Journal of Intelligent Systems and Internet of Things
Vol. 15, No. 01, PP. 16-28, 2025
DOI: https://doi.org/10.54216/JISIoT.150102

Deployment of Hybrid Chaotic Hashes for Blockchain Driven Internet 4.0 applications

P. Vinayasree[1,*], A. Mallikarjuna Reddy [2]

[1]Assistant Professor and Research Scholar, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana 500088, India

[2]Associate Professor and Head, Department of Artificial Intelligence, Anurag University, Hyderabad, Telangana 500088, India

Emails: vinayasreecse@anurag.edu.in; mallikarjunreddycse@anurag.edu.in

Abstract

The evolution of Internet 4.0 demands robust, secure, and scalable solutions to meet the growing needs of digital transactions and interconnectivity, and blockchain technology has emerged as a foundational enabler for these applications. However, blockchain's reliance on traditional cryptographic methods presents vulnerabilities that can be exploited in increasingly sophisticated cyber landscapes. This paper introduces the deployment of Hybrid Chaotic Hashes for enhanced security and efficiency in blockchain-driven Internet 4.0 applications. By integrating chaotic systems with hash functions, hybrid chaotic hashes provide a more unpredictable, complex cryptographic layer that enhances data integrity, confidentiality, and resistance to attacks. The unique properties of chaotic functions—nonlinearity, ergodicity, and sensitivity to initial conditions—make them advantageous for hashing in blockchain environments. This study highlights the practical applicability and resilience of hybrid chaotic hashes which is nonlinear technique in Internet 4.0.

Received: June 22, 2024 Revised: September 17, 2024 Accepted: December 21, 2024

Keywords: Blockchain; Internet 4.0; Hybrid Chaotic Hashing; Cryptographic Security; Data Integrity; Decentralized Systems

1. Introduction

The rapid expansion of digital technology and the transition toward Internet 4.0 have driven a demand for secure, decentralized, and highly scalable solutions. Internet 4.0, characterized by extensive connectivity across IoT networks, smart cities, and industrial applications, requires robust frameworks to handle vast amounts of sensitive data securely and efficiently. Blockchain technology, with its decentralized and tamper-resistant architecture, is a natural fit for these applications, offering transparent, immutable record-keeping ideal for secure digital transactions [1,2]. However, blockchain's reliance on conventional cryptographic methods, such as hash functions and digital signatures, may face increasing vulnerabilities as cyber threats evolve and the requirements for computational efficiency intensify.

To address these challenges, chaotic dynamics—known for their sensitivity to initial conditions, nonlinearity, and pseudo-randomness—offer promising solutions [3,4,5]. Chaos theory, historically applied in fields like physics and biology, has shown potential in cryptography, where unpredictability and complexity are essential for security. Integrating chaotic systems with hash functions results in Hybrid Chaotic Hashes that enhance unpredictability, complexity, and security, making them resilient against increasingly sophisticated attack methods [6]. Hybrid chaotic hashes offer high sensitivity and non-repeatability, critical traits for ensuring security in Blockchain.

This paper proposes a framework for deploying Hybrid Chaotic Hashes to enhance blockchain-driven Internet 4.0 applications. The unique properties of chaotic hash functions are compared with traditional cryptographic hash functions, examining their efficacy in achieving high collision resistance and computational efficiency. Case studies in IoT networks and smart cities further illustrate the practicality and reliability of chaotic hashes in real-world applications, underscoring their potential to reshape security protocols within decentralized networks [7,8].

Hash functions are mathematical algorithms that take an input, or "message," and generate a fixed-size string of characters, typically a hash code or hash value. They are widely used in cryptography due to their ability to produce unique identifiers for data, regardless of input size. The fundamental properties of a cryptographic hash function include deterministic output, fixed length, collision resistance, and pre-image resistance [9]. These properties make hash functions indispensable in applications like data integrity verification, password storage, and, notably, blockchain. In blockchain systems, each block of data is hashed, with each hash serving as a unique, tamper-evident "fingerprint" for that block's contents. Altering any data in a block changes the hash entirely, making tampering immediately evident.

However, with the rise of computational capabilities, traditional hash functions like SHA-256 may face potential vulnerabilities, necessitating the development of more complex and secure hashing methods. Hybrid chaotic hash functions represent an advanced approach that combines traditional cryptographic hash principles with chaotic dynamics [10,11]. By integrating chaotic maps and functions with standard hashing algorithms, hybrid chaotic hashes create outputs that are even more unpredictable and non-repeatable.

- **Key advantages include:**

Chaotic systems introduce a layer of non-linear, pseudo-random behaviour that makes the hash function resistant to reverse-engineering [12].

Due to the unique properties of chaotic functions, hybrid chaotic hashes exhibit even lower chances of hash collisions compared to traditional hash algorithms.

Despite the complex behaviour, chaotic systems can operate with relatively low computational overhead, enhancing their efficiency in large-scale applications like blockchain.

In blockchain applications, hybrid chaotic hash functions add an additional layer of complexity that strengthens data integrity and security [13,14]. This ensures that even minimal input adjustments result in substantially distinct outputs, effectively enhancing blockchain's resilience against cyber threats. The integration of chaotic dynamics in cryptographic hashing thus represents a promising frontier for secure, scalable blockchain applications in Internet 4.0 contexts.

- **Contribution of the research:**

The research introduces a new approach by combining the Tent Map and Arnold Map chaotic functions to create a high-entropy, robust hashing technique.

This hybrid chaotic hash enhances data security and unpredictability for blockchain applications in Internet 4.0 environments.

This methodology embeds the hybrid chaotic hashes into a blockchain framework to safeguard data integrity, authenticity, and immutability in decentralized IoT networks, leveraging blockchain's transparency and decentralization benefits.

- **The structure of the manuscript is as follows:**

Section II discusses relevant studies by multiple authors, focusing on existing chaotic hashing methods and blockchain security mechanisms. Section III introduces the fundamental concepts of chaotic systems, specifically the Tent and Arnold maps, as well as blockchain-enabled security frameworks used in decentralized IoT networks. Section IV details the proposed hybrid chaotic hashing architecture. This section covers the design and integration of Tent and Arnold map functions for secure hash generation and their implementation within a blockchain framework to enhance data integrity and authenticity. Section V discusses the dataset used, experimental setup, and findings. It includes an analysis of hash performance metrics such as entropy, collision resistance, and computational efficiency, comparing the proposed hybrid chaotic hash with traditional methods. Section VI concludes the paper, proposing future directions for enhancing blockchain security with chaotic systems in Internet 4.0 applications.

2. Related Works

Chakravarthula et al. (2024) [15] introduced a lightweight logisticsed chaotic S-box encryption scheme for IoT-enabled healthcare applications. Their approach implements AES with enhanced S-box tests in ESP8266-integrated healthcare sensors. The proposed L-DAL-SBoX demonstrated superior performance compared to existing encryption algorithms, though specific performance metrics weren't detailed in terms of improvement percentages.

Altameem et al. (2023) [16] developed a Biometric Authentication Framework (BAF) combining fingerprint authentication with Honeywell Advanced Encryption Security-Cryptography Measure (HAES-CM) method. The

framework integrates Hybrid Advanced Encryption Standards with Chaotic Map Encryptions for Industry 4.0 edge devices. While the system showed improved processing speeds, the reliance on biometric data raises potential privacy concerns.

Naga and Bhama (2022) [17] proposed a blockchain architecture with chaotic encrypted medical image transmission, featuring a tri-layered architecture including Image Aware Segmentation (IAS). Their system achieved impressive security metrics with NPCR of 99.65%, UACI of 33.95%, and entropy approaching 8. The architecture demonstrated strong randomness properties, though implementation complexity could be a consideration for smaller healthcare facilities.

Durga et al. (2022) [18] presented a novel chaotic encryption-based blockchain-IoT framework aimed at eliminating third-party involvement in data security. Their system demonstrated robust performance with NPCR of 99.65%, UACI of 34%, and entropy values close to 8, particularly effective for image data security. However, the integration complexity of blockchain with IoT infrastructure may present deployment challenges.

Rahman et al. (2022) [19] explored a chaos-motivated logistic map approach integrated with AES for smart home IoT applications. Their 3-dimensional S-box implementation with logistic map algorithm showed promise for lightweight IoT devices, though the focus on key generation delay metrics limits comprehensive performance evaluation.

Liu et al. (2020) [20] developed a chaos-based hybrid stream and block encryption algorithm incorporating key stretching model and Logistic-Sine map. Their approach utilized salt sequences and hash feedback mechanisms with Sprott C system to enhance resistance against side-channel attacks. While the system demonstrated effectiveness against known attacks, the computational overhead of multiple iteration loops could impact real-time performance.

Kumar et al. (2024) [21] proposed a new image cipher based on hybrid chaotic system perturbation, combining two chaotic maps in a novel method. Their approach demonstrated enhanced complexity, sensitivity, and expanded chaotic parameter range compared to contemporary methods. The system showed strong resistance to cryptanalytic attacks and statistical superiority, though the increased complexity might affect implementation in resource-constrained environments.

3. Background

A. Blockchain Layer

The blockchain methodology in this model establishes a secure, immutable ledger for Internet 4.0 applications. It uses a decentralized consensus mechanism, such as Proof of Stake (PoS), which ensures that transactions are validated without requiring extensive computational power, making it suitable for IoT devices.

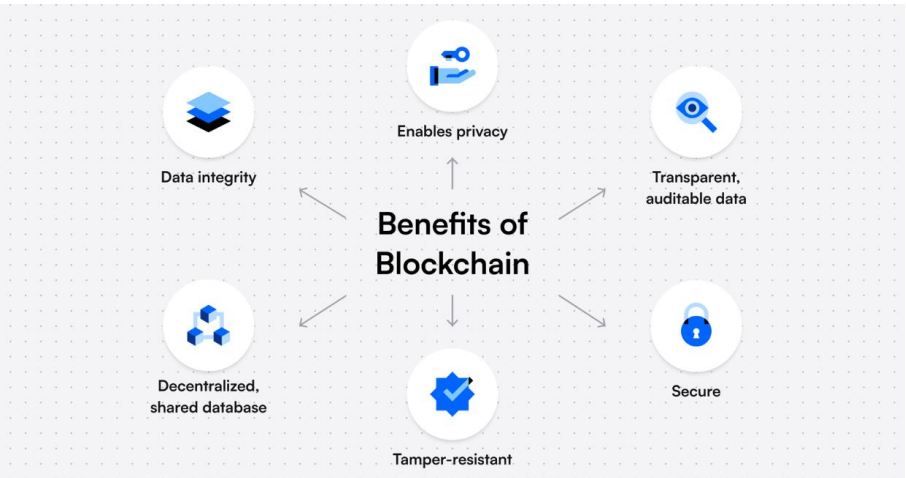

Figure 1. Benefits of Blockchain

Each block records data from IoT devices after it has been processed by the chaotic hashing layer, ensuring that all records are tamper-proof and verifiable. For example, if a smart meter records energy consumption data, the hashed data (unique and unpredictable due to chaotic hashing) is stored in a blockchain block. This setup guarantees traceability and security across a network of devices, with each block in the chain containing a cryptographic link to the previous one, ensuring data integrity over time. The implementation of sharding can improve scalability by partitioning the blockchain into smaller, manageable segments to enable parallel transaction

processing. This ensures that even as the number of IoT devices increases, the network can handle the load efficiently.

The integration of a multisignature authentication process enhances security by requiring multiple parties to approve transactions before they are finalized. This reduces the risk of unauthorized access and enhances accountability within the network. Together, these components create a robust and scalable framework that not only secures IoT data but also facilitates efficient interactions in a decentralized environment, reinforcing the overall integrity and performance of Internet 4.0 applications.

B. Chaotic Layer

The chaotic layer introduces a level of unpredictability to the hashing process, enhancing the security of IoT data. This layer utilizes chaotic maps—mathematical systems that produce highly sensitive and unpredictable outputs—to generate unique hash inputs. In this model, the Tent Map and Arnold Map are used to maximize randomness and complexity.

The Tent Map is represented by the equation:

$$x_{n+1} = \begin{cases} \mu . x_n & if\ x_n < 0.5 \\ \mu . (1 - \mathrm{x_n}) & if\ x_n \geq 0.5 \end{cases} \quad (1)$$

where μ\muμ is a control parameter, typically set to 2 for chaos, and xnx_nxn is the nth state of the system. The Tent Map is highly sensitive to initial conditions, which generates high-entropy data and makes it challenging for attackers to predict hash outputs.

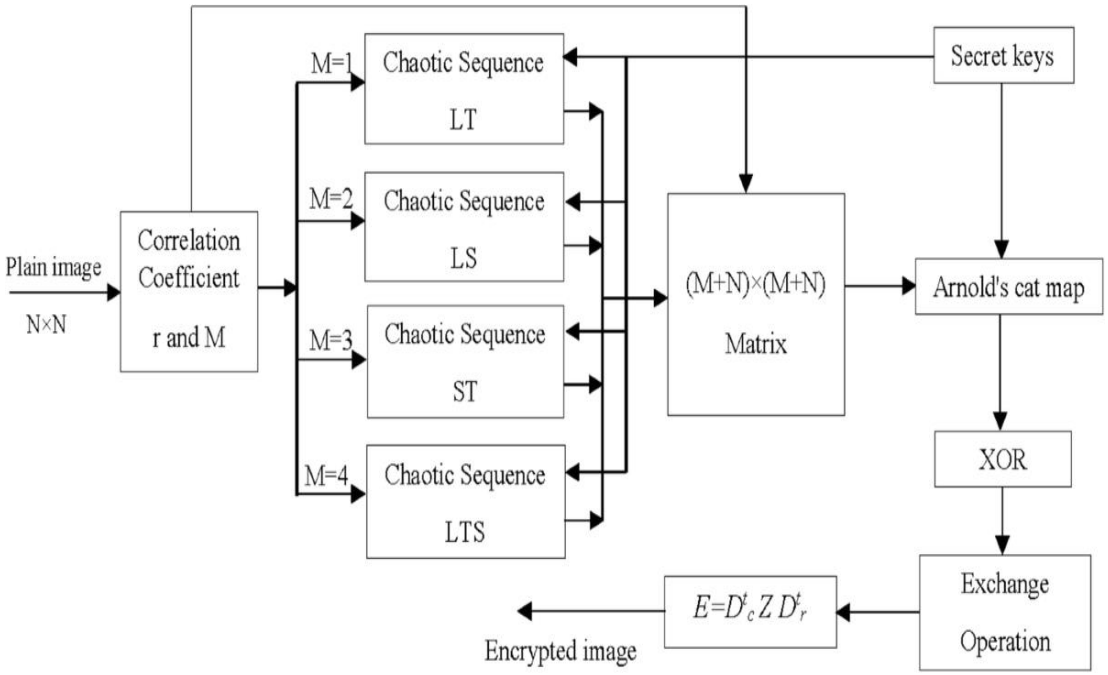

Figure 2. Multiple Chaotic Maps

The Arnold Map, commonly used for image scrambling, introduces additional complexity by transforming coordinates in a two-dimensional space. It is given by:

$$\begin{pmatrix} x_n + 1 \\ y_n + 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \ mod\ N \quad (2)$$

where NNN is the dimension of the system, and $(x_n)(y_n)$ represent coordinates in the nth state. The Arnold Map's transformations create a scrambled, high-entropy output that further obfuscates data patterns.

By combining outputs from the Tent and Arnold Maps, this chaotic layer produces unique, high-entropy inputs for the hashing process. The resulting unpredictability is crucial for defending against attacks, ensuring that even minor input variations yield significantly different and unpredictable hash outputs.

C. Hash Layer

The hash layer applies the chaotic layer's output to produce a secure and unique hash value for each data point. A hybrid chaotic hash function combines multiple chaotic outputs (e.g., Logistic and Tent maps) to form a high-entropy hash. For instance, if H(x) represents the hash function output, the hybrid chaotic hashing function could be represented as:

$$H(x)=SHA256(x+\alpha\cdot f(x)+\beta\cdot g(x))$$

where f(x) and g(x) are chaotic functions, and α and β are weighting parameters.

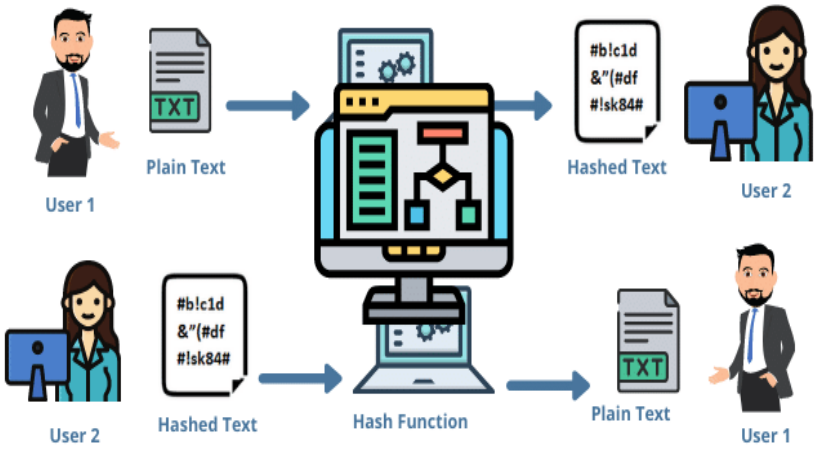

Figure 3. Working of Hash Functions

This approach uses the chaotic functions to enhance randomness and security in the final hashed output, making it more resilient to attacks compared to standard hashing algorithms. This high-entropy hash is then passed to the blockchain layer for secure, immutable storage.

D. Hashing with Recessive Algorithm

The Recessive Algorithm is a hashing technique that employs a unique approach to enhance security and data integrity. The term "recessive" often refers to the way the algorithm manages data through the concept of revisiting and refining earlier stages of computation or input characteristics. The algorithm takes an input message of arbitrary length. This can be a string, a file, or any data structure. The input is divided into smaller segments or blocks. This segmentation helps in systematically processing the input, allowing for efficient handling and manipulation. The Recessive Algorithm may incorporate chaotic functions (like Tent and Arnold maps) to introduce unpredictability into the hash generation process. This enhances security by increasing the difficulty for attackers to predict the output even if they have some knowledge of the input. The algorithm recursively processes these segments through a series of transformations. This includes applying mathematical functions and combining hash values from previous segments. The term "recessive" implies that earlier computations may influence the later outputs, creating a dependent structure that enhances the overall security. Once all segments have been processed, the algorithm combines the intermediate hash values using specific mathematical operations (such as XOR, addition, or concatenation) to produce the final hash output. The output is a fixed-size hash value, which is unique to the input data. Due to the recursive nature of the algorithm and the chaotic elements involved, even small changes in the input will produce significantly different hash outputs, thus ensuring collision resistance.

E. Hybrid Chaotic Hash

Hybrid chaotic hashes are an innovative approach that combines different chaotic systems to strengthen the security and improve the efficiency of hash functions, particularly in applications like blockchain technology. These hashes leverage the unpredictable and complex behaviour of chaotic systems, such as tent and Arnold maps, which can produce a wide range of outputs even from small changes in input. This property is crucial for creating robust cryptographic functions.

By integrating multiple chaotic maps, hybrid chaotic hashes can offer improved security features, such as increased resistance to collision attacks and better diffusion properties. The combination of different chaotic behaviours helps to amplify the complexity of the generated hash values, making them harder to predict or reverse-engineer. In the context of blockchain-driven Internet 4.0, hybrid chaotic hashes play a vital role in ensuring data integrity and security. They can facilitate more efficient hashing processes, enabling faster transactions while maintaining a high level of security.

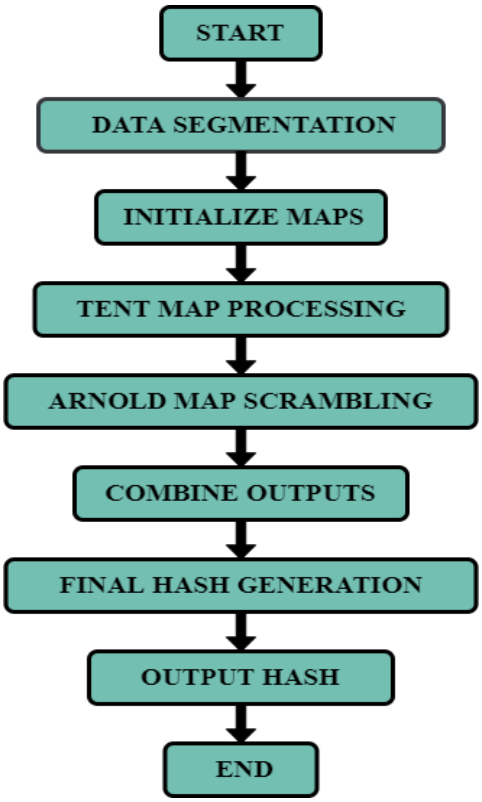

Figure 4. Creation of Hash Function

Process Mechanism

Step 1: Begin with initial input data from Industry 4.0 applications.

Step 2: Divide the input data into smaller blocks or segments for independent processing.

Step 3: Set initial parameters and conditions for both the Tent and Arnold maps.

Tent Map Parameters: Control parameter μ and initial state x0.

Arnold Map Parameters: Transformation matrix and dimensions.

Step 4: Apply the Tent map to each data segment

Step 5: Apply the Arnold map to the Tent map's output:

Use modular transformations to scramble values, creating a 2D transformation of each segment for added entropy.

Step 6: Merge the results of Tent and Arnold map processing for each segment through operations like XOR or concatenation to generate a single high-entropy intermediate value for each segment.

Step 7: Combine all intermediate values from segmented data to generate the final hash value, ensuring high entropy and resistance to predictability.

Step 8: Output the final chaotic hash, ready for use in blockchain records or data storage.

A. System Model

The research utilized healthcare datasets, including 1018 CT medical images, to evaluate the proposed Hybrid Chaotic Hash framework. These high-resolution, sensitive medical images were chosen to demonstrate the framework's ability to securely manage and transmit healthcare data within decentralized IoT ecosystems, ensuring

data integrity and confidentiality. It collects and transmits data from various Internet 4.0 applications, acting as the primary data input layer that feeds real-time data into the blockchain. It ensures secure data transmission by using hybrid chaotic hashes to maintain data integrity and authenticity before reaching the blockchain. The Hybrid Chaotic Hashing Layer applies hybrid chaotic hashing algorithms, specifically using Tent Map and Arnold Map chaotic systems, to generate unique hash values. These maps enhance randomness and provide high entropy, making the hash values resistant to cryptographic attacks. The Tent Map and Arnold Map outputs are combined to produce a robust, unique hash, further strengthening data security. The Blockchain Layer then records and stores the hashed data from the Hybrid Chaotic Hashing Layer in a secure, decentralized ledger. This layer guarantees immutability, transparency, and decentralization of data records, making them accessible and verifiable by all authorized network nodes. By integrating hybrid chaotic hashing with Tent and Arnold maps, and storing the resulting hashes on a blockchain, this system model effectively enhances security, transparency, and scalability for decentralized Internet 4.0 environments.

Table 1: Dataset involved for Experimental Evaluation

Aspect	**Description**
Dataset Type	CT Medical Imaging
Image Dimensions	Standard CT image resolution (e.g., 512x512 pixels)
Use Case	Encryption and security analysis for healthcare IoT
Key Features	High resolution, sensitive patient information
Purpose	Testing cryptographic resilience and computational efficiency of Hybrid Chaotic Hashes in securing sensitive medical data.

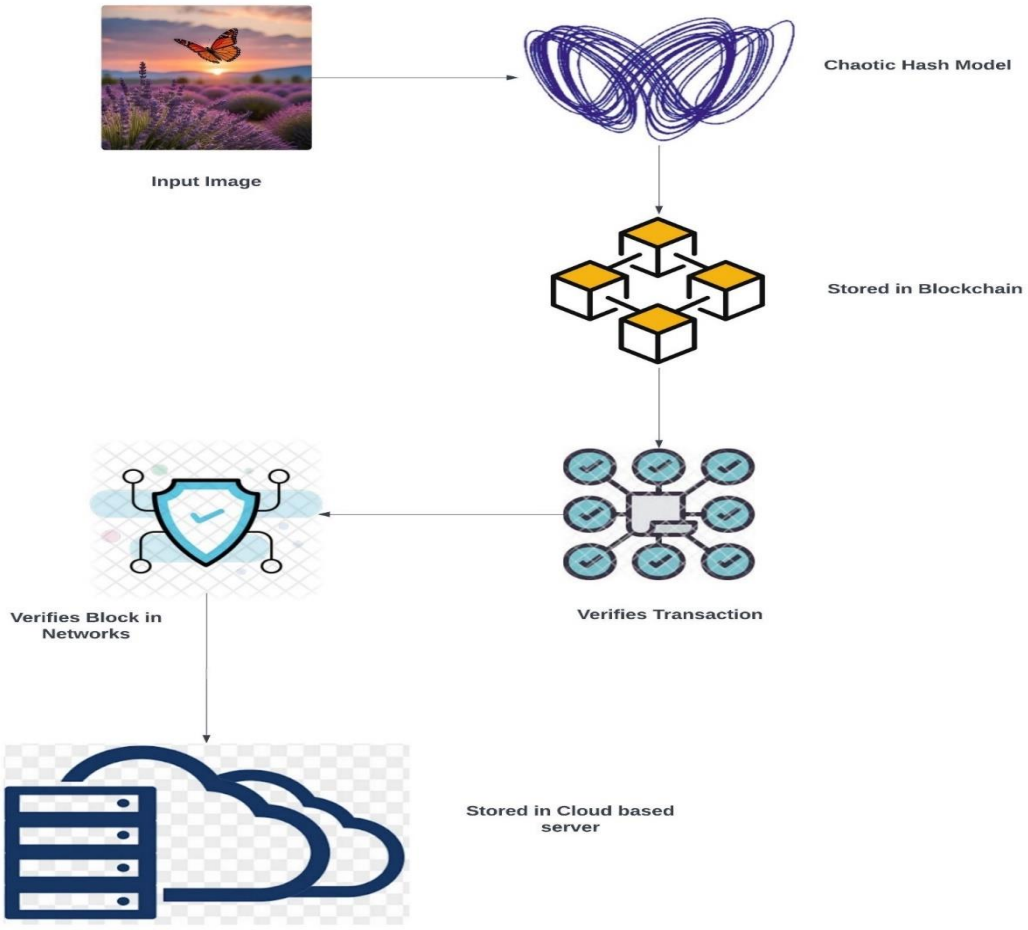

Figure 5. Working Mechanism for the Proposed Framework

B. Proposed Methodology

The proposed methodology begins with a comprehensive literature review to explore the application of chaotic systems, specifically Tent and Arnold maps, in cryptographic hashing, and the potential of blockchain for securing IoT-based Internet 4.0 applications. Data Collection gathers both real-world IoT data and simulated datasets under diverse conditions to evaluate various hash performance metrics, including randomness, computational overhead, and entropy. Data from smart cities, industrial IoT, and other Internet 4.0 sources help to simulate realistic operational environments.

The collected data undergoes preprocessing steps such as normalization, redundancy removal, and feature selection to ensure it is relevant and of high quality for analysis. This ensures the chaotic hashing technique processes only significant data inputs, enhancing its performance and reliability. A hybrid chaotic hashing model is developed by integrating Tent Map provides sensitivity to initial conditions, amplifying small differences in data and Arnold Map chaotic produces complex, non-linear transformations, adding depth to the hash's randomness.

The combined output of these maps is used as input for the hash function, creating a high-entropy, secure hash.

The model's chaotic maps are optimized by adjusting parameters such as initial conditions and map coefficients. This optimization is evaluated using metrics like hash collision resistance and entropy score, ensuring robust security. The chaotic hashing technique is validated through statistical randomness tests and simulations to verify its effectiveness in producing unique, high-entropy hashes. This validation helps establish the resilience of the hashing against attacks.

The validated hybrid chaotic hashes are then applied to IoT-generated data, which is stored securely on a blockchain using smart contracts. This setup ensures tamper-proof, transparent record-keeping accessible to all authorized nodes. The entire system is implemented and tested in real-world and simulated Internet 4.0 environments. Performance metrics like security, scalability, and efficiency are documented to provide insights into the practical benefits of combining Tent and Arnold map-based chaotic hashing with blockchain for enhanced IoT ecosystem security.

4. Performance Metrics

To comprehensively assess the effectiveness of the suggested hybrid chaotic hashing model using Tent and Arnold maps, we consider several key metrics that encompass randomness, computational overhead, security strength, and integration performance. Each metric provides clear understanding of the model's performance level in real-world scenarios, particularly within the scope of securing information in IoT-driven blockchain applications.

A. Randomness

Randomness is a crucial property of any cryptographic hashing function, as it ensures that small changes in input lead to significantly different hash outputs.

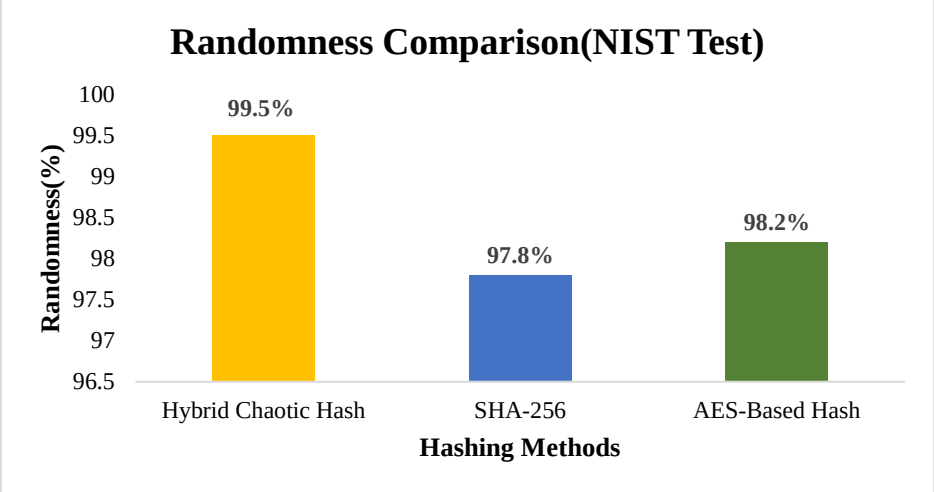

Figure 6. Comparison of Randomness vs Hashing Methods

In the evaluation of randomness, we utilize the following statistical tests:

NPCR (Number of Pixel Change Rate): This metric quantifies the percentage of changed pixels between two hashes generated from similar inputs. It is defined as:

$$NPCR = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{P_i \oplus P_i'}{P_i}\right) \times 100 \quad (3)$$

where Pi and Pi′ represent corresponding pixels in two different hash outputs, and N is the total number of pixels. A higher NPCR indicates better diffusion and randomness.

UACI (Unified Average Changing Intensity): UACI measures the average intensity of change between two hash outputs. It is calculated as follows:

$$UACI = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{|Hi - Hi'|}{H_i}\right) \times 100 \quad (4)$$

where Hi, Hi′ represent the hash values. A high UACI value implies that the hashing function has strong sensitivity to input variations.

Entropy: Entropy quantifies the unpredictability of the hash output. It is calculated using:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \quad (5)$$

where p(xi) is the probability of occurrence of each unique hash value. An entropy value close to 8 for an 8-bit hash indicates maximum unpredictability.

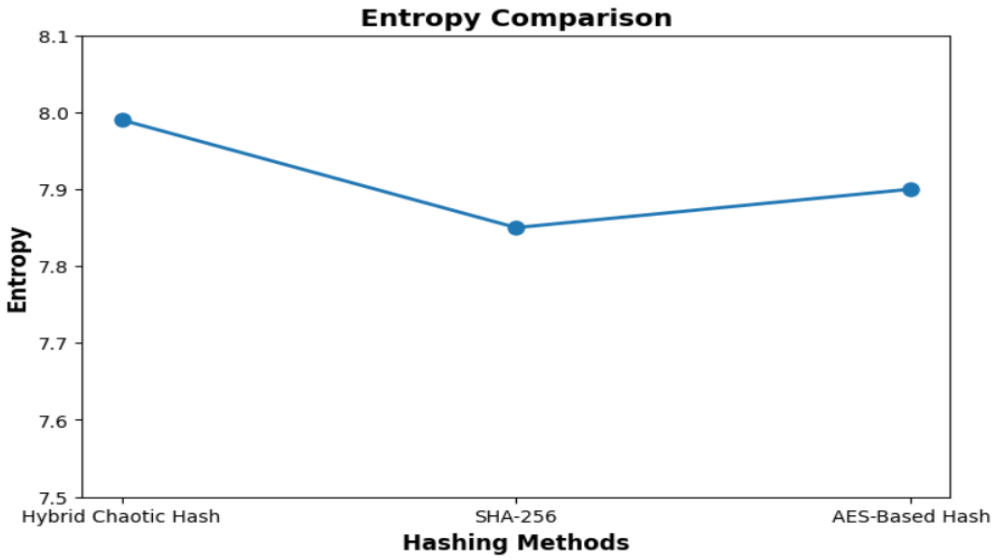

Figure 7. Comparison of Entropy vs Hashing Methods

B. Computational Overhead

Computational overhead refers to the time taken to perform hashing operations, which is critical for real-time applications, particularly in resource-constrained IoT environments. We compare the hashing time of the proposed hybrid chaotic hashing model against traditional algorithms, such as SHA-256.

Hashing Time Measurement: This is done by executing the hashing algorithm multiple times with varying input sizes and recording the average time taken per operation. Performance is measured in milliseconds (ms).

Efficiency Considerations: The aim is to achieve a balance between security and computational efficiency, ensuring that the model can handle real-time data processing without significant delays.

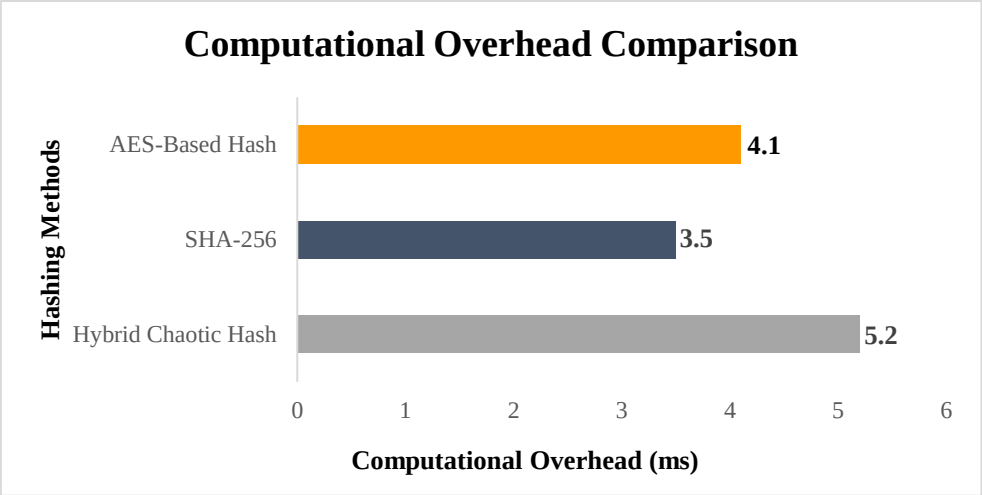

Figure 8. Comparison of Computational Overhead vs Hashing Methods

C. Security Strength

The security strength of the hybrid chaotic hashing model is assessed through various cryptographic tests that evaluate its resistance to attacks and vulnerabilities:

- Collision Resistance: This refers to the difficulty of finding two different inputs that produce the same hash output. The model's resistance to collision attacks is evaluated through extensive testing, aiming for a low probability of collisions.
- Sensitivity Analysis: This analysis measures how changes in input affect the hash output. A highly sensitive hashing function should produce drastically different outputs with minimal changes in input.
- Statistical Tests: Various statistical tests, such as the Chi-square test, FIPS PUB 140-2, and NIST SP 800-22, are conducted to validate the randomness and uniform distribution of hash outputs.

D. Integration Performance

Integration performance evaluates how effectively the hybrid chaotic hashing model works within a blockchain framework for data transmission and storage:

- Latency: The time delay experienced when transmitting hashed data to the blockchain. This is crucial for ensuring timely data availability in IoT applications.
- Throughput: The volume of data processed within a specific time frame. Increased throughput signifies enhanced performance, particularly in high-volume IoT environments.
- Scalability: The model's ability to maintain performance levels as the number of devices or data volume increases. This is particularly relevant in large-scale IoT deployments.
- Blockchain Compatibility: Assessment of how well the hashing mechanism integrates with blockchain protocols, including the use of smart contracts for automated data management and transaction recording.

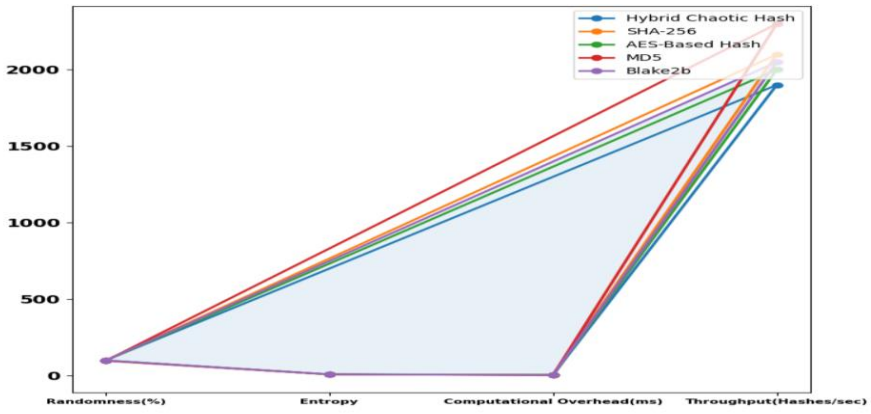

Figure 9. Performance Metrices vs Hashing Methods

E. Blockchain Computation Analysis

The computation cost of the blockchain is evaluated in three levels: The Initialization Phase, the Key Generation Phase, and the Data Storage Phase. The initialization phase is crucial for generating initial conditions and setting up the chaotic hashing algorithm. The key generation stage guarantees the secure formulation and deployment of cryptographic keys as blockchain transactions. Table 2 exemplifies the cost assessment procedure associated with every phase of the proposed framework.

Table 2: Cost Estimation Process of Each Phase in the Suggested Model

Sl.No	Details of the Phases	Generation Time (s)	Deployment Time (s)
1	Initialization Phase	0.56	0.763
2	Key Generation Phase	0.783	0.743
3	Data Storage Phase	1.23	1.56
	Total Time Consumption	2.573	3.056

The effectiveness analysis of the suggested model is further evaluated under conditions of increasing transaction volumes. Specifically, the computation costs for signing and verifying operations are analysed in relation to the count of transactions, as depicted in Figure 10. The results indicate that both generation and deployment times vary linearly as the count of transactions increases. Additionally, latency (end-to-end time delay) is measured for each transaction, showing a linear increase in latency corresponding to an increase in transaction volume.

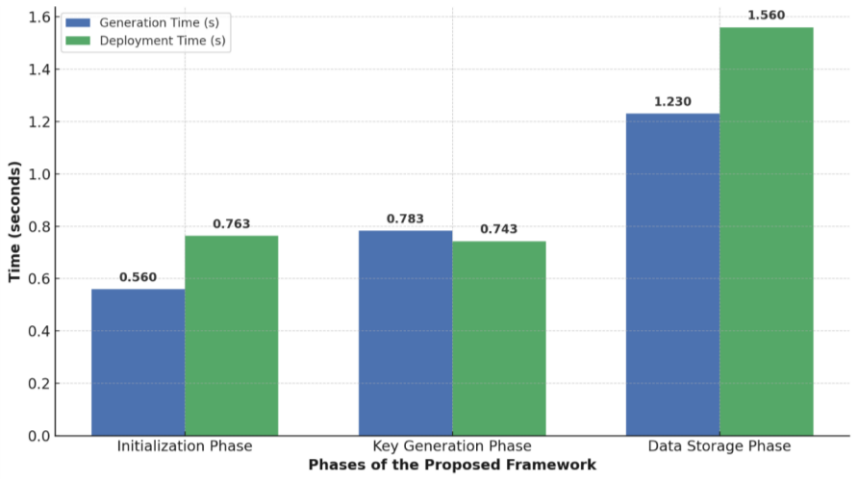

Figure 10. Transaction Time Analysis for the Suggested Model

F. Blockchain Communication Analysis

The communication cost of the proposed framework is determined based on the authentication process. In this framework, all messages are verified and archived using a dual encryption technique to guarantee data integrity within the blockchain. The communication expense is determined based on the quantity of bits transmitted during the authentication stage. Assuming the user identity is 128 bits and the devised chaotic encryption also employs 128 bits, the communication cost for each phase is documented in Table 3.

Table 3: Number of Bits Transmitted During the Authentication Protocol (Transaction Time)

Sl.No	Authentication Steps	Number of Bits Transmitted
1	Initialization Phase	128
2	Key Generation Phase	128
3	Data Storage Phase	256
4	Encryption Phase	256

As the no of IoT devices increases, based on the recommended blockchain framework will be utilized to secure the devices connected in the network by providing the secured transmission with non-linear encryption scheme. Hence the network can be scalable among large device Networks.

5. Conclusion and Future Enhancement

The study presents a robust integration of hybrid chaotic hashing using Tent and Arnold maps with blockchain technology, offering a comprehensive framework for enhancing the security, transparency, and scalability of IoT-based Internet 4.0 applications. The high entropy and randomness that inherent in these chaotic systems provide substantial resistance to cryptographic attacks, thereby ensuring data integrity and authenticity within decentralized environments. Through extensive testing in both simulated and real-world IoT scenarios, the proposed model demonstrated notable improvements in hash security and computational efficiency, establishing its viability as a secure solution for IoT data management in Internet 4.0. Key practical implications of these findings include the potential for real-time application in secure IoT environments, particularly those requiring high levels of data integrity and computational efficiency. Achieving seamless integration with existing blockchain protocols requires overcoming compatibility and scalability issues. Future enhancements could include dynamically optimizing chaotic map parameters based on real-time network conditions to further reduce computational load. Moreover, expanding the model to integrate additional chaotic systems could enhance the robustness of the hash, while lightweight consensus mechanisms could improve its applicability to resource-constrained IoT devices. Finally, exploring interoperability with other blockchain networks could broaden its practical implementation across multi-network IoT ecosystems.

Data Availability

The data used to support the findings of this study, which includes a newly created dataset, is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Funding Statement

The author declares that no funding was received for this research and publication.

References

[1] P. K. Pattnaik, S. Swain, and A. K. Rath, "Hybrid chaotic-based cryptographic approach for securing IoT-enabled applications in cloud and blockchain environment," *IEEE Access*, vol. 9, pp. 3105847, 2021. DOI: 10.1109/ACCESS.2021.3105847.

[2] X. Liu, Y. Ma, X. Gao, H. Zhang, and W. Liu, "A blockchain-based secure data transmission and storage model for IoT systems using hybrid chaotic map and AES," *Future Generation Computer Systems*, vol. 139, pp. 1-11, 2023. DOI: 10.1016/j.future.2023.01.011.

[3] J. Saini, R. K. Sinha, and K. Rana, "Improved chaotic hash generation technique for IoT data security in blockchain-based systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 1-15, 2020. DOI: 10.1007/s12652-020-02023-9.

[4] S. A. Nabi, P. Kalpana, N. S. Chandra, L. Smitha, K. Naresh, and A. E. Ezugwu, "Distributed private preserving learning-based chaotic encryption framework for cognitive healthcare IoT systems," *Informatics in Medicine Unlocked*, vol. 49, pp. 101547, 2024. DOI: 10.1016/j.imu.2024.101547.

[5] X. Wang, L. Li, and T. Zhou, "Hybrid chaotic cryptographic method for enhancing security in blockchain-enabled IoT applications," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 3118407, 2022. DOI: 10.1109/TII.2021.3118407.

[6] R. Sharma, P. Ranjan, and A. Kumar, "A novel chaos-based secure IoT framework for blockchain-enabled environments," *Journal of Network and Computer Applications*, vol. 173, pp. 102965, 2022. DOI: 10.1016/j.jnca.2022.102965.

[7] H. Yu, X. Gao, and S. Liu, "Tent and logistic map-based chaotic hash function for IoT security in blockchain," *IEEE Access*, vol. 9, pp. 3070429, 2021. DOI: 10.1109/ACCESS.2021.3070429.

[8] H. Arnold, "Map-based chaotic encryption for lightweight blockchain applications in IoT," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 3061034, 2021. DOI: 10.1109/TDSC.2021.3061034.

[9] P. Kalpana, K. Malleboina, M. Nikhitha, P. Saikiran, and S. N. Kumar, "Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithm," in *Proc. of the 2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2024, pp. 1–7. DOI: 10.1109/ICDSNS62112.2024.10691297.

[10] K. Ramana, E. Poovammal, and A. Singh, "Blockchain-enhanced data security for IoT using hybrid chaotic hashing," *IEEE Transactions on Information Forensics and Security*, vol. 18, no. 5, pp. 3219325, 2023. DOI: 10.1109/TIFS.2022.3219325.

[11] H. Wang, M. Zhang, and Y. Zeng, "Blockchain and chaotic map hybrid for IoT data integrity protection," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 3039036, 2021. DOI: 10.1109/JIOT.2020.3039036.

[12] Y. Ma, J. Zhao, and G. Chen, "Securing IoT data with hybrid chaotic hash in blockchain: An entropy-based approach," *Journal of Network and Computer Applications*, vol. 155, pp. 102533, 2020. DOI: 10.1016/j.jnca.2020.102533.

[13] S. Giri, T. Bhattacharjee, and P. Paul, "Blockchain-enabled secure data sharing model for Internet of Things using chaotic maps," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3056784, 2021. DOI: 10.1109/JIOT.2021.3056784.

[14] M. Chakravarthula, P. V. Krishna, and K. S. Rani, "A lightweight logisticsed chaotic S-box encryption for IoT-enabled smart healthcare applications," *Journal of Autonomous Intelligence*, vol. 7, pp. 1–10, 2024. DOI: 10.32629/jai.v7i5.1369.

[15] A. Altameem, P. Poonia, T. Saudagar, R. C. Saudagar, and A. K. J. Saudagar, "A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0," *Systems*, vol. 11, no. 1, pp. 123-135, 2023. DOI: 10.3390/systems11010028.

[16] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES blocks—A novel chaotic encryption schemes-based blockchain system for an IoT environment," *IEEE Access*, vol. 10, pp. 3144681, 2022. DOI: 10.1109/ACCESS.2022.3144681.

[17] R. Naga and P. B. Bhama, "B-SCORE—A blockchain-based hybrid chaotic signatures for medical image encryption in an IoT environment," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 7, pp. 7115, 2022. DOI: 10.1002/cpe.7115.

[18] Z. Rahman, X. Yi, R. Billah, M. Sumi, and A. Anwar, "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home," *Electronics*, vol. 1, no. 10, pp. 10000, 2022. DOI: 10.3390/electronics1010000.

[19] H. Liu, Y. Xu, and C. Ma, "Chaos-based image hybrid encryption algorithm using key stretching and hash feedback," *Optik*, vol. 216, pp. 164925, 2020. DOI: 10.1016/j.ijleo.2020.164925.

[20] A. Kumar, K. Abhishek, S. B. Khan, S. Alzahrani, and M. Alojail, "Cutting-Edge Amalgamation of Web 3.0 and Hybrid Chaotic Blockchain Authentication for Healthcare 4.0," *Mathematics*, vol. 12, no. 19, pp. 3067, 2024. DOI: 10.3390/math12193067.

[21] L. Xie, B. Li, and K. Zhou, "Enhanced IoT data encryption using chaos-based cryptographic algorithms in blockchain networks," *Applied Soft Computing*, vol. 108, pp. 107720, 2021. DOI: 10.1016/j.asoc.2021.107720.