FPGA Implementation of GPS Location Based Secured Data Accessing System

Fazal Noorbasha, M. Sai Devansh, M. Vinay Kumar, A. Surya Kiran, G. Sree Pavani, K Hari Kishore

Abstract: ***Now a day's Field Programmable Gated Array (FPGA) are advanced architectures for various cryptographic systems and algorithm applications. Due to the reprogrammable flexibility of FPGAs, the advanced cryptographic algorithms are exploited to achieve high throughputs at the expense of very low chip area. The security can be improved by using standardized and proven-secure block ciphers like advanced encryption standard (AES). In this paper, we had designed our hardware optimization strategies for AES for high-speed, low-power algorithm for IoT applications with multiple levels of security. Main objective of action includes having user location data in the form of latitude/longitude followed by incorporating that with a randomly generated key for encryption. Receiver can only access the data of the host system and decrypt the cipher text only if the location coordinates and keys are matched.***

Keywords: AES, GPS Location, Data, FPGA, Verilog HDL.

I. INTRODUCTION

Date security is very crucial now a days for the entire private and government organizations. For data security we are using different type of cryptography algorithms [1]. When any organization transmits interactive media information, for that data the cryptography system gives security. Cryptography in such a way that make sure of availability, integrity, identification, confidentiality, authentication of user and as well as privacy of data can be provided to the user [2]. Consequently, this paper shows an equivalent security in cryptosystem by Advance Encryption Standard Using FPGA design process [3]. Proposed encryption standard is an affirmed cryptographic algorithm that can be utilized to ensure electronic information. AES is a symmetrical calculation of encoding planned to supplant DES which had just demonstrated certain issues of security in the information protection [4]. We propose this advanced AES block cipher for rising IoT proposals, such as IEEE 802.15.4 [5].

The level of security depends on different IoT applications and may require different security levels with different throughputs and various power/energy budgets [6].

Revised Manuscript Received on April 14, 2019.

Fazal Noorbasha, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
M. Sai Devansh, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
M. Vinay Kumar, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
A. Surya Kiran, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
G. Sree Pavani, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
K Hari Kishore, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India

At the algorithmic stage, security level decides the type of algorithm and key length [7]. With three different key sizes AES supports multiple security levels [8]. By using this AES algorithm we had proposed a modified cryptography process for secured data accessing process. It depends on the key and the user GPS location.

II. PROPOSED CRYPTOGRAPHY ALGORITHM

Enhancing security at high level has been the prime objective of our research, under which have used the following steps.

1. User Location coordinates
2. AES Cryptography
3. Matching Location with given coordinates
4. Decryption through Key and User location coordinates

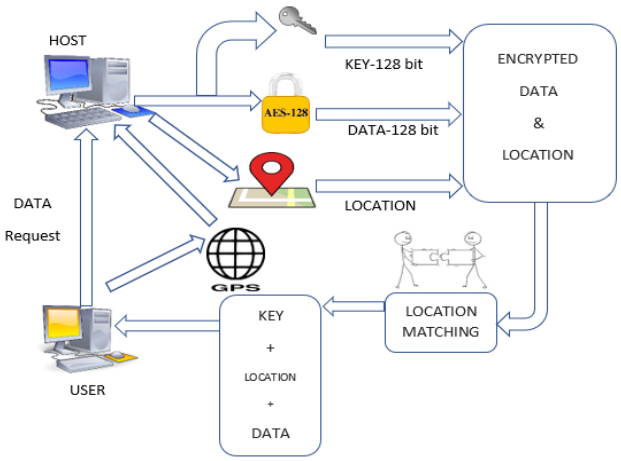

Fig. 1 Proposed Cryptography Block Diagram

Fig. 1 shows the process taking place here all the way from a user requesting data to receiving it safely. Initially, user requests data, which reaches the host or moderator. The work of the host is to maintain location check, encrypt location data as well as the requested data by the User with the help of a key which needs to be sent to the user too [9]. This is done with the help of AES cryptography algorithm.This algorithm is be used the three different key lengths stated above, and as a result these different "flavours" are referred to as AES-128, AES-192, and AES-256 [10]. Once the encryption is complete, the data will be in channel enroute to the User, which upon a match on the Location data will reach the User. Upon receiving the data, the User shall need the Key, the very key used in Encryption to be able to Decrypt the data else the data will as good as corrupted.

Step 1: User requests data to the host from a location.
Step 2: Host receives request as well as location coordinates or the user.
Step 3: Making use of AES algorithm, host encrypts the requested data; Location coordinates and sends them along with a Key.
Step 4: User needs to be matched upon which the User receives the data, key and location coordinates.
Step 5: If the right key and location coordinates are matched, data decryption happens else data will not decrypt.

Global Positioning System

As known, the importance for Authenticity, Integrity of the data increases with the increase of hackers day by day, being able to break into the security features available [11]. In one such attempt to secure the GPS locations of say a data transfer systems which are a Sender and a Receiver, were proposing this system to be able to provide aneven enhanced Encryption/Decryption system in an attempt to secure data from both aspects such as Location and data in channel respectively [12].

Advanced Encryption Standard (AES)

We proceed onward to examine about the ongoing alterations that have been done on the AES conspire and their shortcomings. AES comprises of 128 square lengths of bits and backings 128, 192 and 256 key length bits. A AES comprises of four changes: Byte Substitution (subbytes), Row Shifting (shiftrows), Mixing of sections (mixcolumns) and pursued by expansion of Round Key called (addroundkey) [13]. From each cycle, a round key is produced from the first key through key booking Process. The last round comprises of subbytes, shiftrows and addroundkey change. Subbytes Transformation is actualized utilizing S-Box. The S-Box is a standout amongst the most tedious procedure since it is required in each round [14]. A changed Rijndael calculation and its usage utilizing fpga are given here. In this paper, an altered Rijndael calculation that performs encryption process through three ward stages is exhibited.

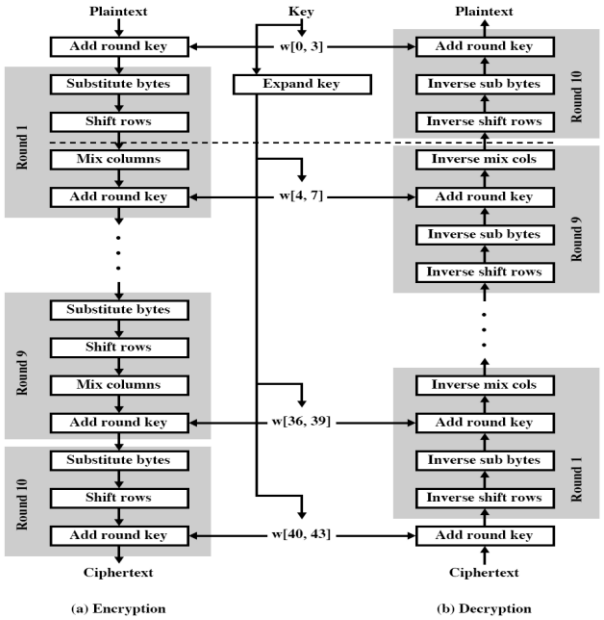

Fig. 2 Encryption and Decryption block diagram

Fig. 2 is showing our proposed AES based encryption and decryption process. By using this AES method we had encrypted the data and generating the key [15]. That encrypted data and key generation will done when the system received the user's position latitude/longitude position values. These values will received by GPS system. If GPS generates these values then the host system will send the encrypted data and key with the user GPS location.

III. FPGA SYNTHESIS AND RESULTS

Field Programmable Gate Arrays (FPGAs) are becoming a critical part of every digital system design. This proposed cryptography system design we have used Xilinx (Spartan-3- xc7a100t-3csg324) family. We have developed total hardware using Verilog HDL code. Figure 4 shows the RTL (FPGA) schematic view. The encryption and decryption FPGA device utilization is used as number of slice registers 5949, LUTs 5212, LUT-FF pairs 2707, IOBs 388, Block RAMs 20 and BUFG/BUFGCTRL 1. Speed grade is 3, maximum period is 5.105ns, maximum frequency is 195.875MHz, minimum input arrival time before clock is 3.009ns and maximum output required time after clock is 0.640ns. Fig. 3 shows the RTL schematic view of proposed cryptography system.

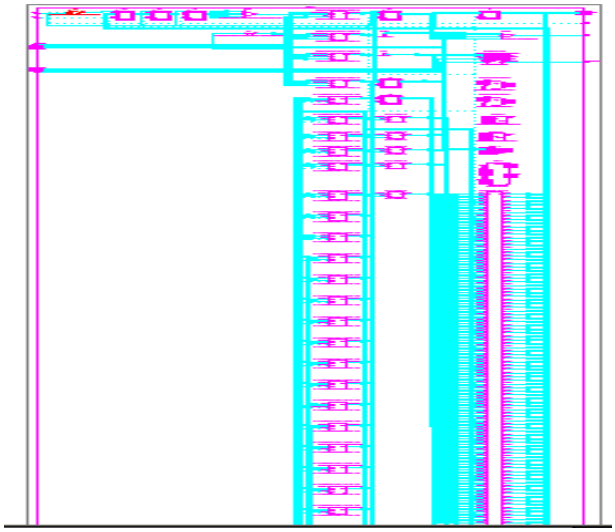

Fig. 3 RTL Schematic view of Proposed Cryptography system

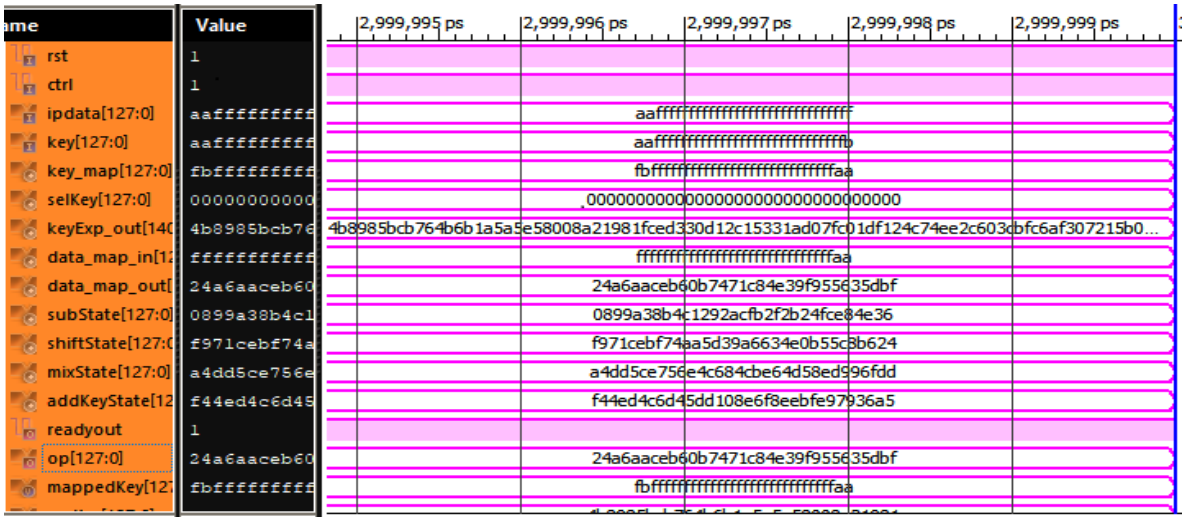

Fig. 4 Data encryption simulation timing diagram

Fig. 4 shows the data encryption simulation timing diagram, we have an encrypted output provided we give a key. The same key will be needed at the output end i.e., the user side in order to be able to decrypt and get the data back [16]. So, encryption has been done successfully and now the data can be sent through a channel with the user having the same key which was used for encryption. All the blocks are dependent with the Key and not being the same for all blocks. Instead of Feistel Network, Substitution Permutation network has been used ensuring more security.

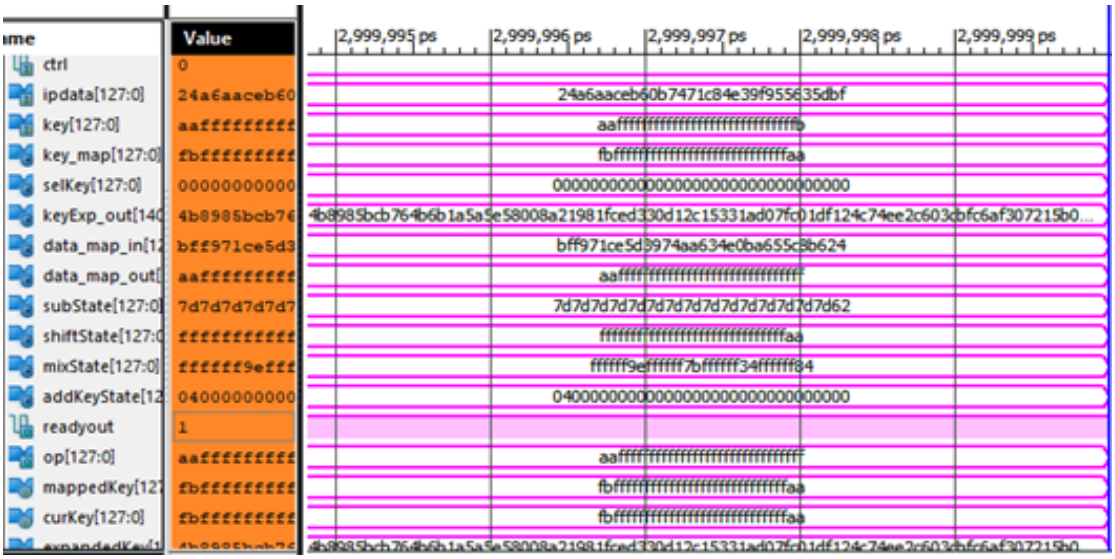

Fig. 5 Data decryption simulation timing diagram

Fig. 5 shows the data decryption simulation timing diagram the encrypted data is input for decryption and as said, the same key only will help decrypt the data for the user, which has been done in encryption side. Hence, the initial input has been obtained marking successful decryption done and data obtained. But the decryption will done when the location of the user is matched by the host received location of the user. Table 1 shows the power and timing report.

Table. 1 Power and Timing Report

Parameters (units)	Magnitude
POWER (mw)	810
TIME (ns)	5.105
Junction Temp (C)	26.1

IV. CONCLUSIONS

In this paper we have proposed a GPS Location Based Secured Data Accessing System using AES key, that increase complexity in each round thus it can increase the security. So that it gives the more efficiency and good accuracy. By using same security algorithm, we are optimizing the resource utilization. The total process is tested on FPGA Spartan 3 Kit. The total power consumed by cryptography module is 810mW. The memory utilization of encryption module is 782.5 MB with the gain of 483.3 as well as for the decryption module the memory utilization is 785.7 MB with the gain of 486.3. For online data transitions this algorithm secures the data.

Hackers cannot hack the data even if key an algorithm are known because user GPS location is one of the key factor.

REFERENCES

1. Qiang Li , Miaowen Wen , Yuekai Zhang, Jun Li , Fangjiong Chen , and Fei Ji , "Information-Guided Pilot Insertion for OFDM-Based Vehicular Communications Systems", IEEE Internet Of Things Journal, Vol. 6, No. 1, February 2019, PP. 26-37.
2. Antonio Marcos Alberti, Gabriel Dias Scarpioni, Vaner J. Magalhães, Arismar Cerqueira S., Jr., Joel J. P. C. Rodrigues, and Rodrigo da Rosa Righi, "Advancing NovaGenesis Architecture Towards Future Internet of Things", IEEE Internet Of Things Journal, Vol. 6, No. 1, February 2019, PP. 215-229.
3. Fazal Noorbasha, G. Jaswanth Varma, B. Ajani Kumar, Harikishore Kakarla, M. Manasa, "Data Security Based On DNA Cryptography Using S-Box Encryption", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 429-434.
4. Fazal Noorbasha, Harikishore Kakarla, Deekshatha.A, P.G.Mounika, N.Ganga Dheeraj, M. Manasa, "Implementation of Quarter Cycle Key Cryptographic Algorithm Using Verilog HDL", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 423-427.
5. Fazal Noorbasha, B. Anjani Kumar, G. Jaswanth Varma,Harikishore Kakarla, M. Manasa, "Data Encryption and Decryption Cryptography Using Modified AES Algorithm", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP.435-440.
6. Fazal Noorbasha, M. Manasa, R. Tulasi Gouthami, S. Sruthi, D. Hari Priya, N. Prashanth, And Md. Zia Ur Rahman, "FPGA Implementation Of Cryptographic Systems For Symmetric Encryption", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2038-2045, ISSN: 1992-8645.
7. M. Manasa, Fazal Noorbasha, Ch.L.Sudheshna, M.Santhosh, V.Naresh, Md. Zia Ur Rahman, "Comparative Analysis of CORDIC Algorithm and Taylor Series Expansion ", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2015-2022, ISSN: 1992-8645.
8. Upputuri Neelima, Fazal Noorbasha, "Data Encryption and Decryption using Reed-Muller Techniques", International Journal of Engineering and Technology (IJET), ISSN : 0975-4024 Vol 8 No 1 Feb-Mar 2016, PP. 83-91.
9. P. Santhamma, B. Raghavaiah, N. Suresh Babu, "Implementation of Pipelined DES using Verilog", International Journal of Computer & Communication Technology, Volume – 3, Issue – 5, 2012.
10. Dr. Ananathi Shesashaayee, D Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2014, PP 6193-6201.
11. Dilovan Asaad Zebari, Habibollah Haron, Subhi R. M. Zeebaree, Diyar Qader Zeebaree "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations", International Conference on Advanced Science and Engineering (ICOASE), Vol.978(1), PP.312-317,2018.
12. Wenting Yuan, Xuelin Yang, Wei Guo, Weisheng Hu, "A double-domain image encryption using hyper chaos" 19th International Conference on Transparent Optical Networks (ICTON), 2017, PP. 1-4.
13. J. S. Park, K. S. Bae, C. Y. Choi, D. H. Choi, and J. C. Ha, "A fault resistant implementation of AES using differential bytes between input and output," Journal of Supercomputing, vol. 67, no. 3, pp. 615-634, Mar. 2014.
14. Abdullah, A. M., and Aziz, R. H. H. "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm", International Journal of Computer Applications, Vol. 143, No.4, 2016, June, pp. 11-17.
15. N Sivasankari, K Rampriya and A Muthukumar ," Implementation of Area Efficient 128-bit Based AES Algorithm in FPGA", European Journal of Advances in Engineering and Technology, 2017, 4(7), PP 541-548.
16. Z Liu, L Li and X Zou, A Low-Cost Low-Power Ring Oscillator-Based Truly Random Number Generator for Encryption on Smart Cards, IEEE Transactions on Circuits and Systems II, 2016, 63 (6), PP 608-612.
17. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
18. Bindu Bhargavi, K., Hari Kishore, K. Low Power Bist on Memory Interface Logic (2015) International Journal of Applied Engineering Research, 10 (8), pp. 21079-21090.
19. Charan, N.S., Kishore, K.H. Recognization of delay faults in cluster based FPGA using BIST (2016) Indian Journal of Science and Technology, 9 (28).
20. Hari Kishore, K., Aswin Kumar, C.V.R.N., Vijay Srinivas, T., Govardhan, G.V., Pavan Kumar, C.N., Venkatesh, R.V. Design and analysis of high efficient UART on spartan-6 and virtex-7 devices (2015) International Journal of Applied Engineering Research, 10 (9), pp. 23043-23052.
21. Kante, S., Kakarla, H.K., Yadlapati, A. Design and verification of AMBA AHB-lite protocol using Verilog HDL (2016) International Journal of Engineering and Technology, 8 (2), pp. 734-741.
22. Bandlamoodi, S., Hari Kishore, K. An FPGA implementation of phase-locked loop (PLL) with self-healing VCO (2015) International Journal of Applied Engineering Research, 10 (14), pp. 34137-34139.
23. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.
24. A. Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian "Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints" IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
25. N Bala Dastagiri K Hari Kishore "A 14-bit 10kS/s Power Efficient 65nm SAR ADC for Cardiac Implantable Medical Devices" International Journal of Engineering and Technology (UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 34-39, March 2018.
26. N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
27. N Bala Dastagiri, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
28. Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
29. Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
30. P Bala Gopal, K Hari Kishore, R.R Kalyan Venkatesh, P Harinath Mandalapu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.
31. Avinash Yadlapati, Hari Kishore Kakarla **"**Design and Verification of Asynchronous FIFO with Novel Architecture Using Verilog HDL**"** Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No: 14, Issue No: 1, Page No: 159-163, January 2019.