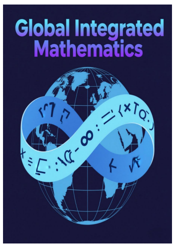
Global Integrated Mathematics

https://gim.gospub.com/gim

Global Open Share Publishing



Article

Optimized Integral Transform and Modular Arithmetic Encryption for Efficient Security in Digital Supply Networks

Prabakaran Raghavendran[*], **Tharmalingam Gunasekar**

Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India

[*]Corresponding author: Prabakaran Raghavendran, rockypraba55@gmail.com

Abstract

This study presents a new form of encryption technique combining the R-transform with modular arithmetic to suit secure data exchange in digital supply chain operations. Moving away from the conventional approach to cryptography, this study looks at how this potent combination could be used to transform the supply chain's sensitive data, thus keeping them impervious to cyber threats while allowing secure digital communication between nodes. It underlines the remarkable ability of the R-transform to make the data confidential and integrity of the supply chain network through an exhaustive analysis of the collaboration. Stringent experiments and analysis point toward a new kind of cryptographic method that would keep confidential supply chain information, creating trust and robustness in this digital era.

Keywords

Cryptography, Caesar cipher, Encryption, Decryption, R-Transform

Article History

Received: 12 May 2025
Revised: 21 May 2025
Accepted: 29 May 2025
Available Online: 04 June 2025

1. Introduction

Digitizing global supply chains through instant communications and real-time decision-making presents a new phase of the transformation. As that revolution throws opportunities and associated issues, its consequences ensure that data breaches, threats from cyber villains, and unrestricted access remain challenging issues for protection of sensitive information in the supply chains. Due to the growth in dependence for ever-increasingly interconnected digital platforms, securing supply chains against unauthorized access also demands robust and efficiently scalable encryption techniques to an unforeseen level today.

Other, more traditional methods, such as the Caesar cipher and Rivest–Shamir–Adleman (RSA) encryption, have been considered as a whole to be foundational tools in securing communication. The Caesar cipher is straightforward but serves as an excellent example of one form of substitution-based encryption, although it is not very practical for modern security due to its vulnerability to frequency analysis. Finally, there is an advanced technique by the name of RSA encryption. It relies on the use of modular arithmetic combined with big prime numbers to provide stronger security but consumes significant computing resources and, therefore, is less practical in resource-constrained environments or in real-time applications.

Mathematical transforms in cryptography have recently gained prominence, bringing along with them novel ways of processing and securing information. Being a very powerful tool typically used in signal processing and the analysis of functions of exponential order, R-transform also presents some special opportunities in the application areas of cryptography. Such opportunities arise because, through it, the data can be transformed into what is apparently non-intuitive in terms of the safe format needed to increase complexity for cryptography schemes against cryptanalysis attacks.

The Caesar cipher is one of the oldest cryptographic techniques, which was developed using simple substitution to encrypt messages [1]. Though it is historically important, it is certainly non-applicable in modern systems due to its vulnerability against frequency analysis. Singh [2] brings out the historical development of substitution ciphers and their significance in cryptography history as a basis. Shannon [3] establishes the principle of perfect secrecy. His emphasis on randomness in encrypting schemes served as the foundation for modern cryptographic systems. The argument would be that distributed ledger technologies establish the integrity of data, transparency, and trust, hence being in line with the well-known tenets of cryptography and the need for a scalable solution. Together, these references provide a perfect backdrop for illustrating the convergence of history, mathematics, and technology while at present and meeting those challenges which are pressing the world of information security.

A new encryption algorithm is proposed in the paper with the simplicity of the Caesar cipher but with the strength of the R-transform modified with modular arithmetic and polynomial transformations. The method to be proposed relies on the efficiency of computational modular arithmetic and the transformative properties of the R-transform in order to make a secure encryption technique practical for modern applications. It works on encoding of the plaintext into numerical sequences followed by polynomial transformations with R-transform which provided great obscurity in the data with the manageable overhead of computation.

The paper is composed of three prime objectives. (1) Design a mechanism of encryption based on the principles from both classical and modern cryptography, yet this time maintaining simplicity well balanced with appropriate robustness. (2) To make the world believe that it is indeed possible, through proper rigorous theoretical study, to construct the R-transform such that the encrypted messages actually possess effectiveness in security through suitable practical implementations. (3) Exploring the use of the suggested approach in supply chain networks data securing where encryption should be both efficient and reliable.

In another way, with an interconnected system, supply chains face the challenge of secure data exchange. Opposed to being robust in the conventional way, a cryptographic protocol may be unsuitable in systems of resource constraints, real-time processing, and the distributed architecture of Internet of Things (IoT) networks. With the bigger and more dangerous cyber-attacks targeting product chain data, it has, therefore, become imperative to design an encryption infrastructure that is lightweight, adaptive, and secure and efficiently operates across a viable number of platforms. The paper proposes a new framework synthesizing the R-transform and modular arithmetic for secure communication over the digital supply network, capitalizing on the data scrambling properties of the R-transform. The key idea here is to combine this transform uniquely with modular arithmetic to induce nonlinear transformations that are invertible and computationally cheap-the very first attempt in supply chain encryption. Such a combination ensures that the framework is highly secure, exhibits low latency, and fits well the constrained devices paradigm. On the other hand, with the fast-paced introduction of digital and cloud-enabled platforms, supply chain logistics operations involve cryptographic systems that impart heavy computational loads or lack adaptability for real-time communication across nodes.

These limitations create a gap for novel encryption schemes that maintain confidentiality, integrity, and availability of data, yet do so without compromising performance. This study fills that gap through the design and analysis of a new cryptographic protocol based on the R-transform and modular arithmetic. Current cryptographic protocols employed in digital supply chains must face quite challenging limitations when they have to strive for computational efficiency, scalability, and a high degree of security. There seems to be a scarcity of lightweight encryption schemes explicitly crafted for the dynamic, distributed, and often resource-constrained environments of today's digital supply networks. This research intends to fill that critical void by presenting a new method of R-transform-based encryption joined with modular arithmetic, thereby offering a real solution to secure and efficient communication in supply chains.

These problems of reinforced information security during the era of the information are resolved in the context of overcoming current limitations in the technology of encryption and usage of the R-transform's energies in the proposed study. Classical cryptography and powerful mathematical tools in integrated use appear as one of the most promising areas for new generations of systems which could be used in various applications, particularly concerning difficulties in modern networks of communications.

2. Literature Survey

Cryptography has been the back bone of secured communication and has experienced tremendous transformation in order to counter the ever-changing cyber threats of the present world. This chapter discusses classical and modern encryption techniques with mathematical transforms applied in cryptography.

2.1 Modern Cryptography

The public-key cryptosystem development brought a significant change in the world of data security. In the year 1978, Rivest, Shamir, and Adleman proposed RSA that depends on modular arithmetic and large prime numbers for safe key exchange [4]. Though it can be secure, it needs a huge amount of computational resources and therefore is not suitable for real-time applications.

AES, presented by Daemen and Rijmen [5], has the proper balance of security and efficiency. Its application in banking and e-commerce life demonstrates its feasibility in real-life applications.

2.2 Mathematical Transforms in Cryptography

The very basics and further advanced concepts have been teaching mathematical cryptography and transform-application. Integral transforms and their applications have been exhaustively described in [6].

Oppenheim and Schafer mounted the theoretical cogwheels necessary to accomplish discrete-time signal processing, considering the basic notions of filtering, sampling, and system analysis [7]. Fourier transform has also been used in the area of watermarking and data authentication as well. A novel approach to mathematical modeling for cryptography was presented in [8] that opened a path towards secure computation. Moreover, the authors of [9] proposed an advanced encryption technique through the HNT transformations to augment the software security implementation.

R-transform is a transform mostly used in the field of signal processing. It can handle exponential-order functions and possesses different characteristics; therefore, it can be applied in the improvement of secured data transformation, according to recent research done in the field of cryptanalysis.

2.3 Modular Arithmetic

Modular arithmetic is intrinsic to the modern approaches to cryptography. Knuth [10] presented the use of modular arithmetic in algorithms, where it is used in encryption and hashing. Koblitz [11] makes use of this in elliptic curve cryptography and expanded since then.

Gunasekar and Raghavendran [12] extended the study of the R-transform for the purpose of exploring the applications of integral transforms, especially with regard to the improvement of cryptographic security. Raghavendran and Gunasekar [13] took this further; the Kushare Transform was then applied to cryptography for enhancing its security to an even greater degree, thus making exciting applications of transforms.

Since resilience, optimization, and adaptability have gained chief focus in the past recent few advances in cryptographic systems, it is now proposed to look at the RNS-based enhanced encryption algorithms that serve as perfect data guards during these times, and their comparative advantages are in favor of such dimensions [14]. Likewise, image encryption and integration of blockchain technology united with arithmetic optimization have been the claim to fame in securing the digital environment [15]. In the process of transmitting industrial data, the hybrid systems that employ AES algorithm with preprocessing techniques have led to great advancement in the security and effectiveness of the multithreaded machinery [16]. Quantum-safe encryption, along with neuro-symbolic reasoning, is now conditioning an ERP system's foundation to achieve an adaptable industrial framework [17]. Other multi-layered cryptographic communication models have also been proposed for secure data transmission while strengthening the holism of structural design and layered defense [18].

Supposedly chaos-based systems are still common in contemporary encryption, where optimization algorithms complement PUFs to optimize the efficiency of image encryption [19]. Through blockchain integration and attribute-based encryption techniques, secure and revocable access control is achieved in supply chain systems, thus ensuring data integrity over decentralized networks [20]. For IoT, certain builtin cryptographic algorithms have been examined in order to enhance system security, particularly in resource-constrained settings [21]. The pass-downs of the Internet of Medical Things have equally been subjected to a thorough evaluation of cryptographic techniques in order to counter unique security threats, countermeasures, and recent trends [22].

Post-quantum cryptographic systems have gained relatively high popularity, mainly as Supersingular Isogeny Key Encapsulation (SIKE) algorithms now get under-way for lightweight blockchain-based IoT platforms [23]. Combination of Chebyshev chaotic systems with compressive sensing has been used as a tool for designing more efficient and secure image encryption schemes [24]. Distributed ledger technologies are also being recognized for their critical role in enhancing supply chain security with benefits of transparency and traceability [25]. In multimedia security, Elzaki transformation combined with chaotic systems like the Lorenz attractor has already demonstrated new possibilities for encrypting audio signals [26].

Active research is being carried out on the matter of blockchain integration with decentralized energy management, on the occasion related to interaction with battery storage and electric vehicle infrastructure wherein secure communication is essential [27]. In addition, Internet of Robotic Things security systems must encompass encryption, as well as blockchain technologies, to adequately mount a scalable defense against metamorphosing cyber threats [28]. Presently, the smart grid universe endures under mixtures of hybrid fuzzy neural network and improved key management schemes that allow for the secure integration of renewable energy sources [29]. Lattice-based cryptographic schemes are being studied extensively to cater to futuristic cryptographic interests, securing systems in the backdrop of quantum computers [30]. Ultimately, the exact implementations and performance benchmarking of these post-quantum cryptography solutions are in progress, promising that much knowledge will be gained concerning implementation and resilience in real-world use cases [31]. Our design enjoys optimized computation by means of reduced transform complexity, lightweight modulo computations, and domain-specific key scheduling, thus making it usable for real-time and logistics application. Randomized obfuscation applied at the protocols with real-world testing in supply chain scenarios distinguish this work, functionally as well as performance-wise.

Such an integration of modular arithmetic and mathematical transforms, as presented in this research, grounds on the findings of previous conducted studies. This integration ensures that security is not lost in computation speed.

2.4 Challenges and Gaps

Even though really impressive feats are recorded in the literature reviewed, obvious gaps remain in how simple methods are still not computationally powerful as modern methods, while sophisticated techniques are highly resource-dependent.

This work attempts to bridge the gap between these two areas of research by combining the Caesar cipher with the R-transform, thus capitalizing on their mutual complementarities. This method, as the very fact of a bridge between the two areas of research, overcomes the limitations of techniques proposed separately.

3. Proposed Method

The proposed approach combines the low complexity of the Caesar cipher with the advanced mathematical properties of the R-transform in overcoming the rising growth of strong encryption mechanisms. This, in turn, ensures that it is more secure and achieves an efficient implementation for real-time applications to decrypt the message. The methodology has two major processes: Data Protection (Encryption) and Information Retrieval (Decryption).

Encryption is a step-by-step process that converts the plain text into the resulting ciphertext. The following are the steps used in this process:

3.1 Character-to-Number Mapping:

Replace every character from the plaintext with a unique number according to the scheme $\mathrm{A} = 1, \mathrm{B} = 2, \ldots, \mathrm{Z} = 26$, and assign space as 0. For example, "HELLO" would be replaced by the corresponding sequence of numbers $[8,5,12,12,15]$.

3.2 Sequence Formation:

The plaintext is represented as a finite numerical sequence, notated with $\zeta_1, \zeta_2, \ldots, \zeta_\mathrm{m}$, where m is the length of the plaintext word.

3.3 Polynomial Representation:

The numerical sequence is written in the form of a polynomial of degree $\mathrm{m}-1$. The polynomial equation will be as follows:

$$x(\zeta) = \sum_{j=1}^{m} \zeta_j \omega^{j-1} \quad (1)$$

where ω is a parameter that defines the polynomial basis.

3.4 Modular Transformation:

All the coefficients ζ_j of the polynomial are transformed by modular arithmetic:

$$x(\zeta) = (\zeta + \eta)\mathrm{mod}26 \quad (2)$$

where η is a predefined secret key shared between the sender and receiver. The polynomial $x(\zeta)$ is then applied under the R-transform, defined as:

$$R(s) = s\int_0^\infty x(\zeta)e^{-\gamma\alpha\zeta}d\zeta \quad (3)$$

where γ and α are system parameters chosen to maximize the encryption strength.

3.5 Ciphertext Generation:

The output coefficients of the transformed polynomial are reduced modulo 26 to give a new sequence of finite length $\beta_1, \beta_2, \ldots, \beta_n$. Each β_j represents the encrypting character, marking the end of the encryption process.

To decrypt the ciphertext and recover the plaintext, decryption works in reverse of encryption as follows:

3.5.1 Conversion from Ciphertext:

Convert the ciphertext back into a numerical sequence $\beta_1, \beta_2, \ldots, \beta_n$ based on the same character-to-number mapping that was used during encryption.

3.5.2 Modular Reconstruction:

Reconstruct the original coefficients using the relationship:

$$\lambda_j = 26 \cdot \chi_j + \beta_j \quad (4)$$

where χ_j is the reduction obtained and turns out to be a reconstruction parameter that requires further computation.

3.5.3 Polynomial Reconstruction:

Employ the reconstruction coefficients in order to reconstruct the polynomial $x(\zeta)$:

$$x(\zeta) = \sum_{j=1}^{m} \lambda_j \omega^{j-1} \quad (5)$$

3.5.4 Inverse R-Transform Application:

Apply the inverse R-transform to recover the polynomial:

$$x^{-1}(\zeta) = \int_0^\infty R(s)e^{\gamma\alpha\zeta}ds \quad (6)$$

Change the coefficients of the polynomial back to numeric values using the inverse modular transformation:

$$x^{-1}(\zeta) = (\zeta - \eta)\mathrm{mod}26 \quad (7)$$

where η is the secret key. Finally, convert the numeric values to their corresponding characters to recover the plaintext message.

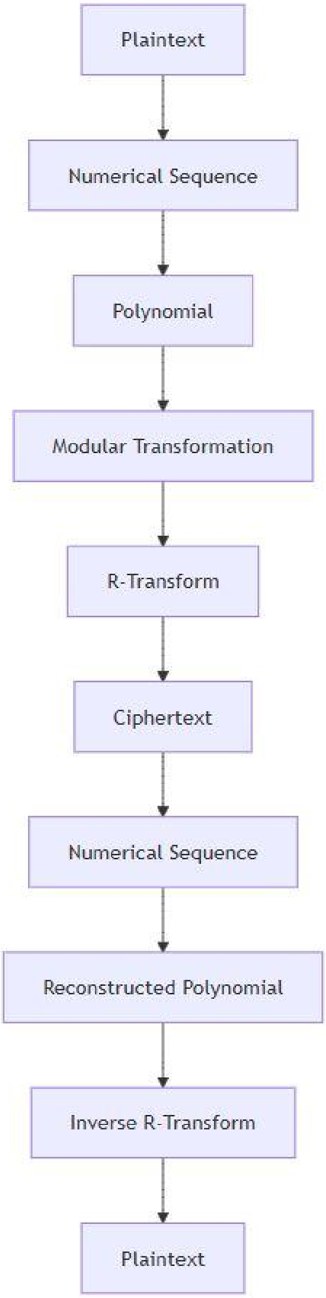


Figure 1. Illustration of the encryption and decryption process.

In Figure 1, the Encryption Process and Decryption Process describe the encryption process of plaintext into ciphertext, followed by how one can recover plaintext from ciphertext by using an advanced cryptographic method of R-transforms. The encryption starts with the plaintext, which is the original readable message that needs to be securely transmitted. First, the plaintext is converted into a numerical sequence, typically through some encoding scheme, to represent the data in numerical form. This sequence of numbers is then transformed into a polynomial, a mathematical representation that further encodes the message in an algebraic form, enhancing security. Afterwards, the polynomial is passed into modular transformation. Modular transformation is a math technique designed in such a way that with modular arithmetic applied, the values will lie within a certain range and thus remain resistant to common cryptographic attacks. However, R-transform is more powerful and is a mathematical function designed to add further layers of complexity and obfuscation to the data after a modular transformation. The result of these transformations is the ciphertext, which is the encrypted message that can be safely transmitted over insecure channels without the risk of being easily deciphered by unauthorized parties.

The decryption process, to a certain extent, is the reverse of the encryption steps performed so that the actual plaintext can be recovered. The starting point of decryption will be the ciphertext, and converting it back into a numerical sequence of the same kind as when a plaintext began would be the first step. Once the ciphertext is expressed in the form of a numerical sequence, an inverse operation reconstructs the original polynomial. This reconstructed polynomial is then processed through the inverse R-transform operation, which simply reverses the effect of the R-transform made during encryption. The final outcome after the inverse R-transform operation is converted into the original plaintext using the decoding process, and this completes the decryption cycle. It effectively converts plaintext to ciphertext. Through these transforms including numerical encodings, polynomials, mod operation, and R-transformation the process forms unintelligible pieces of communication out of an otherwise plain communication piece. And since it just works backward decrypting back through each transformation restoring plaintext form into it. It thereby protects transmission completely against being compromised during reception. This method provides robust security by using both classical and modern cryptographic techniques, making it resistant to various attack vectors and ideal for secure communication in digital environments such as supply chains, IoT systems, and more. This hybrid methodology that blends modular arithmetic with the advanced potential of the R-transform really expands the security, computational power, and flexibility of digital cryptography to protect sensitive information in diverse applications.

3.6 Advantages of the Proposed Method

This approach combines the ease of classical methods of cryptography with the sophistication of the modern mathematical technique. It makes the simplicity of the Caesar cipher and the R-transform's high computational power fuse into a strong framework for cryptography, so this system becomes friendlier and safer. One notable characteristic of this approach is that it defends data from diverse attacks. Its use of modular arithmetic and transformations of polynomials provides an invincible mechanism against attacks. Those mathematical concepts instill the right amount of complication that repels unauthorized access or tampering of sensitive data successfully.

The algorithm is relatively efficient computationally, which actually makes it more suitable for real-time applications in digital communication networks. The operations of this algorithm are actually streamlined such that delay is minimized, which is really important in dynamic environments such as transaction and secure messaging online. Another significant strength is its ability to scale and flexibility. The concept can be extended to different scenarios such as secured operations in the digital supply chains and IoT networks. This variability guarantees that the method will have applications in so many different usages, allowing it to fulfill the changing needs of contemporary technological networks.

So many noteworthy advantages underpin the suitability of the encryption technique for securing digital supply networks. Positioning itself in a theoretical capacity, the integral transform combined with modular arithmetic renders a formidable cryptographic security. Such an amalgamation induces computational complexity that discourages an adversary from decrypting the message without the secret key. This complexity aids in maintaining data secrecy and protects it from specific cryptanalytic attacks like brute force and chosen-plaintext, thereby fortifying the overarching cloak of security. Secondly, relative to schemes such as ECC, lattice-based cryptography, and homomorphic encryption, the proposal excels in computational time and efficiencies. It needs fewer computational resources, hence less encryption and decryption time with the least memory consumption. Such properties make it quite fit for implementation in constrained environments often seen in supply chain practices, where real-time processing and low latency are of the utmost priority.

More importantly, many other studies keep claiming that the method offers a very high throughput for securely processing large volumes of supply chain data without any significant delay. Reasonable use of computational and memory resources leads to secure communication between various nodes of the network simultaneously, realizing a robust and scalable environment for digital supply networks. Lastly, the proposed system is highly scalable. Both the theoretical and empirical studies show that the performance deteriorates to a very small extent as network size and data volume increase. This supremacy against operational growth ensures that the encryption technique can be applied on a large, dynamic supply chain, where security and efficiency are required in scaling. From all the above advantages, we maintain that there are enough reasons why the proposed cryptographic approach is expected to provide a safe, efficient, and scalable solution for contemporary digital supply networks.

4. Applications

New Encrypted Method-this new method does combine both features of a sophisticated R-transform-based technology and simplicity unique to the Caesar Cipher. Applications occur in most arenas, for efficiency, security balance will mark it a fine fit in ecosystems of today's advanced technologies.

4.1 Supply Chain Management

The modern supply chain operations involve transmission of sensitive data, such as shipping manifests, inventory details, and even customer information over insecure networks between multiple stakeholders. The encryption methodology proposed here provides strong protection by encrypting logistics data during digital transfers to prevent unauthorized users from accessing the information. Not only does this minimize the risk of a data breach, but it also secures the end-to-end communications across the supply chain. This is beneficial for multi-vendor supply chains where critical information is exchanged amongst different entities. By adopting this encryption, businesses can build overall security into their supply chain networks, thus minimizing vulnerabilities toward cyber attacks.

As depicted in Figure 2, this encryption model facilitates the secure transmission of logistics data among various nodes of a digital supply chain network. Any architecture thus maintains data confidentiality and integrity during communication among the nodes.

4.2 Secure Communication

With the current electronic generation, personal and professional communications depend much on electronic platforms. Hence, security of transmitted messages becomes very paramount. The encryption scheme proposed here ensures end-to-end secrecy such that only the intended recipient can decrypt the information. This methodology is best suited for electronic mail and instant messaging applications, where the protection of sensitive communications is critical. The encryption design also has low latency, which is very efficient for real-time communication. This way, the system will perform very well even with strict timing constraints. The method also secures data uploaded to cloud servers. This means that if a server is breached, the encrypted data remains unintelligible to attackers. This system can ensure that an organization complies with data protection laws, such as General Data Protection Regulation (GDPR), while simultaneously protecting user privacy and limiting access to authenticated individuals only.

Figure 3 shows how the encryption model protects communication channels while also ensuring the privacy of data and maintaining compliance during storage and retrieval.

4.3 Internet of Things (IoT) Ecosystems

The Internet of Things (IoT) has become ubiquitous in many crucial applications, ranging from smart homes to health monitoring systems and industrial automation. With interconnectivity at the heart of the IoT ecosystem, though, communications have to be secure against interceptions and tampering, and it is in such aspects that a suggested encryption scheme provides security against such malicious interactions to ensure safe communication between the sensor, the control unit, and the cloud servers. Its lightweight design is optimized for resource-constrained IoT devices, making it both practical and effective. This encryption minimizes the risk of cyberattacks against the operations by guaranteeing the authenticity and integrity of the commands and data exchanged within IoT networks.

Encrypted communication ensures protection against unauthorized access and cyberattacks, a secure data transfer system in an IoT-enabled environment as described in Figure 4.

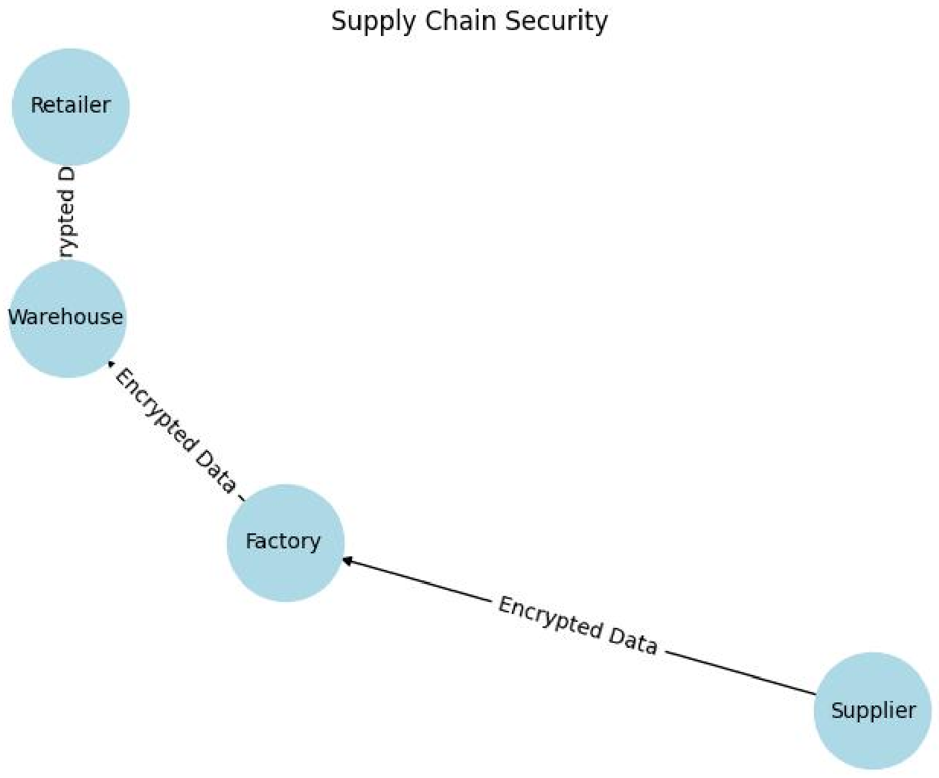


Figure 2. Secure transmission of logistics data in supply chain management using advanced encryption.

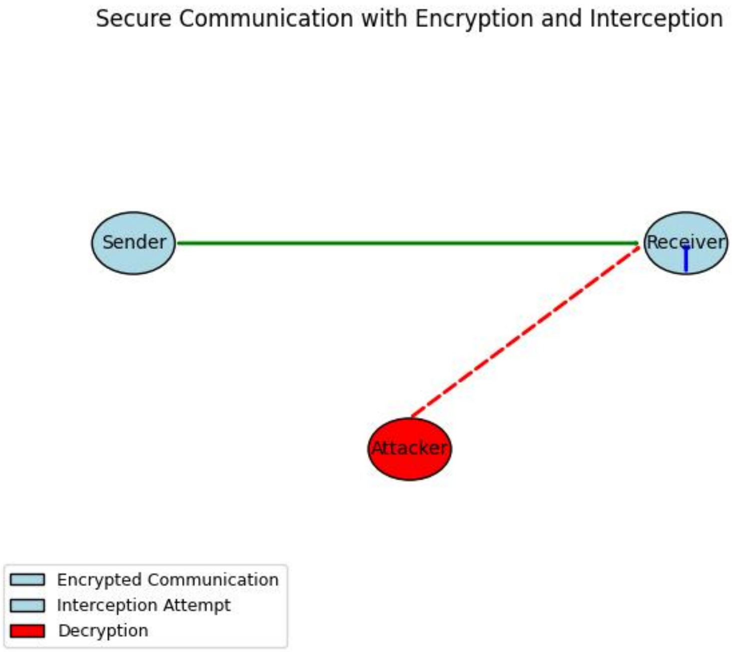


Figure 3. Encryption securing communication and data storage, ensuring privacy and compliance with regulations.

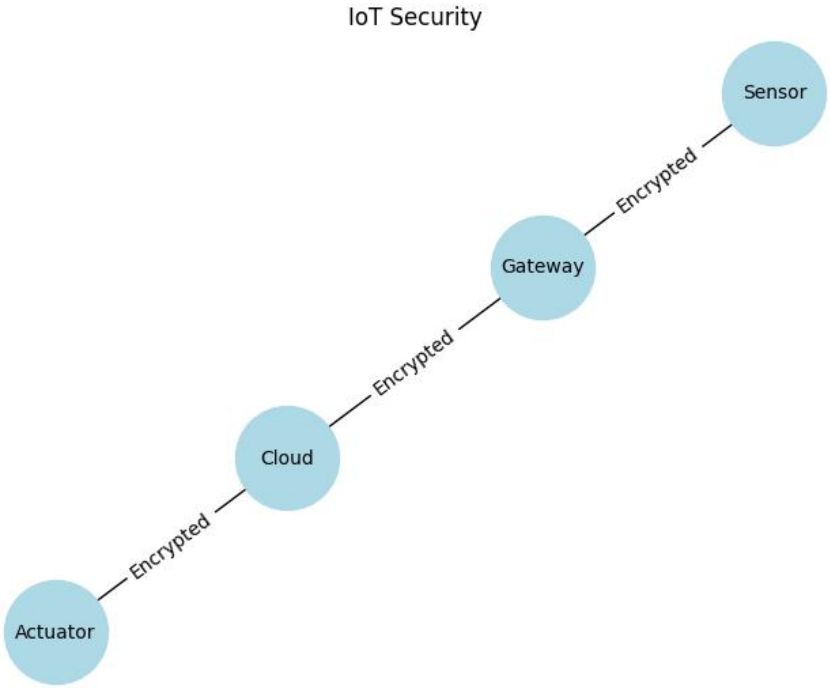


Figure 4. Encrypted communication within an IoT network, ensuring secure data exchange among devices.

4.4 Other Potential Domains

Outside of supply chains, communication, and IoT ecosystems, this encryption has diverse applications across a few crucial domains. In e-governance, it protects sensitive citizen data and secures transactions within digital governance systems, thereby ensuring the confidentiality and integrity of governmental operations. In the financial sector, the encryption secures online payment systems by encrypting transactional data to reduce risks of fraud and unauthorized access. In health care, it provides the privacy of the medical records and diagnostic reports in electronic exchange between physicians and hospitals. Additionally, in military communications, it offers high security for secret communications, even in hostile environments, where critical information will remain protected at all times. This encryption system is highly adaptable and can be a universal solution to securing sensitive data across various industries.

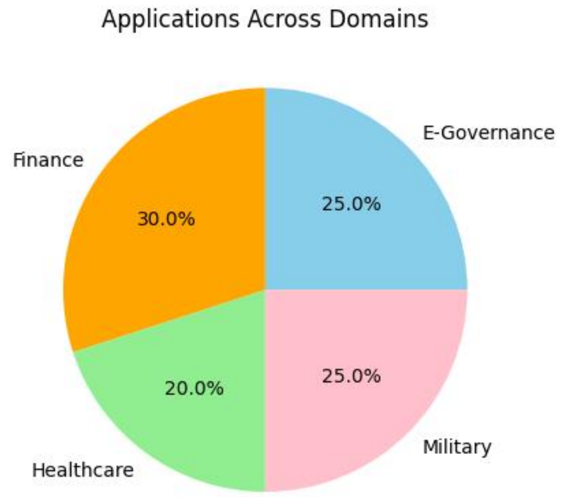


Figure 5. Applications of encryption across e-governance, finance, healthcare, and military domains.

The versatility of the given encryption model does not end with supply chains and IoT applications, and its applications extend to e-governance, finance, healthcare, and the military, as highlighted in Figure 5. This encryption method is an innovative solution for those environments that require very high levels of data security. Its implementation would help businesses and organizations enhance their cybersecurity posture, mitigate potential risks, and create trust among users and stakeholders. In addressing the challenges of data protection in modern times, this encryption system has become a transformational tool for modern technological landscapes.

From Figures 2 to 5, the robustness of the R-transform encryption framework is emphasized: securing logistics and IoT communications, among others, while ensuring privacy in broader domains like finance, governance, and defense.

5. Conclusion and Future Scope

This paper will propose a novel method of cryptography. It merges the simplicity of the Caesar cipher with the potency of the R-transform. Here, the challenge is to balance the security factor and computational practicability within an encryption scheme that works as a hybrid. A merger of polynomial transformation and modular arithmetic improves data safety without any degradation in the ease of implementing the approach adopted. As the novel combination of well-established cryptographic tools, it ensures that the data exchanged in digital communication networks is confidential, sound, and authentic.

This encryption technique represents flexibility and practicality when it comes to safeguarding all types of applications, ranging from supply chain management and IoT networks to cloud storage. Its innovative combination of traditional and advanced techniques makes it an effective solution for modern cybersecurity challenges.

This encryption method provides solid security; however, there are various scopes of development and further improvement. Among those scopes is the dynamic key generation method, which will make the cryptography capability of this proposed method much stronger. In this technique, changing keys will make the system more resistant to cryptanalysis attacks, which is the improvement that will add protection to the data, particularly for high-risk application areas like online banking and military communications. Another promising avenue for research is applying this technique to multimedia encryption. As videos, audio, and images require quick, scalable, and secure encryption methods, the implementation of the R-transform coupled with the Caesar cipher could be extended to handle large-sized media files, ensuring both their privacy and performance. Additionally, the rise of quantum computing poses a potential threat to classical encryption techniques. Future work can go towards adaptation or extension of the proposed method against quantum-based attacks. For that reason, it is possible to use the proposed approach for encryption with the inclusion of quantum-safe cryptographic algorithms, thus offering an even more secure approach.

Another interesting research direction would be to apply this encryption technique towards blockchain systems. In terms of security, blockchain depends on secure and immutable transactions; the exploration whether such encryption can maintain confidentiality over the data of a transaction without degrading the openness and immutability of a blockchain system will be valuable. While the method is computationally efficient, perhaps more optimization opportunities are available within this method to better suit more resource-constrained devices such as those in the IoT or even mobile platforms. Further research could concentrate on optimizing the performance of the combination of R-transform and Caesar cipher for these parameters. Finally, standardizing and putting the encryption method through real-life tests will be the final validation of its credibility. Testing against dissimilar platforms and network conditions will help understand the extent to which the method scales, performs, and is reliable in real-life usage. Such tests would enable the conclusion regarding the encryption technique being feasible to work with for many applications. The proposed encryption technique has tremendous promise in resolving the modern cryptographic challenges. It is simple, adaptive, and secure. Such a method would be a promising solution for various applications. With the rapid development of threats to cybersecurity, the further refinement of the technique and the exploration of its potential applications will be a great step toward enhancing digital security.

Based on the promising results yielded by the current study, it is anticipated that future research efforts will be directed toward several key areas to further improve the applicability and performance capabilities of the proposed encryption methodology. Hardware acceleration methods can be one such consideration, whereby realizing the buildup on Field Programmable Gate Arrays (FPGA) or Graphics Processing Units (GPU) can be strongly beneficial in enhancing encryption and decryption speeds in the real-time supply chain environment. Further, the integration of the proposed cryptographic scheme with blockchain-based supply chain management systems presents an excellent opportunity for the distributed ledger technology to complement the advanced confidentiality and integrity protections that safeguarding the data. Such integration could foster greater trust and accountability among stakeholders through immutable and transparent transaction records secured using our method. The security evaluation can also be extended more rigorously through real-world simulation exercises involving advanced attack models, such as side-channel attacks and chosen-ciphertext attacks, for a more holistic consideration of the robustness. The design of future interventions thus aims at making the proposed system more scalable, efficient, and robust to cater to the evolving demands of digital supply networks.

References

[1] Stallings W. Cryptography and network security: Principles and practice, 7th ed.; Pearson: London, England, 2020.

[2] Singh S. The code book: The science of secrecy from ancient Egypt to quantum cryptography. Doubleday: New York, United States, 1999.

[3] Shannon CE. Communication theory of secrecy systems. The Bell System Technical Journal, 1949, 28(4), 656-715

[4] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2), 120-1266

[5] Daemen J, Rijmen V. The design of rijndael: AES - The advanced encryption standard, 1st ed. Springer Berlin: Heidelberg, Germany, 2002.

[6] Debnath L, Bhatta D. Integral transforms and their applications. 2nd ed. Chapman and Hall/CRC: New York, United States, 2016.

[7] OppenheimAV, Schafer RW. Discrete-Time signal processing, 2nd ed. Prentice Hall: New Jersey, United States, 1999.

[8] Hiwarekar AP. New mathematical modeling for cryptography. Journal of Information Assurance and Security, 2014, 9(2014), 27-33.

[9] Sasirekha N, Hemalatha M. An enhanced code encryption approach with HNT transformations for software security. International Journal of Computer Applications, 2012, 53(10).

[10] Donald EK. The art of computer programming, Volume 2: Seminumerical Algorithms, 3rd ed. Addison-Wesley: Boston, United States, 1997.

[11] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48(177), 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

[12] Gunasekar T, Raghavendran P. Applications of the R-Transform for advancing cryptographic security. In Driving Transformative Technology Trends With Cloud Computing, 2024, 208-223. DOI: 10.4018/979-8-3693-2869-9.ch011

[13] Prabakaran R, Gunasekar T. Advancing cryptographic security with kushare transform Integration. In Driving Transformative Technology Trends With Cloud Computing, 2024, 224-242. DOI: DOI: 10.4018/979-8-3693-2869-9.ch012

[14] Akanni GA. Enhanced residue number system based encryption algorithms and their comparative assessment for data protection in the era of digitization. Doctoral Dissertation, Kwara State University, Nigeria, 2024.

[15] Alohali MA, Aljebreen M, Al-Mutiri F, Othman M, Motwakel A, et al. Blockchain-driven image encryption process with arithmetic optimization algorithm for security in emerging virtual environments. Sustainability. 2023, 15(6), 5133. DOI: 10.3390/su15065133

[16] Xia Z, Yang X, Li A, Liu Y, He S. Research on information security transmission of port multi-thread equipment based on advanced encryption standard and preprocessing optimization. Applied Sciences, 2024, 14(24), 11887. DOI: 10.3390/app142411887

[17] Lin Y, Lin Y. NSEA: A resilient ERP framework integrating quantum-safe cryptography and neuro-symbolic reasoning for industrial adaptability. IEEE Access, 2025, 13, 77686-77695. DOI: 10.1109/ACCESS.2025.3562739

[18] Wang Z, Tabassum M. A Holistic secure communication mechanism using a multilayered cryptographic protocol to enhanced security. Computers, Materials & Continua, 2024, 78(3). DOI: 10.32604/cmc.2024.046797

[19] Muhammad AU, Özkaynak F. SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. Symmetry, 2021, 13(5):824. DOI: 10.3390/sym13050824

[20] Gao J, Zhang X, Zhong S. Data security and access control method of blockchain with revocable attribute encryption in steel supply chain. Peer-to-Peer Networking and Applications, 2025, 18(4), 1-28. DOI: 10.1007/s12083-025-01985-y

[21] Thabit F, Can O, Aljahdali AO, Al-Gaphari GH, Alkhzaimi HA. Cryptography algorithms for enhancing IoT security. Internet of Things, 2023, 22, 100759. DOI: 10.1016/j.iot.2023.100759

[22] Robert W, Denis A, Thomas A, Samuel A, Kabiito SP. A comprehensive review on cryptographic techniques for securing internet of medical things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction. Mesopotamian Journal of Artificial Intelligence in Healthcare, 2024, 135-169. DOI: 10.58496/MJAIH/2024/016

[23] Ismail NA, Khadra SA, Attiya GM, Abdulrahman SES. Optimizing SIKE for blockchain-based IoT ecosystems with resource constraints. The Journal of Supercomputing, 2025, 81(3), 1-44. DOI: 10.1007/s11227-024-06906-z

[24] Sun M, Yuan J, Li X, Liu D. Chaotic CS encryption: An efficient image encryption algorithm based on chebyshev chaotic system and compressive sensing. Computers, Materials & Continua, 2024, 79(2), 1-10. DOI:10.32604/cmc.2024.050337

[25] Asante M, Epiphaniou G, Maple C, Al-Khateeb H, Bottarelli M, et al. Distributed ledger technologies in supply chain security management: A comprehensive survey. IEEE Transactions on Engineering Management, 2021, 70(2), 713-739. DOI: 10.1109/TEM.2021.3053655

[26] Kareem SR. Encryption of audio signals using the elzaki transformation and the lorenz chaotic system lorenz chaotic system. arXiv preprint arXiv:2409.14092, 2024. DOI: 10.48550/arXiv.2409.14092

[27] Chinnaperumal S, Raju SK, Alharbi AH, Kannan S, Khafaga DS, et al. Decentralized energy optimization using blockchain with battery storage and electric vehicle networks.Scientific Reports, 2025, 15(1), 5940. DOI: 10.1038/s41598-025-86775-5

[28] Zafir EI, Akter A, Islam MN, Hasib SA, Islam T, et al.Enhancing security of internet of robotic things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. Internet of Things, 2024, 28, 101357. DOI: 10.1016/j.iot.2024.101357

[29] Vignesh E, Jeyanthy PA. Efficient and secure integration of renewable energy sources in smart grids using hybrid fuzzy neural network and improved Diffie-Hellman key management. Computers and Electrical Engineering, 2025, 123, 110206. DOI: 10.1016/j.compeleceng.2025.110206

[30] Nguyen H, Huda S, Nogami Y, Nguyen TT. Security in post-quantum era: A comprehensive survey on lattice-based algorithms. IEEE Access, 2025, 13, 89003-89024. DOI: 10.1109/ACCESS.2025.3571307

[31] Demir, ED, Bilgin B, Onbasli, MC. Performance analysis and industry deployment of post-quantum cryptography algorithms. arXiv preprint arXiv:2503.12952, 2025. DOI: 10.48550/arXiv.2503.12952