RES MILITARIS Social Science Journal

NOVEL DESIGN AND IMPLEMENTATION OF AES WITH LFSR KEY FOR IMPROVING DATA SECURITY

[1]Dr.K. Srihari Rao, [2]Dr. Saidaiah Bandi, [3]Dr.M.Rakesh
[1]Professor & H.O.D. Dept. of ECE, NRI Institute of Technology, Guntur, A.P., India.
[2]Professor, Dept. of ECE, NRI Institute of Technology, Guntur, A.P., India.
[3]Associate Professor, Dept. of ECE, RISE Krishna Sai Prakasam Group of Institutions, Ongole, A.P., India.

ABSTRACT: Data storage and data communication are the two essential aspects to the data security. In the communication field, the significant factors are information confidentiality and security. To various fields such as Military and medical applications, applied the cryptographic algorithms against all kinds of unauthorized access to provide high-level security. To promote the communication system's security, proposed the several techniques for decryption and encryption. Key generation is a significant encryption part and it is most powerful. Presently, the modern high computing machines helps to break the key by the hackers. Globally, for the cryptographic process, the most secure algorithm was acknowledged by a symmetric cryptographic algorithm which was known as Advanced Encryption Standard (AES). 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 system is using LFSR with AES. In terms of security, area and speed are evaluated by the presented approach's performance. The performance of presented technique will provide effective and efficient security to data.

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

I. INTRODUCTION

Today, the most valuable assets are regarded as the information and a large amount of information is processed and shared per second in this technology world. With the development of information technology and internet communication, the security and credibility of information have gained more importance. Now a days, in online, there will be every person's medical, criminal, social and financial history are available digitally, for individuals of both nature (i.e. bad and good). Now-a-days, exponentially growing the demand for the security of data.

For developing algorithms, the data security deals fundamentally with two practices namely: i) On consideration, the data integrity was preserved; ii) On consideration, the data's information was preserved [1].

In the computer, to protect the stored information (data), the need of developing tools raised after the computer invention. From hackers, protecting the information is a main goal that presented in the computer, number of tools designed and developed to fulfill this requirements. Generally, these facilities are called as computer security. Between computers, to share the information it was possible made by the facilities of network and communication development, data security developed from this concept due to arises of information hacking problems [4].

Hiding data technique is known as the cryptography that can view only by the authorized receivers. In communication, securing information is a powerful way. Generally, cryptographic algorithm, plain text, cipher text and key are the fundamental components consisted by the cryptographic methods. Against unauthorized access, the cryptographic mechanism is the major objective for enhancing the information privacy [5]. To make the information confidential is the cryptography's main goal. There has Developed the various cryptography algorithms. On three parameters, the focus was required by any design of the cryptographic algorithms: these are cost, performance and security. For that application, one can choose suitable better algorithm on particular depending

application [2]. The trade-offs between performance, security, and cost, the trade-offs must copy by every lightweight cryptography designer. Any two of the three designs goals are generally optimized easily they are security and performance, cost and performance, or security and cost. However, at once, all three goals of design's optimization would be very difficult [6].

For both operations of decryption and encryption, a secret key is used. As asymmetric and symmetric algorithms classified by the cryptographic algorithms in terms of secret keys usage. Also, based on the number of bits, the stream and block cipher algorithms are classified by the algorithms. On the cryptographic process key, analytical and statistical techniques depended which were relied by cryptographic algorithms. Through the techniques to find the secret key is the aim of cryptographic attacks that must withstand for secure communication using algorithms and to convert the plain text to cipher-text, used the mathematical operation [3].

Asymmetric and symmetric are the cryptographic ciphers. For decryption and encryption, the same key was used by symmetric ciphers where as different keys are used for encryption and decryption by Asymmetric ciphers. For symmetric ciphers, the LRD (Load Random Data) ciphers are often designed. Block ciphers and stream ciphers are classified by the encrypted ciphers based on the number of bits while the fixed size plain text block's (16 bits, 32 bits, 48 bits and so on) was encrypted by the block ciphers, while, bit by bit or byte was encrypted by the stream ciphers. The size, block's size are the parameters depended by the block ciphers [9].

To keep information secure, the cryptographic algorithms are used by the researchers, while the information is received and transmitted on an insecure channel. The information where it is stored must be secured sometimes. Before transmitting, the encryption operation was performed on the original plain text and from the insecure channel, after receiving the encrypted text the decryption operation was performed by the cryptographic algorithms [7].

In applications such as smart cards, RFID (Radio Frequency Identification) tags and sensor nodes, to provide security it was failed by the standardized algorithms like DES(Data Encryption Standard) RCA (Reversible cellular automata) etc. For these application alternatively used the lightweight cryptography, more resources support's the demand of these algorithms, compared to the algorithms of standardized cryptography, a better security was given [6]. In this work, Novel design and implementation of AES with LFSR key for improving data security is presented. A literature survey was described in section II. The section III presents Novel design and implementation of AES with LFSR key. The analysis of result was evaluated in section IV. In section V, finally concluded the work.

II. LITERATURE SURVEY

Archana Mishra, Sourabh Sharma et. al., [11] for Data security, a high speed algorithm of AES's implementation and design was described. In this approach, an encryption of AES (Advanced Encryption Standard) which is based on VLSI (Very Large Scale Integration) was presented by authors that espionage the addresses effectively and cyber attacks which are based on cybercrime of fraudulent. The cipher algorithm of symmetric block was used most commonly, into obscure data, the information transformed based on key defined transformation set. In addition, with the input size, the operation is a lossless and the same can be same and extended to a wide range application it could be extended. In the results of simulation, each of the transformation was

analyzed using Xilinx ISE (Integrated Software Environment) tool on FPGA (Field Programmable Gate Array) for coding which is incorporated.

M. Malleswari, Sharmini Enoch and G. G. Bremiga et. al., [12] in cryptography, for modular operation of an improved VLSI algorithm was described. A new proposed algorithm has presented in this analysis where an efficient method of modular multiplication was performed, which is advantage because of software and hardware reduction. A systematic approach was implied by this proposed method, when compared to the previous versions, the parallelism level increases. By other method, the classical algorithm was replaced by this paper, the number of iterations reduced effectively. In hardware, a drastic reduction was made in computation by this reduction and time delay to execute algorithms. Better modifications are done in this analysis to the existing method of parallelism method in terms of time delay and hardware reduction, a great improvement was shown further.

Prof.Brig.R.M. Khaire, Ms. Ashwini Y. Mate et. al., [13] using encryption algorithm, a security system implementation in a VLSI Hardware architecture was discribed. For video security system, a hardware tectonics implementation was presented in this work. With FPGA, on chip, the digital media system modulated by the real time video camera. A novel security module is having, with the FPGA independently that performed the security function and video processing. The rule of associated modulo algorithm encrypts the real time video signal data and projected. Up to 50MHz, the minimum operating frequency for the knowledge of weak video will be coded by the security module. Less hardware components are used for a high video streaming security system to enlist the encryption methodology which was objected by the paper.

R. Krishna, Vijayaprakash, K.V.Prasad, Satish Shivaram et. al., [14] describes a block cipher's secure architecture and efficient resource implementation of VLSI. Over the user, to make the given data more secure, the given original data is converted to cipher text which was concentrated by the block cipher. Developed the two different block cipher algorithms (Area reduced, Throughput enhanced) with verilog language and the Xilinx ISE design tool was used in terms of area occupation by comparing their performance. Security key of 128 bit and 64 bit are used in implementing block cipher designs. In the VLSI sector, this module on implementation of FPGA is concern due to the area reduced design.

M. A. Patil and P. T. Karule et. al., [15] for cryptography, keccak hash function design and implementation was presented. The main examples included MACs (Message Authentication Codes), smart cards and digital signatures. Permutation and padding module are consisted in this paper, the SHA-3 (Secure Hash Algorithm), keccak has been discussed. This is a one way encryption process. This algorithm has exhibited the high level parallelism. This has been implemented on FPGA. The process implementation is very effective and fast. Reducing the area and increasing the throughput were aimed by the algorithm.

Rajneet kaur, Prof. V K Banga et. al., [18] presents Enhancing the Speed of Encryption and Decryption. The most common six evaluated encryption algorithms are provided in this work namely: RSA (Rivest Shamir Adleman) AES (Advanced Encryption Standard (Rijndale), DES, 3DES (Triple DES) RC2 (Rivest Cipher 2), RC6 (Rivest Cipher 6) and Blowfish. In this work, authors compared the various cryptographic

algorithms. Various cryptographic algorithms on different size evaluated on the basis of parameter taken as time. Each algorithm's effectiveness was demonstrated by giving the simulation results. Compared to other algorithms, much longer decryption time was taken by the RSA algorithm, therefore, it is clear from the results. For decryption, least time was consumed by the Blowfish algorithm.

G. L. Prakash, M. Prateek and I. Singh et. al., [19] before sending an encrypt sensitive data to the cloud server, an efficient data encryption in the cloud server for data security and key rotations are used by the data decryption and encryption algorithms as described. With rotation, the symmetric key of 256 bit was used by the block level data encryption that was exploited. In addition, shared secret key was used to reconstruct the requested data by the data users from cloud server. With the variable size, an experiment was carried out on the repository text files by using privacy protection of outsourced data that was analyzed. The analysis of performance and security shows that, when compared with the performance of existing methods, the proposed method is highly efficient.

H. Li, S. Yang, S. Han and X. Zhang et. al., [20] for AES, Balanced Hardware implementation method and High performance was described. For AES, described several existing implementations which are considered the implementation and design of a balanced hardware. Higher speed solution was offered by the FPGA implementation and to protocol changes, it can be easily adapted although, with pure hardware or software can implement the AES. So, FPGA is used for implementation. The Quartus II 10.0 software's design entry was developed by the Synthesizable and optimized Verilog HDL (Hardware Description Language) ModelSim SE (Simulator Environment) 6.1f is used to perform simulation timing after obtaining gate-level netlists. Tested the both 128 bit data block decryption and encryption process.

V.Jeevan kanth, P.Bujji babu et. al., [21] High-End Safer and Encryption algorithm implementation and design were described. For wireless systems, safer a very good choice was made due to its high speed implementation and combination of security. In Bluetooth mechanisms authentication a basic component is safer algorithm. It is described the relation between VLSI architecture and algorithm properties. Based on the frequency, security level and data throughput evaluated the algorithms performance. Compared to the existing algorithms, security has enhanced by the modified Safer plus algorithm that was shown in the results.

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 presented approach's block diagram was shown in the Fig.1.

Specific tasks are needed to complete by the individuals which is a typical local data is known as user data. For user data, specifically created in the file system or in home file system this data is to be kept. User's data means any transcripts, files, chat logs, documents, image, profile picture, messages, recording and similar data that maintain the data on users behalf.

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

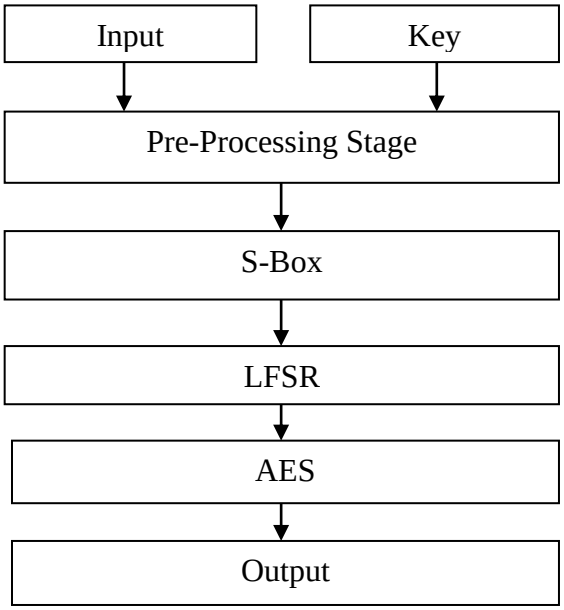

Fig. 1: Block Diagram of Presented Approach

In the process of data mining, an important step is Data pre-processing. For encryption, in order to make it ready the data integrating, cleaning and transforming were referred. For specific task, the data is make it more suitable and its quality is improved through data pre-processing. For both decryption and encryption operations, used a single secret key in a symmetric cryptographic algorithm is known as AES. There are three different versions in AES, and at different bit levels of a secret key operated by each version. In the secret key, based on the number of bits, AES can be classified into AES-256, AES-128, and AES-192. The presented approach's block diagram was shown in the Figure.

Operations on 128 bit plain text was performed by the AES algorithms and for encryption as well as decryption, identical key was used. The facts of 128 bit parts, obstruct are processed by AES algorithm and cipher secret duration 128-bits, 192 bit, and 256 bits are employed by performing the 10, 12 and 14 rounds operation respectively. The state is a comprised of a 4x4 byte matrix on data block that was operated by algorithm. AES algorithm's essential procedures are carried out on the state. From the main key different sub-keys are generated that are used in every round of the AES algorithm. For all versions, the number of bits is remained same to communicate securely from the original data and for each version there are different key sizes.

For decryption/encryption process it requires a key. Hence, to generate random numbers used the LFSR, which is the key input to the AES Add round key phase. In stream ciphers, a random numbers are generated by the LFSR it is used as key. For ciphers, it is well suited with requirements of high and low speed. For key generation, to improve cryptographic algorithms performance, security and efficiency the several techniques are implemented such as matrix based key distribution, pair-wise key distribution, etc. The much significant in the energy constrained cryptosystems is size of key.

Randomness was ensured by a large key size, with high complexity, the network load was proportionally maximized. In the proposed algorithm, a key is used to overcome this problem, LFSR is used to generate random numbers. In each round from the original key generated the sub key. LFSRs are frequently used as pseudorandom pattern generators to generate a random number of 1s and 0s. Exclusive-or (XOR) is a single bits linear function which was used most commonly. Thus, a shift register is most often by an LFSR, overall shift register value of some bits of XOR drives the input bit.

Inside the FPGA platform the series of flip-flops are implemented as a LFSR. A number taps off of the shift register chains are utilized to either an XNOR/XOR (Exclusive Not OR/Exclusive OR) gate. Therefore, in LFSR the feedback was employed to the shift register chain at beginning as the feedback by this gate output. Pseudo random number is a

individual flip-flop that generates the pattern when an LFSR is running. Since, from any LFSR pattern state it is not random. The 4-bit LFSR key was created by the Verilog. For each and every width of bit, the maximum possible LFSR length was made by polynomials to employ.

The different transformations were comprised by AES in an iterated block cipher that operands over the secret keys variable length and the size of 128 bits fixed block. Varying length's secret key which was dictated based on the sequence transformation that was processed by an array in each stage. Based on four different transformations, for both decoding and encoding the round function was utilized by AES: i) A substitution table (Sub-Bytes) is used for Byte substitution; ii) Different offsets (Shift-Rows), for state array shifting rows; iii) Within each state array (Mix-Column) column, the data is mixing; iv) To the state array (Add-Round Key), a round key is adding.

S-Box Substitution: In this process, for other bytes substituted a byte value. Substitution is only one non-linear process that was contained by the AES (Advanced Encryption Standard) algorithm. Affine transformation and multiplication are the core process of substitution. Inverse S-box substitution was employed by the decryption process, when directly replacing the Rijndael S-box byte value. SubBytes: Independently, each byte transformed with substitution by affine based non-linear byte which is reversible is known as Sub-Bytes transformation. In this module, a non-linear transformation f is updated independently by the Ms of state matrices, each byte is *Si, j*. A Substitution box (S-box) performs the mapping *f*, from *Ms* one input byte was taken and at the same position, it transforms in to another byte. In AES, half of the total gates are accounted by the module of Sub-Bytes, as fixed Look-Up Table's (LUT) storage elements are used with register.

An 8-bit input was addressable in each memory location with an 8-bit word which was pre-configured by each S-box. Hence, 2^8x8 = 2048 bits are the LTU size. Depending on how the S-box is implemented that may vary this module by utilizing in the hardware resources percentage. XOR gates become the dominant resources if the combinational logic circuit implements the S-box, which accounts for AES implementation that utilized the more than 70% of gate. Rows 1, 2 and 3 of the state matrix are cyclically shifted towards left by 1, 2 and 3 positions, respectively, by the Shift Rows transformation. On row number, the offset value is dependent. Thus, the first row remains unchanged. In AES algorithm, a diffusion property was imparts by the cyclic rotation rows. Mix Column: Now, a special mathematical function is used to transform each four bytes in a column. The four bytes of one column was taken as input in this function and the original column replaces completely with new bytes of four outputs. The 16 new bytes are consisted in another new matrix which is the result. It should be noted that, in the last round, this step is not performed.

Now, as 128 bits considered the 16 bytes matrix and the round key's 128 bits are XORed. If this is the last round, cipher-text will be the output. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round. Based on the secret key dictated all the necessary parameters by a straight forward process is known as decoding process. For the AES algorithms, the encoding process at each simple inverse application is known as cipher transformations, which are listed below: i) Add-Round Key; ii) Inv Shift Rows; iii) Inv Sub Bytes; iv) Inv Mix Columns.

In algorithm as described, the same key is used in reverse order to perform the decryption process on the receiver side. As encryption, the decryption process is same but it is in reverse manner. There must be an inverse process for the mix column steps and shift column steps in the decryption process 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. In terms of speed, area, security and delay evaluated the presented approach's performance. 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.

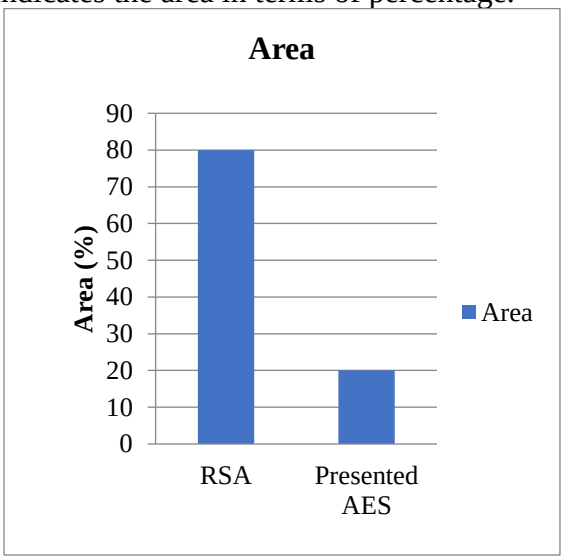

Fig. 2: Area Performance Comparative graph

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.

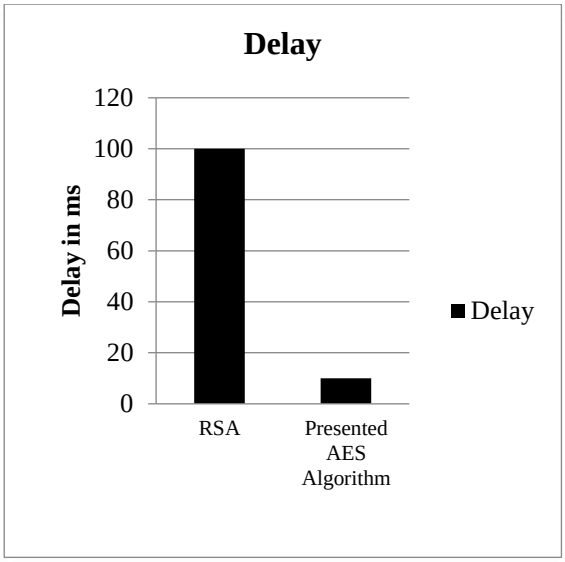

Fig. 3: Delay Performance Comparison

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.

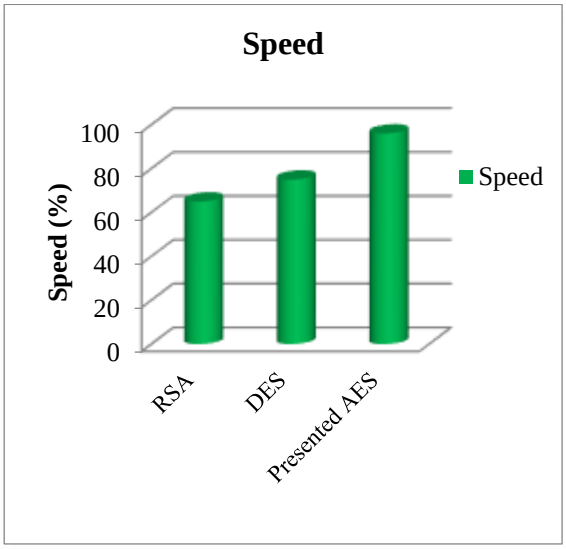

Fig. 4: Speed Performance Comparison

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

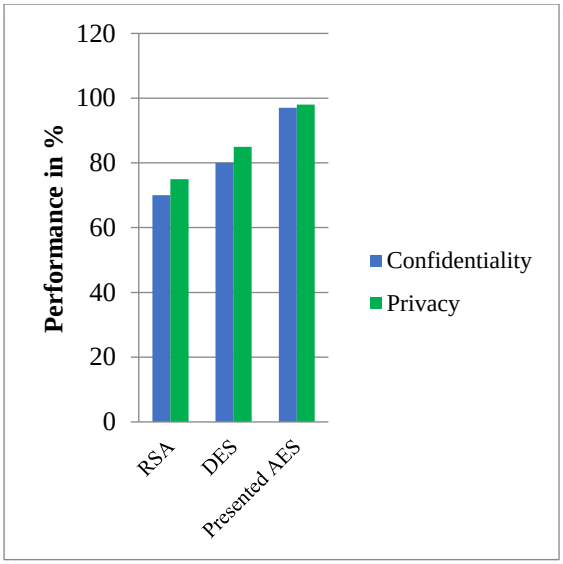

Fig. 5: Performance Comparison

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

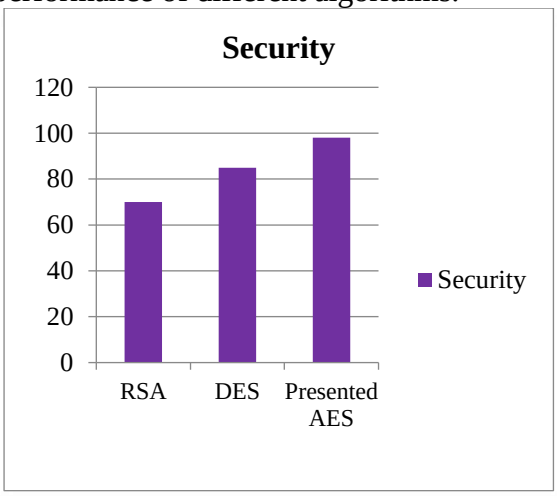

Fig. 6: Security Comparison

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

A strong need to protect data from manipulation and theft, especially, financial and sensitive data, has led the large volume of data transform over the internet. 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 worried about two fundamental issues are delay, safe and secure data transfer. With different lengths of bit key, the both decryption and encryption operation were supported by the architecture. For key function, a scheme of Linear Feedback Shift Register (LFSR) was used to generate the random numbers. The AES algorithm is performed in different stages include s-box, shift rows, mix column and add round key. In terms of area, delay, speed and security evaluated the presented approach's performance. 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, vol. 5, no. 8, 2016, 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), 2014, 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