COMPARATIVE STUDY OF CHAOTIC SYSTEM FOR ENCRYPTION

Doaa S. Salman

Informatics Institute for Postgraduate Studies, Iraqi

Commission for Computers and Informatics,
Imam Al-Kadhum College, Baghdad, Iraq
ms202110664@iips.icci.edu.iq

Jolan Rokan Naif

Informatics Institute for Postgraduate Studies, Iraqi
Commission for Computers and Informatics,
Baghdad, Iraq

newjolan@gmail.com

***Abstract* - Chaotic systems leverage their inherent complexity and unpredictability to generate cryptographic keys, enhancing the security of encryption algorithms. This paper presents a comparative study of 13 chaotic keymaps. Several evaluation metrics, including key space size, dimensions, entropy, statistical properties, sensitivity to initial conditions, security level, practical implementation, and adaptability to cloud computing, are utilized to compare the keymaps. Keymaps such as Logistic, Lorenz, and Henon demonstrate robustness and high security levels, offering large key space sizes and resistance to attacks. Their efficient implementation in a cloud computing environment further validates their suitability for real-world encryption scenarios. The context of the study focuses on the role of the key in the encryption and provides a brief specification of each map to assess the effectiveness, security, and suitability of the popular chaotic keymaps for encryption applications. The study also discusses the security assessment of resistance to the popular cryptographic attacks: brute force, known plaintext, chosen plaintext, and side channel. The findings of this comparison reveal the Lorenz Map is the best for the cloud environment based on a specific scenario.**

Index Terms - chaotic keymaps, encryption key, cryptography, security, cloud encryption, cryptography attacks.

I. INTRODUCTION

In today's era, the abundance of information transferred and stored electronically has raised substantial concerns about data security. Protecting data from access, interception, and manipulation is important for individuals, businesses, and governments, and encryption is a tool for ensuring data security. Encryption involves the conversion of data into text using cryptographic techniques and an encryption key. The resulting scrambled text appears as a sequence of characters, preventing anyone without the correct decryption key from understanding its meaning. This transformation ensures that even if an unauthorized individual accesses the encrypted data, the contents cannot be comprehended without the relevant decryption key [1].

Encryption plays a pivotal role in securing data during transmission over untrusted networks, such as the Internet. As cloud computing becomes more prevalent, encryption becomes essential for securing data stored and processed in cloud environments. Encryption is as an indispensable technology for ensuring data security, confidentiality, and integrity in the digital age. By incorporating encryption into various data processing and communication workflows, organizations and individuals can remarkably reduce the risks associated with data breaches and unauthorized access [2]. To classify the importance of encryption in cloud security, a percentage can be assigned to each criterion, which can vary depending on the specific use case and the organization's priorities, as shown in Figure 1.

Encryption keys play a crucial role in the encryption process, serving as the cornerstone of data security. Briefly, the role of encryption keys can be summarized as follows [3], [4]:

- **Key Generation**: Encryption keys are randomly generated using specialized algorithms. The strength and randomness of the key directly affect the security of the encryption.
- **Key Distribution**: The encryption key needs to be securely distributed to authorized parties who are allowed to encrypt or decrypt the data. Key distribution mechanisms should protect against interception or unauthorized access to the key.
- **Encryption**: During encryption, the plaintext data are combined with the encryption key using a cryptographic algorithm. The encryption key serves as the parameter to control the transformation, producing the ciphertext as the output.
- **Decryption**: The correct decryption key is used to retrieve the original plaintext from the ciphertext in the decryption, which is mathematically related to the encryption key. The decryption key enables inverse transformation, reverting the ciphertext to its original plaintext form.
- **Key Management**: Appropriate key management envelops secure key stockpiling, access control, and key rotation to prevent key compromise. Key management practices guarantee the security and lifecycle management of encryption keys.
- **Confidentiality and Integrity**: Encryption keys ensure data confidentiality by making the ciphertext mixed up with unapproved parties. Only users

possessing the correct decryption key can access the original plaintext. Furthermore, encryption keys safeguard data integrity by detecting any unauthorized modification to the ciphertext during decryption.

The utilization of chaotic maps in the field of cryptography has garnered substantial interest owing to their crucial role in encryption based on their inherent characteristics such as sensitivity to initial conditions, unpredictability, and complex dynamics, to furnish a secure, efficient approach for the generation of encryption keys [5].

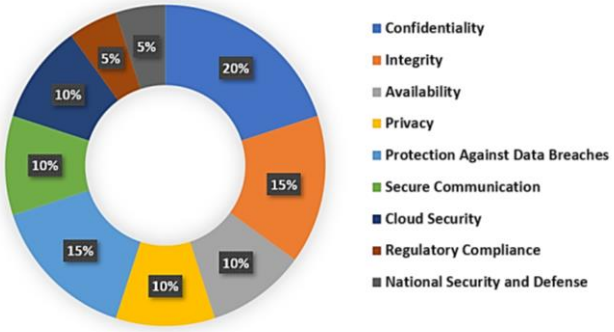

Fig. 1: Importance of encryption in securing data

II. AIM OF THE STUDY

A. The purpose of the study is to furnish a comprehensive comprehension of the selection of distinct chaotic keymaps and their effectiveness for applicability in encryption, particularly in the realm of cloud computing. The range of the comparative study includes the following aspects:

B. **Selection of Chaotic Keymaps**: The study entails a diverse set of heterogeneous assemblages of chaotic keymaps from a multitude of families including the logistic map, Henon Map, Lorenz Map, and others.

C. **Evaluation Criteria**: The present study delineates explicit parameters for the assessment and measurement of the performance, randomness, security, and resistance against cryptographic attacks of the designated chaotic keymaps.

D. **Testing and Analysis**: The comparative analysis comprises a sequence of examinations and assessments performed on some keymaps utilizing recognized techniques and instruments. These assessments consist of randomness analysis, sensitivity analysis, entropy effect evaluation, statistical properties, and others.

E. **Security Assessment**: The study conducts a security assessment to identify the resistance of keymaps to cryptographic attacks.

F. **Applicability in Cloud Environment**: The comparative study investigates how the recommended chaotic keymap performs in a cloud computing environment.

III.LITERATURE REVIEW

This review examines existing literature on chaotic keymaps and their application in encryption:

A. **Theoretical Foundations of Chaotic Keymaps**:

- Alexander N. Pisarchik et al. (2010) discussed the theoretical foundations of chaotic systems and reviewed the main achievements in the field of chaotic cryptography [6].
- Chih-Hsueh Lin et al. (2021) discussed how synchronizing chaotic systems led to the concept of using synchronized chaotic systems as a source of secure keys [7].

B. **Chaotic Key Generation Techniques**:

- Christophe Guyeux et al. (2010) discussed various techniques proposed for generating chaotic keys, such as chaos-based pseudorandom number generators [8].
- Sellami Benaissi et al. (2023) introduced a novel approach using a hybrid of three modified, improved chaotic systems for key generation [9].

C. **Cryptographic Properties of Chaotic Keymaps**:

- Studies have also explored the cryptographic properties of chaotic keymaps, including their sensitivity to initial conditions, robustness against attacks, and their effect on encryption strength [6].
- Nasser Abdellatif et al. (2023) analyzed the correlation properties and security of chaotic keymaps for practical cryptographic applications [10].

D. **Chaos-Based Encryption Algorithms**:

- Amal H. Khaleel et al. (2021) proposed numerous encryption algorithms that utilize chaotic keymaps, such as chaos-based image encryption algorithms, and

discussed many different chaos-based encryption techniques [11].

- Fethi Dridi et al. (2022) discussed the application of chaotic maps in block ciphers that have been investigated to improve the security and confusion properties of encryption [12].

E. Dimensions of Chaos Maps:

- Noor Naser et al. (2022) discussed chaotic map-based cryptography, categorizing them into 1D, 2D, and multidimensional maps. A novel 4D NSJR chaotic system was employed, which resulted in an expedited speed of encryption/decryption and rendered it impervious to known cryptanalysis attacks [13].
- Hayder Najm et al. (2021) explained the intricacies of the 5D system that manifested more intricate dynamic characteristics than the lower-dimensional chaotic system. The proposed chaotic system underwent rigorous testing and demonstrated remarkable proficiency, thereby resulting in a super chaotic system with (5 positive Lyapunov) exponents [14].

F. **Security Analysis and Vulnerabilities**:

- Linqing Huang et al. (2018) examined the security of chaotic encryption algorithms, vulnerabilities to known plaintext attacks, chosen plaintext attacks, and related-key attacks [15].
- Mihir Bellare et al. (2011) addressed the design of robust encryption algorithms that are resistant to related-key attacks [16].

G. **Performance Evaluation**:

- Research focused on evaluating the performance of chaotic keymaps in terms of key generation speed, entropy generation, and computational overhead, as mentioned in [17] [18] [19].
- Extensive studies compared the performance of different chaotic maps in generating keys for practical encryption applications [20] [21].

The literature on chaotic keymaps and their application in encryption reveals a diverse range of studies exploring the theoretical foundations, cryptographic properties, and practical implementations of chaotic systems in cryptography. While chaotic keymaps demonstrate promising features for secure key generation, further research is needed to address challenges related to key distribution, system parameters, and resistance to cryptanalytic attacks. Future studies could explore hybrid encryption schemes, combining the strengths of chaotic keymaps with traditional cryptographic algorithms, to improve security and efficiency in data encryption.

IV. SELECTION OF CHAOTIC KEYMAPS

Different chaotic keymaps offer unique properties and behaviors, making them suitable for different applications. Well-known chaotic keymaps widely used in encryption systems are listed below:

13. Logistic Map [22]:

- Mathematical Equation:
  $x_{\{n+1\}} = r * x_n * (1 - x_n)$
- Specialties: 1D, simple logistic growth model, exhibits bifurcation and chaotic behavior at specific parameter values

2. Lorenz Map [23]:

- Mathematical Equation:
  $dx/dt = \sigma * (y - x)$,
  $dy/dt = x * (\rho - z) - y$,
  $dz/dt = x * y - \beta * z$
- Specialties: 3D chaotic system with the iconic "butterfly" attractor, widely used in weather prediction and atmospheric modeling

3. Henon Map [24]:

- Mathematical Equation:
  $x_{\{n+1\}} = 1 - a * x_n^2 + y_n$,
  $y_{\{n+1\}} = b * x_n$
- Specialties: 2D, dissipative chaotic map, simple and efficient, used in various cryptographic applications

13. Tent Map [25]:

- Mathematical Equation:
  $x\{_{n+1\}} = \text{if } (x_n < c)\ , c * x_n\ , \text{else } 2 - c * x_n$
  $x_{(n+1)} = \mu(\ 1 - 2\ |\ x_n - 1/2\ |\ )$.
- Specialties: 1D piecewise linear chaotic map (PWLCM), simple, used in pseudo random number generation and cryptography

13. Arnold's Cat Map [26]:

- Mathematical Equation:
  $x\_\{n + 1\} = (x_n + y_n) \bmod 1$,
  $y\_\{n + 1\} = (x_n + 2y_n) \bmod 1$
- Specialties: 2D area-preserving map, used in image encryption and scrambling

13. Baker Map [27]:

- Mathematical Equation:
  $x_{\{n+1\}} = \text{floor}\ (x_n) \bmod 1$,
  $y_{\{n+1\}} = (y_n + \text{floor}(x_n)) \bmod 1$
- Specialties: 2D chaotic map with stretching and folding, used in signal processing and cryptography

7. Ikeda Map [28]:

- Mathematical Equation:
  $x_{\{n+1\}} = 1 + u * (x_n * \cos(t) - y_n * \sin(t))$,
  $y_{\{n+1\}} = u * (x_n * \sin(t) + y_n * \cos(t))$

- Specialties: 2D iterative map with a parameterized angle, used in laser dynamics and chaos synchronization

8. Cubic Map [28]:

- Mathematical Equation:
  $x_{\{n+1\}} = a * x_n^3 + b * x_n^2 + c * x_n + d$
- Specialties: 1D cubic chaotic map, chaotic and exhibits periodic windows, used in chaos-based communication

9. Standard Map [29]:

- Mathematical Equation:
  $x_{\{n+1\}} = x_n + y_n - (k/2\pi) * \sin(2\pi * x_n)$,
  $y_{\{n+1\}} = y_n - (k/2\pi) * \sin(2\pi * x_n)$
- Specialties: 2D area-preserving map, used in studies of Hamiltonian systems and chaos diffusion

10. Gauss Map [30]:

- Mathematical Equation:
  $x_{\{n+1\}} = e^{-\alpha xn2} + \beta$
- Specialties: 1D chaotic map derived from the Gaussian probability distribution, used in image encryption and chaotic oscillators

11. Piecewise Linear Chaotic Map [31]

- Mathematical Equation:

$$f(x_n, y_n) = \begin{cases} \begin{pmatrix} -ax_n + y_n \\ bx_n + y_n \end{pmatrix} & \text{if } x_n \geq 0 \\ \begin{pmatrix} ax_n + y_n \\ bx_n + y_n \end{pmatrix} & \text{if } x_n < 0 \end{cases}$$

- Specialties: 2D noninvertible discrete piecewise map, used in pseudorandom number generation and chaotic cryptography

12. Tinkerbell Map [28]:

- Mathematical Equation:
  $x_{\{n+1\}} = x_n^2 - y_n^2 + ax_n + by_n$,
  $y_{\{n+1\}} = 2x_ny_n + cx_n + dy_n$
- Specialties: 2D quadratic chaotic map, exhibits various shapes when iterated

13. Gingerbread-man Map [32]:

- Mathematical Equation:
  $x_{\{n+1\}} = 1 - y_n + |x_n|$,
  $y_{\{n+1\}} = x_n$
- Specialties: 2D chaotic map with a self-replicating structure, used in image encryption and pattern generation

These properties play a crucial role in selecting the appropriate chaotic map for encryption applications based on the desired security level, computational efficiency, and specific requirements of the encryption system. The selection should consider the trade-offs between complexity, security, and resource requirements to achieve a suitable balance for the encryption application.

1.1 Keymaps' Suitability for Encryption Applications

To assess the effectiveness, security, and suitability of three popular chaotic keymaps, namely, the Logistic Map, the Lorenz Map, and the Henon Map, for encryption applications, the evaluation is based on findings from the studies cited in references [31], [32], and [33].

- **Randomness:** A suitable keymap should produce key sequences that appear random and exhibit a high degree of entropy.
  - The Logistic Map demonstrates chaotic behavior and can generate key sequences possessing substantial randomness as a result of its sensitivity to initial conditions.
  - The Henon Map is renowned for its irregular, unpredictable behavior, rendering it appropriate for the generation of random key sequences.
  - The Lorenz Map, due to its chaotic nature, can produce key sequences with elevated randomness, particularly when parameters are selected suitably.

- **Mathematical Formulation**: This formulation is used to determine if it is dynamic or continuous to compute its efficiency.
  - Logistic Map: The Logistic Map is a 1D map defined by the recurrence relation
    $x_{(n+1)} = r * x_n * (1 - x_n)$, where r is the control parameter. It exhibits simple dynamics and can be efficiently computed.
  - Lorenz Map: The Lorenz Map is a continuous-time 3D chaotic system with the equations $dx/dt = \sigma * (y - x)$, $dy/dt = x * (\rho - z) - y$, $dz/dt = x * y - \beta * z$, where σ, ρ, and β are system parameters. It involves complex dynamics and continuous-time equations.
  - Henon Map: The Henon Map is a 2D map defined by the equations $x_{(n+1)} = y_n + 1 - a * x_n^2$ and $y_{(n+1)} = b * x_n$, where a and b are control parameters. It displays elementary dynamics and is characterized by computational efficiency.

- **Key Generation Efficiency:** This metric measures the proportion of computational time to system resources.
  - Logistic Map: The Logistic Map presents a computationally efficient approach for key generation owing to its 1D nature and direct iteration formula.
  - Lorenz Map: The Lorenz Map requires more computational resources for key generation due to its continuous-time equations and 3D dynamics.
  - Henon Map: The Henon Map is computationally efficient for key generation, similar to the Logistic Map, due to its simple 2D equations.

- **Security and Sensitivity**: Chaotic keymaps should exhibit high sensitivity to initial conditions. Minor changes in initial values should result in markedly distinct key sequences. Additionally, they should possess resistance against cryptographic attacks.
  - Logistic Map: The Logistic Map manifests a remarkable sensitivity to initial conditions, thereby conferring a heightened degree of security. Nevertheless, its 1D nature renders it susceptible to certain cryptanalytic attacks.
  - Lorenz Map: The generation of keys for the Lorenz Map demands a substantial allocation of computational resources due to the intricate continuous-time equations and 3D dynamics that operate within its system.
  - Henon Map: The Henon Map is renowned for its computational efficiency in generating keys and analogous to the logistic map owing to its uncomplicated 2D equations.

- **Key Space Size**: A larger chaotic key space enhances security by making some attacks more computationally infeasible.
  - Logistic Map: The Logistic Map's key space is confined to the interval [0, 1] for variable "x", which may result in a comparatively diminished key space in relation to chaotic systems of higher dimensions.
  - Lorenz Map: The Lorenz Map is particularly adept at facilitating image encryption and other scenarios necessitating the generation of high entropy keys.
  - Henon Map: The Henon mapping exhibits a 2D domain of keys, thereby presenting a superior key space in contrast to the logistic mapping.

- **Applicability in Encryption**: Each map works better in some environments based on its specifications.
  - Logistic Map: The Logistic Map is a fitting choice for straightforward encryption techniques and stream ciphers owing to its efficiency and susceptibility to initial conditions.
  - Lorenz Map: The Lorenz Map is particularly suitable for image encryption and other applications requiring high-entropy key generation.
  - Henon Map: The Henon Map exhibits suitability for implementation in lightweight encryption scenarios and image encryption endeavors owing to its dynamic properties in two dimensions.

The comparative study highlights the strengths and weaknesses of the three chaotic keymaps, namely, Logistic, Lorenz, and Henon for encryption purposes. The Logistic Map excels in computational efficiency and simplicity but may have limitations in key space size and security. The Lorenz Map provides high security and sensitivity but requires more computational resources. The Henon Map offers a balance between computational efficiency and security with its 2D dynamics. The choice of the most appropriate keymap is contingent upon the particular encryption criteria, the desired level of security, and the computational resources accessible within a given application. The graphical representation in Figure 2 exhibits the level of randomness inherent in the Lorenz keymap, while its specifications contribute to a heightened level of security when implemented in conjunction with my RC6 encryption algorithm.

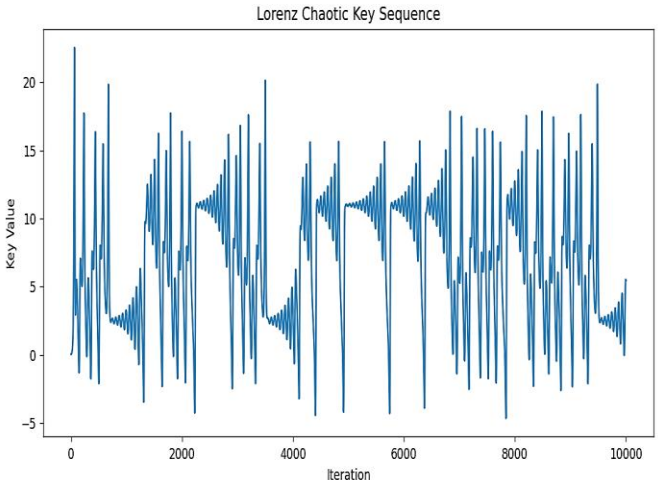

Fig.2 Randomness of Lorenz chaotic key sequence

V. Comparative Analysis Criteria

To provide a comprehensive comparison [33] [34], the following test criteria are used:

- **Dimensions**: The dimensionality of the keymap is evaluated: 1D maps involve a single variable, whereas 2D maps have two variables, and so on. Higher-dimensional maps can provide more complex encryption, but they may require more computational resources.
- **Mathematical Formulation**: Understanding the mathematical equations that define the keymap involves studying the iterative formulas and parameter values used to generate the chaotic sequence.
- **Key Space Size**: The size of the key space generated by the chaotic map is determined. A larger key space provides higher security against brute-force attacks, making guessing the key more difficult for adversaries.
- **Computational Efficiency**: Measuring the computational efficiency of the keymap considers the time taken to generate key sequences. Faster maps can lead to quicker encryption and decryption.
- **Sensitivity to Initial Conditions**: The sensitivity of the keymap to initial conditions is assessed. A good chaotic map should exhibit sensitive dependence on initial values to ensure similar inputs generate highly distinct outputs.
- **Security Level**: The security level provided by the keymap is evaluated against various cryptographic attacks. Resistance to known attacks is crucial for secure encryption.
- **Applicability in Encryption**: The keymap's suitability for encryption purposes is considered. It should provide chaotic and unpredictable sequences, essential for generating secure encryption keys.
- **Entropy**: The entropy of the keymap's output sequences is measured. Higher entropy indicates more randomness and better security.
- **Statistical Properties**: The statistical properties of the keymap's output, including Monobits test, Runs test, and autocorrelation test, are analyzed to ensure it meets cryptographic requirements.
- **Robustness to Perturbations**: How the keymap responds to parameter perturbations and variations in initial conditions is assessed. A robust map should remain chaotic and secure even with slight changes.
- **Time Complexity**: The time complexity of the keymap's iterations is evaluated. Complex maps may require more computational resources, affecting overall encryption performance.
- **Space Complexity**: The memory or storage requirements of the keymap is considered. Lower space complexity is preferable for efficient implementation.
- **Practical Implementation**: The feasibility of implementing the keymap in real-world scenarios is examined, considering hardware and software constraints.
- **Application Suitability**: The suitability of the keymap for specific encryption applications, such as symmetric or asymmetric encryption, is determined.
- **Adaptability to Cloud Computing**: How well the keymap can be integrated into a cloud computing environment is assessed, considering parallelization and distributed computing capabilities.

To select the six best tests to apply to chaotic keymaps, those crucial for evaluating the security, randomness, and practicality of the keymaps in an encryption context are considered. The recommended tests based on [23] [35] are key space size, entropy, statistical properties, sensitivity to initial conditions, security level, and practical implementation, as shown in Table 1.

TABLE I. RECOMMENDED TESTS ON KEYMAPS

Key Map	Key Space Size	Entropy	Statistical Properties	Sensitivity to Initial Conditions	Security Level	Practical Implementation
Logistic Map	2^{32}	0.994	63.557%	44%	38.29 %	Yes
Lorenz Map	2^{96}	1.00	97.869%	56.25%	58.88 %	Yes
Henon Map	2^{64}	0.872	93.098%	41.4%	56.00 %	Yes

Table 1 compares the specified chaotic keymaps based on the six tests. The experiment examines the efficacy of a 256-bit key, which has the potential to be longer. To gauge the unpredictability of the key, the entropy test is utilized. A key with a high level of entropy is more resilient against statistical attacks due to its increased randomness, and its value is constrained within the range of 0 to 1. One noteworthy characteristic of chaotic systems is their susceptibility to initial conditions. Even a slight alteration in the initial condition can

result in a substantially distinct key. This attribute can enhance security by rendering the key highly unpredictable, even when one possesses knowledge of the system. To obtain the statistical characteristics, three examinations are employed. The initial examination is the Monobits test, which evaluates the proportion of 0s and 1s. Ideally, a random sequence should possess an approximately equal quantity of both digits. The subsequent examination is the Run test, which identifies a continuous sequence of identical bits, such as 0000 or 111. This examination determines if the frequency of runs of various lengths aligns with the expected occurrence in a random sequence. The final examination is the autocorrelation test, which investigates patterns by comparing a sequence with shifted versions of itself. Lastly, the level of security for each keymap can be adjusted based on the perceived significance of each factor.

VI. Keymap Suitability for Cloud Environment

Choosing the best chaotic keymap for encryption in a cloud environment is a multifaceted decision, considering factors such as security, performance, and adaptability to cloud computing. Commonly considered options include the Logistic, Lorenz, Henon, Standard, and Gauss maps. After the previous comparative analysis, the Lorenz Map emerges as the prime choice. It boasts a generous key space size, ensuring a formidable defense against brute-force attacks. The Lorenz Map's sequences exhibit high entropy, guaranteeing the generation of robust, unpredictable keys. It also demonstrates good statistical properties, resulting in keys resembling true randomness. Furthermore, it is sensitive to initial conditions, enhancing key security. In terms of security levels, the Lorenz Map ranks first, with resistance to known cryptographic attacks. It is practically implementable, facilitating efficient encryption processes. Lastly, its adaptability to cloud computing environments seals its suitability. Considering these factors and the results in Table 1, the Lorenz Map is the optimal choice for securing a cloud-based system [36].

VII. Security Assessment

This study provides a general overview of the security assessment considerations for the three keymaps (Logistic, Lorenz, and Henon) and their resistance to cryptographic attacks as mentioned in [37], [38], [39] [40]. The assessments include brute-force attack resistance, known-plaintext and chosen-plaintext attacks, differential cryptanalysis, meet-in-the-middle attacks, side-channel attacks, and security analysis standards. The assessment relevant for the cloud computing environment is selected to evaluate the strength of encryption schemes using chaotic keymaps:

- **Brute-Force Attack Resistance:** Brute-force attacks involve trying all possible combinations of keys to decrypt the ciphertext. The strength of the keymap depends on the size of the key space [41], [42].
    - The Logistic Map has a limited key space size, making it susceptible to brute-force attacks, especially with modern computing capabilities.
    - The Lorenz Map and the Henon Map, with larger continuous parameter spaces, generally offer higher resistance to brute-force attacks.
- **Known- and Chosen-Plaintext Attacks:** Known-plaintext attacks involve an attacker having access to plaintext and corresponding ciphertext pairs. Chosen-plaintext attacks involve the attacker choosing plaintexts and observing the corresponding ciphertexts [43].
    - The Lorenz Map's chaotic behavior and sensitivity to initial conditions can provide some resistance against these attacks as extracting information about the key becomes challenging.
    - The Henon Map and the Logistic Map might be less resistant to these attacks due to their potentially weaker chaotic properties.
- **Side-Channel Attacks:** Side-channel attacks exploit information leaked by a system during the encryption, such as power consumption or timing [44].
    - The complexity of the Lorenz Map and its chaotic behavior may make side-channel attacks more challenging.
    - The Henon Map and the Logistic Map might be more susceptible to certain side-channel attacks due to their simpler mathematical formulations.

Professional cryptanalysts typically evaluate these maps using various cryptographic attack techniques to assess their security levels and their suitability and security in a cloud computing environment. More secure encryption schemes usually involve combining multiple chaotic keymaps or using them as part of hybrid encryption systems to enhance their resistance to attacks.

VIII. Conclusion

The comparative study of chaotic keymaps for encryption in a cloud computing environment yielded several remarkable findings:

- **Security and Robustness**:
    - The Lorenz Map exhibits the highest level of security and robustness among the keymaps due to its strong chaotic behavior and sensitivity to initial conditions.
    - The Henon Map provides a reasonable level of security, making it suitable for certain encryption scenarios, although it is not as robust as the Lorenz Map.
    - The Logistic Map's security is limited due to its potentially weaker chaotic behavior and smaller key space.
- **Computational Efficiency and Scalability**:

- The Logistic Map stands out among the keymaps in terms of computational efficiency and scalability owing to its simple, straightforward mathematical formulation.
- The utilization of the Lorenz Map necessitates additional computational resources due to its differential equation system, which may affect performance during cloud deployments on a large scale.
- The implementation of the Henon Map displays a moderate level of efficiency, with a notable advantage in terms of scalability when compared to the Lorenz Map.

- **Sensitivity and Randomness**:
  - The sensitivity of the Lorenz Map to initial conditions constitutes an additional layer of data integrity and security, rendering it appropriate for scenarios where the preservation of chaotic behavior is essential.
  - The Henon Map exhibits a moderate degree of sensitivity, making it a suitable choice for ensuring a desirable level of robustness in specific use cases of cloud encryption.
  - The overall robustness of the Logistic Map is influenced by its limited sensitivity.
- **Applicability in Cloud Environments:**
  - The computational efficiency and simplicity of the Logistic Map render it highly appropriate for parallel computing and real-time encryption in cloud environments characterized by high-throughput demands.
  - The security and robustness of the Lorenz Map render it an appropriate selection for cloud-based applications, where data integrity and resistance to cryptographic attacks are of utmost importance.
  - The Henon Map's equilibrium between safeguarding and effectiveness renders it appropriate in specific cloud encryption scenarios.
- **Limitations and Future Research**:
  - Some keymaps, such as the Logistic Map, display limitations with regard to their security and the magnitude of their key space. As a result, additional research and prospective enhancements are necessary.
  - Future studies could potentially investigate further keymaps, hybrid encryption algorithms, and optimizations to enhance the efficiency and security of chaotic encryption within cloud-based settings.

The comparative analysis reveals the Lorenz Map exhibits robust security and sensitivity features and emerges as a potential contender for employment in applications that necessitate high-security levels and data integrity in a cloud computing environment.

REFERENCES

[1] [1] S. L. Graham, R. L. Rivest, A. Shamir, and L. Adleman, "Programming Techniques A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," 1978.

[2] William Stallings, *CRYPTOGRAPHY AND NETWORK SECURITY (PRINCIPLES AND PRACTICE)*, SEVENTH EDITION. British Library Cataloguing-in-Publication Data, 2017.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography Invited Paper." IEEE Transaction on information theory, 1976.

[4] E. Barker and A. Roginsky, "Transitioning the use of cryptographic algorithms and key lengths," Gaithersburg, MD, Mar. doi: 10.6028/NIST.SP.800-131Ar2. 2019.

[5] H. Zaini and Z. Alqadi, "Improving the Use of Chaotic Keys in Message Cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 12, no. 1, pp. 32–46, doi: 10.47760/ijcsmc.2022.v12i01.005, Jan. 2023.

[6] C. D. B. (Courtlandt D. B. Bryan, *CHAOTIC MAP CRYPTOGRAPHY AND SECURITY*. 2010.

[7] C.-H. Lin, G.-H. Hu, C.-Y. Chan, J.-J. Yan, and J. Chaos-Based, "Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm," doi: 10.3390/app, 2021.

[8] C. Guyeux, Q. Wang, J. Bahi, J. A. Bahi, and J. M. Bahi, "Pseudo Random Numbers Generator Based on Chaotic Iterations" , [Online]. Available: https://hal.science/hal-00563317. 2010.

[9] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg)*, vol. 272, Feb. 2023, doi: 10.1016/j.ijleo. 170316. 2022.

[10] A. Manasreh, M. Khrisat, and Z. Alqadi, "MULTIPLE ROUNDS USING MIXED CHAOTIC KEYS METHOD FOR SECURE MESSAGE CRYPTOGRAPHY". ARPN Journal of Engineering and Applied Sciences. VOL. 18, NO. 8, APRIL 2023.

[11] A. H. Khaleel and I. Q. Abduljaleel, "Samarra Journal of Pure and Applied Science www.sjpas.com Chaotic Image Cryptography Systems: A Review," [Online]. Available: www.sjpas.com . 2021.

[12] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "Design, Implementation, and Analysis of a Block Cipher Based on a Secure Chaotic Generator," *Applied Sciences*, vol. 2022, no. 19, doi: 10.3390/app12199952ï, 2022.

[13] J. Rokan, N. M. Naser, and J. R. Naif, "New Ultra-Lightweight IOT Encryption Algorithm Using Novel Chaotic System" International Journal on 'Technical and Physical Problems of Engineering' IJTPE Journal,

Issue, vol. 53, pp. 253–259, [Online]. Available: www.iotpe.com , 2022.

[14] H. Najm, H. K. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 2, pp. 184–199, doi: 10.3991/ijim.v15i02.19961. 2021.

[15] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion", doi: 10.3390/e20070535, Entropy, vol. 20, no. 7, Jul. 2018.

[16] M. Bellare, D. Cash, and R. Miller, "LNCS 7073 - Cryptography Secure against Related-Key Attacks and Tampering", International Association for Cryptologic Research, 2011.

[17] M. Yildirim, "Comparative analysis of the effects of chaotic systems on the robustness of image encryption", doi: 10.5152/electrica.2021.21027, *Electrica*, vol. 21, no. 2, pp. 209–215, May 2021.

[18] C. García-Grimaldo and E. Campos-Cantón, "Comparative analysis of chaotic features of maps without fixed points." Springer link, 2022.

[19] M. Uddin, F. Jahan, M. K. Islam, and M. Rakib Hassan, "A novel DNA-based key scrambling technique for image encryption," *Complex and Intelligent Systems*, doi: 10.1007/s40747-021-00515-6, vol. 7, no. 6, pp. 3241–3258, Dec. 2021.

[20] A. Yousif and A. H. Kashmar, "Key generator to encryption images based on chaotic maps", doi: 10.24996/ijs.2019.60.2.16. *Iraqi Journal of Science*, vol. 60, no. 2, pp. 362–370, Feb, 2019.

[21] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," doi: 10.1007/s10207-022-00588-5. *Int J Inf Secur*, vol. 21, no. 4, pp. 917–935, Aug. 2022.

[22] J. O. Adeleke, "Analysis of Logistic Maps Magnetic Properties of Superconducting Metals and Alloys. View project", doi: 10.13140/RG.2.2.27790.23367. Illinois Institute of Technology, 2022.

[23] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," doi: 10.11591/ijece.v10i5.pp4824-4834, *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 4824–4834, Oct. 2020.

[24] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," doi: 10.1109/ACCESS.2020.3032403. *IEEE Access*, vol. 8, pp. 194289–194302, 2020.

[25] Institute of Electrical and Electronics Engineers, IEEE Circuits and Systems Society, C. IEEE International Conference on Electronics, and ICECS 20 2013.12.08-11 Abu Dhabi, *Image Encryption Using Generalized Tent Map*. 2013.

[26] C. E. C. Souza, D. P. B. Chaves, and C. Pimentel, "One-Dimensional Pseudo-Chaotic Sequences Based on the Discrete Arnold's Cat Map over Z3m," doi: 10.1109/TCSII.2020.3010477, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 1, pp. 491–495, Jan. 2021.

[27] Y. Shi and Y. Deng, "Hybrid control of digital baker map with application to pseudo-random number generator," doi: 10.3390/e23050578, *Entropy*, vol. 23, no. 5, May 2021.

[28] R. B. Naik and U. Singh, "A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption," doi: 10.1007/s40745-021-00364-7, *Annals of Data Science*. Springer Science and Business Media Deutschland GmbH, 2022.

[29] J. D. Meiss, "Visual Explorations of Dynamics: The Standard Map," doi: 10.1007/s12043-008-0103-3, Indian Academy of Sciences, Jun 2008.

[30] M. T. Suryadi, Y. Satria, and L. N. Prawadika, "An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, doi: 10.1088/1742-6596/1490/1/012045, Jun. 2020.

[31] M. Mammeri, N. E. Kina, and M. Fadel, "Analytical Solution of the Chaotic Piecewise Linear Planar Map," [Online]. Available: https://publishoa.com , *J Algebr Stat*, vol. 13, no. 3, pp. 5446–5453, 2022.

[32] M. Agarwal and R. Ratan, "On the characteristics of 1D-HD chaotic maps for cryptographic applications", doi: 10.14704/nq.2022.20.9. NQ44708. Neuroquantology, September 2022.

[33] asheets on asheets, "NONLINEAR DYNAMICS AND CHAOS." HAL open science, 2021.

[34] A. A. Zaher and A. Abu-Rezq, "Chaos-based secure communications in a large community system," doi: 10.1016/j.cnsns.2010.12.032. Commun Nonlinear Sci Numer Simul, vol. 16, no. 9, pp. 3721–3737, Sep. 2011.

[35] A. Siswanto, N. Katuk, and K. Ruhana Ku-Mahamud, "Chaotic-Based Encryption Algorithm using Henon and Logistic Maps for Fingerprint Template Protection," 2020.

[36] A. T. Velte, T. J. Velte, and R. C. Elsenpeter, Cloud computing: a practical approach. McGraw-Hill, 2010.

[37] F. A. Abdulatif and M. Zuhiar, "Improve Security of Cloud Storage by Using Third Parity Authentication, One Time Password and Modified AES Encryption Algorithm," doi: 10.11591/ijict.v7i1.pp24-30, International Journal of Informatics and Communication Technology (IJ-ICT), vol. 7, no. 1, p. 24, Apr. 2018.

[38] S. B. Sadkhan, "Network attacks: Methods of cryptanalysis", Report 2012.

[39] A. Kumar et al., "Cloud Computing Security, Risk, and Challenges: A Detailed Analysis of Preventive Measures and Applications," Practical Applications, 2023.

[40] A. Alismail, E. Altulihan, R. Bukhowah, and M. Frikha, "SECURITY THREATS, COUNTERMEASURES AND DATA ENCRYPTION TECNHINQUIES ON THE CLOUD COMPUTING ENVIROMENT," Available: www.jatit.org. J Theor Appl Inf Technol, vol. 15, no. 5, 2023.

[41] M. Mishra and V. H. Mankar, "A chaotic encryption algorithm: Robustness against brute-force attack," doi: 10.1007/978-3-642-30111-7_17, in *Advances in Intelligent and Soft Computing*, pp. 169–179, , 2012.

[42] N. A. Ali, A. M. S. Rahma, and S. H. Shaker, "3D Content Encryption Using Multi-Level Chaotic Maps," doi: 10.24996/ijs.2023.64.5.35, *Iraqi Journal of Science*, vol. 64, no. 5, pp. 2521–2532, 2023.

[43] Shunqin Zhu, Congxu Zhu, and Xiujuan Li "An efficient chosen-plaintext attack and improvement on an image encryption algorithm based on cyclicshift and multiple chaotic map" Multimedia Tools and Applications, 2023.

[44] M. S. Acikkapi, F. Ozkaynak, and A. B. Ozer, "Side-Channel Analysis of Chaos-Based Substitution Box Structures," doi: 10.1109/ACCESS.2019.2921708, IEEE *Access*, vol. 7, pp. 79030–79043, 2019.