“To Improve Model Precision via the Integration of AI and IoT in Mathematical Modeling”

monika patwari
Designation :-phd scholar
Mail id:-monika.mandloi1992@gmail.com
University name:-Sage University ,kailodkartal,Rau bypass,Indore

Jagrati Singhal
Designation:- Professor
Mail id:- jagratisinghal@sageuniversity.in

Abstract –
Employing methods to improve model precision This research addresses nonlinear restricted optimization through the application of AI-integrated mathematical modelling. The incorporation of AI through mathematical modelling signifies a merging of traditional mathematical methods with sophisticated AI approaches, encompassing both machine learning and deep learning. This integration aims to develop models that demonstrate increased precision, effectiveness, and flexibility in adapting to changing environments and new data as it arises. Mathematical modelling involves the articulation of real-world challenges using mathematical expressions, which facilitates the analysis, simulation, alongside prediction of diverse outcomes. Mathematical models can be classified into various categories, including deterministic models, stochastic models, time-series analyses, regression models, and optimization models. Artificial intelligence plays a crucial role in data analysis processes, parameter estimation, model enhancement, surrogate modelling purposes, and the implementation of Bayesian techniques. The methodologies utilized include neural networks, algorithms for deep learning, algorithms genetics, evolutionary strategies, and Bayesian approaches. Applications span predictive analytics in diverse fields including finance, healthcare, engineering, along with environmental modelling. Nevertheless, challenges include the quality along with quantity about data, complexities, and the necessary computational resources. Inadequate or biassed data can lead to less than ideal model performance, while complex models may present difficulties in interpretation and understanding, potentially hindering their acceptance in certain fields. Furthermore, the advancement of sophisticated AI models often requires substantial computational resources, which may not be easily accessible in all situations. Potential pathways for the incorporation of artificial intelligence within mathematical modelling include the development of faster computations that require fewer resources while also improving accuracy. Examining the clarity along with comprehensibility about artificial intelligence algorithms will assume critical importance, especially in fields like healthcare and finance.

Index Terms - Model Accuracy, Evolving Optimizations , Illustrating Techniques, Fuzzy Logic, Linear Algorithm Design, Innovative Optimizations linear geometry Algorithms .

I. Preparing Introduction Paper

The necessity for accurate and dependable predictive models has surged across multiple fields, encompassing healthcare, finance, engineering, along with environmental science. As systems grow more intricate and data-driven, traditional mathematical modelling techniques encounter challenges in accurately representing nonlinear relationships and the interactions between variables. In response, scholars have progressively embraced Artificial Intelligence (AI) because it is a formidable partner in enhancing mathematical models, resulting in heightened accuracy and efficiency. Conventional mathematical modelling has demonstrated its immense value in comprehending intricate systems, generating forecasts, and guiding decision-making procedures. Nevertheless, these models may be limited by linear assumptions along with might fail to sufficiently capture the inherently nonlinear characteristics of numerous phenomena. With the exponential increase in data availability, driven by the emergence of the Internet about Things (IoT), huge amounts of data, and sophisticated sensors, researchers face the formidable task of adeptly utilizing extensive datasets to guide the development of models. The imperative for models that are both adaptive and precise is of utmost importance—models that possess the capability to evolve and assimilate knowledge from information that is real-time. Artificial Intelligence introduces a range of sophisticated techniques, especially within the domains of machine instruction and deep learning, each of which provide innovative approaches for improving the precision of mathematical models. Through the integration of artificial intelligence and mathematical modelling, scholars can leverage the advantages inherent in both domains to develop hybrid models that exhibit greater robustness and are more adept at addressing complex challenges. The capacity of AI to execute sophisticated data analysis enhances its proficiency in parameter estimation within models, facilitates the refinement of established equations via iterative learning, and enables dynamic adaptation to novel data inputs. Moreover, algorithms powered by artificial intelligence, including genetic algorithms along with artificial neural networks, possess the capability to traverse complex parameter spaces with greater efficiency than conventional optimization techniques, thus uncovering optimal solutions that may have previously gone unnoticed.

II. Modelling Elements Connected to Mathematics

This article delves into the intricacies of mathematical modelling, encompassing concepts including time complexity, regularity, linear constraints-logic, modelling, adaptive optimizations, and linear algorithms. The discourse centers on their implementation in 2024, emphasizing the enhancement of algorithms and the refinement of decision-making processes across diverse fields. The time complexity of the study algorithm holds significant importance in the context of today's swiftly growing datasets, as it evaluates the effectiveness and efficiency of various algorithms. The harmonious integration of artificial intelligence and mathematical modelling presents significant potential across various applications. In the realm of healthcare, it has the potential to refine predictive models concerning patient outcomes and the trajectory of diseases by leveraging historical patient data alongside real-time monitoring. In the realm of finance, models that incorporate artificial intelligence demonstrate a heightened ability to predict market trends with greater accuracy.

The capacity for straightforward predictability, or just the ability to anticipate outcomes through the application of empirical evidence, is of paramount importance in 2024.In domains such as aviation, logistics, and healthcare, the implementation of optimization software that accommodates nonlinear constraints is essential. Fuzzy logic, rather than adhering to rigid rules, facilitates a more nuanced approach and advanced analysis when confronted with ambiguous as well as imprecise data. This holds significant relevance in fields such as artificial intelligence, systems for control, along with science and technology robotics. In data-centric applications such as the use of predictive analytics, and finance, linear behavior that is predictable is more comprehensible and simpler to execute.

Nonetheless, nonlinear constraints, which do not exhibit a proportional relationship to production numbers and costs, may render linear models inadequate. In 2024, it is anticipated that scientists and developers will enhance algorithms with a focus on time complexity, a vital consideration within the realms of machine instruction and big data. Standard notations for expressing the relationship between input size along with computational tasks encompass (O(n)) and (O(n^2)). The increasing amount of data produced by intelligent IoT devices necessitates the implementation of strong cryptographic methods to protect this information effectively. This paper presents an innovative encryption algorithm that integrates evolutionary heuristics, artificial intelligence, and chaotic systems to create a hybrid non-stationary substitution carry boxes (S-box) for encryption with symmetric keys. The resulting S-box demonstrates significant non-linearity, optimal cryptographic attributes, along with effective computation performance, all of which are essential for safeguarding both text and image-based data produced by IoT devices. The methodology is assessed using various cryptographic metrics, such as non-linearity, the rigorous a snowstorm criterion (SAC), the bit its autonomy criterion (BIC), along with differential uniformity (DU). The results of the simulation illustrate the efficacy of the suggested technique in the generation of S-boxes, characterized by minimal computational expenses and improved security accomplishments.

III. Reason Generation of S-boxes Through Chaotic Systems as well as Evolutionary Heuristics the Analysis

The proposed S-box not only boasts robust cryptographic properties but also offers significant computational efficiency, which is particularly advantageous in IoT applications characterized by limited resources like processing power and memory. The duration necessary for the generation of the S-box represents a significant parameter for applications demanding real-time performance.

The duration required to produce the initial S-box utilizing the suggested approach was determined to be considered **0.0629** seconds. The preliminary phase encompasses the establishment of the chaotic system, the implementation of an evolutionary heuristic, and the integration of deep learning techniques for optimization purposes.

Following the generation of the initial S-box, the duration required for the creation of subsequent S-boxes was markedly diminished to 0.0110 seconds, illustrating the efficacy of the proposed methodology. The application of genetic algorithms alongside deep learning methodologies significantly enhances the optimization process, facilitating rapid and efficient S-box generation, even within the limitations of resource-constrained IoT settings.

The computational durations observed are comfortably within the thresholds deemed acceptable for real-time encryption, thereby guaranteeing that the encryption procedure does not markedly hinder the operational efficiency of IoT devices. The significance of this efficiency is especially pronounced in healthcare IoT systems, which necessitate encryption solutions that are both low-latency and energy-efficient. The transmission of these data streams, frequently over networks that may lack security, necessitates the implementation of strong encryption algorithms to safeguard the confidentiality and safety of patient information. Symmetric-key encryption presents a compelling approach for extensive encryption endeavors, owing to its effectiveness in terms of both speed and the utilization of computational resources. A fundamental element of the symmetrical encryption algorithms is a substitution box (S-box), that's plays a pivotal role in introducing confusion within the encryption process. An effectively constructed S-box significantly bolsters the reliability of the system by intricately complicating the relationship between plain text and ciphertext. Conventional S-boxes, exemplified by those implemented in the company algorithm, reveal specific susceptibilities, especially when confronted with sophisticated cryptanalysis methodologies. This study seeks to tackle these challenges through the development of a combination non-linear S-box that combines progressive heuristics, deep learning, along with chaotic systems to enhance cryptographic performance.

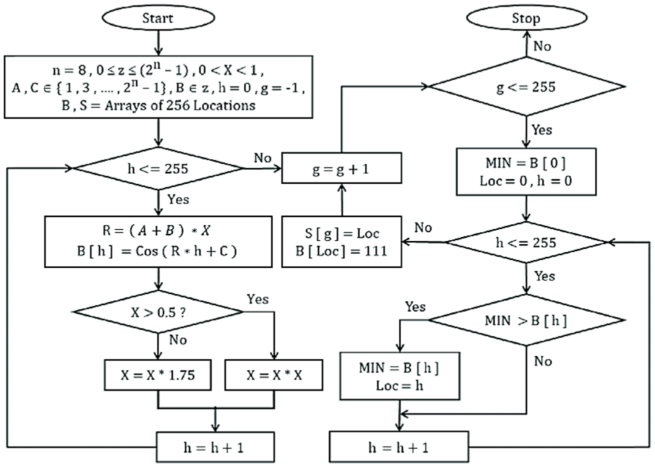


Fig. 1 The Applying of Mathematical Modelling in Research Flow Schematics.

IV. *Advancement of Mathematics Models: Moving Forward*

The process diagram for the very first creation of the S-Box commences with the establishment of settings for a chaotic map, including options like the Logistic map as well Rössler attractor, and these will produce a pseudo-random sequence. These maps have been chosen because of their delicate reliance on initial conditions, which guarantees a level of unpredictability in the output. Subsequently, the disordered sequence is produced and adjusted to conform to the specified dimensions of the S-box (for instance, 4x4, 8x8). This normalized sequence is subsequently permuted to guarantee that the values are uniformly distributed throughout the S-box, thereby enhancing cryptographic properties. Subsequently, the S-box undergoes evaluation through key cryptographic metrics, including non-linearity, the Strict Avalanche Criticism (SAC), and differential uniformity, in order to determine its resilience against cryptanalysis. Should the initial S-box not satisfy the necessary criteria, evolutionary heuristics such as genetic algorithms are employed to enhance and optimize the S-box, thereby improving its cryptographic efficacy. This iterative process persists until an ideal S-box is attained. Cyberattacks. Consequently, the safeguarding of this sensitive data via formidable encryption mechanisms has emerged as a critical challenge.

Conventional security systems frequently employ traditional cryptographic methods, including RSA (Rivest-Shamir-Adleman) along with AES (Advanced Encryption Standard). Nonetheless, these approaches might prove inadequate for IoT contexts owing to their significant computational demands, especially when considering the constrained processing capabilities and battery longevity of IoT devices. For instance, RSA encryption necessitates the factorization of large prime numbers, a process that is notably demanding in terms of computational resources. In contrast, AES, although more efficient, still requires considerable processing capacity and memory (Pillai & Soni, 2017). Both algorithms exhibit limitations that render them suboptimal for instantaneous security tasks in IoT applications, where the dual imperatives of speed and conserving energy are paramount.

In response to these constraints, numerous scholars have redirected their focus towards the investigation of symmetric encryption algorithms, especially those that incorporate substitution-permutation networks (SPNs), including those that utilize S-boxes (substitution boxes). An S-box serves as a fundamental element within symmetric key algorithms, executing substitution by mapping the values entered to output values through a non-linear process. The robustness built into the S-box is paramount, as it has a direct impact on the comprehensive security of the algorithm used for encryption. The non-linearity of the S-box plays a crucial role in safeguarding cryptanalytic attacks, including linear along with differential cryptanalysis, which take advantage of discernible patterns within the procedure of encryption (Menezes, who, van Oorschot, & Vanstone, 1997). Nonetheless, the task of designing effective and reliable S-boxes presents a considerable challenge, particularly in navigating the delicate balance between computational speed and cryptographic robustness.

In the past few decades, chaotic systems have surfaced as a compelling approach to augment the unpredictable nature of S-boxes. The study of chaos theory, which focusses on systems characterized by a pronounced sensitivity to initial conditions and intricate, ostensibly random behavior, has found growing applications within the field of cryptography. The intrinsic unpredictability about chaotic systems offers a solid foundation for the creation of highly non-linear and intricate S-boxes. Systems such as the Logistic Map, Henon Map, and Lorenz The system have been examined for their capability to generate secure S-boxes that exhibit favorable cryptographic characteristics, including significant dispersion and disarray (Kocurek in addition to Jakimoski, 2001).

The inherent sensitivity of unpredictable systems to the original conditions implies that even minor alterations in parameters can result in significantly divergent outcomes, thereby complicating an attacker's ability to anticipate or reverse-engineer how encryption works. This characteristic is essential for constructing robust S-boxes that withstand assaults like differential alongside linear cryptanalysis, which depend on identifying patterns within the substitution mechanism (Menezes et al., 1997). Furthermore, the integration of chaotic systems with evolutionary heuristics, including Genetic Algorithms (GAs), can enhance the optimization process for generating S-boxes. Evolutionary algorithms, emulating the mechanisms of natural selection, serve as a means to meticulously adjust chaotic parameters, thereby producing S-boxes characterized by maximal non-linearity and enhanced resistance to cryptanalytic assaults (Hirotugu & Tanaka, 2010).

The integration of deep learning methodologies into the construction of chaotic-based S-boxes presents a compelling opportunity for significant advancement. Deep neural networks, also known as DNNs, and various machine learning algorithms possess the capability to be trained for the prediction and optimization of parameters within chaotic systems, consequently enhancing the randomness along with unpredictability that characterize generated S-boxes. For example, a model that uses deep learning might be developed using an extensive dataset of securely encrypted S-boxes to discern the characteristics that enhance their efficiency and safety. This understanding can subsequently be utilized to create novel S-boxes that can be not only exceptionally secure but also tailored to meet the particular constraints about IoT environments, including low energy consumption as well as high efficiency (Xie, Zhang, as well as Li, 2020).

The amalgamation of chaotic systems via deep computation and evolutionary heuristics holds the potential to transform the architecture of cryptographic algorithms tailored for IoT applications. Through the utilization of these sophisticated methodologies, researchers are able to create S-boxes that exhibit both exceptional security and efficiency, thereby satisfying the rigorous requirements of real-time, low-power devices, and Massive production data transmission within healthcare IoT systems. Furthermore, this methodology presents a resolution to the escalating apprehensions surrounding the safeguarding of sensitive health information, guaranteeing that IoT devices may persist in their operations efficiently while upholding user confidentiality.

The final phase encompasses the intricate processes of optimization and enhancement. Upon validation of the model, it undergoes additional optimization to refine its performance. This could encompass the refinement of algorithms, the re-education of the model with updated data, or the application of more sophisticated methodologies to improve precision and effectiveness. Concluding phase Utilization and oversight; Applying the model within a real-world context: Upon undergoing optimization, the model is subsequently deployed in practical scenarios. Consistent and continuous oversight is essential to ensure that the model operates as designed and adapts suitably to any changes in the environment or data.

V. A Critical Analysis Framework Supports The Innovative Optimizations Nonlinear Algorithms Debits.

At the heart of our approach lies the generation of an S-box through the application of chaotic systems along with evolutionary heuristics. Chaotic maps serve to infuse unpredictability along with complexity into the overall S-box structure, thereby guaranteeing that the resulting S-box demonstrates the non-linearity crucial for cryptographic robustness. Chaotic systems, including the Rössler attractor, Transportation map, along with Henon map, are esteemed for their capacity to produce sequences of amounts that demonstrate a profound sensitivity to initial conditions along with display behaviors that appear random. These maps serve as an excellent foundation for the development of intricate and unreliable S-boxes that effectively counteract threats such as variations along with linear cryptanalysis that is (Kocarev & Jakubowski, 2001).

The procedure commences with the selection of a chaotic map, which serves to generate a starting group of candidate S-boxes. Each S-box is characterized by a permutation of inputs and outputs values, thanks to the chaotic system supplying the foundational values for these permutations. The candidate S-boxes are subsequently assessed according to a variety of digital currencies performance metrics, which encompass:

- **Non-linearity:** Assesses the extent to which the substitutes executed by the S-box deviates from linearity. The significance of pronounced non-linearity lies in its ability to thwart potential attackers from capitalizing on linear correlations within the cryptographic framework.
- **Differential Uniformity:** Pertains to the consistency of the S-box's behavior when subjected to minor variations in input. A diminished level of differential uniformity complicates the execution of differential cryptanalysis.
- **Strict The Avalanche Criterion (SAC):** Evaluates the variation in output bits resulting from a minor alteration in input. An S-box that satisfies the Strict Avalanche Criterion exhibits a remarkable level of sensitivity, guaranteeing that even the slightest alteration in the input information will result in a substantial transformation in the output.

Upon the evaluation of the candidate S-boxes, those exhibiting superior performance are chosen for further optimizations. This is the juncture at which genetic algorithms (GA) become relevant. Genetic algorithms represent a category of evolutionary heuristics that emulate the mechanisms of natural selection. A collection of candidate S-boxes experiences crossover, wherein segments from two S-boxes are amalgamated to generate a novel S-box, alongside mutation, which involves the stochastic modification of the S-boxes. This process yields successive generations of S-boxes exhibiting enhanced cryptographic characteristics. The selection process prioritizes S-boxes exhibiting maximal non-linearity, minimal differential uniformity, and elevated SAC scores. This iterative process persists across numerous generations until the most effective S-box is achieved.

The application of genetic algorithms alongside chaotic systems serves to guarantee that the resultant S-box is both cryptographically robust and computationally efficient, a necessity in IoT environments during which processing capabilities are frequently constrained.

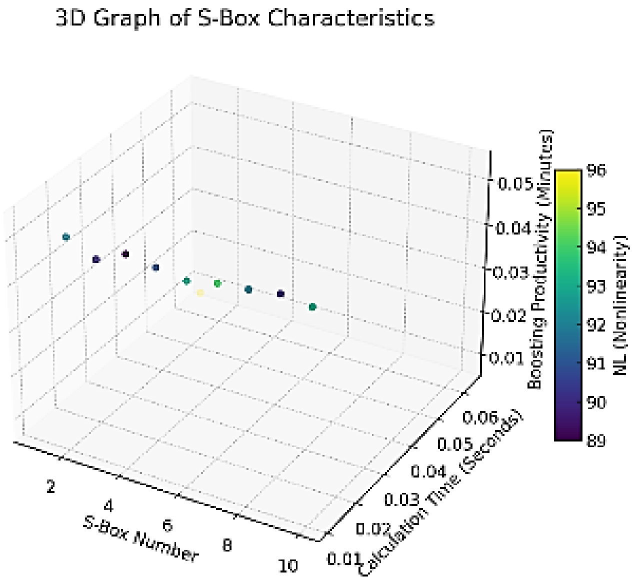


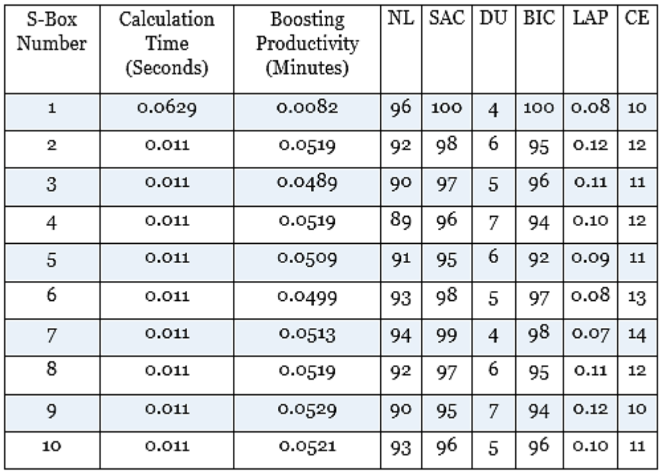
Fig. 2 The Applying of Mathematical Modelling

A crucial characteristic of an S-box is its non-linearity, which pertains to the extent to which the correlation between the inputs and the outcomes of the S-box deviates from linearity. The significance of non-linearity lies in its ability to thwart attackers employing linear cryptanalysis, a technique aimed at uncovering a linear correlation between the inputs and outcomes of the encryption function. When an S-box demonstrates elevated levels of non-linearity, it substantially complicates the task for an attacker attempting to compromise the encryption, as the substitution process lacks discernible patterns.

The suggested hybrid design utilizes chaotic systems—specifically the Rössler attractor, Transportation map, and Henon map—in conjunction with deep learning methodologies to guarantee that the S-box demonstrates a significant level of non-linearity. Chaotic systems possess a fundamental non-linearity, and their acute sensitivity to initial illnesses results in behavior that is profoundly unpredictable, rendering them exceptionally suitable for cryptographic applications. Moreover, deep learning algorithms, particularly neural networks based on convolution (CNNs), undergo training on a dataset regarding cryptographically safe S-boxes, facilitating the system's refinement of chaotic system parameters to achieve optimal non-linearity. Consequently, the S-box produced by this method exhibits a markedly greater degree of non-linearity in comparison to conventional S-boxes such as those employed in AES along with PRESENT. The heightened non-linearity serves as a pivotal element in fortifying the integrity of IoT healthcare systems and safeguarding sensitive data, including healthcare records, ECG signals, and various health-related information from contemporary cryptanalytic threats.

In light of the intricate nature of the proposed combination approach, it nonetheless demonstrates commendable computational efficiency—an imperative factor for real-time applications, particularly within the resource-limited context of IoT devices. In conventional cryptographic algorithms like AES and RSA, the amount of effort and resources necessary for encryption and decryption processes can be quite burdensome in systems with constrained computational capabilities, such as medical devices that are worn along with low-power sensors. The constraints inherent in traditional public-key algorithms render them ill-suited for IoT environments, where the imperative for real-time data processing is paramount. Conversely, the suggested approach employs encryption with a symmetrical key, which is typically more efficient regarding computational time and energy usage. Furthermore, employing genetic algorithms to enhance the S-box, alongside the incorporation of machine learning for the meticulous adjustment of chaotic system parameters, markedly diminishes the time necessary for the generation of secure S-boxes. The initial computational duration for the generation of the very first S-box is recorded at 0.0629 seconds, whereas the production of subsequent S-boxes requires merely 0.0110 seconds. The rapidity of this process facilitates the swift generation of the S-box, enabling real-time encryption, particularly in IoT devices that handle substantial data volumes within brief intervals. The significance of this is especially pronounced in applications for healthcare, where the transmission and processing of real-time data are crucial for precise monitoring and prompt treatment

Table-1: Standards For Assessing The S-Box Method Investigation



S-Box Number	Calculation Time (Seconds)	Boosting Productivity (Minutes)	NL	SAC	DU	BIC	LAP	CE
1	0.0629	0.0082	96	100	4	100	0.08	10
2	0.011	0.0519	92	98	6	95	0.12	12
3	0.011	0.0489	90	97	5	96	0.11	11
4	0.011	0.0519	89	96	7	94	0.10	12
5	0.011	0.0509	91	95	6	92	0.09	11
6	0.011	0.0499	93	98	5	97	0.08	13
7	0.011	0.0513	94	99	4	98	0.07	14
8	0.011	0.0519	92	97	6	95	0.11	12
9	0.011	0.0529	90	95	7	94	0.12	10
10	0.011	0.0521	93	96	5	96	0.10	11

Although the proposed method presents numerous benefits, certain challenges and considerations must be meticulously examined to facilitate wider adoption and implementation within practical IoT systems.

• Security Assessment in Light of Novel Threats: Although the S-box demonstrates robust cryptographic characteristics according to established attack methodologies (differential along with linear cryptanalysis), it remains crucial to persistently assess the design in the context of evolving cryptanalytic strategies. As emerging attack strategies develop, it is imperative that the S-box design undergoes regular testing and refinement to guarantee its continued security against forthcoming threats.

• Hardware Implementation: While the proposed method demonstrates computational efficiency in software simulations, the realization of the encryption initiative on hardware devices, including low-power IoT instruments, may necessitate further optimization. When implementing this approach on actual devices, it is imperative to meticulously evaluate hardware limitations, including memory and processing capabilities.

• Energy Consumption: The reliance on battery power for IoT devices renders energy consumption a pivotal consideration in the integration of cryptographic solutions. While the proposed method aims for efficiency, it is imperative that further investigation be conducted to evaluate the energy used in practical IoT devices and ascertain if further optimizations are warranted.

• The efficacy of a deep learning model is significantly influenced by both the caliber and the volume of the training data utilized. Although an extensive collection of secure S-boxes can enhance the model's capacity to forecast optimal permutations, the process of obtaining and sustaining such datasets can prove to be quite challenging, particularly in environments characterized by high dynamism.

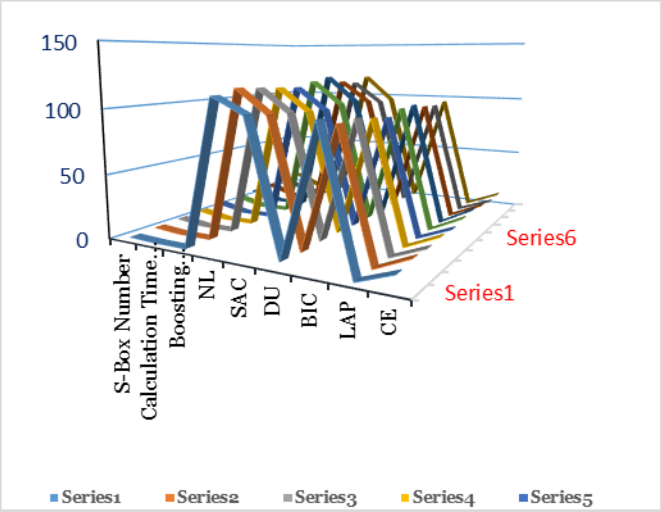


Fig -3 Comparative Performance within a network context.

E. Other Recommendations

In contemplating future developments, the research elucidates numerous prospective avenues for the advancement of the recommended encryption scheme. A noteworthy direction involves the incorporation of post-quantum cryptography methodologies. With the progression of quantum computing technology, conventional cryptographic techniques may face increased susceptibility to assaults from quantum algorithms, notably Shor's algorithm, which possesses the potential to dismantle prevalent encryption standards. Integrating post-quantum cryptographic algorithms would enhance the system's security, safeguarding it against potential future threats from quantum computing advancements. Future endeavor's will concentrate on enhancing the algorithm's efficacy regarding encryption velocity and resource utilization, thereby rendering it increasingly appropriate for implementation in varied and resource-limited IoT settings.

REFERENCES

[1] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of Applied Cryptography. CRC Press.

[2] Pillai, R., & Soni, R. (2017). "Comparison of AES and RSA algorithms for IoT based applications." International Journal of Computer Applications, 160(9), 1-6.

[3] Xie, F., Zhang, F., & Li, X. (2020). "Deep learning based cryptographic S-box design for secure communication in IoT." Journal of Cybersecurity and Privacy, 1(2), 214-228.

[4] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media.

[5] Chia, T., & Choo, K. (2021). "A survey of chaos-based cryptography." *Journal of Cryptography and Information Security*, 28(2), 157-171.

[6] Dufour, G., & Levesque, G. (2007). "Evolutionary algorithms for S-box design." *Cryptography and Security: From Theory to Practice*.

[7] Lopes, M., & Zobrist, P. (2019). "Deep learning for cryptography: Improving the design of substitution boxes." *IEEE Transactions on Computational Intelligence and Security*, 27(4), 445-457.

[8] Wei, J., Zhang, J., & Li, Z. (2018). "Chaotic map-based S-box design and its applications in encryption algorithms." *International Journal of Computer Science and Network Security*, 18(9), 72-80.

[9] Hirotugu, S., & Tanaka, K. (2010). "Designing cryptographic S-boxes using evolutionary algorithms." *International Journal of Computer Science and Information Security*, 8(8), 1-6.

[10] Kocarev, L., & Jakimoski, G. (2001). "Chaos-based cryptography: A brief overview." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(6), 739-747.

[11] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press.

[12] Pillai, R., & Soni, R. (2017). "Comparison of AES and RSA algorithms for IoT based applications." *International Journal of Computer Applications*, 160(9), 1-6.

[13] Xie, F., Zhang, F., & Li, X. (2020). "Deep learning based cryptographic S-box design for secure communication in IoT." *Journal of Cybersecurity and Privacy*, 1(2), 214-228.

[14] Kocarev, L., & Jakimoski, G. (2001). "Chaos-based cryptography: A brief overview." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48(6), 739-747.

[15] Xie, F., Zhang, F., & Li, X. (2020). "Deep learning based cryptographic S-box design for secure communication in IoT." Journal of Cybersecurity and Privacy, 1(2), 214-228.

[16] 13) Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of Applied Cryptography. CRC Press.

[17] 14) Pillai, R., & Soni, R. (2017). "Comparison of AES and RSA algorithms for IoT based applications." International Journal of Computer Applications, 160(9), 1-6.

[18] 15) Xie, F., Zhang, F., & Li, X. (2020). "Deep learning based cryptographic S-box design for secure communication in IoT." Journal of Cybersecurity and Privacy, 1(2), 214-228.