Security Scheme for IoT Environments in Smart Grids

Sebastián Cruz-Duarte(✉), Marco Sastoque-Mahecha,
Elvis Gaona-García, and Paulo Gaona-García

Faculty of Engineering, Universidad Distrital Francisco
José de Caldasé de Caldas, Bogotá, D.C., Colombia
{scruzd,mssastoquem}@correo.udistrital.edu.co,
{egaona,pagaonag}@udistrital.edu.co

Abstract. The following paper proposes a security scheme applied to Smart Grids, using different security mechanisms to comply with confidentiality, authentication, and integrity aspects in a grid implemented with Raspberry Pi 3 nodes. The study presents the evaluation of different encryption modes to establish the final parameters in the construction of a security scheme, satisfying NTC 6079 specified requirements for smart grids infrastructure based on metric comparison developed on various performance criteria.

Keywords: Cyber security · Confidentiality · Integrity · Authentication
Smart grids · IoT · Encryption

1 Introduction

As for IoT and Smart Grids technologies, security is a key factor due to the type of information handled and the existing vulnerabilities in the communication protocols. New concepts in recent years in the world of information such as the Internet of Things (IoT) and smart grids in general entail the redefinition of standards for the coupling of new functions associated with the world of information and communication. This set of standards includes security in data transmission as it plays a fundamental and basic role in the acceptance of new technological approaches.

Smart Grids aim to improve the capabilities of today's grids by seeking to increase their efficiency in three fundamental aspects: capacity, reliability, and efficiency of the grids. However, this integration creates a new set of vulnerabilities caused by cyber intrusion and corruption, which can lead to devastating physical effects and large economic losses.

Based on the set of technical standards described in NTC 6079 [1], three basic security principles are defined to be considered when designing a security system in electricity distribution networks, namely: confidentiality, integrity, and authentication. Based on these requirements, the following study presents the development of a security schema implemented in Python that is applicable to IoT and Smart Grids environments based on the TCP/IP model as a case study. The system was implemented on a communication environment composed of several Raspberry Pi 3 devices with a Quad Core

Á. Rocha and M. Serrhini (Eds.): EMENA-ISTL 2018, SIST 111, pp. 269–281, 2019.
https://doi.org/10.1007/978-3-030-03577-8_30

1.2 GHz Broadcom BCM2837 64 bit CPU (ARM v7 rev 4 [v71]) processor, 1 GB RAM memory, and Raspbian - Linux Raspberry 4.4.38-v7+ operating system.

The rest of the article is organized as follows. Section 2 presents related research on the implementation of security mechanisms on IoT environments. Section 3 presents the methodology proposed for its development. Section 4 presents the security scheme defined for our study. Section 5 presents the results obtained. Section 6 analyzes the results obtained. Finally, Sect. 7 presents the conclusions and future research.

2 Related Research

Several works have been carried out to determine the advantages and disadvantages of the different algorithms of information encryption. Khalid, Rihan, and Osmar [2] propose a research study for the comparison between AES and DES encryption algorithms on MAC and Windows platforms. The results show performance with the use of the AES algorithm with an average data processing rate of 27.76 Kb/sec. on the Windows platform and 31.65 Kb/sec. on the MAC platform; this performance was higher than that obtained with the use of the DES algorithm with data processing performance of approximately 10.13 Kb/sec. and 31.65 Kb/sec., respectively. Rani and Mittal [3] seek to enhance the performance of the AES algorithm by using artificial intelligence techniques to adapt it to different development approaches within security systems. Laue et al. [4] seek a focus on the use of CSRNG to highlight the advantages of AES over other algorithms. Mahajan and Sachdeva [5] follow the same idea as they determined the superior performance potential of the AES algorithm over the DES and RSA algorithms through various simulation processes; this hypothesis was also developed by Alahmadi et al. [6]; Liu and Baas [7]; Masoumi and Hadi [8]; Liu, Xu, and Yuan [9]; and Hun, Hee, and Hong [10].

Sarika et al. [11] identified fundamental characteristics in the design of security systems: confidentiality, integrity, authentication, non-repudiation, and anonymity. Based on these security requirements, there are studies describing different models of attacks such as those conducted by Biryukov and Khovratovich [12] and Eder-Neuhauser et al. [13]. In these studies, the authors analyze different models of security breaches which serve as a basis for preparing countermeasures for attacks on Smart Grids.

3 Methodology

The research methodology used is based on an experimental and applied method, therefore the process comprise a first stage of study of variables, in this stage, main qualitative and quantifiably variables for metric evaluation of security scheme are established based on defined requirements, next stage is the choice of an experimental design and components of the system experimental replication of the proposed scheme on case study, after this comes a stage of data processing and recollection, to identify through a parametric analysis on defined variables the final design of the system and its different parameters, with a successive evaluation of proposed scheme performance, finally an analysis of experimented results is presented and compared to similar approaches.

Therefore, before the scheme approach, the general operation description used to carry out the development of the security scheme is presented below.

3.1 General Description of the Scheme

The proposed scheme aims to meet the requirements of confidentiality, authentication, and integrity of information in a grid where the sending of messages is essential for its functioning.

The scheme is based on a client-server architecture, where each node is represented by a Raspberry Pi 3. This is performed to centralize the distribution of keys for the encryption and decryption of messages between each node of the grid as shown in Fig. 1.

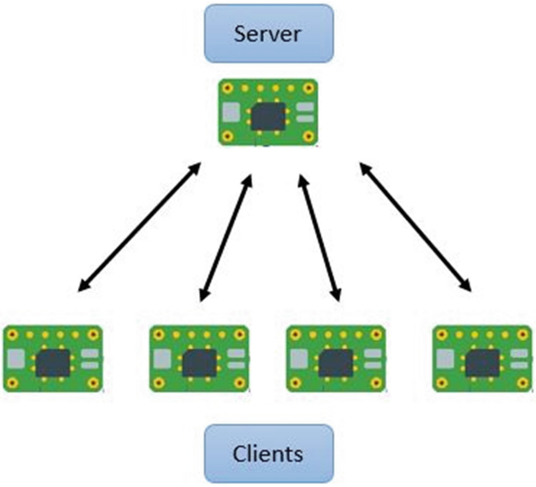

Fig. 1. General architecture of the proposed security scheme.

In order to determine the validity of this communication model, the following series of stages are proposed: (1) IP connectivity verification. Initially, the IP address of the client sending the request is verified in a whitelist on the server, where each IP address authorized to perform encryption key requests to the server is specified. All IP address connections that are not in the list are rejected. (2) Implementation of encryption algorithms. The confidentiality of the information sent and received by each node in the grid is integrated by applying the AES symmetric encryption algorithm to encrypt and decrypt messages sent between every node and by using digital signatures and encryption through the asymmetric RSA algorithm. (3) Communications channel encryption. This can be solved through the TSL/SSL application with a security certificate that allows all the data passing through the communications channel to be encrypted. 4) Verification of integrity of the communications channel. In order to comply with the data integrity requirement, HMAC was applied; this code works with a message authentication code (MAC) to ensure, by means of a hash function and a key, that the message sent has not been intercepted or modified on the way to its destination.

Finally, once the previous work phases have been determined, all activity is recorded in a log file that can be found on both the client and the server.

3.2 Message Flow in the System

Figure 2 shows the message flow in the system between the client and the server.

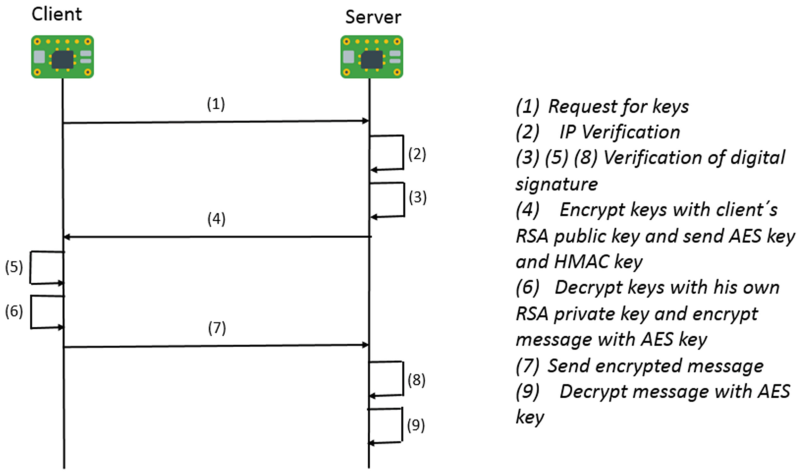
Client
Server
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(1) Request for keys
(2) IP Verification
(3) (5) (8) Verification of digital signature
(4) Encrypt keys with client´s RSA public key and send AES key and HMAC key
(6) Decrypt keys with his own RSA private key and encrypt message with AES key
(7) Send encrypted message
(9) Decrypt message with AES key

Fig. 2. Message flow in the security scheme.

(1) The client sends a request to the server to send the two keys: the key of the symmetric AES algorithm, required to encrypt the message; and the key of the HMAC to verify the integrity of the sent message. This request message is digitally signed by the client.

(2) The server verifies that the IP from which the request is being made is in its whitelist. If the IP is verified, it continues with the system flow. Otherwise, the request is rejected and the connection is closed.

(3) The server verifies the digital signature of the client request message.

(4) The server sends the requested keys, encrypts them with the client's public key through the RSA asymmetric algorithm, and sends them to the client through a message that is digitally signed.

(5) The client verifies the digital signature of the message sent by the server.

(6) The client decrypts the received message containing the keys with its private key using the RSA algorithm, encrypts the data to be sent with the AES key received, and generates the message authentication code (MAC) through HMAC with the second key received.

(7) Based on the encrypted message and the MAC generated in the previous step, a message that is digitally signed is created and sent to the server.

(8) The server verifies the digital signature of the message sent by the client.

(9) The server verifies the integrity of the message received through the MAC generated by the client and finally decrypts the sent message.

Each step described above is recorded in a log file located on both the server and the client. In case the verification of the digital signature of any of the messages fails, the connection is closed.

4 Proposed Security Scheme

4.1 Authentication

One of the ways to guarantee the authentication of an entity is through digital signatures and a whitelist that consists of a registry of entities that have access to a service, privilege, among others. It is possible to ensure that each client in the grid is authenticated by the server and vice versa by applying these two methods. In most cases, digital signatures are used to ensure the integrity and authentication of messages, and their applications range from email to bank funds transfers [18].

RSA is an asymmetric cryptographic system, the first of its kind, named after its creators Robert Rivest, Adi Shamir, and Leonard Adleman [19].

Within the system, each node in the grid has its own RSA key pair, and the client knows the public key of the server and vice versa. With its own private key, each sender signs the message to be sent, and the receiver, knowing the sender's public key, the message signature, and the signed message, verifies the message received, as specified in RFC 8017 [20]. Figure 3 shows the process of signature and verification.

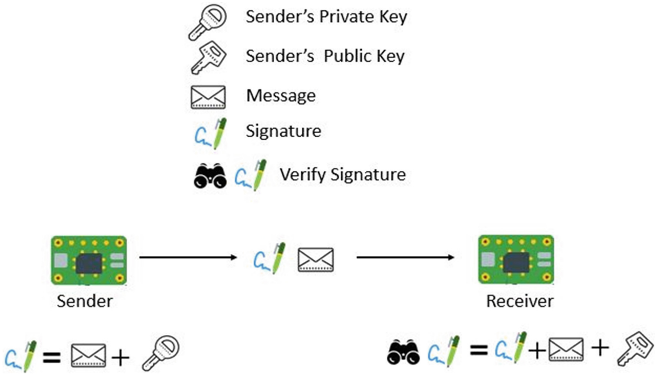

Fig. 3. Signature scheme and verification of digital signatures.

Whitelist is a concept of cyber security that is used to ensure the authentication of users or entities and to control access services. The proposed system implemented a whitelist of IP addresses that have permission and are authorized to make requests for security keys and send messages to the server. This whitelist is encrypted and used every time the server receives a message.

4.2 Integrity

Integrity in cyber security is the ability to guarantee the flow of information without alterations, so the structure of messages received is exactly the same as that of messages sent from one point. For this purpose, hash functions are used to generate authentication codes [14].

HMAC represents a message authentication code obtained through a hash key, calculated through a cryptographic hash function from a secret key [15]; for the specific case of this study, the selected hash function is SHA-256. This is one of the most recommended because of its performance [16] (see Fig. 4.).

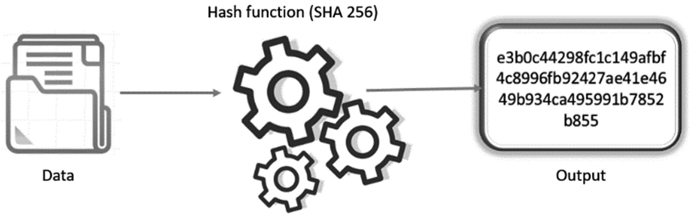

Fig. 4. Transformation scheme with SHA 256.

4.3 Confidentiality

This security requirement is met by applying TLS/SSL protocol and AES and RSA algorithms. The TLS/SSL protocol is a basic element of the confidentiality service in security systems [17]. SSL certificates are used to ensure the main characteristics of confidentiality in security systems in information transmission.

In the proposed security scheme, AES is used with a 256-bit key to encrypt and decrypt the messages that the nodes of the grid send to each other.

In the proposed security scheme, hybrid cryptography is used to distribute the AES and HMAC key from the server to the clients. Its operation is described below:

(1) The server encrypts the AES key by means of the RSA algorithm with the customer's public key.
(2) The server sends the encrypted key to the client.
(3) The client receives the key and decrypts it through RSA with its private key.
(4) Finally, the client encrypts the message to be sent through AES with the key it received from the server.

This is intended to ensure that the distribution of the AES algorithm key is secure and confidential.

5 Results Obtained

5.1 Performance in RSA and AES

The choice of the encryption algorithm to meet the needs of the security scheme is based on the performance comparison between AES and RSA.

Figure 5 shows the difference between the AES and RSA algorithms in terms of performance. Since AES is much faster, it is the selected algorithm.

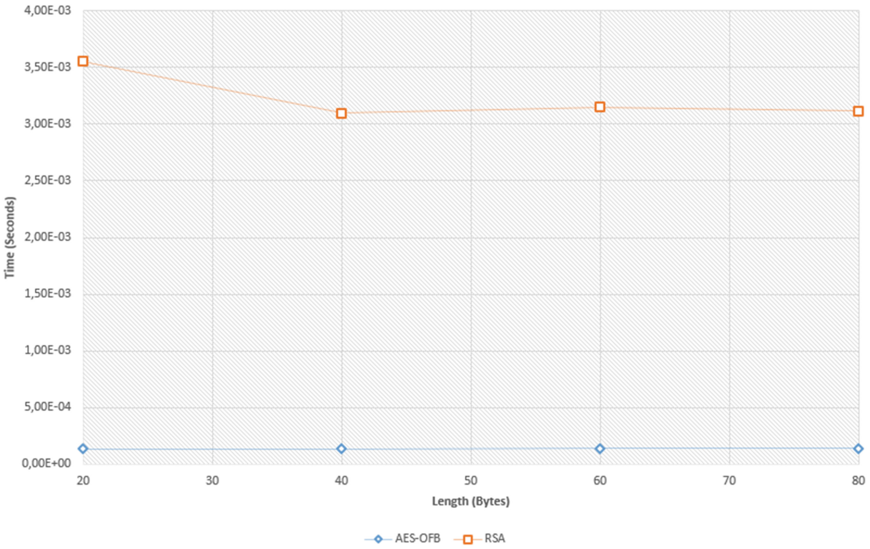

Fig. 5. AES symmetric encryption OFB vs. asymmetric encryption RSA (encryption process).

To define the AES algorithm scheme to be used, six operating modes (ECB, CFB, CBC, OFB, CTR, and OPENPGP) are compared qualitatively (see Fig. 6) within a range of values from 20 bytes to 400 bytes.

Figure 6 shows that the OFB encryption mode has the highest performance for the exposed range. Equation (1) defines the behavior of the OFB mode in relation to the data length with linear behavior.

$$t = 2.08 * 10^{-6} b + 2.18 * 10^{-6} \tag{1}$$

Where t represents the time in seconds of message encryption and b represents the size in bytes of the encrypted data.

Based on the procedures for encryption, the analysis of the decryption process is done with the range from 20 to 400 bytes. According to the graph that represents the behavior of the algorithm (See Fig. 7), the behavior is similar to that observed in the encryption process, so the OFB mode has the highest performance for small length messages.

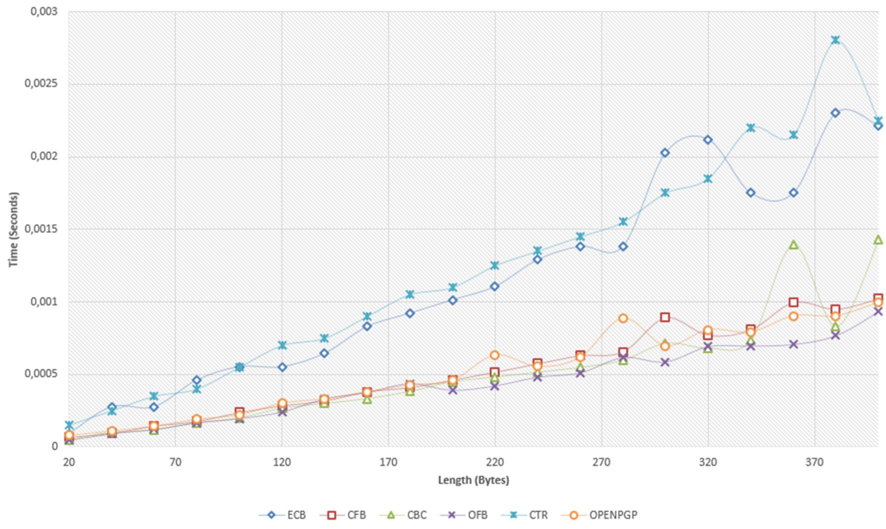

Fig. 6. AES encryption modes for small data lengths

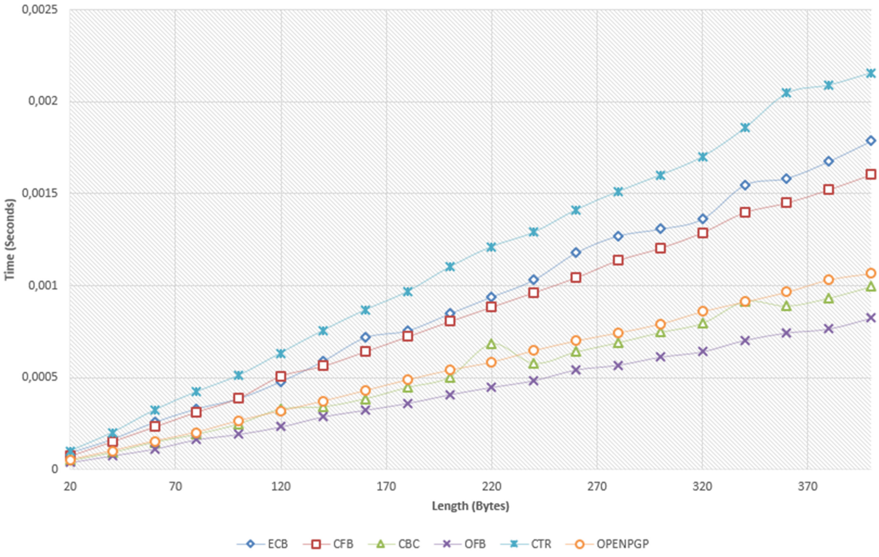

Fig. 7. AES decryption modes for small data lengths

Equation (2) describes the decryption process for small data lengths using OFB mode.

$$t = 4.5 * 10^{-6} b - 3.01 * 10^{-5} \tag{2}$$

Equation (3) describes the behavior in terms of speed in the process of encrypting and decrypting the information.

$$t = 4.15 * 10^{-6} b - 4.31 * 10^{-6} \tag{3}$$

6 Analysis of the Results

According to the parameterization of the encryption system for the confidentiality section within the designed security scheme, the AES encryption algorithm is the symmetric algorithm responsible for meeting the security needs based on its significantly superior performance compared to RSA. As for AES, a higher efficiency in the encryption process is determined with the use of the OFB mode; the approximate performance is 511,688.9127 bytes/sec. for message lengths of less than 100 bytes (see Fig. 8), while in the decryption process its performance is 517,570.3913 bytes/sec. for messages of the same length. When sending messages of longer length, the ECB mode has shorter processing times than those obtained with the OFB method. However, due to the security system requirements, the ECB mode is ignored.

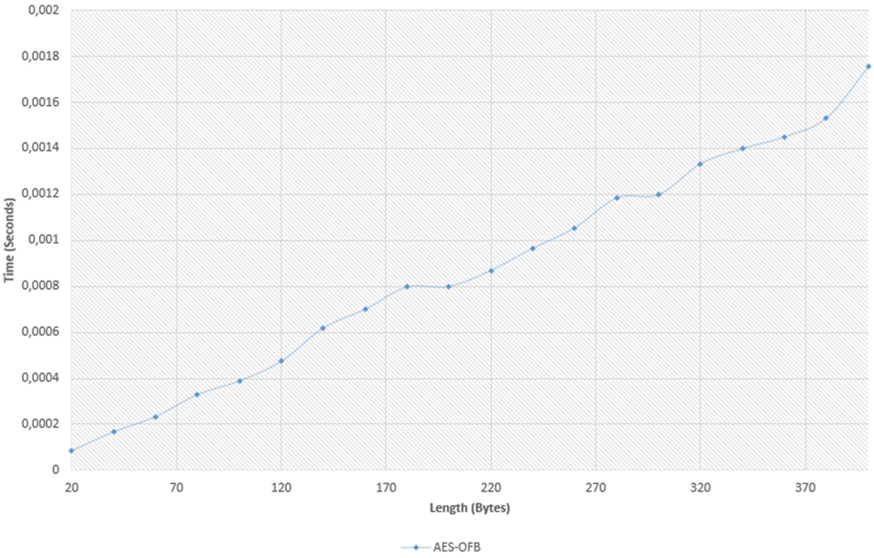

Fig. 8. Behavior of the AES-OFB encryption and decryption process

Using the security scheme proposed through the analysis of the unitary specifications of confidentiality, integrity, and authentication, it is possible to determine the design parameters of the security system with AES encryption algorithm, OFB mode, SHA.256 hash function, use of SSL protocol, and security certificate with digital signature. The system behavior for the total process of data processing and transfer presents constant behavior because the processing times for small information lengths are practically insignificant compared to the data transfer time between the system nodes.

The final average performance obtained for the encryption and decryption process with the AES algorithm in OFB mode is approximately 511,688.9127 bytes/sec. and 517,570.3913 bytes/sec., respectively. As for the transmission of data between the nodes of the grid, including all the processes specified within the study, the performance of the system is 213.43 bytes/sec., which is marked mainly by the times of data transmission.

Within the grid architecture scheme in which the security system is developed, the processing times are very short, so for small data ranges the information transmission time is not significantly altered; its behavior is constant due mainly to the data transfer time as shown in Fig. 9.

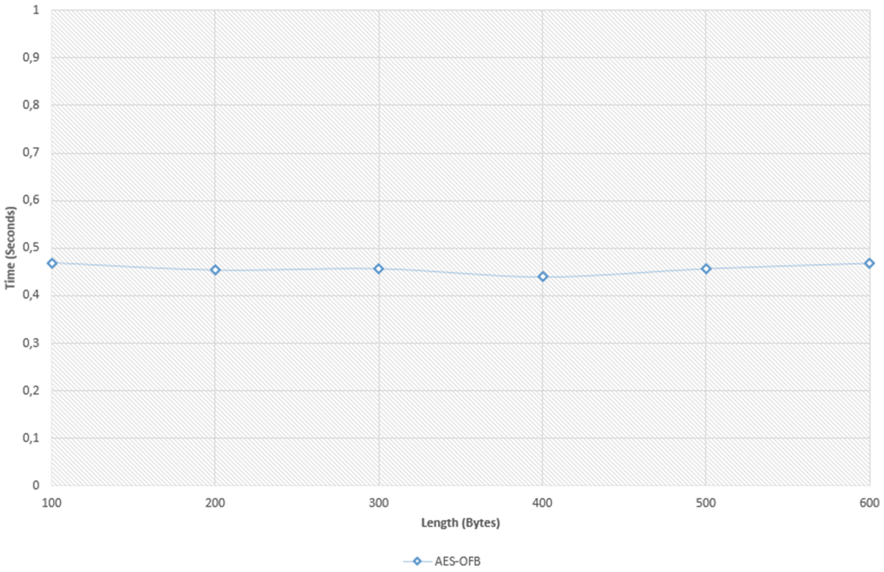

Fig. 9. Behavior of the system when sending information in relation to the change in the length of data sent

The proposed design considers the development of the security scheme in an environment of sending messages of no more than 100 bytes. Thus, the estimated processing time based on the function determined in (3) is approximately $3.88 * 10^{-4}$ sec. with the use of an OFB encryption mode in AES, which presents a higher performance than RSA encryption within the tests performed. For the length of messages specified within the context of this paper, the final evidenced performance of the security scheme, including confidentiality, integrity, authentication, and data transfer services, is approximately 213.43 bytes/sec. However, this performance is determined to a large extent by the characteristics of the information channel and the infrastructure of the grid. The performance review in terms of encryption and decryption of information is represented by an approximate value of 257,306.4239 bytes/sec.

6.1 Comparison to Other Designs

Few papers have been worked with similar approaches where different security mechanisms are used together, however, there are some studies which can be compared in nearly aspects as [21] and [22] where AES study is developed. In [21] an AES implementation is applied with a final performance around 434,000 bytes/sec for encryption process and 482,000 bytes/sec for decryption process. Therefore, the implemented security scheme is approximately 17.74% and 7.05% faster for the encryption and decryption process respectively, using AES OFB mode.

Compared to experimental results showed in [22], our scheme is significantly faster using a similar model for AES data encryption. However, the experimental scenarios are distinct because software platforms used in mentioned paper are Windows and Mac.

7 Conclusions and Future Research

The experimental results of this paper concludes that the message flow performance in the study case is not significantly affected by the proposed security scheme, therefore, it is suitable for smart grids and IoT environments.

Also results determine that AES is the most efficient in comparison to other cypher algorithms and its OFB mode is faster than the others modes in execution time for data length of no more than 100 bytes.

Finally, the security scheme satisfies the NTC 6079 specified security requirements (integrity, authentication and confidentiality) through the implementation of SSL certificates, symmetric and asymmetric encryption algorithms, hash functions and digital signatures.

As future research, the scope of the proposed scheme should be extended to include the principle of security of availability in order to meet the need to protect information in the face of the imminent growth in the use of IoT technologies. Another future study proposed is aimed at the size of the data processed and transmitted within the case study of this paper in order to expand the application scenarios where the proposed security scheme can be adapted.

Acknowledgment. This work was supported by COLCIENCIAS with the project entitled “Low and Medium capacity battery charger with low current THD, high power factor and high efficiency for electric vehicles” and GITUD research group.

References

1. NTC 6079: Requisitos para sistemas de infraestructura de medición avanzada (ami) en redes de distribución de energía eléctrica. ICONTEC
2. Rihan, S.D., Khalid, A., Osman, S.E.F.: A performance comparison of encryption algorithms AES and DES. Int. J. Eng. Res. Technol. IJERT **4**(12), 151–154 (2015)
3. Rani, H.M.S., Mittal, D.H., Director, S.: A compound algorithm using neural and AES for encryption and compare it with RSA and existing AES. J. Netw. Commun. Emerg. Technol. JNCET **3**(1) (2015)
4. Laue, R., Kelm, O., Schipp, S., Shoufan, A., Huss, S.A.: Compact AES-based architecture for symmetric encryption, hash function, and random number generation. In: International Conference Field Programmable Logic and Applications, FPL 2007, pp. 480–484 (2007)
5. Mahajan, P., Sachdeva, A.: A study of encryption algorithms AES, DES and RSA for security. Glob. J. Comput. Sci. Technol. (2013)
6. Alahmadi, A., Abdelhakim, M., Ren, J., Li, T.: Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Trans. Inf. Forensics Secur. **9**(5), 772–781 (2014)
7. Liu, B., Baas, B.M.: Parallel AES encryption engines for many-core processor arrays. IEEE Trans. Comput. **62**(3), 536–547 (2013)
8. Masoumi, M., Rezayati, M.H.: Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis. IEEE Trans. Inf. Forensics Secur. **10**(2), 256–265 (2015)
9. Liu, Q., Xu, Z., Yuan, Y.: High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion. IET Comput. Digit Tech. **9**(3), 175–184 (2015)
10. Baek, C.H., Cheon, J.H., Hong, H.: White-box AES implementation revisited. J. Commun. Netw. **18**(3), 273–287 (2016)
11. Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.: Security issues in mobile ad hoc networks. Procedia Comput. Sci. **92**, 329–335 (2016)
12. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 1–18 (2009)
13. Eder-Neuhauser, P., Zseby, T., Fabini, J., Vormayr, G.: Cyber attack models for smart grid environments. Sustain. Energy Grids Netw. **12**, 10–29 (2017)
14. Krawczyk, H., Canetti, R., Bellare, M.: HMAC: keyed-hashing for message authentication (1997)
15. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In: Annual International Cryptology Conference, pp. 1–15 (1996)
16. Yung, M., Lin, D., Liu, P.: Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, 14–17 December 2008, Revised Selected Papers. Springer Science & Business Media (2009)
17. Rescorla, E.: SSL and TLS: Designing and Building Secure Systems, vol. 1. Addison-Wesley, Reading (2001)
18. Fei, P., Shui-Sheng, Q., Min, L.: A secure digital signature algorithm based on elliptic curve and chaotic mappings. Circ. Syst. Signal Process. **24**(5), 585–597 (2005)
19. Somsuk, K., Thammawongsa, N.: Applying d-RSA with login system to speed up decryption process in client side. In: IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS), pp. 1–5 (2017)

20. Moriarty, K., Kalisky, B., Jonsson, J., Rusch, A.: PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017 (2016)
21. Mahajan, P., Sachdeva, A.: A study of encryption AES, DES, and RSA for security. Global J. Comput. Sci. Technol. Netw., Web Secur. (2013)
22. Khalid, A.: A performance comparison of encryption algorithms AES and DES. Int. J. Eng. Res. Technol. (2015)