*International Journal of Industrial Engineering*
*2021;5(1):7-11.*
***ISSN: 2456-8449***

# High Secure Communication FPGA Implementations of Data Encryption/Decryption

Balachandra Pattanaik[1*], G Suresh[2], P. Epsiba[2], G O Jijina[3]

[1]*Department of Electronics and Communication Engineering, Bule Hora University,Bule Hora, Ethiopia, Africa.*
[2]*Department of Electronics and Communication Engineering, Sri Indu College of Engineering & Technology, Sheriguda, Telangana, India.*
[3]*Department of Electronics and Communication Engineering, Arupadai Veedu Institute of Technology, Paiyanoor, Tamil Nadu, India.*

**Corresponding author: balapk1971@gmail.com*

**Abstract.** Cryptographic algorithms are essential for data transmitting and also allow for the execution of a wide range of key combinations and allows for creative. Rjindael's technique has been chosen as the Data Encryption Standard, and it will continue to be the most commonly used algorithm for data protection in encryption / decryption, as well as for electronically secured data transfer. Today, AES is the most extensively used symmetric method, and it works by converting user text to 'hex' numbers and then executing particular steps using the consumer key. Although among the most widely used algorithms, the Encryption standards has its own drawbacks, such as a fairly basic algebraic structure, the identical sequence of preset stages, and difficult-to-use software. To encrypt data for secure messaging with increased security characteristics, a contemporary authenticating algorithm which is based on the Cryptography Standards computational programme and Secured Hashing Algorithm techniques is developed. The Secured Hash Algorithm will be used in conjunction with the AES mechanism for secrecy, dependability, and integrity tests. The basic idea behind algorithm applications is to create a high level of data security by using Secured Hash Algorithm and Encryption standardized algorithm programmes in operating systems. To reliably send and receive information, the suggested model includes all transmitting and receiving parts. It was created with Xilinx ISE 14.7. As a consequence, the parameters of the suggested algorithmic programme may be compared with numerous distinct ways, and further parameter comparisons may result in satisfied outcomes.

**Keywords**: FPGA, ASIC, AES, DES, Cryptography.

## INTRODUCTION

Various keys can be used to encrypt information/data using a cryptographic technique. The security of a cryptographic system is determined not only by the encryption method, but also by the keys used for encryption. These keys, known as secret keys, are always kept secure from hackers. The key is an integral aspect of the encryption process, which is a key component of cryptography [1]. Because to channel imperfections, the sent data and/or key may get garbled at times. The data will not be retrieved if it is significantly altered or damaged; hence, the key must be transferred through a secure channel [2]. The frequency with which a cryptographic key is used is always directly proportional to how frequently the key should be updated. Encryption methods may be cracked using a computer, which has a high speed and enables the attacker to employ more combinations in a given amount of time [3]. Wireless communication is necessary in today's world, and practically all electronic transactions are conducted online. Encryption is the finest method for protecting the same and maintaining the privacy of the consumers owing to superior reaction even in the absence of advisory [4]. To improve security, also more keys are utilised or the duration of current keys is extended. Because overheads are continued to increase in both strategies, using sub-keys is indeed the best option [5]. Post are only used for nodes that have been compromised by a hacker. The sub keys are always generated from the primary key, which reduces overhead cost [6].

Encrypted funds and E-mails are critical requirements for all of the aforementioned firms, thus it is critical to safeguard the data from attackers. Electronic file transfer is employed in all current applications, including ATM card protection, computers password protection, and ecommerce [7]. Passwords are ineffective for this purpose owing to the narrow range, thus cryptography has a bright future because it can withstand a variety of assaults [8].

*Received: 10.12.2020 Revised: 08.01.2021 Accepted: 22.01.2021*

Confidential is the safeguarding of knowledge against disclosure. Secrecy might apply to entire communications, portions of messages, or even the presence of messages. The shielding of data transmission from passive assaults is referred to as secrecy [9]. The system is focused on ensuring the authenticity of a communications. It is the confirmation of a message's purported source.The confidentiality of data that cryptography can provide is useful not only for legal purposes including such trying to prevent knowledge crimes such as the trade secrets or the unauthorised loss of private health records, but also for unlawful purposes such as shielding a communication between the two terrorists trying to plan to blow up a construction from law enforcement authorities [10]. To accomplish the same goal, two ways can be used: visible ink for composing the text or sending the information through a private person, and the use of a scientific method known as "Cryptographic algorithms." The basic and traditional task of cryptology is to provide confidentiality through data encryption [11]. It is employed in applications found in technologically evolved civilizations, including as Card information security, computer password protection, and ecommerce.

## PROPOSED METHOD

Wider key lengths use more electricity and produce more heat. It is essentially a compromise between protection and overhead. Ongoing efforts are necessary to build a more secure system. A good encryption method should have two characteristics: a quick reaction time and a low level of complexity. By preserving the value of encryption algorithms in secure communication, it is preferable to optimise and/or enhance encrypting approaches, while bringing security overhead cost under limit [12].The digital communication here between staff and the customer should be encrypted so that no service provider may see the information that was transferred. The conversation's participants should additionally confirm that it has been interacting with the present recipient [13]. This necessitated the use of sophisticated cryptographic methods, as well as a dependable mechanism of sharing the recipient's encryption keys inside the business. Also, if it is ever used, the organization's security and privacy rules should account for and promote the use of more secure email [14].

Conventions Public key encryption provides a significant benefit by allowing the use of electronic certificates. Both digital and handwritten identities rely just on fact that it is extremely hard to identify two persons with the same signature digital signatures provide authentication and data integrity [15]. Anyone with connectivity to the signer's public key can validate the signature. In the realm of E-commerce, for instance, an order to the bank for move cash can be validated using an unique identifier.

To transport messages, many separate techniques for completing the final computation are utilised. Many parallel treatments are produced in order to calculate the patient's odds, and the info involved is spread out across all of them using a variety of methods. There are no standardized data, and if one process requires data maintained by another, the 2nd stage must provide it to the first. A protocol for transmitting an MPI message describes an MPI's technical procedures and regulations for sending messages[17]. The message is being processed by two traditional protocols: eager and appointing. Eager is a synchronisation procedure that necessitates a sending procedure to be finished without an acknowledgement. Encounter is a synchronized communication that requires appropriate reception recognition to be completed [18]. Because MPI allows the developer in concurrent MPI system can monitor that flow of information and the synchronisation of the process, challenge segmentation and processes coordinating face two writing challenges. The output of the source code is negatively influenced if proper coding is not used. An efficient FFT architecture is discussed in [19] using Kogge stone adder and a universal low power novel gate is designed in [20].

The transmitter and recipient use different keys to encrypt and decrypt the message in encryption key and encoded in key encryption [16]. When secret messages are conveyed from one end to the other, this encryption method approach is used. In most cases, extremely sensitive data is processed on a machine and sent through the Internet. As a result, ensuring the integrity of data has become a significant concern. The section that follows offers a collection of picture encoding and decoding algorithms.

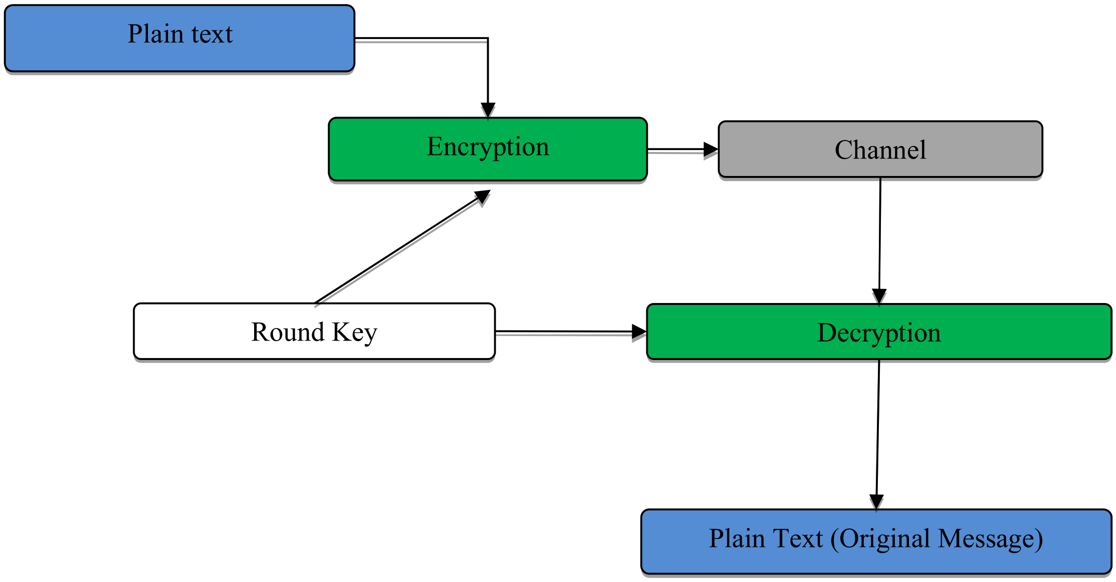

**FIGURE 1**. Proposed Encryption / Decryption Method.

Alternatively, if the current Receiver is required to convey sensitive information to the first Transmitter, of above procedures should indeed be reconfigured for the relevant Transmitting and Receiving task. As a result, the original study objective, the FPGA integration of safe transmitting data utilising cryptographically verification, can be accomplished very effectively, for all reasons, by the attempts of this dissertation, the use of FPGA forums on both the recipient and reciever of the transmitting data, provided that both recipient and reciever are aware of the Cipherkey utilised. The program's goal is to recognise and comprehend the cryptography requirements known as Encryption System, that also is among the most frequently applied and flexible symmetrical methodologies that could have been readily adaptable in the future to the strongest enclosures, as a result of the rapid evolution and key advancements in modern years.

## RESULTS AND DISCUSSIONS

There are several sorts of encryption algorithms as well as decryption algorithms. If the two individuals wish to interact with each other, private key communications must be used. On the other hand, if the data is being sent on a wide scale, both the organiser and the user should have the very own keys. It will solve this huge communication issues. The basic task of cryptography is to figure out how to handle keys. Keys must be handled while maintaining the encrypted strategy in mind. To enlighten, a trustworthy third party that will furnish the recipient with a replica key is there. However, this strategy weakens security because one additional person has access to the key. Each phrase in the stream of data must be transformed into binary throughout the encryption algorithm so that it may be X-ored with the key. The suggested scheme's data flow has been effectively applied. Figure 3 depicts a breakdown of the electricity produced by encrypting and decrypting.

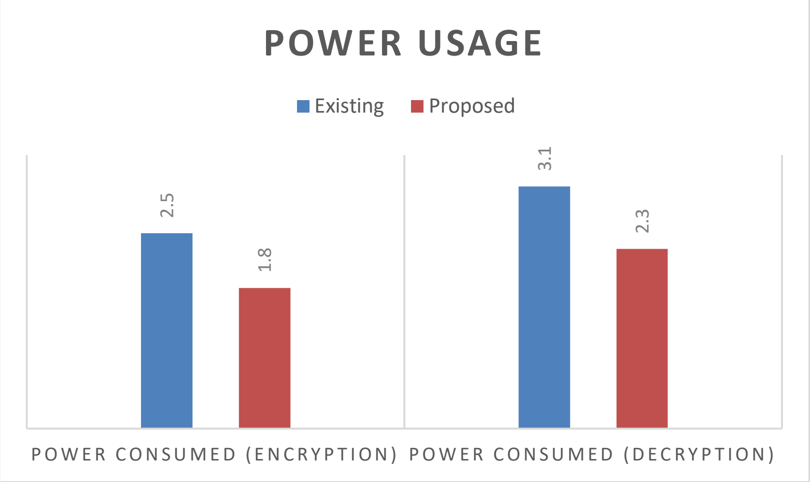

**FIGURE 2**. The Performance of Both Deployments.

Figure 2 illustrates the design of the modified AES algorithm, which is quicker than the regular Encryption and determined to be more power efficient. The encryption method. In order to ensure more security, data or information comprising letters is first transformed into the corresponding numbers, then to the corresponding binary form.

## CONCLUSION

Cryptography algorithmic approaches make it simple to secure information. A plethora of encryption algorithms have been created to protect secret data from cyberpunks. The goal of modern cryptography is to protect data from hackers. The length of the key determines the system's strength. However, this requires a significant amount of computation power, resulting in a significant delay that can be hazardous to us. The use of FPGAs can help us overcome this constraint even though FPGAs provide increased speed. This encryption schemes can be implemented in hardware on FPGAs.The proposed algorithm scheme has been optimised in terms of the time required to create keys or decode data. Because the thesis only lowered the encryption time, the work has been expanded to improve security for more severe attacks. The intricacy and intensity of assaults necessitate a large number of theoretical computations. The potential for further optimising resource consumption has been identified. The design has been upgraded further to achieve more effective resource use and an improvement in max clock rate. To maximise resource use, the key size could be lowered while maintaining the same security. Although a few gaps have been filled, there is still much work to be done to improve data security while also optimising resources.

## REFERENCES

[1]. S. R. Zeebaree, 2020, “DES encryption and decryption algorithm implementation based on FPGA,” *Indones. J. Electr. Eng. Comput. Sci*, **18(2)**, pp.774-781.

[2]. M. Khairallah, A. Chattopadhyay and T. Peyrin,2017, “Looting the LUTs: FPGA optimization of AES and AES-like ciphers for authenticated encryption,” In *Int. Conf. on Cryptology in India* pp. 282-301.

[3]. H. Zodpe, and A. Sapkal, 2020, “An efficient AES implementation using FPGA with enhanced security features,” *J. of King Saud University-Eng. Sciences*, **32(2)**, pp.115-122.

[4]. R. Shashidhar, A. M. Mahalingaswamy, P. Kumar, and M. Roopa, 2018, “Design of High Speed AES System for Efficient Data Encryption and Decryption System using FPGA,” In *2018 Int. Conf. on Electrical, Electronics, Comm., Computer, and Optimization Techniques (ICEECCOT)* pp. 1279-1282.

[5]. A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, 2018, “Fpga speech encryption realization based on variable s-box and memristor chaotic circuit,” In *2018 30th Int. Conf. on microelectronics (ICM)* pp. 152-155.

[6]. A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, 2018, “Fpga speech encryption realization based on variable s-box and memristor chaotic circuit,” In *2018 30th Int. Conf. on microelectronics (ICM)* pp. 152-155.

[7]. H. Kouzehzar, M. N. Moghadam, and P. Torkzadeh, 2018, "A high data rate pipelined architecture of AES encryption/decryption in storage area networks," In *Electrical Eng. (ICEE), Iranian Conf. on* pp. 23-28.

[8]. T. M. Kumar, K. S. Reddy, S. Rinaldi, B. D. Parameshachari, and K. Arunachalam, 2021, "A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application," *Electronics*, **10(16)**, pp.1-22.

[9]. A. Zaky, E. Elmitwalli, M. Hemeda, Y. Ismail, and K. Salah, 2019, "Ultra Low-Power Encryption/Decryption Core for Lightweight IoT Applications," In *2019 15th Int. Computer Eng. Conf. (ICENCO)* pp. 39-43.

[10]. Y. Yao, Z. Wang, X. Chen, X. Tong, and Q. Luo, 2018, "A dynamic reconfigurable design of multiple cryptographic algorithms based on FPGA," In *2018 IEEE Int. Conf.on Smart Internet of Things (SmartIoT)* pp. 105-110.

[11]. S. Madhavapandian, and P. Maruthu Pandi, 2020, "FPGA implementation of highly scalable AES algorithm using modified mix column with gate replacement technique for security application in TCP/IP," *Microprocessors and Microsystems*, **73**, pp.102972

[12]. J. H. Kim, B. Grady, R. Lian, J. Brothers, and J. H. Anderson, 2017, "FPGA-based CNN inference accelerator synthesized from multi-threaded C software," In *2017 30th IEEE Int. System-on-Chip Conf. (SOCC)* pp. 268-273.

[13]. V. Vijayaragavan, 2017, "Reduction of resource usage in fpga by implementing back propagation algorithm," *Int. J. of MC Square Sci. Res.*, **9(1)**, pp.205-214.

[14]. R. P. V. Kappelle, 2019, "Addiction: How We Get Stuck and Unstuck in Compulsive Patterns and Behavior," *Wipf and Stock Publishers*

[15]. D. T. Milton, S. Dhingra, and C. E. Stroud, 2006, "Embedded Processor Based Built-In Self-Test and Diagnosis of Logic and Memory Resources in FPGAs," In *ESA* pp. 87-93.

[16]. S Murugan, S. Mohan Kumar, and T.R. Ganesh Babu, 2020, "Convolutional Neural Network-based MRI Brain tumor classification system," *Int. J. of MC Square Scientific Res.* **12(3),** pp. 1-8.

[17]. MM Ismail, M Subbiah and S Chelliah, 2018, "Design of pipelined radix-2, 4 and 8 based multipath delay commutator (MDC) FFT, *Indian J. of Public Health Res. and Development*, **9(3)**, pp. 765–768.

[18]. V Jaiganesh and S. Murugan, 2005, "PC based heart rate monitor implemented in xilinx fpga and analysing the heart rate,"*Proc. of the Third IASTED Int. Conf. on Circuits, Signals, and Systems, CSS 2005*, pp. 319–323.

[19]. V. Ellapan and J. S. Alaric, 2019, "A Parallel and Pipelined Architecture for Cordic Algorithm," *Int. J. Adv. Sig. Img. Sci*, **5(2)**, pp. 23–31.

[20]. R. Nusullapalli and N. Vaishnavi, 2018, "Design of FFT Architecture Using Kogge Stone Adder," *Int. J. Adv. Sig. Img. Sci*, **4(2)**, pp. 8–15.