IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, 2022

A NOVEL S-BOX BASED ADVANCED ENCRYPTION STANDARD TECHNIQUE FOR IMPROVED DATA SECURITY

Mr. Ch.Rambabu[1], Mrs. K.Srilakshm[2]i, Dr. T.Ananda Babu[3], Mr. P.Anil Kumar[4]

[1]Senior Grade Assistant Professor, Dept. of ECE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt., A.P, India

[2,3,4]Assistant Professor, Dept. of ECE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt., A.P, India

[1]rambabuec41@gmail.com , [2]slkaza06@gmail.com , [3]anand.mits11@gmail.com , [4]anilmtechh@gmail.com

ABSTRACT: Secure communication and data protection are now top priorities in the digital age.

In today's world, everything is running online and a lot of data are transferred over the internet, so data security had become an important issue. Even if one doesn't send a file, hackers can get into the systems and access private data. There exist numerous encryption techniques using symmetric and asymmetric cryptographic technique. The primary objective of cryptography is to protect information from various types of security breaches. To enhance their resilience, most cryptographic techniques modify parameters such as key size, number of iterations, and incorporation of S-boxes. AES (Advanced Encryption Standard) is yet one of the prominent cryptographic algorithms of the 21st century with the reputation of excellent performance and reliability. AES revolves around the S-Box, a nonlinear substitutive table that is essential to attain the level of crypto-security. Substitution-boxes (S-Boxes) are important non-linear components in block cryptosystem, which play an important role in the security of cryptosystems. Constructing S-Boxes with a strong cryptographic feature is an important step in designing block cipher systems. In this analysis, A novel S-box based Advanced Encryption Standard Technique for Improved data security is presented. The performance of this technique is measured in terms of delay, memory usage and Linear Probability (LP).

KEYWORDS: Secure communication, Data security, Cryptography, Advanced Encryption Standard, S-box.

I. INTRODUCTION

Data and information communication has become very important ingredient of today's technological life and considered as significant assets of an individual or organization.

The security and privacy of sensitive information are more important than ever in the age of digitization of big data and increased global connectivity, the reliance on digital data is evident in everything from private conversations and business transactions to medical records and state secrets, and data security risks grow with this reliance [1]. If the confidentiality of information is compromised, then the

information can be used for harmful purposes. Current innovations in information technology and their prolific applications in our life have caused in a gigantic growth in the size of the data being transmitted online. The private information being very sensitive assets require protection from attackers. Therefore, prior to its transmission, data demand its protection and needs methods for its transformation into a meaningless form for the invaders [2].

Data security (i.e., more specifically ensuring data integrity and confidentiality) is an efficient and effective procedure to assure data trustworthiness/dependability. Data security is important that data trustworthiness is assured during the lifecycle of big data stream processing [3]. The information security triad is based in three main angles availability, integrity and confidentiality. Cryptographic algorithms are the mathematical methods and techniques that assist in the protection of data. The goal of cryptography is to cover the major portion of integrity and confidentiality in different application such public and private algorithms, Key distribution management for confidentiality of stored and transmitted data, digital signature for authenticity of electronic transactions activities and for non-repudiation conformities [4].

The word cryptography is based on the Greek words “kryptos” that is means (hidden) & “grafi” which means (writing). So for us IT and cybersecurity professional cryptography is the mathematical equations to manipulate piece of information that help to prevent and protect the information from being disclosed or altered from it is original and intended use. Data can be approach wither in transit or in rest therefore cryptography provides the means for confidential transmission of data, and provides the means of confidential for storing data. There are many terms are used in the cryptography science some of which will be used in this paper such as (plaintext/cleartext-Vs-ciphertext/ cryptogram), (encrypt/ encipher-Vs-Decipher /decrypt/ decode) and so on [5].

Characteristics of Cryptography include i) Data Security: Secures the plain text; Data Breaches: Protects from the release of confidential information to the environment. ii)Authentication and Authorization: Allow only the authentic individual to read/write the data. In encryption process the original message or data called plaintext is given as input to form cipher text. In decryption process the cipher text is transforming into plaintext. Cryptographic algorithms are classified as symmetric and asymmetric. Symmetric key algorithms are the quickest and most commonly used type of encryption. In symmetric cryptography, a single key is used to encrypt and decrypt the data. The key must be known to both the clients to read/write the data [6].

There are different methods of Symmetric key Algorithm like DES, 3DES, AES, and more. In Asymmetric Cryptography approach, there are two different keys to encrypt and decrypt the data. The key used to encrypt the data is called Public Key and the second key is used to decrypt the data

called the Private key. Both keys are different from each other. Private Key is only available to the receiver [7].

Stream ciphers transform the data in a bit-by-bit or byte-by-byte manner. Whereas, the block ciphers transform data in chunks which comprise large number of bits or bytes at a time. In modern symmetric encryption, block ciphers are considered as one of the most effective tools for data protection. Data Encryption Standard (DES), Blowfish, Advanced Encryption Standard (AES), RC5, etc. are examples of contemporary block ciphers [8].

The Data Encryption Standard (DES) was initially a prominent block cipher, but its flaws became apparent over time. This led to the development of the Advanced Encryption Standard (AES), which greatly enhanced cryptographic security. Despite this improvement, the rapid advancement of technology and the rise of cyber threats have prompted experts to investigate alternative techniques for data encryption.

A substitution box is a crucial component of a block cipher as it introduces confusion in the ciphertext. The strength of a cipher directly depends on the design and properties of the S-box used in encryption. In this analysis, A novel S-box based Advanced Encryption Standard Technique for Improved data security is presented. The arrangement of remaining sections is as follows: The section II describes the literature survey. The section III describes A novel S-box based Advanced Encryption Standard Technique for Improved data security. The section IV presents the result analysis. The section V discusses the conclusion of the work.

II. LITERATURE SURVEY

B. Dai, Z. Gao, N. Wada and X. Wang et. al., [9] describes Orthogonal DPSK/CSK Modulation and Public-Key Cryptography-Based Secure Optical Communication. the information security of an optical code-based communication system employing orthogonal differential phase-shift keying (DPSK)/code-shift keying (CSK) modulation is first investigated using two eaves dropping methods, one-bit delay interference detection and differential detection. The investigation results show that the security vulnerability exists only in the CSK channel while the DPSK channel can thwart these attacks. Therefore, the concept of public-key cryptography is introduced into the system to efficiently use these two orthogonal channels for both public key distribution and encrypted data transmission. The privacy of the transmitted data can be double guaranteed by public-key cryptography scheme logically and optical code-processing techniques physically.

K. Liang, W. Susilo, J. K. Liu and D. S. Wong et. al., [10] describes Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. An affirmative result is provided on the long-standing question of building a full Chosen-Ciphertext Attacks (CCA)-secure CPRE system in the standard model and for the first time, we show that a class of Hierarchical Identity-Based Encryption (HIBE) schemes can be

transferred to building a CCA-secure CPRE in the standard model. We also list out some concrete HIBE schemes which fall into this class, e.g., Lewko-Waters HIBE. All existing CCA-secure PRE schemes in the standard model are not conditional while all existing CPRE schemes are either not CCA secure or not in the standard model.

B. Qin, R. H. Deng, S. Liu and S. Ma et. al., [11] describes Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption. A Security model of ABE with verifiable outsourced decryption is presented by introducing a verification key in the output of the encryption algorithm. Then, we present an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general, and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some nondominant operations (e.g., hash computations), nor expands the ciphertext size except adding a hash value (which is <;20 byte for 80-bit security level). We show a concrete construction based on Green et al.'s ciphertext-policy ABE scheme with outsourced decryption, and provide a detailed performance evaluation to demonstrate the advantages of our approach.

T. Shen, F. Wang, K. Chen, K. Wang and B. Li et. al., [12] describes Efficient Leveled (Multi) Identity-Based Fully Homomorphic Encryption Schemes. The first identity-based fully homomorphic encryption (IBFHE) scheme was constructed from identity-based encryption (IBE) and lattice-based cryptography by Gentry, Sahai, and Waters in CRYPTO 2013. Their IBFHE scheme is improved in this paper, exploiting Alperin-Sheriff and Peikert's tight and simple noise analysis method when evaluating homomorphically and Micciancio and Peikert's powerful and novel trapdoor. Furthermore, using the masking scheme(Mukherjee and Wichs in EUROCRYPT 2016), an efficient multi-identity fully homomorphic encryption (MIFHE) scheme is constructed by expanding a “fresh” ciphertext under a single identity key to an “expanded” one under a combined key that enables ciphertexts under different identities to be homomorphically evaluated.

I. Hussain, M. C. Negi and N. Pandey et. al., [13] describes A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer. The implementation part of the proposed technique was conceded out at the C&I department of NTPC, Dadri India and the data security issues were taken care of using RSA and DES encryption schemes at layer 2 of the communication protocol. The proposed technique was agreed upon by the same department but the encryption decryption time utilized by both the algorithms is more than expected, which in turn creates a time delay in the whole process.

N. Jayapandian, A. M. J. M. Z. Rahman, S. Radhikadevi and M. Koushikaa et. al., [14] describes Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption. The study of symmetric DES and

asymmetric key RSA encryption algorithms is done according to different needs. The key used is defined in terms of encryption and decryption either it is same or different. The algorithm used is defined according to its type symmetric or asymmetric. The key length is used according to bit value. The speed is defined in terms of fast or slow. The power consumption takes as low or high. The security is defined as excellent, not secure and least secure. The cost is defined as cheaper or costly. The implementation according to its algorithm used is simple or complex. so it mainly depends on the data and needs of security to that message.

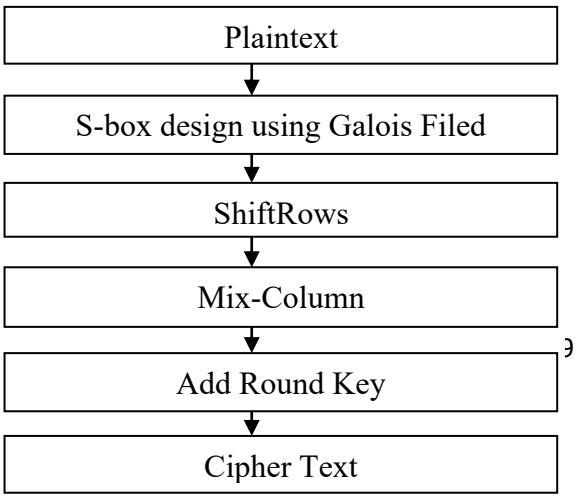
M. Panda et. al.,[15] describes Performance analysis of encryption algorithms for security. This paper provides evaluation of both symmetric as well as asymmetric (RSA) cryptographic algorithms by taking different types of files like Binary, text and image files. A comparison has been conducted for these encryption algorithms using evaluation parameters such as encryption time, decryption time and throughput. Simulation results are given to demonstrate the effectiveness of each.

H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri et. al., [16] describes A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography. The main focus has been given to secure healthcare private data in the cloud using a fog computing facility. To this end, a tri-party one-round authenticated key agreement protocol has been proposed based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely. Finally, the private healthcare data are accessed and stored securely by implementing a decoy technique.

S. Liu, Y. Hong and E. Viterbo et. al., [17] describes Unshared Secret Key Cryptography. The unshared secret key (USK) cryptosystem is described where the AN (Artificial Noise) is redesigned as a one-time pad secret key aligned within the null space between a transmitter and a legitimate receiver. The proposed USK cryptosystem is a new physical-layer cryptographic scheme, which was obtained by combining traditional network-layer cryptography and physical-layer security. Unlike previously studied AN techniques, rather than ensuring nonzero secrecy capacity, the USK is valid for an infinite lattice input alphabet and guarantees Shannon's ideal secrecy and perfect secrecy without the need for secret key exchange.

III. A NOVEL S-BOX BASED ADVANCED ENCRYPTION STANDARD

In this analysis, A novel S-box based Advanced Encryption Standard Technique for Improved data security is presented. The Figure 1 describes the block diagram of presented techniques.



ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 06, 2022

Figure 1: Novel S-box based AES Technique

AES is non-Feistel cipher defined in three versions with 10, 12, and 14 rounds, the key size is 128, 192, and 256 respectively.3 Round key is always 128 bits. To obtain security AES uses four transformations byte substitution,shift rows,mix column and addroundkey as shown in figure 1. Each transformation takes a state and generates new state for next step and finally generates ciphertext.

Here, the main focus is on efficient design of S-box so that constraints are mapped. Substitution implementation is done by Shannon's confusion-diffusion principles. Confusion is most desirable requirement of encryption algorithm. A strong confusion property is required to secure data in the form of ciphertext. Diffusion is randomness required in substitution, for change in one bit of input, the substituted output should be changed by at least half of bits. This makes it unpredictable and hence more secure communication is possible.

Byte Substitution(S-box): In this process the state is considered as 4x4 matrix of bytes. Transformation is carried out on one byte at a time. Each byte is changed independently. Total 16 independent byte transformation takes place. In symmetric key algorithm S-box is most important component. In SubByte block transformation is done by using nonlinear transformation. On each byte SubByte transformation is performed. Using polynomial representations the SubByte Transformation can be implemented on hardware.4 The software implementation can be done using 16x16 Look Up Table (LUT). SubByte transformation using Composite Field Arithmetic reduces the complexity and also adds pipelining concept in its structure. Realization of Composite field arithmetic can be done by using different irreducible polynomials.

The S-box operation is the only nonlinear transformation of AES algorithm.5.An invertible map, fractional linear transformation on Galois field can be used for S-box generation. LUTs in composite field arithmetic is carried out for S-box and multiplication process which decreases computation time and hardware complexity

S-box Implementation using Galois field: In first stage multiplicative inverse is used to replace each byte. In Second stage invertible affine transformation is performed. Complexity is depend on representation of field elements. S box transformation is represented as a lookup table. Elements of Galois field are defined as

$$GF = (0,1,2,\dots,xl-1) \cup (xl, xl+1, xl+2,\dots, xl+xl-1) \cup (xl^2, xl^2+1, xl^2+2,\dots, xl^2+xl-1) \cup \dots \cup (xl^{n-1}, xl^{n-1}+1, xl^{n-1}+2,\dots, xl^{n-1}+xl-1) \quad (1)$$

Multiplication of polynomial is given as

$$M(xi) = \big(f(xi).g(xi)\big)\big(modm(xi)\big)$$

The Multiplicative inverse of f(x) is given by a(x) such that it follows:

$$\big(f(xi).a(xi)\big)\big(modm(xi)\big) = 1 \quad (2)$$

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 06, 2022

where m(x) is an irreducible polynomial of degree at least n in GF. The modulo polynomial for finding the multiplicative inverse is given as

$$m(xi) = xi^8 + xi^4 + xi^3 + xi^1 + xi^0 \quad (3)$$

Shift rows: In this transformation rows of the state are shifted in cyclic manner over different offsets. It operates on one row at a time. In this operation row 0 is not shifted and last row shifted three times.

Mix columns: New column is transformed from each column of the state. It is a matrix multiplication with modulus 10001101. The columns are multiplied modulo xl4+1 with polynomial a1(xl) as polynomials over Galois Field (2^8), where xl is characteristics of the field. For mix columns the overall utilization of redundant bits is minimized in the boolean expression using resource sharing architecture and gate replacement technique, which helps to lower power consumption and cost of the encryption algorithm.

Addroundkey: This transformation operates one column at a time. With each column matrix a round key word is added. XOR operation is performed on each column with key word. 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, Result analysis of a novel S-box based Advanced Encryption Standard Technique for Improved data security is presented. The performance of this system is evaluated in terms of s-box linear probability, Delay and Memory usage

A secure cryptosystem should have strong confusion and diffusion effects. Strong S-Boxes help cryptosystems to achieve strong confusion and diffusion effects through nonlinear mapping between input and output data. The lower linear probability (LP) of an S-Box, the higher the nonlinear mapping feature and the stronger the performance resistance against the linear cryptanalysis. Therefore, linear probability (LP) is used to measure the resistance of an S-Box to linear cryptanalysis.

The table 1 describes the performance comparison.

Table 1: Parameters Comparison

Parameter/Encryption Model	DES	AES
Delay (ns)	13.78	7.02
Memory Usage(MB)	34	21.34
LP	1.56	0.20

Compared to previous encryption techniques, s-box based AES has exhibited better performance. The Figure2 shows the delay performance comparison.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 06, 2022

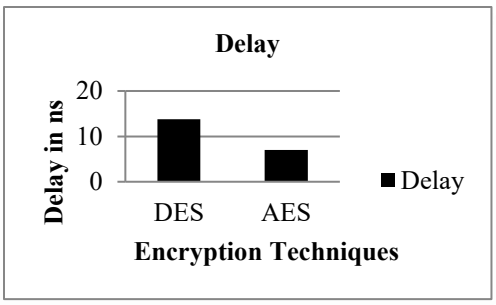


Figure 2: Delay Comparison

In Figure 2, the x-axis represents the encryption techniques and y-axis indicates the delay values in terms of nano seconds (ns). This AES has very less delay than DES. The Figure 3 describes the memory usage comparison.

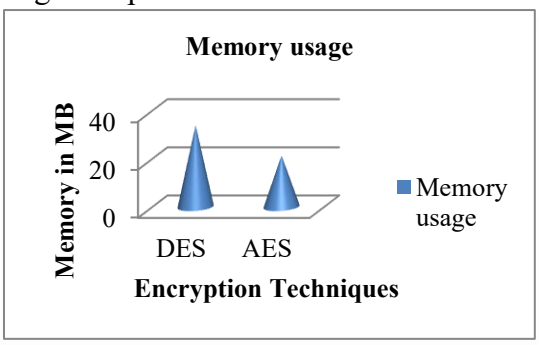


Figure 3:Memory Usage Comparison

In figure 3, the memory usage of encryption techniques is represented on x-axis and y-axis. Presented AES technique has used very less memory than DES. The Figure 4 describes the Linear Probability comparison.

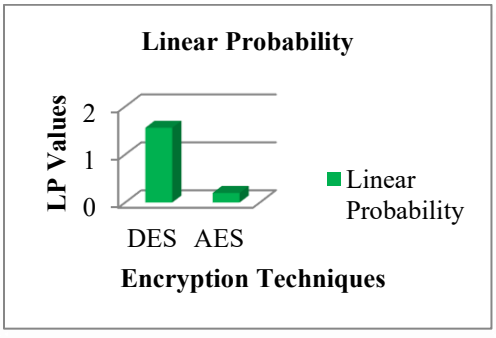


Figure 4: LP Comparative Graph

In Figure 4, encryption techniques are indicated on x-axis and Linear Probability values are indicated on y-axis. Presented AES has very less LP. Here, the less LP indicates the strong security. From the results, it is clear that, presented s-box based AES has better security, consumes less delay and memory for performing data security.

V. CONCLUSION

In this analysis, A novel S-box based Advanced Encryption Standard Technique for Improved data security is presented. The input plaintext is applied to s-box. The s-box is designed with Galois Filed. This architecture implementation gives more security with cryptographic algorithm of S-box. In the s-box, firstly stage multiplicative inverse is used to replace each byte. In Second stage invertible affine transformation is performed.. S box transformation is represented as a lookup table. In this method S box contains pre computed value stored at predefined address. This alternative memory architecture is very much optimized. The entire table entries are fixed in the lookup table. Shiftrows transform rows of the state are shifted in cyclic manner over different offsets. Mixcolumn performs Mixing the data within each column of the State array. AddRoundkey adds a Round Key to the State. The performance of presented approach is evaluated in terms of delay, Memory Usage and Linear probability. This AES method has consumed very less delay, uses less memory and less Linear probability. Less LP results higher security.

Hence this model can be used for providing security and privacy to data.

VI. REFERENCES

[1] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.

[2] N. Jeyanthi, S. B. Shastri, P. Baranwal, R. Thandeeswaran and Akash, "Implementation and Analysis of Various Visual Cryptographic Techniques for Sensitive Data Protection," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 375-379, doi: 10.1109/CICN49253.2020.9242612.

[3] D. Puthal, X. Wu, N. Surya, R. Ranjan and J. Chen, "SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams," in IEEE Transactions on Big Data, vol. 5, no. 3, pp. 379-392, 1 Sept. 2019, doi: 10.1109/TBDATA.2017.2702172

[4] K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography," 2020 SoutheastCon, Raleigh, NC, USA, 2020, pp. 1-5, doi: 10.1109/SoutheastCon44009.2020.9368301.

[5] H. Cui, R. Paulet, S. Nepal, X. Yi and B. Mbimbi, "Two-Factor Decryption: A Better Way to Protect Data Security and Privacy," in The Computer Journal, vol. 64, no. 1, pp. 550-563, Nov. 2019, doi: 10.1093/comjnl/bxaa080.

[6] H. N. Almajed and A. S. Almogren, "SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography," in IEEE Access, vol. 7, pp. 175865-175878, 2019, doi: 10.1109/ACCESS.2019.2957943.

[7] D. Naidu, A. K. K S, S. L. Jadav and M. N. Sinchana, "Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques," 2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2019, pp. 1360-1364, doi: 10.1109/RTEICT46194.2019.9016974.

[8] Rismayani and C. Susanto, "Using AES and DES Cryptography for System Development File Submission Security Mobile-Based," 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, 2020, pp. 1-7, doi: 10.1109/CITSM50537.2020.9268805.

[9] B. Dai, Z. Gao, N. Wada and X. Wang, "Orthogonal DPSK/CSK Modulation and Public-Key Cryptography-Based Secure Optical Communication," in IEEE Photonics Technology Letters, vol. 25, no. 19, pp. 1897-1900, Oct.1, 2013, doi: 10.1109/LPT.2013.2279407.

[10] K. Liang, W. Susilo, J. K. Liu and D. S. Wong, "Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption," in The Computer Journal, vol. 58, no. 10, pp. 2778-2792, Oct. 2015, doi: 10.1093/comjnl/bxv050.

[11] B. Qin, R. H. Deng, S. Liu and S. Ma, "Attribute-Based Encryption With Efficient

Verifiable Outsourced Decryption," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1384-1393, July 2015, doi: 10.1109/TIFS.2015.2410137.

[12] T. Shen, F. Wang, K. Chen, K. Wang and B. Li, "Efficient Leveled (Multi) Identity-Based Fully Homomorphic Encryption Schemes," in IEEE Access, vol. 7, pp. 79299-79310, 2019, doi: 10.1109/ACCESS.2019.2922685.

[13] I. Hussain, M. C. Negi and N. Pandey, "A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, United Arab Emirates, 2017, pp. 464-470, doi: 10.1109/ICTUS.2017.8286054.

[14] N. Jayapandian, A. M. J. M. Z. Rahman, S. Radhikadevi and M. Koushikaa, "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/STARTUP.2016.7583904.

[15] M. Panda, "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.

[16] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in IEEE Access, vol. 5, pp. 22313-22328, 2017, doi: 10.1109/ACCESS.2017.2757844.

[17] S. Liu, Y. Hong and E. Viterbo, "Unshared Secret Key Cryptography," in IEEE Transactions on Wireless Communications, vol. 13, no. 12, pp. 6670-6683, Dec. 2014, doi: 10.1109/TWC.2014.2364022.