to the Smart Grid," *Cooper Power Systems*, 2011.

[14] S. Hameed, F. Riaz, R. Moghal, G. Akhtar, A. Ahmed, and A. G. Dar, "Modified Advanced Encryption Standard For Text And Images," *Computer Science Journal*, vol. 1, 2011.

[15] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *Proceedings of the 26th Annual Computer Security Applications Conference*, 2010, pp. 107-116.

[16] S. Fries, H. J. Hof, T. Dufaure, and M. G. Seewald, "Security for the Smart Grid–Enhancing IEC 62351 to Improve Security in Energy Automation Control," *International Journal on Advances in Security Volume 3, Number 3 & 4, 2010*, 2010.

[17] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-8.

[18] P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, "Modified Advanced Encryption Standard," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 4.

[19] H. Alanazi, B. Zaidan, A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "*New Comparative Study Between DES, 3DES and AES Within Nine Factors*," *arXiv preprint arXiv:1003.4085*, 2010.

[20] U. Kretzschmar, "AES128–AC Implementation for Encryption and Decryption," *TI-White Paper*, 2009.

[21] S. M. Wadi and N. Zainal, "Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption," *Procedia Technology*, vol. 11, pp. 51-56, 2013.

[22] M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric algorithm survey: a comparative analysis," *arXiv preprint arXiv:1405.0398*, 2014.

[23] S. Ju, M. Choi, C. Kim, and Y. Lim, "Security Architecture for Advanced Metering Infrastructure," *Advances in Computer Science: an International Journal*, vol. 2, pp. 71-75, 2013.

Zephania Philani Khumalo (Pr Tech Eng) He was born on 06 January 1978 in KZN South Africa. He is currently a Masters of Engineering student at Durban University of Technology. He received his Bachelor of Technology Degree in Electronic Engineering in the year 2013 from Durban University of Technology. His research interests are in the fields of Smart Grids, Data Security, SCADA Systems, Artificial Intelligence, Power Line Communications, and Cryptology.