*International Journal for Modern Trends in Science and Technology*
*Volume 12, Special Issue 01*, pages 527-537.
ISSN: 2455-3778 online
Available online at: http://ijmtst.com/ICRCSET2026.html
DOI: https://doi.org/10.5281/zenodo.19561927

# Reversible Logic–Based Cryptographic Architecture for Secure Text Message Transmission

**RH Naik, Kakarla Mounika, Kondameedi Venkata Gopi, Dintakurthi Srikanth, K J Pavan Kumar**

*Department of Electronics and Communications Engineering, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India.*

**To Cite this Article**
RH Naik, Kakarla Mounika, Kondameedi Venkata Gopi, Dintakurthi Srikanth & K J Pavan Kumar (2026). Reversible Logic–Based Cryptographic Architecture for Secure Text Message Transmission. International Journal for Modern Trends in Science and Technology, 12(SI01), 527-537. https://doi.org/10.5281/zenodo.19561927

**Article Info**
Received: 02 March 2026; Revised: 01 April 2026; Accepted: 04 April 2026.



***KEYWORDS***

*Reversible Logic Circuits; Cryptography; Secure Text Communication; Toffoli Gate; CNOT Gate; Power Analysis Attack Resistance; Energy-Efficient Hardware; Internet of Things (IoT)*

**ABSTRACT**

*Cryptography plays a vital role in securing communication within modern digital systems. However, conventional hardware implementations of cryptographic algorithms are often susceptible to power-based side-channel attacks such as Differential Power Analysis (DPA) and Simple Power Analysis (SPA). To mitigate these vulnerabilities, reversible logic has emerged as a promising paradigm due to its ability to perform lossless computation with theoretically minimal energy dissipation. This paper proposes a symmetric cryptographic model for secure text message encryption and decryption based on reversible logic circuits. The proposed framework utilizes reversible gates, including CNOT, Toffoli, and k-CNOT gates, to perform cryptographic transformations while preserving information integrity. Furthermore, a secure key distribution mechanism is incorporated to enable safe transmission of the sender's private key to the receiver. Experimental evaluation demonstrates that the proposed model maintains data integrity, provides resilience against power analysis attacks, and achieves nearly identical encryption and decryption times even as the input size increases. Owing to its low theoretical power consumption and enhanced security characteristics, the proposed reversible logic–based cryptographic model is well suited for resource-constrained environments such as Internet of Things (IoT) devices, mobile platforms, and embedded systems.*

## I. INTRODUCTION

Cryptography has become an essential component for ensuring secure communication in modern digital environments. With the rapid expansion of internet-based applications, mobile computing, and digital transactions, protecting sensitive information such as personal data, financial records, and confidential messages from unauthorized access has become increasingly important. Cryptographic techniques enable secure communication by transforming readable information, known as plaintext, into an encoded form called ciphertext, which can only be interpreted by authorized users possessing the appropriate key. In general, the cryptographic process involves two main

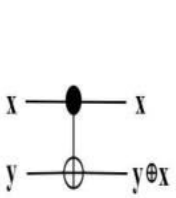
phases: encryption and decryption. During encryption, plaintext is converted into ciphertext using a secret key, whereas in decryption, the ciphertext is transformed back into its original plaintext form using the corresponding key. In symmetric cryptography, the same key is utilized for both encryption and decryption operations [1].

Conventional symmetric cryptographic algorithms, such as the Advanced Encryption Standard (AES), are primarily implemented using irreversible digital logic circuits [1]. These circuits inherently lead to information loss during computation, resulting in increased energy dissipation and heat generation. Traditional cryptographic systems rely on one-way computational functions, where forward computation is straightforward but reversing the computation is computationally complex [2]. This characteristic increases the computational overhead in modern cryptographic systems and also contributes to energy inefficiency.

Reversible computing has emerged as a promising alternative to overcome the limitations associated with irreversible computation. In reversible logic circuits, every output state uniquely corresponds to a specific input state, thereby ensuring a bijective input–output mapping [18]. This property allows computations to be performed in both forward and reverse directions without losing information. The theoretical foundation for reversible computation was established by Landauer, who stated that the loss of one bit of information during irreversible computation leads to the dissipation of kTln2 joules of energy, where k represents the Boltzmann constant and T denotes the absolute temperature of the system [3]. Later, Bennett demonstrated that this energy dissipation can be minimized by designing computational circuits using reversible logic, which preserves information throughout the computation process [4]. As a result, reversible logic circuits offer significant advantages in terms of reduced energy consumption and minimal heat generation.

A reversible logic function is defined as a function in which every output pattern is uniquely mapped to an input pattern, thereby ensuring bijective mapping between inputs and outputs [3]. In reversible systems, the number of inputs must be equal to the number of outputs, and the mapping between them must be one-to-one [5]. Reversible logic functions are implemented using reversible gates, which form the basic building blocks of reversible circuits. Several reversible gates have been proposed in the literature, including the NOT gate, CNOT gate [6], Toffoli gate [7], and k-CNOT gate [7]. These gates are widely used in the design of reversible circuits and cryptographic systems.

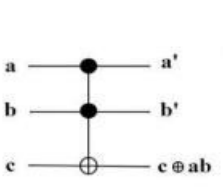
The CNOT gate consists of two inputs and two outputs, where one input acts as the control signal and the other serves as the target signal. The state of the target bit is inverted when the control bit is in the specified state. The structure and truth table of the CNOT gate are illustrated in **Fig. 1**.




| input | | output | |
|---|---|---|---|
| x | y | x | y⊕x |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

**Figure1**: **Figurative representation of CNOT gate and its truth table**

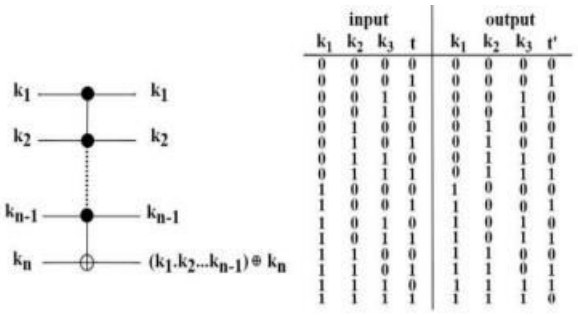
The Toffoli gate is a three-input and three-output reversible gate with two control inputs and one target input. It is considered a universal reversible gate because it can implement any Boolean function by appropriately configuring the control signals. The structure and operation of the Toffoli gate are shown in **Fig. 2**.




| input | | | output | | |
|---|---|---|---|---|---|
| a | b | c | a' | b' | c⊕ab |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 |

**Figure 2**: **Figurative representation of Toffoli gate and its truth table**

Similarly, the k-CNOT gate extends this concept by incorporating multiple control inputs along with a single target input. The target bit changes its state only when all control inputs satisfy the required condition. The structure and truth table of the k-CNOT gate are depicted in **Fig. 3**.




| input | | | | output | | | |
|---|---|---|---|---|---|---|---|
| $k_1$ | $k_2$ | $k_3$ | t | $k_1$ | $k_2$ | $k_3$ | t' |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |

**Figure 3**: **Figurative representation of k-CNOT gate and its truth table**

Reversible circuits are constructed by cascading reversible gates while maintaining an equal number of input and output lines. Unlike conventional digital circuits, reversible circuits do not allow fan-out or feedback connections, ensuring that the computation remains reversible throughout the circuit [8], [9]. The arrangement of reversible gates in a cascade structure enables efficient implementation of reversible computations. An example of such a reversible structure is the **hwb4 benchmark reversible circuit**, which contains four input lines and multiple reversible gates arranged in sequence. This circuit is composed of CNOT and Toffoli gates and serves as a common benchmark for evaluating reversible circuit designs. The architecture of the hwb4 reversible circuit is illustrated in **Fig. 4**.

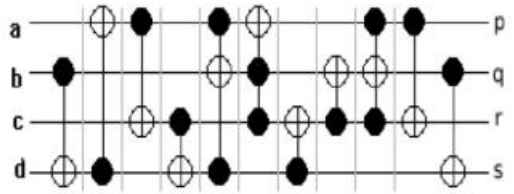



**Figure 4**: **Illustration of hwb4 reversible benchmark circuit**

Motivated by the advantages of reversible logic, this work focuses on designing a symmetric cryptographic model that supports lossless encryption and decryption of text messages. The proposed reversible cryptographic system ensures that no information is lost during the communication process between the sender and the receiver. Because reversible circuits allow the input to be uniquely determined from the output and vice versa, they are well suited for secure communication systems. In addition, reversible logic circuits exhibit reduced energy dissipation and lower heat generation, which improves their suitability for lightweight cryptographic applications.

Furthermore, the proposed model provides resilience against side-channel attacks such as Differential Power Analysis (DPA) and Simple Power Analysis (SPA), where attackers attempt to extract secret keys by observing power consumption patterns and heat generation. The efficient power usage, reduced circuit complexity, and reversible computation characteristics contribute to enhancing the security and performance of the proposed cryptographic system. Consequently, the proposed reversible logic–based cryptographic model can be effectively applied to energy-constrained platforms such as Internet of Things (IoT) devices, mobile systems, and embedded hardware platforms.

## 2.LITERATURE REVIEW

In this section, some of the previous research findings related to our proposed work are reviewed. In 2004, the authors in [10] discussed that in the present era of computers and the internet, communication is a major factor in the growth of technology. Therefore, the communicated data needs to be protected. In 2006, Gennaro [12] reviewed the utilization of randomness in cryptography and explained that it is crucial in cryptographic systems which makes it difficult for hackers to break the algorithm. In 2013, the authors in [13] implemented a standard data encryption technique by using reversible gate logic. In this work, no bit of information loss and less power consumption were stated as compared to traditional dataencryption.

In 2015, Kuchhal et al. [14] prepared a model of a Data Encryption Standard (DES) using reversible logic that demonstrated increased data security and reduced power consumption. In 2019, Elmogy et al. [11] proposed a symmetric cryptography algorithm to produce a new cipher text from text messages serving a better connection between encrypted characters and original characters depending on their ASCII value. In 2020, B. M. Krishna et al. [15] proposed a Field Programmable Gate Array (FPGA) implementation of a cryptography system for image encryption and decryption with the help of reversible logic to reduce power consumption and information loss. In 2024, Bhoyar et al. [16] designed a lightweight Concurrent Error Detection (CED) architecture for the Simeck cryptographic algorithm for IoT devices to enhance fault detection capabilities. Fault detection can be improved with the help of reversible logic by resisting temporary and permanent faults due to information loss.

In 2024, Sultan et al. [17] proposed Internet of Things sensor nodes and an energy efficient encryption technique that can be improved by adding reversible logic to the cryptographic components. The already optimized AES algorithm in this research can achieve further power consumption reductions, making it more appropriate for low-energy Internet of Things applications while maintaining cryptographic strength. The literature studies show that with the advancement in the field of reversible logic, reversible circuits can be designed to implement encryption as well as decryption efficiently without loss of data while restricting power consumption. Very limited research is done in symmetric cryptography to encrypt and decrypt text messages using reversible logic circuits, including network security for the secured key distribution process. Therefore, in this paper, we have proposed a symmetric cryptography model using reversible logic circuits that can encrypt and decrypt text messages in bulk. As a part of network security, we have designed a secured key distribution technique to send the private key to the receiver securely.

## 3.EXISTING SYSTEM

Over DES is a secret-key archetypal block cipher with block size of 64 bits. DES encrypts a block of 64-bit plaintext into 64-bit cipher text using 64-bit secret key (Left most bit of a block is bit one). Block diagram of the DES algorithm is shown in the Figure 5.

DES adopted in 1977 by the National Bureau of Standards now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).

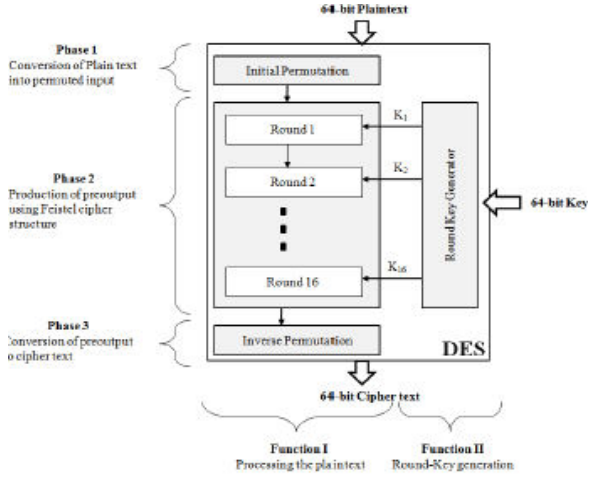



**Figure 5. General block diagram of DES algorithm**

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of

the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. A TDEA key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipherand decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force “exhaustion attack.” Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

DES Encryption process has two functions

A. Processing the plaintext

B. Round-Key generation

A. Processing the plaintext

The processing of plaintext proceeds in three phases.

1. Conversion of Plain text into permuted input

2. Production of preoutput using Feistel cipher structure

3. Conversion of preoutput to cipher text

### 1.Conversion of Plain text into permuted input

The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input, which is split into two 32-bit halves L0 and R0 where first 32 bit is L0 and next 32-bit is R0.

Permutation is keyless and can be predetermined. This has no cryptographic significance but included to facilitate loading blocks in and out of hardware and to make DES run slower in software.

### 2.Production of preoutput using Feistel cipher structure

Most symmetric block encryption algorithms are based on Feistel [14] structure. Feistel proposed the use of a cipher that alternates substitutions and permutations which is a practical application of a product cipher that alternates confusion and diffusion functions producing Substitution-Permutation Network (SP Network) [15].

**3.Conversion of preoutput to cipher text**

The preoutput is passed through a permutation (IP-1) that is the inverse of the initial permutation function, to produce the 64-bit cipher text. This stage has no cryptography significance in DES. The initial and final permutations are straight P-boxes that are inverses of each other.

**B. Function 2- Round-Key generation**

DES takes 64-bit key as input. Among 64-bit key only 56 bitsare effective and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection or set arbitrarily or can be ignored [13]. The 8 error detecting bits are set to make the parity of each8-bit byte of the key odd, i.e., there is an odd number of "1"s in each byte. The round-key generator creates sixteen 48-bit round/sub keys out of a 56-bit cipher key. The round key generation block is shown in Figure 2

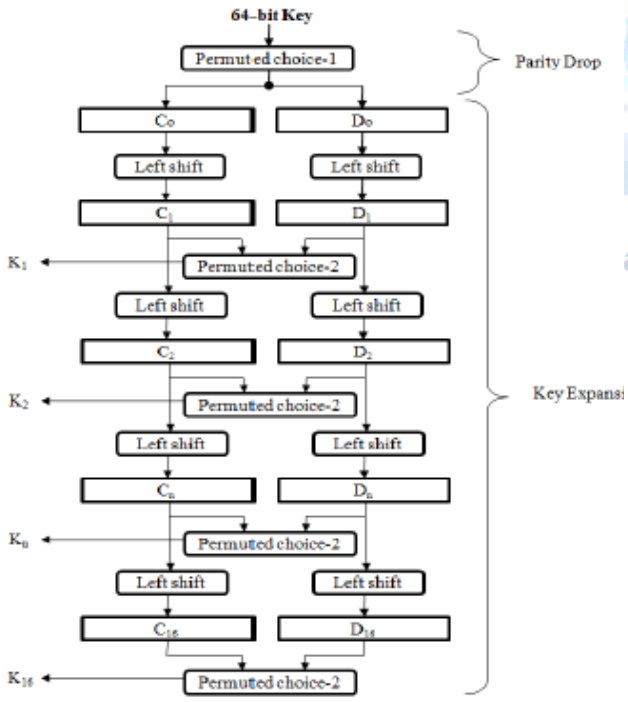



**Figure 6. General block diagram of DES algorithm**

## 4.REVERSIBLE LOGIC–BASED CRYPTOGRAPHIC ARCHITECTURE FOR SECURE TEXT MESSAGE TRANSMISSION

The proposed cryptographic system is developed using reversible logic gate (RLG) architecture to enhance data security while minimizing power consumption and information loss. The methodology begins with the design and optimization of reversible logic gates that form the core of the encryption and decryption units. These gates are selected and arranged to ensure that each output can be uniquely mapped back to its input, guaranteeing lossless computation. Circuit-level simulations are performed to validate the functional correctness and reversibility of the designed logic structures.

The next phase involves the integration of a Linear Feedback Shift Register (LFSR) to generate dynamic and unpredictable cryptographic keys. The LFSR is designed to operate efficiently with the reversible logic architecture, ensuring low power dissipation and improved randomness compared to traditional key generation methods. The key stream produced by the LFSR is used to drive the encryption and decryption processes, enabling secure data transformation with reduced complexity. Various tap sequences and polynomial configurations are analyzed to maximize key strength and resistance to cryptanalysis.

Finally, the reversible cryptographic system is implemented and evaluated against conventional cryptography methods such as AES-based designs. Performance metrics—including power consumption, resource utilization, encryption/decryption time, and security robustness—are measured using simulation tools and hardware-level testing when applicable. The results are compared with existing approaches to demonstrate improvements achieved through reversible logic. The proposed RLG-based cryptosystem shows enhanced efficiency and performance, validating the effectiveness of the methodology.

**4.1 Problem Identification**

Conventional cryptographic systems, such as AES and other scalable symmetric algorithms, rely on complex iterative processes for encryption and decryption. Although these methods provide strong security, they also introduce significant drawbacks, including high power consumption, elevated computational cost, and increased processing time. These limitations make such systems less suitable for applications requiring fast, low-power, and resource-efficient data protection—particularly in modern environments like embedded systems, IoT devices, and portable medical or banking applications. Additionally, traditional logic

circuits used in cryptographic hardware suffer from irreversible computation, which leads to information loss and heat dissipation, ultimately reducing system efficiency and security.

To address these issues, there is a need for a cryptographic model that minimizes power dissipation, prevents information loss, and delivers faster encryption and decryption. Existing methods do not fully leverage reversible logic principles, which can theoretically offer zero information loss and near-zero power consumption. Furthermore, key generation in traditional systems often lacks efficiency and may not provide adequate randomness for advanced security threats. Therefore, a new approach—such as using reversible logic gates (RLGs) combined with a robust LFSR-based key generator—is required to overcome the limitations of conventional models and enhance both the performance and security of cryptographic systems.

### 4.2 Proposed System

The proposed system introduces a reversible logic–based cryptographic architecture designed to overcome the limitations of conventional encryption methods. This system leverages the unique properties of reversible logic gates (RLGs), which inherently avoid information loss and significantly reduce power dissipation during computation. By replacing traditional irreversible logic components with reversible gates, the architecture ensures that every output can be traced back to its corresponding input, enabling secure and energy-efficient data processing. This forms the foundation of a more reliable and sustainable cryptosystem suitable for modern low-power applications.

A key feature of the proposed system is the integration of a Linear Feedback Shift Register (LFSR) for dynamic key generation. The LFSR is designed to operate within the reversible logic environment, ensuring efficient generation of high-quality pseudorandom keys. These keys are continuously updated and synchronized with the encryption process, enhancing security by making the cryptosystem resilient to brute-force and statistical attacks. Different polynomial taps and feedback paths are examined to identify the most secure and resource-efficient configuration.

The encryption and decryption units of the proposed cryptosystem are constructed purely using reversible logic gates. This ensures that both processes maintain lossless computation, reduced heat generation, and improved operational speed. Data is transformed using reversible circuits that maintain a one-to-one mapping between inputs and outputs, allowing error-free reconstruction. The design also minimizes garbage outputs and constant inputs, optimizing circuit performance and reducing resource overhead. As a result, the system delivers faster execution with lower energy requirements compared to traditional AES-based models.

Finally, the proposed system undergoes performance evaluation through simulation and hardware-level analysis to validate its efficiency. Metrics such as power consumption, execution time, propagation delay, resource utilization, and security strength are measured and compared against conventional cryptographic approaches. The results demonstrate that the RLG-based cryptosystem provides enhanced performance, particularly in low-power environments. With its combination of reversible logic and efficient key generation, the proposed system offers a viable and improved solution for secure communication in applications such as banking, healthcare, embedded devices, and IoT networks.

### 4.3 Block Diagram

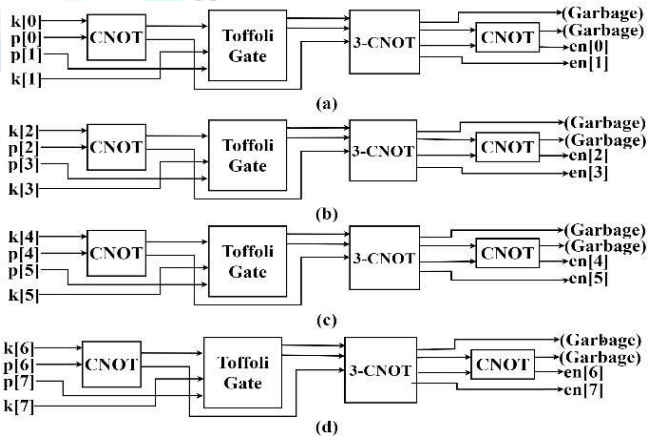



**Figure 6. Reversible logic circuit design for encryption process: (a) First bit pair of k[i] and p[i]. (b) Second bit pair of k[i] and p[i]. (c) Third bit pair of k[i] and p[i]. (d) Fourth bit pair of k[i] and p[i]**

### 4.4 Working Principle

In our proposed encryption model, to encrypt each character of the plain text, 8 CNOT gates, 4 TOFFOLI gates, and 4 3-CNOT gates are used as illustrated in Fig. 6. In the encryption process, the plain text is read from

an input file. First, each character of the plain text is converted to American Standard Code for Information Interchange (ASCII) value and then to their equivalent 8-bit binary number and is denoted as p[i]. Similarly, the first character of the sender's key is represented as k[i]. the circuit takes four inputs p[0], p[1], k[0], and k[1]. At first, p[0] and k[0] are sent to the first CNOT gate, then the first output bit of the first CNOT gate, k[1] and p[1] are fed as the 3-inputs to the TOFFOLI gate, respectively. The first two and the third output bits of the TOFFOLI gate are sent as the first two and fourth input bits of the 3-CNOT gate, respectively, and the second output bit of the first CNOT gate is sent as the third input of the 3-CNOT gate. Next, the second and third output bits of the 3-CNOT gate are fed as our first encrypted character, and the remaining outputs are garbage bits. Similarly, the same reversible circuit structures are considered for the p[2], p[3], k[2],k[3], p[4],p[5],k[4],k[5] and p[6],p[7],k[6],k[7]. The pair of the encrypted bits en[0], en[1], . . ., en[7] along with two garbage bits are generated from the primary gate of each circuit. This encrypted 8-bit binary is converted to the corresponding decimal value and then converted to the encrypted ASCII character to get the ciphertext.

In the decryption process, at first, each ciphertext character is converted into an 8-bit binary number, based on their ASCII value, and initialize them as en[i]. Similarly, the Key is initialized as k[i]. Circuit are similar and reverse of the encryption process. The 8-bit value of each character of the ciphertext and the private key is given as 3-input to our proposed decryption model. As depicted in Fig. 7, the circuit takes four inputs en[0], en[1], k[0], and k[1], and similar to encryption it produces two bits of the first character of the plaintext p[0] and p[1] along with two garbage bits. Similarly, the remaining bits of the Key and Ciphertext are given as input to the reversible circuits, and get the remaining bits of the plaintext. The circuits give outputs p[0] to p[7] along with garbage bits, as shown in Fig. 7. This decrypted 8-bit binary is similarly converted to its equivalent ASCII character to get the original character of our plaintext.

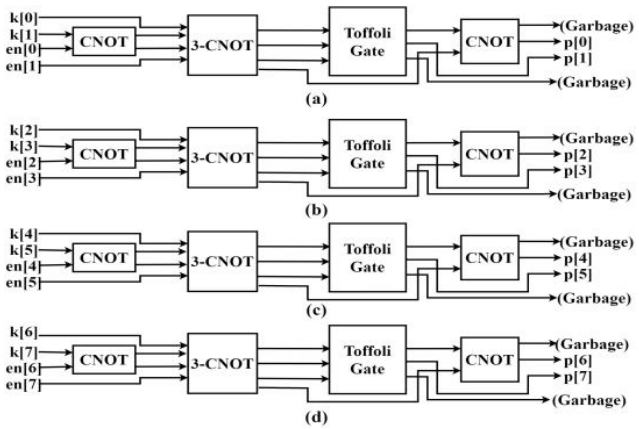



**Figure 7. Reversible logic circuit design for decryption process: (a) First bit pair of k[i] and en[i]. (b) Second bit pair of k[i] and en[i]. (c) Third bit pair of k[i] and en[i]. (d) Fourth bit pair of k[i] and en[i]**

## 4. RESULTS& DISCUSSION

Figure 8 shows the RTL (Register Transfer Level) schematic generated in the Vivado environment. The schematic represents the logical structure of the designed digital circuit using interconnected logic blocks

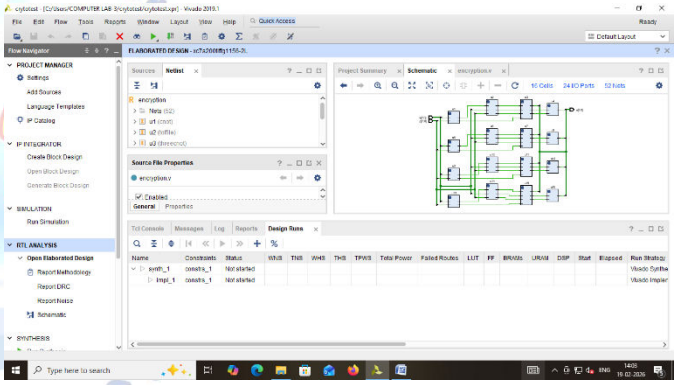


**Figure 8: RTL Schematic of the Designed Circuit**

Figure 9 shows the device view after implementation, where the synthesized circuit is mapped onto the FPGA device.

Analysis:

- Illustrates the physical placement of logic elements on the FPGA.
- Shows how design resources are allocated across the chip.
- Helps visualize the placement and routing of components.

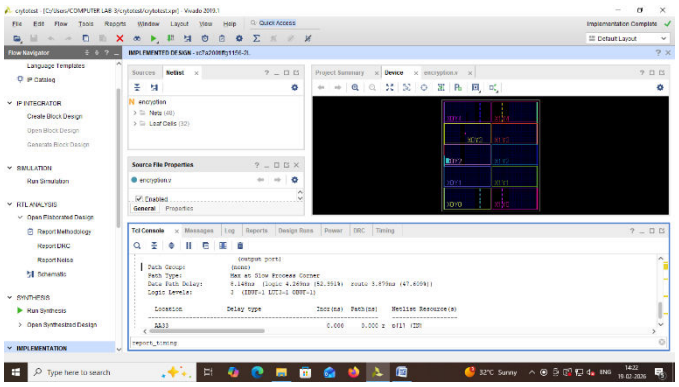


**Figure 9: Device Layout After Implementation**

Figure 10 presents the device resource utilization report generated after synthesis.

Analysis:

- Displays the number of resources used such as:
  - Slice LUTs
  - Slice Registers
  - Input/Output buffers
  - Block RAM or DSP units
- Useful to evaluate the hardware efficiency of the design.

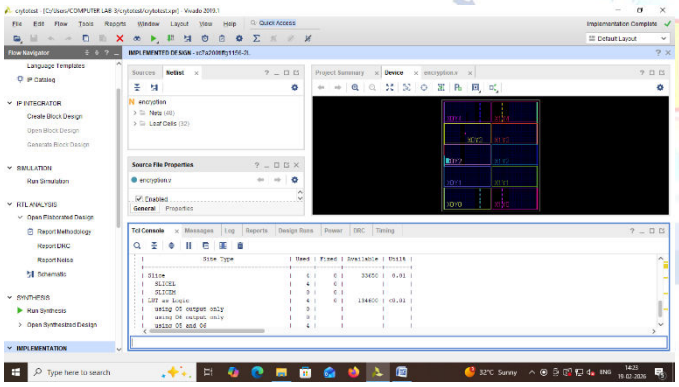


**Figure 10: Resource Utilization Report**

Figure 11 shows the power consumption report generated by the Vivado tool.

Analysis:

Displays the estimated power consumption of the circuit.

Includes parameters such as:Static power, Dynamic power. It helps to determine the energy efficiency of the VLSI design.

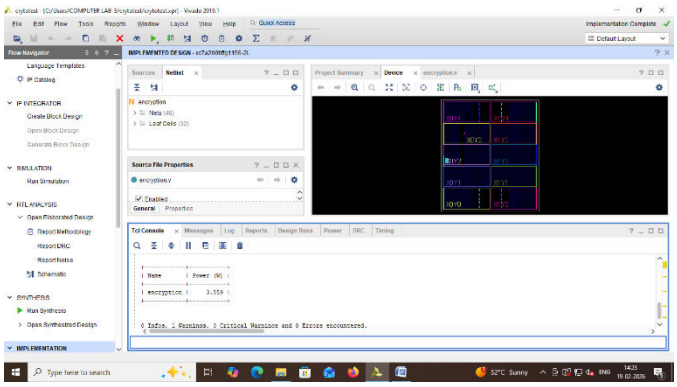


**Figure 11: Power Analysis Report**

Figure 12 shows the post-synthesis schematic of the circuit.

Analysis:

- Represents the optimized logic structure after synthesis.
- Shows how high-level RTL design is converted into actual logic gates and connections.

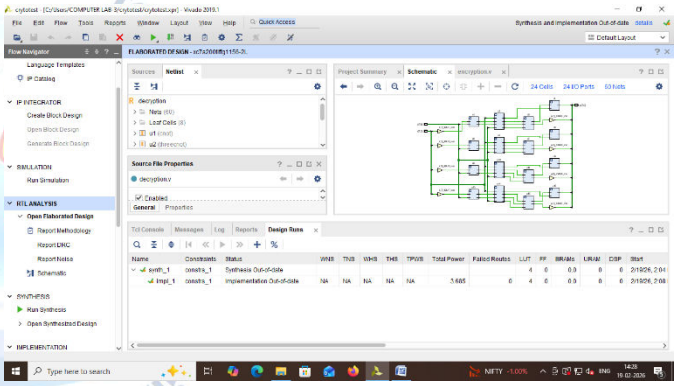


**Figure 12: Synthesized Circuit Schematic**

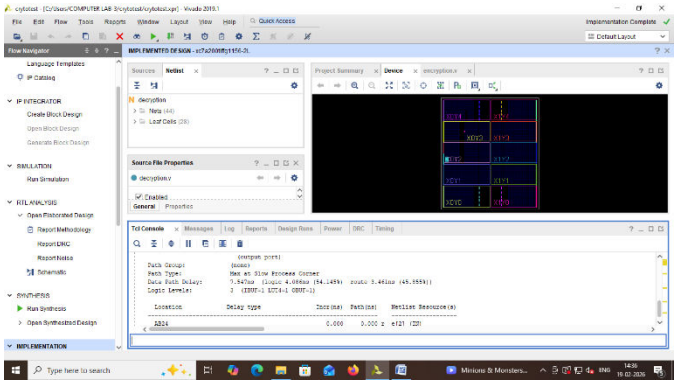


**Figure 13: Timing Analysis Summary**

Figure 13 shows the timing analysis summary generated after implementation.

Analysis:

- Provides important parameters such as:
  - Worst Negative Slack (WNS)

- Timing paths
- Clock delays

- Used to verify whether the design meets timing constraints.

Figure 14 displays the detailed timing report showing the critical paths of the design.

Analysis:

- Identifies the longest signal propagation paths in the circuit.
- Helps optimize the design to improve performance and speed

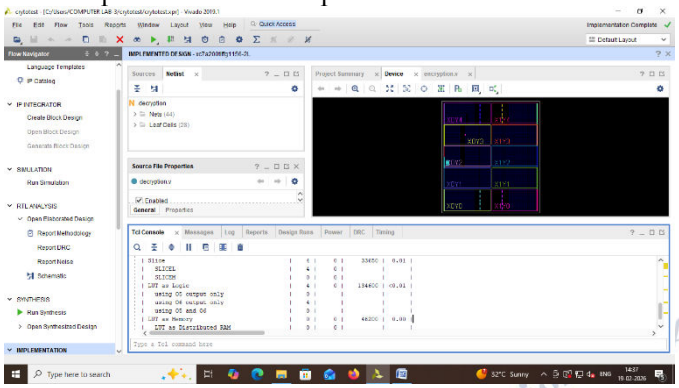


**Figure 14: Detailed Timing Path Report**

Figure 15 shows the final implementation and design rule check report.

Analysis:

- Confirms that the design completed implementation successfully.
- Indicates no critical warnings or errors.
- Ensures the design is ready for FPGA deployment.

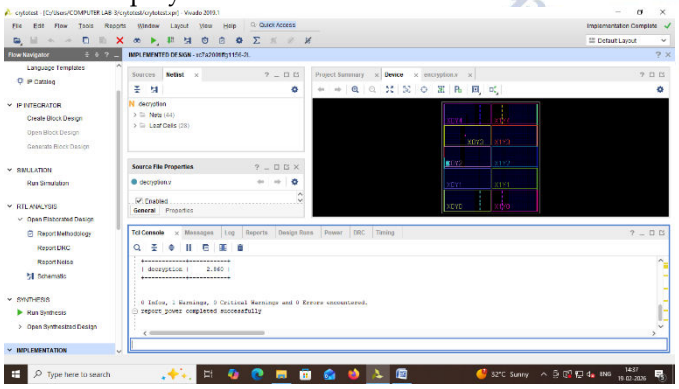


**Figure 15: Design Rule Check and Implementation Status**

## 5. CONCLUSIONS

The proposed reversible logic–based cryptographic system successfully addresses the limitations of conventional encryption methods by offering a low-power, secure, and efficient alternative. By integrating reversible logic gates with an LFSR-based key generation mechanism, the system achieves lossless computation, reduced power dissipation, and improved processing speed. Simulation and analysis demonstrate that the RLG architecture outperforms traditional cryptographic models in terms of resource utilization, execution time, and security strength. Overall, the proposed design provides a robust and energy-efficient solution suitable for modern applications such as IoT, medical devices, and secure communication systems.

Future work can focus on extending the proposed reversible logic–based cryptographic system to support more complex encryption algorithms and larger key sizes for enhanced security. The design can be further optimized by reducing the number of garbage outputs and constant inputs, improving the overall efficiency of the reversible circuits. Hardware implementation on FPGA or ASIC platforms will provide deeper insights into real-time performance, power consumption, and scalability. Additionally, integrating the system with IoT and edge-computing environments can help evaluate its suitability for lightweight and resource-constrained applications. Exploring adaptive key-generation techniques, quantum-resistant architectures, and machine-learning-based threat detection can further strengthen the robustness and future potential of the proposed cryptosystem.

### Conflict of interest statement

Authors declare that they do not have any conflict of interest.

### REFERENCES


[1] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," in 2016 International Conference on ICTin Business Industry and Government (ICTBIG), IEEE, pp. 1–4, 2016.

[2] H. F. Chau and H. K. Lo, "One-way functions in reversible

[3] computations," Cryptologia, vol. 22, no. 2, pp. 139–148, 1997.

[4] R. Landauer, "Irreversibility and heat generation in the computing process," IBM journal of research and development, vol. 5, no. 3, pp.183–191, 1961.

[5] C. H. Bennett, "Logical reversibility of computation," IBM J. Res.Dev., vol. 17, no. 6, pp. 525–532, November 1973.

[6] X. Ma, J. Huang, C. Metra and F. Lombardi, "Reversible gates andtestability of one-dimensional arrays of molecular QCA," Journal ofElectronic Testing, 24, pp. 297–311, 2008.

[7] R. P. Feynman, "Quantum mechanical computers," Foundation ofPhysics, vol. 16, no. 6, pp. 507–553, 1986.

[8] T.Toffoli, "Reversible computing," In: J. Bakker, J. Leeuwen, (eds.)ICALP 1980, LNCS, Springer, Heidelberg, vol. 85, pp. 632–644, 1980.

[9] K. N. Patel, J. P. Hayes, and I. L. Markov, "Fault testing for reversiblecircuits," IEEE Transactions on Computer-Aided Design

of IntegratedCircuits and Systems, vol. 23, no. 8, pp. 1220–1230, 2004.
[10] M. A. Nielson and I. L. Chuang, “Quantum Computation and QuantumInformation,” Monograph Collection (Matt - Pseudo), 2000.
[11] O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani,“Communications cryptography,” in 2004 RF and Microwave
[12] Conference (IEEE Cat. No. 04EX924), IEEE, pp. 220–223, 2004.
[13] A. Elmogy, Y. Bouteraa, R. Alshabanat and W. Alghaslan, “A NewCryptography Algorithm Based on ASCII Code,” in 2019 19thInternational Conference on Sciences and Techniques of AutomaticControl and Computer Engineering (STA), pp. 626–631, IEEE, 2019.
[14] R. Gennaro, “Randomness in cryptography,” IEEE security & privacy,vol. 4, no. 2, pp. 64–67, 2006.
[15] A. C. Nuthan, C. Nagaraj, and V. B. Havyas, “Implementation of dataencryption standard using reversible gate logic,” International Journalof Soft Computing and Engineering, vol. 3, no. 3, pp. 270–272, 2013.
[16] S. Kuchhal and R. Verma, “Security design of DES using reversiblelogic,” International Journal of Computer Science and NetworkSecurity (IJCSNS), vol. 15, no. 9, pp. 81, 2015.
[17] B. M. Krishna, K. C. S. Kavya, P. S. Kumar, K. Karthik, and Y. SNagababu, "FPGA implementation of image cryptology usingreversible logic gates," International Journal of Advanced TrendsinComputer Science and Engineering, vol. 9, no. 3, 2020.
[18] P. Bhoyar, P. Sahare, M.F. Hashmi, S. B. Dhok, and R. Deshmukh,"Lightweight architecture for fault detection in Simeck cryptographicalgorithms on FPGA," International Journal of InformationTechnology, vol. 16, no. 1, pp. 337-343, 2024.
[19] I. Sultan, M.T. Banday, "An energy efficient encryption technique forthe Internet of Things sensor nodes," International Journal ofInformation Technology, vol. 16, no. 4, pp. 2517–2533, 2024.
[20] M. K. Thomsen, "Describing and optimising reversible logic using afunctional language," International Symposium on Implementation andApplication of Functional Languages, pp. 148-163, 2011.
[21] R. Saravanakumar et al., “Dual-band performance enhancement of square wheel antennas with FR4 substrate for sub 7 GHz applications,” in Proc. ACROSET, IEEE, Sept. 2024, pp. 1–7.
[22] D. N. Ravikiran et al., “Secure visual data processing: Image encryption and decryption through reversible logic gates in VLSI design,” Int. J. Modern Trends Sci. Technol., vol. 10, no. 2, 2024.
[23] S. Saranya et al., “Meta surfaces with hole arrays for MIMO applications,” in Proc. ICOEI, IEEE, Apr. 2025, pp. 340–347.
[24] R. Thommandru, “Survey on MIMO antenna for 5G applications,” 2022.
[25] S. S. Vellela et al., “Improving network security using intelligent ensemble techniques,” in Proc. AMATHE, IEEE, May 2024, pp. 1–7.
[26] S. Sree Chandra et al., “Fruit classification based on shape, color and texture using image processing techniques,” Int. J. Modern Trends Sci. Technol., vol. 10, no. 3, pp. 100–107, 2024.
[27] R. Thommandru et al., “Millimetre wave self-isolated MIMO antenna with high isolation and radiation efficiency,” in Proc. IDCIoT, IEEE, Jan. 2024, pp. 191–196.
[28] S. Sree Chandra et al., “Verilog-based solution for multi-vehicle parking,” Int. J. Modern Trends Sci. Technol., vol. 10, no. 2, pp. 394–400, 2024.
[29] D. N. Ravikiran and C. G. Dethe, “Improvements in routing algorithms to enhance lifetime of wireless sensor networks,” Int. J. Comput. Netw. Commun., vol. 10, no. 2, pp. 23–32, 2018.
[30] R. Saravanakumar et al., “Cross scoop fractal antenna design with notch at 15 degree for emerging applications at 5.2 GHz,” in Proc. RAEEUCCI, IEEE, Apr. 2024, pp. 1–7.
[31] V. K. R. Devana et al., “A novel compact MIMO-UWB antenna with improved isolation using parasitic elements,” Arab. J. Sci. Eng., 2025.
[32] R. Thommandru and R. Saravanakumar, “Performance analysis of circularly polarised MIMO antenna for wireless applications,” in Proc. ICICNIS, IEEE, Dec. 2024, pp. 513–518.
[33] B. Nancharaiah et al., “Implementation and performance comparison of novel optimization approaches to counter starvation in wireless networks,” Int. J. Comput. Netw. Inf. Secur., vol. 17, no. 1, pp. 17–27, 2025.
[34] R. Thommandru, “Cost-effective circularly polarized MIMO antenna for Wi-Fi applications,” Nov. 2024.
[35] D. N. Ravikiran et al., “Optimized advanced encryption standard (AES) with enhanced S-box and automated key generation.”
[36] R. Saravanakumar et al., “Analysis circular wave guide antenna for 5G mid-band applications,” in Proc. ICACCS, IEEE, Mar. 2024, pp. 560–566.
[37] S. Swarna and V. R. Kolluru, “Active channel selection by sensors using artificial neural networks,” Int. J. Eng. Educ. Res., vol. 12, no. 4, pp. 1466–1473, 2024.
[38] D. N. Ravikiran et al., “Parametric facial landmark detection using active shape models.”
[39] C. H. Nagaraju et al., “Assimilation of blockchain for augmenting IoT-based smart home security,” in Blockchain Technology for IoT and Wireless Communications, CRC Press, 2023, pp. 79–87.
[40] R. Saravanakumar et al., “An armor-mounted antenna with deflected ground for sub-6 GHz applications,” in Proc. ICRISST, IEEE, Mar. 2024, pp. 1–7.
[41] D. N. Ravikiran and C. V. Akhil, “A face recognition method for security applications in smart homes and cities.”
[42] S. Swarna and V. R. Kolluru, “An intelligent data communication in IoT-based healthcare application using optimized routing protocol,” J. High Speed Netw., vol. 31, no. 2, pp. 159–179, 2025.
[43] D. N. Ravikiran et al., “Reversible logic-based cryptography design for secure and efficient data processing.”
[44] S. Swarna et al., “Optimized low-energy adaptive uneven clustering hierarchy for cognitive radio sensor networks,” 2026.
[45] R. Thommandru, “Innovative meta ring array antenna design for Ka-band,” 2004.
[46] D. N. Ravikiran et al., “IoT-based advanced automatic toll collection and vehicle detection system.”
[47] P. B. M. Krishna et al., “Design of CMOS ring modulator by built-in thermal tuning,” in Cognitive Computing Models in Communication Systems, 2022.
[48] B. Potti et al., “Genetic algorithmic approach to mitigate starvation in wireless mesh networks,” in Proc. ICCT, Springer, 2016.
[49] K. K. . Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
[50] Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w
[51] “Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks,” International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.
[52] K. K. Kommineni, P. Ande, “Blockchain-driven key management and privacy-preserving data Aggregation Scheme for SDN-enabled MANETs,” International Journal of Intelligent Engineering and Systems, vol. 18–18, no. 9, pp. 601–615, 2025, doi: 10.22266/ijies2025.1031.39.
[53] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on

Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.
[54] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic survey on security and privacy methods of cloud computing environment. Journal of Next Generation Technology, 2(1).
[55] Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.
[56] Polasi, P. K., Vellela, S. S., Narayana, J. L., Simon, J., Kapileswar, N., Prabu, R. T., & Rashed, A. N. Z. (2026). Data rates transmission, operation performance speed and figure of merit signature for various quadurature light sources under spectral and thermal effects. Journal of Optics, 55(1), 633-643.
[57] Vellela, S. S., Rao, M. V., Mantena, S. V., Reddy, M. J., Vatambeti, R., & Rahman, S. Z. (2024). Evaluation of Tennis Teaching Effect Using Optimized DL Model with Cloud Computing System. International Journal of Modern Education and Computer Science (IJMECS), 16(2), 16-28.
[58] Praveen, S. P., Vellela, S. S., & Balamanigandan, R. (2024). SmartIris ML: harnessing machine learning for enhanced multi-biometric authentication. Journal of Next Generation Technology (ISSN: 2583-021X), 4(1).
[59] Vellela, S. S., Rao, M. V., Krishna, C. V. M., Rao, T. S., & Dasthavejula, R. (2026). Piezoelectric and Shape-Memory Materials for Actuators and Energy Harvesting in Mechanical, Electronics, and Biomedical Engineering Using AI-Based Design. In Advanced Materials for Biomedical Devices (pp. 195-206). CRC Press.
[60] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.
[61] Praveen, S. P., Nakka, R., Chokka, A., Thatha, V. N., Vellela, S. S., & Sirisha, U. (2023). A novel classification approach for grape leaf disease detection based on different attention deep learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023.
[62] Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.