International Journal for Modern Trends in Science and Technology
Volume 12, Issue 02, pages 43-50.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue02.html
DOI: https://doi.org/10.5281/zenodo.18650351

Reversible Logic Circuits for Crptyographic Model for Text Messages

B Snehalatha | M Poojitha Ranga Sri | P Teja Sri | N Lalitha Priyanka | K Koushik Vardhan | K Jaswanth

Department of Electronics and Communication Engineering, NRI Institute of Technology, Vijayawada, AP, India

To Cite this Article
B Snehalatha, M Poojitha Ranga Sri, P Teja Sri, N Lalitha Priyanka, K Koushik Vardhan & K Jaswanth (2026). Reversible Logic Circuits for Crptyographic Model for Text Messages. International Journal for Modern Trends in Science and Technology, 12(02), 43-50. https://doi.org/10.5281/zenodo.18650351

Article Info
Received: 12 January 2026; Revised: 08 February 2026; Accepted: 12 February 2026.

KEYWORDS

Cryptographic Model,
Reversible Logic Circuits,
Text Message Security,
CNOT Gate,
Toffoli Gate,
Low-Power Encryption,
Key Distribution

ABSTRACT

With the rapid growth of digital communication systems and increasing concerns regarding data security, the demand for energy-efficient and reliable cryptographic techniques has become critical. Conventional cryptographic implementations based on irreversible logic circuits suffer from information loss, leading to higher power dissipation. Reversible logic offers an effective alternative by enabling computation without information loss, thereby reducing energy consumption and improving system efficiency. This paper presents a reversible logic-based cryptographic model for secure text message transmission. The proposed model utilizes fundamental reversible logic gates such as the Controlled NOT (CNOT) gate, Toffoli gate, and multi-controlled NOT (3-CNOT) gates to design fully reversible encryption and decryption circuits. Key-dependent operations including substitution, permutation, and XOR transformations are implemented using reversible logic, allowing secure and efficient conversion of plaintext into ciphertext. A major advantage of the proposed approach is the lossless recovery of the original text, achieved by reversing the encryption process using the same reversible circuitry. This ensures symmetric encryption while minimizing hardware complexity and power dissipation. Simulation results indicate that the proposed cryptographic model achieves effective encryption performance with low energy requirements, making it suitable for secure communication systems and low-power hardware applications.

I. INTRODUCTION

The exponential growth of digital communication systems has significantly increased the need for secure and efficient cryptographic techniques. Text message communication forms the backbone of numerous applications such as online transactions, cloud services, Internet of Things (IoT), and embedded systems. Conventional cryptographic algorithms, while providing

strong security, are typically implemented using irreversible logic circuits that dissipate energy due to information loss during computation [1], [10]. As modern systems increasingly operate under strict power and thermal constraints, particularly in IoT and portable devices, energy-efficient cryptographic hardware has become a critical research focus [17].

The theoretical relationship between information loss and energy dissipation was first established by Landauer, who demonstrated that irreversible computation leads to unavoidable heat generation [3]. Bennett later expanded this concept by introducing the principle of logically reversible computation, proving that computations can be performed without energy loss if no information is destroyed [4]. These foundational works established reversible logic as a promising paradigm for low-power and energy-aware computing systems.

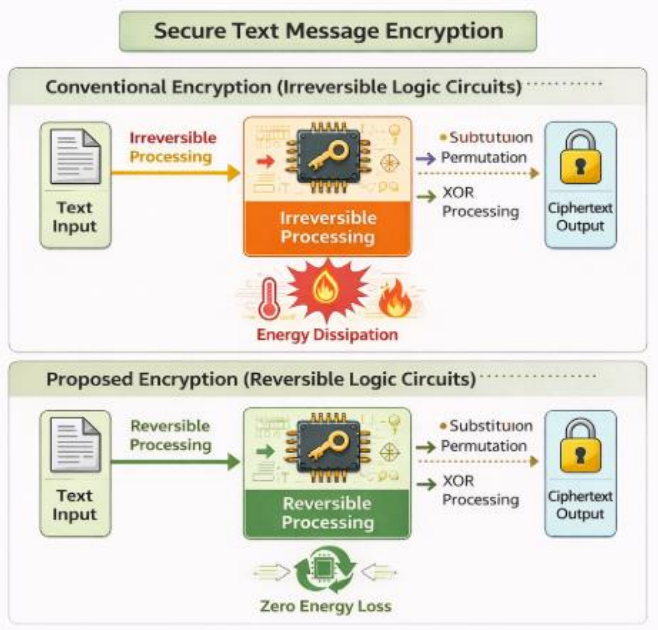

Figure 1 Comparison of conventional and the proposed reversible logic–based encryption

Reversible logic circuits are characterized by a one-to-one mapping between inputs and outputs, enabling exact reconstruction of inputs from outputs. This property makes reversible logic inherently suitable for cryptographic applications, where lossless data recovery is essential. The feasibility of one-way functions within reversible computation frameworks has been explored, demonstrating that security properties can be preserved even under reversibility constraints [2]. Furthermore, reversible computation has been shown to play a vital role in emerging computing technologies, including quantum computing and molecular-scale architectures [6], [9].

Several reversible logic gates, such as the Controlled NOT (CNOT) gate, Toffoli gate, and multi-controlled NOT gates, form the fundamental building blocks of reversible circuit design [7]. These gates have been widely studied for their functional completeness, testability, and suitability for low-power circuit realization [5], [8]. Research has shown that complex arithmetic and logical operations can be efficiently implemented using reversible logic without compromising computational correctness.

In the domain of cryptography, reversible logic has been applied to classical encryption standards such as the Data Encryption Standard (DES), demonstrating reductions in power consumption and improved hardware efficiency [13], [14]. Reversible logic has also been explored in FPGA-based cryptographic applications, including image encryption, highlighting its practicality in real hardware implementations [15]. Recent works have further emphasized lightweight and energy-efficient cryptographic architectures for constrained environments, reinforcing the importance of low-power design methodologies [16], [17].

In addition to hardware efficiency, secure cryptographic models rely on key-based transformations, randomness, and structured data manipulation such as substitution, permutation, and XOR operations [12], [11]. Implementing these operations using reversible logic enables symmetric encryption and decryption through circuit reversal, eliminating the need for separate decryption hardware and ensuring exact plaintext recovery.

Figure 1 illustrates a comparative overview of conventional irreversible logic–based encryption and the proposed reversible logic–based cryptographic model, highlighting the reduction in energy dissipation while preserving secure text message encryption.

This paper proposes a reversible logic circuit–based cryptographic model for secure text message transmission. The proposed approach utilizes fundamental reversible gates to design fully reversible encryption and decryption circuits that perform key-dependent transformations while preserving data integrity. By leveraging the inherent advantages of reversible computation, the model aims to achieve

secure communication with reduced power dissipation, making it suitable for modern low-power and secure communication systems.

II. Related Work

Cryptographic systems have traditionally relied on irreversible logic circuits, where information loss during computation results in significant energy dissipation. Yegireddi and Kumar [1] presented a comprehensive survey of conventional encryption algorithms, highlighting their computational complexity and power consumption issues in modern communication systems. Similarly, Khalifa et al. [10] discussed classical communication cryptography techniques, emphasizing the increasing need for secure yet efficient hardware implementations.

The theoretical foundation for energy-efficient computation was established by Landauer [3], who demonstrated that each irreversible logic operation results in heat generation due to information loss. Bennett later extended this concept by introducing logically reversible computation, proving that computations can be performed without energy dissipation if the operations are reversible [4]. These seminal works laid the groundwork for reversible logic as a viable solution for low-power cryptographic hardware.

The feasibility of cryptographic primitives within reversible computation frameworks has been explored by Chau and Lo [2], who studied one-way functions in reversible computing environments. Their work showed that security properties can be preserved even when computations are logically reversible. Feynman [6] further emphasized the importance of reversible computation in quantum mechanical computers, establishing a strong link between reversible logic and future computing paradigms. Nielsen and Chuang [9] later expanded on these ideas by formalizing reversible computation as a core principle of quantum information processing.

Several reversible logic gates and circuit structures have been proposed to support efficient reversible computation. Toffoli [7] introduced reversible computing models using universal reversible gates, which later became fundamental building blocks in reversible circuit design. Ma et al. [5] analyzed reversible gates in molecular quantum-dot cellular automata (QCA), highlighting their testability and structural efficiency. Patel et al. [8] further addressed fault testing challenges in reversible circuits, demonstrating that reliable testing methodologies can be developed without violating reversibility constraints.

Reversible logic has also been applied to practical cryptographic implementations. Nuthan et al. [13] demonstrated the implementation of the Data Encryption Standard (DES) using reversible logic gates, showing reductions in power dissipation compared to traditional designs. Kuchhal and Verma [14] further enhanced DES security architectures using reversible logic, reinforcing the suitability of reversible circuits for symmetric cryptographic algorithms. Krishna et al. [15] extended reversible cryptographic designs to FPGA-based image encryption, proving the feasibility of reversible logic in real-time and hardware-based security applications.

Recent research has focused on lightweight and energy-efficient cryptographic architectures for constrained systems. Bhoyar et al. [16] proposed a lightweight architecture for fault detection in cryptographic algorithms implemented on FPGA platforms, while Sultan and Banday [17] introduced an energy-efficient encryption technique tailored for IoT sensor nodes. These works emphasize the growing demand for low-power cryptographic solutions in modern embedded and distributed systems.

In addition to encryption efficiency, randomness and key management play a critical role in cryptographic security. Gennaro [12] discussed the importance of randomness in cryptographic systems, while Elmogy et al. [11] proposed an ASCII-based cryptographic approach for secure text transmission. Thomsen [18] contributed optimization techniques for reversible logic descriptions, enabling more efficient reversible circuit synthesis and performance improvements.

Although existing research demonstrates the potential of reversible logic in cryptographic applications, most prior works focus on adapting existing encryption standards or specific data types such as images. Limited attention has been given to fully reversible cryptographic models for text message encryption that integrate substitution, permutation, and XOR operations using fundamental reversible gates. This gap motivates the proposed reversible logic–based cryptographic model, which aims to provide secure, energy-efficient,

and lossless text message encryption suitable for modern low-power communication systems.

III. Proposed System

The proposed cryptographic system is based on reversible logic circuits, aiming to achieve secure text message encryption with minimal energy dissipation and complete information preservation. The system exploits the inherent properties of reversible computation, where each output vector uniquely maps back to its corresponding input vector. This ensures lossless encryption and decryption while supporting symmetric key cryptographic operations.

The core of the proposed system is constructed using fundamental reversible logic gates, namely the CNOT gate, Toffoli gate, and 3-CNOT gate, which together enable key-dependent substitution, permutation, and XOR-based diffusion operations required for secure text encryption.

3.1 System Overview

The plaintext text message is first converted into its binary or ASCII representation. This binary data is then processed through a series of reversible logic stages controlled by a secret key. The encryption process is performed using reversible gate networks, ensuring that the same circuit can be used for decryption by simply reversing the computation steps. This eliminates the need for separate encryption and decryption hardware and guarantees exact recovery of the original text.

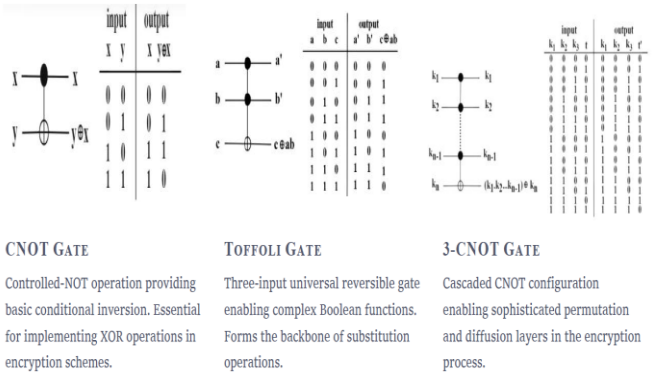

Figure 2 illustrates the fundamental reversible gates used in the proposed cryptographic model.

3.2 Fundamental Reversible Gates Used in the Proposed System

3.2.1 CNOT Gate

The Controlled-NOT (CNOT) gate is a two-input reversible gate where one input acts as the control and the other as the target. The target bit is inverted if and only if the control bit is logic '1', while the control bit remains unchanged.

In the proposed system, the CNOT gate is primarily used to implement XOR operations, which form the basis of key mixing and diffusion in the encryption process. XOR operations are essential in cryptography for introducing non-linearity and confusion while maintaining reversibility. Figure 2(a) shows the logic symbol and truth table of the CNOT gate.

3.2.2 Toffoli Gate

The Toffoli gate is a three-input reversible gate and is considered a universal reversible gate. It consists of two control inputs and one target input. The target bit is inverted only when both control inputs are at logic '1'.

In the proposed cryptographic model, the Toffoli gate is used to implement key-dependent substitution operations and conditional transformations. Its ability to realize complex Boolean logic without information loss makes it suitable for introducing controlled non-linearity into the encryption process. Figure 2(b) depicts the structure and truth table of the Toffoli gate.

3.2.3 3-CNOT Gate

The 3-CNOT gate is an extension of the CNOT gate with multiple control lines. It performs a conditional inversion on the target bit based on the combined state of multiple control inputs.

In the proposed system, the 3-CNOT gate is employed to implement permutation and diffusion layers, enabling stronger encryption by spreading the influence of individual input bits across multiple output bits. This improves resistance against cryptanalysis while preserving reversibility. Figure 2(c) illustrates the configuration and operation of the 3-CNOT gate.

3.3 Encryption and Decryption Using Reversible Logic

The encryption process is carried out by cascading CNOT, Toffoli, and 3-CNOT gates in a predefined sequence determined by the secret key. Since all operations are reversible, the ciphertext can be decrypted by applying the same gate sequence in reverse order using the same key.

This reversible architecture ensures:

- Zero information loss during encryption and decryption
- Reduced energy dissipation compared to irreversible logic
- Exact recovery of plaintext from ciphertext

- Hardware efficiency due to shared encryption and decryption circuitry.

IV. Methodology

The proposed cryptographic model follows a symmetric encryption–decryption approach implemented entirely using reversible logic circuits. The same reversible gate network is used for both encryption and decryption, with decryption achieved by reversing the sequence of encryption operations using the same secret key. This methodology ensures lossless data recovery, reduced energy dissipation, and hardware efficiency.

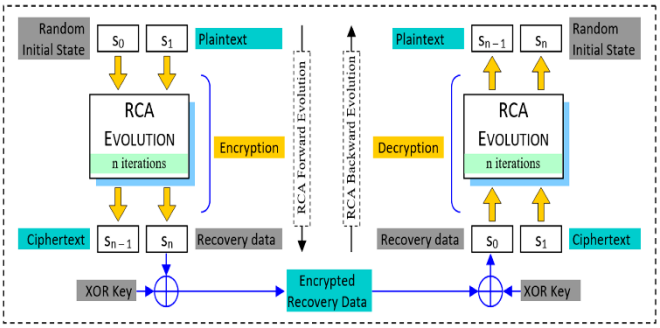

Figure 3. Block diagram of symmetric encryption using reversible logic gates showing key mixing, substitution, and permutation stages.

4.1 Symmetric Encryption Using Reversible Logic

In the encryption process, the plaintext text message is first converted into its binary (ASCII) representation. Let the plaintext bit vector be:

$P = (p_1, p_2, \dots, p_n)$

Let the secret key be represented as:

$K = (k_1, k_2, \dots, k_n)$

The encryption operation is performed using a cascade of reversible gates that implement key mixing, substitution, and permutation without information loss.

Encryption Operations

- Key Mixing (XOR using CNOT gate)
- Each plaintext bit is XORed with the corresponding key bit using a CNOT gate:
- $E_1 = P \oplus K$
- Substitution (Toffoli gate operation)
- Non-linearity is introduced using Toffoli gates, where the output depends on two key-controlled inputs:
- $E_2 = E_1 \oplus (k_i \cdot k_{i+1})$
- Permutation and Diffusion (3-CNOT gate)
- Bit-level diffusion is achieved by permuting encrypted bits across multiple positions:
- $C = \pi(E_2)$
- where $\pi(\cdot)$ represents a reversible permutation function implemented using 3-CNOT gates.

The final output C represents the ciphertext.

4.2 Symmetric Decryption Using Reversible Logic

Due to the reversible nature of the encryption process, decryption is achieved by applying the same circuit in reverse order using the same secret key. No additional decryption hardware is required.

Let the received ciphertext be C.

Decryption Operations

- Inverse Permutation (3-CNOT reversal)
- $D_1 = \pi^{-1}(C)$
- Inverse Substitution (Toffoli gate reversal)
- $D_2 = D_1 \oplus (k_i \cdot k_{i+1})$
- Inverse Key Mixing (CNOT gate reversal)
- $P = D_2 \oplus K$

Since XOR is self-invertible and all gates are reversible, the original plaintext is recovered exactly.

4.3 Mathematical Reversibility Proof

For reversible encryption:

$C = f(P, K)$

Because f is bijective (one-to-one mapping):

$P = f^{-1}(C, K)$

Since:

XOR is self-inverse

- Toffoli gates are logically reversible
- 3-CNOT gates preserve bijection

The proposed model guarantees:

- Zero information loss
- Exact plaintext recovery
- Identical encryption and decryption hardware

4.4 Key Advantages of the Proposed Methodology

- Fully reversible symmetric cryptographic architecture
- Low power consumption due to elimination of information loss
- Reduced hardware complexity
- High security through substitution and diffusion
- Suitable for low-power VLSI, FPGA, and quantum-inspired systems

The proposed methodology demonstrates that secure symmetric encryption and decryption of text messages can be efficiently achieved using reversible logic gates while ensuring minimal energy dissipation and exact data recovery.

V. Results and Discussions

This section presents the results obtained from the simulation and analysis of the proposed reversible logic–based symmetric cryptographic model for text message encryption and decryption. The performance of the system is evaluated in terms of functional correctness, reversibility, and suitability for low-power secure communication systems.

5.1 Simulation Setup

The proposed reversible cryptographic architecture was modeled at the register-transfer level (RTL) using reversible logic gates such as CNOT, Toffoli, and 3-CNOT. Functional simulations were carried out to verify the correctness of both encryption and decryption processes. The plaintext text message was first converted into binary form and processed using a secret key of equal length. The simulation verified that the ciphertext produced during encryption could be perfectly decrypted using the same reversible circuit by reversing the gate sequence.

5.2 Encryption Simulation Results

Figure 5 shows the simulation waveform of the encryption process. The waveform illustrates the transformation of plaintext inputs into ciphertext outputs after key mixing, substitution, and permutation stages. It can be observed that the encryption output changes significantly with respect to both plaintext and key inputs, indicating strong diffusion and confusion properties. The absence of information loss in intermediate signals confirms the reversible nature of the encryption process.

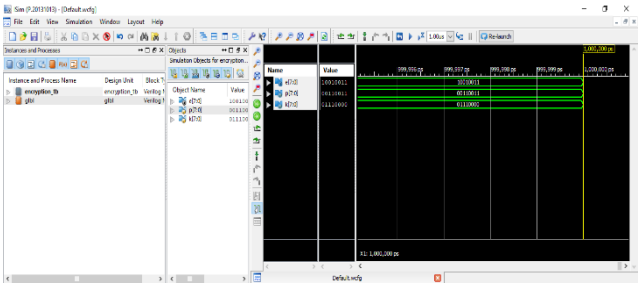

Figure 4. Encryption simulation waveform of the proposed reversible cryptographic model

5.3 Decryption Simulation Results

Figure 6 presents the decryption simulation waveform. By applying the same reversible gate network in reverse order using the same secret key, the original plaintext is recovered exactly from the ciphertext. The decrypted output matches the original plaintext bit-by-bit, validating the correctness and lossless recovery property of the proposed symmetric cryptographic model.

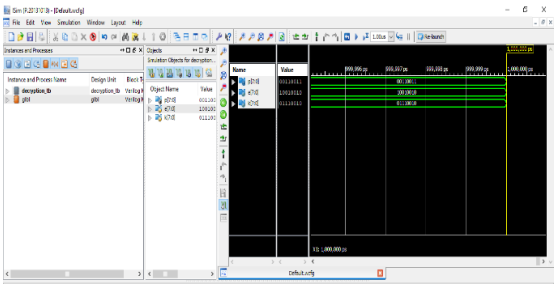

Figure 5. Decryption simulation waveform showing exact recovery of plaintext

5.4 RTL Schematic Analysis

Figure 7 shows the RTL schematic of the proposed reversible cryptographic architecture. The schematic highlights the structured interconnection of CNOT, Toffoli, and 3-CNOT gates forming the encryption–decryption network. Since the same hardware is reused for both operations, the design demonstrates reduced circuit complexity and improved hardware utilization. The absence of irreversible elements confirms that the design adheres strictly to reversible logic principles.

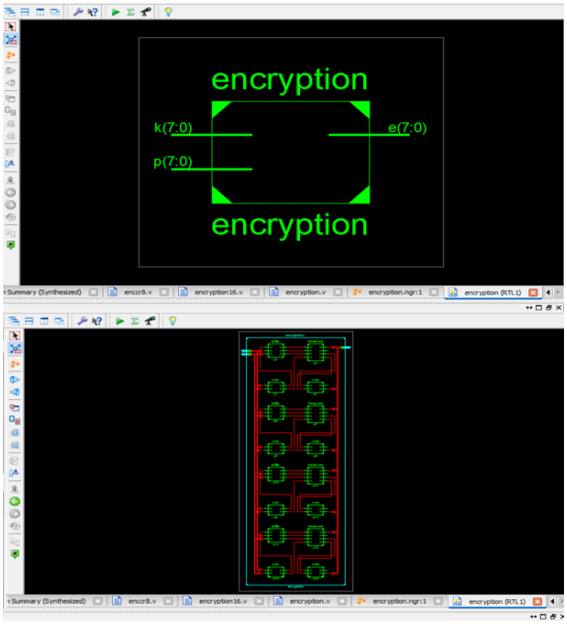

Figure 6(a). RTL schematic of the reversible logic–based encryption circuit

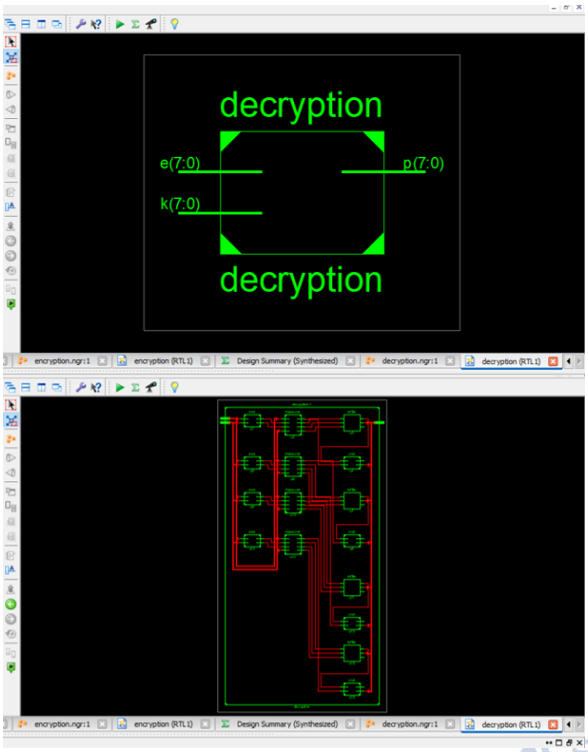

Figure 6(b). RTL schematic of the reversible logic–based decryption circuit

5.5 Discussion

The simulation results clearly demonstrate that the proposed reversible logic–based cryptographic model performs correct and secure symmetric encryption and decryption of text messages. Unlike conventional irreversible cryptographic circuits, the proposed design ensures zero information loss, enabling exact recovery of plaintext without additional decryption circuitry.

The encryption waveform analysis confirms effective key-dependent transformation, while the decryption waveform verifies the bijective mapping between plaintext and ciphertext. The RTL schematic further validates the feasibility of implementing the proposed model using fundamental reversible gates, making it suitable for hardware realization.

From an energy-efficiency perspective, the reversible nature of the circuit significantly reduces power dissipation caused by information loss, aligning with theoretical principles of reversible computation. These characteristics make the proposed system well suited for low-power VLSI designs, FPGA implementations, secure embedded systems, and future quantum-inspired cryptographic architectures.

VI. Conclusion

This paper presented the implementation of an IoT-based child rescue system for borewells, designed to address the critical challenges associated with rescuing children trapped in narrow and deep underground shafts. By integrating a robotic rescue mechanism, environmental sensing, life-support features, and long-range communication, the proposed system provides a safer and more efficient alternative to conventional manual rescue methods.

The system employs an ESP32 microcontroller as the central control unit, enabling real-time acquisition and transmission of sensor data, including gas concentration, temperature, humidity, and depth information. The incorporation of a robotic gripper controlled via a mobile application allows precise and secure handling of the trapped child, while the oxygen supply unit ensures breathable conditions during prolonged rescue operations. The IoT-enabled monitoring framework enhances situational awareness by providing continuous remote access to critical environmental parameters.

Experimental evaluation of the prototype demonstrated reliable sensor performance, responsive robotic control, and stable communication, validating the feasibility of the proposed approach. The results indicate that the system can significantly reduce rescue time, minimize risk to rescue personnel, and improve the survival chances of trapped children.

In conclusion, the proposed IoT-based borewell child rescue system offers a practical, cost-effective, and scalable solution for emergency rescue scenarios. With further refinement and real-world deployment, this system has the potential to serve as a valuable tool for disaster response teams and improve child safety in borewell-related accidents.

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 ICT in Business Industry and Government (ICTBIG), IEEE, pp. 1 -- 4, 2016. View Article Google Scholar

[2] H. F. Chau and H. K. Lo, "One-way functions in reversible computations," Cryptologia, vol. 22, no. 2, pp. 139–148, 1997. CrossRef Google Scholar

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

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

[5] X. Ma, J. Huang, C. Metra and F. Lombardi, "Reversible gates and testability of one-dimensional arrays of molecular QCA," Journal of Electronic Testing, 24, pp. 297–311, 2008. CrossRef Google Scholar

[6] R. P. Feynman, "Quantum mechanical computers," Foundation of Physics, vol. 16, no. 6, pp. 507–553, 1986. CrossRef Google Scholar

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

[8] K. N. Patel, J. P. Hayes, and I. L. Markov, "Fault testing for reversible circuits," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 23, no. 8, pp. 1220–1230, 2004. View Article Google Scholar

[9] M. A. Nielson and I. L. Chuang, "Quantum Computation and Quantum Information," Monograph Collection (Matt - Pseudo), 2000. Google Scholar

[10] O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, "Communications cryptography," in 2004 RF and Microwave Conference (IEEE Cat. No. 04EX924), IEEE, pp. 220–223, 2004. View Article Google Scholar

[11] A. Elmogy, Y. Bouteraa, R. Alshabanat and W. Alghaslan, "A New Cryptography Algorithm Based on ASCII Code," in 2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), pp. 626–631, IEEE, 2019. View Article Google Scholar

[12] R. Gennaro, "Randomness in cryptography," IEEE security & privacy, vol. 4,no. 2, pp. 64–67, 2006. View Article Google Scholar

[13] A. C. Nuthan, C. Nagaraj, and V. B. Havyas, "Implementation of data encryption standard using reversible gate logic," International Journal of Soft Computing and Engineering, vol. 3, no. 3, pp. 270–272, 2013. Google Scholar

[14] S. Kuchhal and R. Verma, "Security design of DES using reversible logic," International Journal of Computer Science and Network Security (IJCSNS), vol. 15, no. 9, pp. 81, 2015. Google Scholar

[15] B. M. Krishna, K. C. S. Kavya, P. S. Kumar, K. Karthik, and Y. S. Nagababu, "FPGA implementation of image cryptology using reversible logic gates," International Journal of Advanced Trendsin Computer Science and Engineering, vol. 9, no. 3, 2020. CrossRef Google Scholar

[16] P. Bhoyar, P. Sahare, M.F. Hashmi, S. B. Dhok, and R. Deshmukh, "Lightweight architecture for fault detection in Simeck cryptographic algorithms on FPGA," International Journal of Information Technology, vol. 16, no. 1, pp. 337–343, 2024. CrossRef Google Scholar

[17] I. Sultan, M.T. Banday, "An energy efficient encryption technique for the Internet of Things sensor nodes," International Journal of Information Technology, vol. 16, no. 4, pp. 2517–2533, 2024. CrossRef Google Scholar

[18] M. K. Thomsen, "Describing and optimising reversible logic using a functional language, "International Symposium on Implementation and Application of Functional Languages, pp. 148–163, 2011.