Designing New Aes and Implementing It with Lfsr Key to Improve Data Security

Mr. K.V. Gautham[1], Mr. G. Subrahmanyam[2]

[1,2]RISE Krishna Sai Prakasam Group of Institutions, Ongole, A.P.

ABSTRACT:

Data security is an essential aspect of data communication and data storage. The security and confidentiality of the information has become a significant factor in the communication field. To provide high-level security against all kinds of unauthorized accesses, cryptographic algorithms have been applied to various fields such as medical and military applications. Several techniques for encryption and decryption are proposed to promote the security of the communication systems. Most powerful and significant part of the encryption is a key generation. Presently, hackers are able to break the key with help of the modern high computing machines. Advanced Encryption Standard (AES), a symmetric cryptographic algorithm, is acknowledged as the most secure algorithm for the cryptographic process globally. In this work, Novel design and implementation of AES with LFSR (Linear Feedback Shift Register) key for improving data security is presented. The novelty of this work is using LFSR with AES. The Performance of presented approach is evaluated in terms of speed, area and security. The performance of presented technique will provide effective and efficient security to data.

KEYWORDS: Data Security, Cryptography, Advanced Encryption Standard (AES).

I. INTRODUCTION

Information is regarded as the most valuable asset today, and a large amount of information is processed and shared per second in this technological world. With the development of information technology and internet communication, the security and credibility of information have gained more importance Now a days, every person's financial, medical, social and criminal history would be online and digitally available for individuals of both nature (i.e. good and bad).

Henceforth, the demand for the data security has been growing exponentially now-a-days. Fundamentally data security deals with the two practices for developing algorithms namely: i) For preserving the integrity of data in consideration; ii) For preserving the information of data in consideration [1].

After the computer invention the need of developing tools to protect the information (data) stored in the computer raised. To fulfill this requirements number of tools designed and developed with the main goal of protecting information present in the computer from hackers. These facilities are generally called as computer security. The development of communication and network facilities make it possible to share the information between computers and then the problem of hacking of information arises from this the concept of data security developed.

Cryptography is the technique of hiding data so that only authorized receivers can view it. It is a powerful way of securing information in communication. Generally, cryptographic methods consist of fundamental components such as plain text, cipher text, key and cryptographic algorithm. Enhancing the privacy of the information against unauthorized access is the major objective of the cryptographic mechanism [5]. The main goal of cryptography is to make our information confidential. There are various cryptographic algorithms have been developed. The design of any cryptographic algorithm requires the focus on three parameter: these are security, cost and performance‖. So depending on particular application one can choose better algorithm suitable for that application [2]. Every designer of lightweight cryptography must cope with the trade-offs between security, cost, and performance. It's generally easy to optimize any two of the three design goals security and cost, security and performance, or cost and performance; however, it is very difficult to optimize all three design goals at once.

A secret key is used for both encryption and decryption operations. In terms of the usage of secret keys, cryptographic algorithms can be classified as symmetric and asymmetric algorithms. Also, the algorithms can be classified as block and stream cipher algorithms based on the number of bits. Cryptographic algorithms rely on statistical and analytical techniques that depend on the key of the cryptographic process. Algorithms used for secure communication must withstand the cryptanalytic attacks that aim to find the secret key through the techniques and mathematical operations used to convert the plain text to ciphertext [3].

Cryptographic Ciphers can be symmetric and asymmetric. Symmetric ciphers use same key for encryption and decryption, Asymmetric ciphers use different keys for encryption and decryption. The ciphers for LRDs are often designed for symmetric ciphers. Based on the number of bits encrypted the ciphers are classified as stream ciphers and block ciphers, the stream ciphers encrypt bit by bit or byte, while, the block ciphers encrypt fixed block size plain-text block (16-bits,32-bits, 48-bits and so on). The block ciphers depend on three parameters the size of the block, size [9].

Researchers use cryptographic algorithms to keep information secure while the information is transmitted and received on an insecure channel. Sometimes, information must be secure where it is stored. Cryptographic algorithms perform encryption operations on the original plain text before transmitting and perform decryption operations after receiving the encrypted text from the insecure channel [7].

Standardized algorithms like RCA, DES etc, failed to provide security in applications such as RFID tag, sensor nodes, and smart cards. These algorithms demands the support of more resources, lightweight cryptography can be used as an alternative for these application, which gives better security compared to standardized cryptographic algorithms [6]. In this work, Novel design and implementation of AES with LFSR key for improving data security is presented. The section II describes the literature survey. The section III presents Novel design and implementation of AES with LFSR key. The section IV evaluates the result analysis. Finally the work is concluded in section V.

II. LITERATURE SURVEY

Archana Mishra, Sourabh Sharma et. al., [11] describes Design and Implementation of High Speed AES Algorithm for Data Security In this approach, authors presented a VLSI based AES (Advanced Encryption Standard) encryption that effectively addresses espionage and fraudulent cybercrime based cyber attacks. It is most commonly used symmetric block cipher algorithm that transform information into obscure data based on key-defined transformation set. In addition, it is lossless operation with size of input and output being the same and could be extended to a wide range of applications. In the simulations results, authors analyzed each of the transformation that is incorporated for coding on FPGA using Xilinx ISE tool.

G. G. Bremiga, M. Malleswari and Sharmini Enoch et. al., [12] describes An Improved VLSI Algorithm for Modular Operation in Cryptography. This paper presents a new proposed algorithm which performs an efficient modular multiplication method which is advantage because of its reduction in hardware and software. This proposed method implies a systematic approach which increases the parallelism level when compared to the previous versions. This paper replaces the classical algorithm by other method which effectively reduces the number of iterations. This reduction in computation makes a drastic reduction in hardware and time delay to execute the algorithms. This paper shows a modification in the existing parallelism method which further shows a great improvement in reduction of hardware and time delay.

Ms. Ashwini Y. Mate, Prof.Brig.R.M. Khaire et. al., [13] describes A VLSI Hardware Architecture Implementation of Security System Using Encryption Algorithm This work presents the implementation of a hardware tectonics for video security system. The real time video camera will modulate the digital media system on chip with FPGA. The video processing and security function will be performed independently with FPGA having a novel security module. The real time video signal data is encrypted by associated Modulo algorithm rule and projected. Security module will code the weak video knowledge with a minimum operating frequency up to 50MHz. The paper objects that the encryption methodology enlists a high video streaming security system by using less hardware components.

Satish Shivaram, R. Krishna, Vijayaprakash, K.V.Prasad et. al., [14] describes A VLSI Implementation of a Resource Efficient and Secure Architecture of a Block Cipher. Block cipher concentrates on converting the given original data into cipher text to make the given data more secure over the user. Two different designs of block Cipher algorithms (Throughput enhanced, Area reduced) are developed and their performance is compared in terms of area occupation using Xilinx ISE design tool with verilog language. The block cipher designs are implemented using 64 bit secure key and 128 bit secure key. The area reduced design is of the concern to have this module on the FPGA implementation in the VLSI sector.

M. A. Patil and P. T. Karule et. al., [15] presents Design and implementation of keccak hash function for cryptography. The main examples include digital signatures, MAC (message authentication codes) and in smart cards. Keccak, the SHA-3 (secure hash algorithm) has been discussed in this paper which consists of padding and permutation module. This is a one way encryption process. High level of parallelism is exhibited by this algorithm. This has been implemented on FPGA. The implementation process is very fast and effective. The algorithm aims at increasing the throughput and reducing the area.

Rajneet kaur, Prof. V K Banga et. al., [18] presents Enhancing the Speed of Encryption and Decryption. This work provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, RC6 and RSA. In this work, authors compared various cryptographic algorithms. On the basis of parameter taken as time various cryptographic algorithms are evaluated on different size.

Simulation results are given to demonstrate the effectiveness of each algorithm. From the results it is clear that RSA algorithm takes much longer decryption time compare to decryption time taken by other algorithm. BLOWFISH algorithm consumes least time for decryption.

G. L. Prakash, M. Prateek and I. Singh et. al., [19] describes Data encryption and decryption algorithms using key rotations for data security in cloud system an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. We analyze the privacy protection of outsourced data using experiment is carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

X. Zhang, H. Li, S. Yang and S. Han et. al., [20] describes a High-Performance and Balanced Method of Hardware Implementation for AES. A balanced hardware design and implementation for AES, considering several existing implementations is described. FPGA implementation offers higher speed solution and can be easily adapted to protocol changes, although the AES can be implemented with software or pure hardware. So, this implementation is equipped with regard to FPGA. Optimized and Synthesizable Verilog HDL is developed as the design entry to Quartus II 10.0 software. After obtaining gate-level netlists, timing simulations are performed using ModelSim SE 6.1f. Both 128 bits data block encryption and decryption processes are tested.

V.Jeevan kanth, P.Bujji babu et. al., [21] describes Design and Implementation of the High-End SAFER + Encryption Algorithm. The combination of security, and high speed implementation, makes SAFER+ a very good choice for wireless systems. The SAFER+ algorithm is a basic component in the authentication Bluetooth mechanism. The relation between the algorithm properties and the VLSI architecture are described. Performance of the algorithm is evaluated based on the data throughput, frequency and security level. The results show that the modified SAFER plus algorithm has enhanced security compared to the existing algorithms.

III. NOVEL DESIGN AND IMPLEMENTATION OF AES WITH LFSR KEY

In this section, novel design and implementation of AES with LFSR key for improving data security is presented. The Fig. 1 shows the block diagram of presented approach.

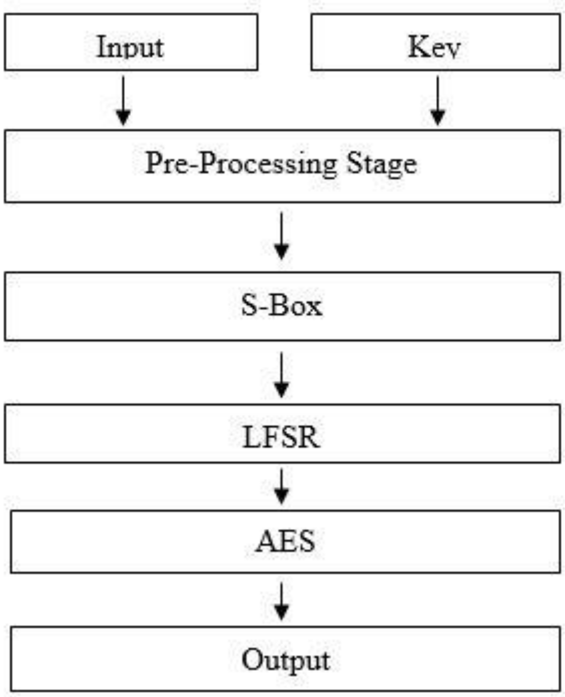

Fig. 1: Block Diagram of Presented Approach

User data is typically local data that individuals need to complete their specific tasks. This data is to be kept in the /home file system or in file systems that are created specifically for user data. User's Data means any files, documents, image, profile picture, messages, recordings, chat logs, transcripts, and similar data that we maintain on your or your Users' behalf, as well as any other information you or your .

Users may upload to the Service account in connection with the Platform. In this approach, user data is applied as a input. Data encryption is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). Users can access encrypted data with an encryption key and decrypted data with a decryption key.

Data preprocessing is an important step in the data mining process. It refers to the cleaning, transforming, and integrating of data in order to make it ready for encryption. The goal of data preprocessing is to improve the quality of the data and to make it more suitable for the specific task. AES is a symmetric cryptographic algorithm in which a single secret key is used for both encryption and decryption operations. AES has three different versions, and each version operates at different bit levels of a secret key. Based on the number of bits in the secret key, AES can be classified into AES-128, AES-192, and AES-256. The Figure shows the block diagram of presented approach.

The AES algorithm performs operations on 128-bit plaintext and uses identical key for encryption as well as decryption. The AES algorithm processes facts obstruct of 128-bit parts and performs 10, 12 and 14 rounds of operations employing a cipher secret of duration 128-bits, 192-bits and 256-bits respectively. The algorithm operates on data block comprised of a 4x4 byte matrix known as the state. The essential procedures of AES algorithm are carried out on the state. Every round of the AES algorithm uses a different subkey that is generated from the main key. Though the key sizes are different for each version, the number of bits from the original data to be communicated securely remains the same for all versions.

The key is required for the encryption/decryption process. Hence, random numbers are generated using LFSR which is the key input to the AES Add round key phase. The LFSR generates random numbers which can be used as key in stream ciphers. It is well suited for ciphers with low and high speed requirements. Several techniques are implemented for key generation to improve the efficiency, security and performance of cryptographic algorithms, such as pairwise key distribution, matrix based key distribution, etc. The size of key is much significant in the energy constrained cryptosystems.

A large key size ensures the randomness, but proportionally maximizes the network load with high complexity. To overcome this problem, random numbers generated using LFSR are used as key in the proposed algorithm. The sub keys are generated from the original key in each round. LFSRs are frequently used as pseudorandom pattern generators to generate a random number of 1s and 0s. The most commonly used linear function of single bits is exclusive-or (XOR). Thus, an LFSR is most often a shift register whose input bit is driven by the XOR of some bits of the overall shift register value.

The LFSR is implemented as a series of the flip flops inside of the FPGA platform. A number taps off of the shift register chain are utilized to either an XOR/XNOR gate. The output of this gate is employed as feedback to the beginning of the shift register chain, therefore the feedback in LFSR. When an LFSR is running, the pattern is generated by individual flip flop is pseudo random number. It’s not completely random since form any state of LFSR pattern. The Verilog creates 4-bit LFSR key. It employs polynomials to make the maximum possible LFSR length for each and every bit width.

The AES comprises of different transformations that operate in an iterated block cipher over the 128-bit fixed block size and a variable length secret key. Each stage is array of which are processed based on the sequence of transformations dictated by the secret key of varying length. AES utilizes round function for both encoding and decoding based of four different transformations: i) Byte substitution using a substitution table (SubBytes). ii) Shifting rows of the State array by different offsets (ShiftRows). iii) Mixing the data within each column of the State array (MixColumns) iv) Adding a Round Key to the State (AddRoundKey).

S-Box Substitution: A byte value is substituted for other bytes in this process. The AES algorithm contains only one non-linear process: substitution. The core processes of substitution are matrix multiplication and affine transformation. By replacing the Rijndael S-box byte value directly, the decryption process employs inverse S-box substitution. SubBytes: The SubBytes transformation is a reversible, affine based non-linear byte substitution with each byte transformed independently Each byte Si, j of the state matrix Ms will be independently updated by a nonlinear transformation f in this module. The mapping f is performed by a substitution-box (S-box), which takes one byte of input from Ms and transforms it into another byte at the same position. The SubBytes module accounts for half of the total gates in AES, with registers used as fixed storage elements of the look-up table (LUT).

Each S-box is preconfigured with an 8-bit word in each memory location addressable by an 8-bit input. Hence the LUT size is 2^8x8 = 2048 bits. The percentage of hardware resources utilized by this module may vary depending on how the S-box is implemented. If the S-box is implemented by combinational logic circuit, XOR gates become the dominant resources, which account for more than 70% of gate utilization for the AES implementation. The ShiftRows transformation shifts rows 1, 2 and 3 of the State matrix cyclically towards left by 1, 2 and 3 positions respectively. The offset value is dependent on the row number. Thus the first row remains unchanged. Cyclic rotation of rows imparts diffusion property in AES algorithm. Mix Column: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round. The decoding process is a straightforward process where all necessary parameters are dictated based on the secret key. The Cipher transformations are simple inverse application of the encoding process at each for the AES algorithm that are listed below: i) InvShiftRows; ii) InvSubBytes; iii) InvMixColumns; iv) AddRoundKey.

On the receiver side, the decryption process will be performed in reverse order using the same key as described in Algorithm. The decryption process is the same as encryption but in a reverse manner. In the decryption process, there must be an inverse process for the mix column step and an inverse process for the shift column step, which are performed in the same manner in a different order. Hence in this way, the user data is secured very effectively.

IV. RESULT ANALYSIS

In this section, novel design and implementation of AES with LFSR key for improving data security is presented. The performance of presented approach is evaluated in terms of speed, area, delay and security. The Fig. 2 shows the area performance comparison. In figure 2, the x-axis represents the encryption algorithms like RSA (Rivest, Shamir, Adleman) and presented AES algorithm. the y-axis indicates the area in terms of percentage.

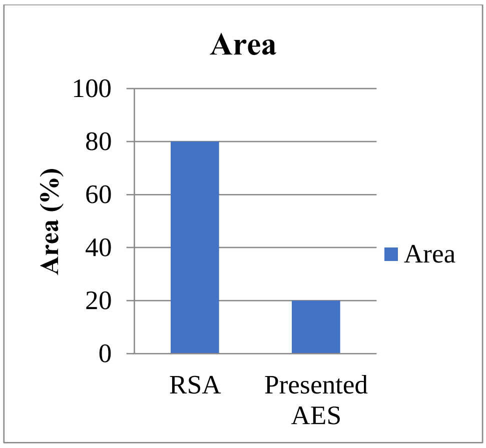

Fig. 2: Area Performance Comparative graph

From the results, it is observed that, the presented AES algorithm with LFSR key has required very less area than RSA. The Fig. 3 shows the delay performance.

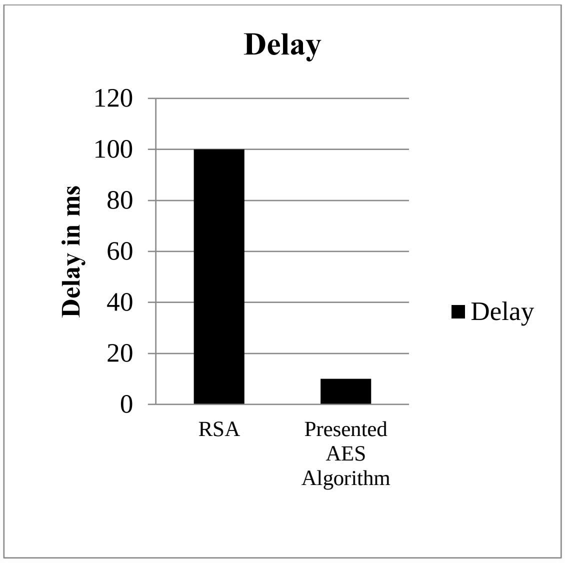

Fig. 3: Delay Performance Comparison

In Figure 3, delay performance is measured in terms of milli seconds(ms). Compared to RSA algorithm, presented approach has very less delay. As the delay is less then speed is more. The Fig. 4 shows the speed performance comparison. In figure 4, the x-axis indicates different encryption algorithms like RSA, DES (Data Encryption Standard) and presented AES algorithms whereas y-axis shows the speed in terms of percentage. The AES algorithm has more speed than DES and RSA.

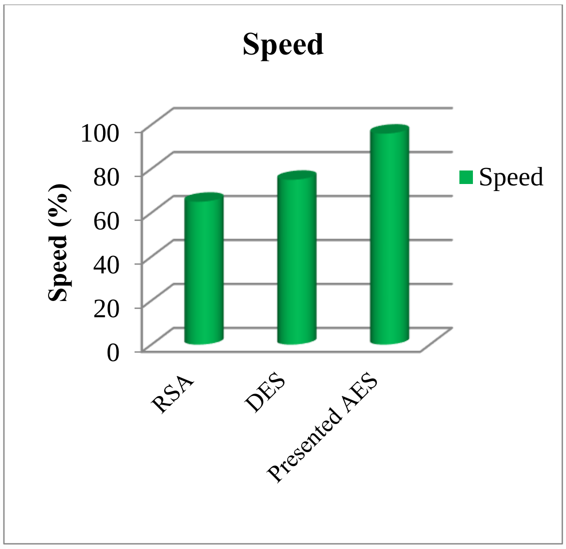

Fig. 4: Speed Performance Comparison

The Fig. 5 shows the comparison of confidentiality and privacy of data.

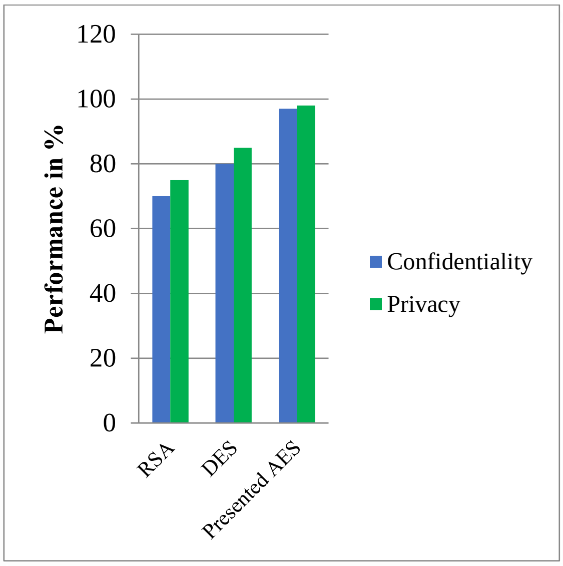

Fig. 5: Performance Comparison

Presented AES algorithm has better confidentiality and privacy than DES and RSA. The Fig. 6 shows the security performance of different algorithms.

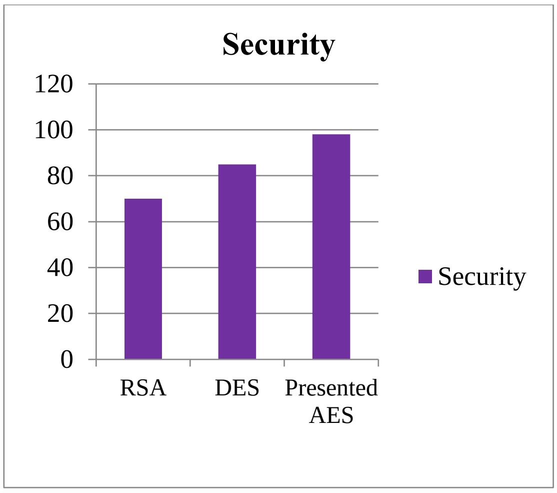

Fig. 6: Security Comparison

In Figure 6, the y-axis indicates the speed in terms of percentage. The x-axis indicates different encryption algorithms. Compared to DES and RSA algorithms, presented AES provides greater security. Hence, this approach has improved the data security and privacy compared to other encryption techniques.

V. CONCLUSION

The large volume of data transformed over the Internet has led to a strong need to protect data from theft and manipulation, especially sensitive and financial data. To solve these issues, in this work, novel design and implementation of AES with LFSR key for improving data security is presented. The world is deeply worried about two fundamental issues are delay, safe and secure data transfer. The architecture supports both the encryption and decryption operations with different bit key lengths. The random numbers are generated using a Linear Feedback Shift Register (LFSR) scheme for key function. The AES algorithm is performed in different stages include s-box, shift rows, mix column and add round key. The performance of presented approach is evaluated in terms of area, delay, speed and security. Compared to different algorithms, presented approach has very less delay and occupied very less area. This algorithm has high speed and provides greater security to user data. In addition confidentiality and privacy is also measured and are better than previous algorithms. Hence this approach has efficiently improved the data security.

VI.REFERENCES

1. T. Pattalu Naidu, Dr. A. Kamala Kumari, “A High-Performance VLSI Architecture for the PRESENT Lightweight Cryptography”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 9 Issue 01, January-2020, Doi:10.17577/IJERTV9IS010225
2. Y. Tao, Qingqin Fu, Jia Liu, Yongxu Cui, Zhaoqing Liang; Rui Nie, Shengbo Qu “Design and implementation of high speed encryption and decryption system based on PCIE bus," *2020 IEEE* 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT, Weihai, China, 2020, pp. 369-372, doi: 10.1109/ICCASIT50869.2020.9368599.
3. F. Valocký, M. Puchalik and M. Orgon, "Implementing Asymmetric Cryptography in High-Speed Data Transmission over Power Line," *2020 11th* IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2020, pp. 0849-0854, doi: 10.1109/UEMCON51285.2020.9298107.
4. Islam, M.M., Hossain, M.S., Hasan, M.K.; Shahjalal, M.; Jang, Y.M. Design and Implementation of High-Performance ECC Processor with Unified Point Addition on Twisted Edwards Curve. Sensors 2020, *20*, 5148, doi:10.3390/s20185148
5. Shailaja Acholli Krishnamurthy Gorappa Ningappa, “VLSI Implementation of Hybrid Cryptography Algorithm Using LFSR Key”, International Journal of Intelligent Engineering and Systems, Vol.12, No.4, 2019, DOI: 10.22266/ijies2019.0831.02
6. M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal and Y. M. Jang, "FPGA Implementation of High-Speed Area-Efficient Processor for Elliptic Curve Point Multiplication Over Prime Field," in *IEEE Access*, vol. 7, pp. 178811-178826, 2019, doi: 10.1109/ACCESS.2019.2958491.
7. Amit Nevase, Nagnath Hulle, “Novel Advanced Encryption Standard (AES) Implementation approach using Genetic Algorithm”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 12, Dec-2017,
8. Hemalatha S, Rajamani V, Parthasarathy V, “Design of Optimal Elliptic Curve Cryptography by using Partial Parallel Shifting Multiplier with Parallel Complementary”, International Journal of Computer Science Systems and Engineering, 2017, Vol 32, No. 5,
9. Karim Shahbazi, Mohammad Eshghi, Reza Faghih Mirzaee, “Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5”, Engineering Science and Technology, an International Journal 20 (2017) 1308–1317, doi: 10.1016/j.jestch.2017.07.002
10. J. G. Pandey, Aanchal Gurawa, Heena Nehra, A. Karmakar, “An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation”, 2016 International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA), 978-1-5090-0033-3/16, doi: 10.1109/VLSI-SATA.2016.7593054

11. Archana Mishra, Sourabh Sharma, “Design and Implementation of High Speed AES Algorithm for Data Security”, International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, doi: 10.5281/zenodo.59643
12. G. G. Bremiga, M. Malleswari and Sharmini Enoch, “An Improved VLSI Algorithm for Modular Operation in Cryptography”, Indian Journal of Science and Technology, Vol 9(30), DOI: 10.17485/ijst/2016/v9i29/90830, August 2016
13. Ms. Ashwini Y. Mate, Prof.Brig.R.M. Khaire, “A VLSI Hardware Architecture Implementation of Security System Using Encryption Algorithm”, International Journal of Scientific & Engineering Research, Volume 7, Issue 5, May-2016 444 ISSN 2229-5518,
14. Satish Shivaram, R.Krishna, Vijayaprakash, K.V.Prasad, “A Vlsi Implementation Of A Resource Efficient and Secure Architecture Of A Block Cipher”, International Journal Of Research In Engineering And Technology, Volume: 05 Issue: 08, Aug-2016 Eissn: 2319-1163,
15. M. A. Patil and P. T. Karule, "Design and implementation of keccak hash function for cryptography," *2015* International Conference on Communications and Signal Processing *(ICCSP)*, Melmaruvathur, India, 2015, pp. 0875-0878, doi: 10.1109/ICCSP.2015.7322620.
16. M. Selim Hossain and Y. Kong, "FPGA-based efficient modular multiplication for Elliptic Curve Cryptography," *2015* International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 2015, pp. 191-195, doi: 10.1109/ATNAC.2015.7366811.
17. Firoz Ahmed Siddiqui, Ranjeet Kumar, “VLSI Design of Secure Cryptographic Algorithm”, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331 PP 01-05
18. Rajneet kaur, Prof. V K Banga, **“**Enhancing the Speed of Encryption and Decryption”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 6, June – 2014, DOI: 10.17577/IJERTV3IS061060
19. G. L. Prakash, M. Prateek and I. Singh, "Data encryption and decryption algorithms using key rotations for data security in cloud system*,"* 2014 International Conference on Signal Propagation and Computer Technology *(ICSPCT 2014)*, Ajmer, India, 2014, pp. 624-629, doi: 10.1109/ICSPCT.2014.6884895.
20. X. Zhang, H. Li, S. Yang and S. Han, "On a High-Performance and Balanced Method of Hardware Implementation for AES," *2013 IEEE* Seventh International Conference on Software Security and Reliability Companion, Gaithersburg, MD, USA, 2013, pp. 16-20, doi: 10.1109/SERE-C.2013.13.
21. V.Jeevan kanth, P.Bujji babu Design and Implementation of the High-End SAFER + Encryption Algorithm”, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 9, November – 2012, ISSN: 2278-0181