International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 849-857
Journal homepage: http://iieta.org/journals/ijsse

Enhancement of Multi-Level Mutual Authentication Systems Using High-Entropy Chaotic Key Generation

Gregor Alexander Aramice*, Radhi Sehen Issa, Zahraa Ghalib Mustafa, Hussein Ghani Abdulkareem

Electrical Engineering Department, College of Engineering, Mustansiriyah University, Baghdad 46049, Iraq

Corresponding Author Email: gregoralexander1977@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.160412

Received: 3 March 2026
Revised: 16 April 2026
Accepted: 26 April 2026
Available online: 30 April 2026

Keywords:
multi-factor mutual authentication, deterministic chaos, One-Time Password, internet of things security, Avalanche effect, Butterfly effect

ABSTRACT

Traditional multi-factor authentication frameworks frequently rely on linear or static cryptographic keys, which are increasingly vulnerable to sophisticated pattern recognition and channel attacks. To address these vulnerabilities, this paper proposes an enhanced security protocol that leverages the non-linear dynamics of deterministic chaotic engines. The core of the system integrates Logistic Map to generate dynamic One-Time Passwords (OTPs), where the initial seed is derived from hardware token's Unique Identifier, and the control parameter (r) is dynamically mapped from the user's mobile phone suffix. This dual parametric approach ensures that both the hardware identity and the user's personal device contribute to the chaotic entropy. Validation is experimentally performed through 5,000 Monte Carlo simulation cycles demonstrates a near-uniform distribution, confirming the elimination of statistical bias. Furthermore, sensitivity analysis reveals that a marginal parameter perturbation of 10^{-6} results in total bit-sequence divergence. The protocol achieves a Strict Avalanche Criterion near the ideal 50% and a Bit Independence Criterion correlation reaching the theoretical ideal of 0.0000, establishing high resistance against brute-force, cloning, and differential attacks. The results indicate that this chaotic framework provides a computationally efficient, high-entropy solution for mutual authentication in Internet of Things embedded environments.

1. INTRODUCTION

The expansion of the Internet-of-Things (IoT) has introduced billions of interconnected devices into global infrastructure across various domains, including smart cities, healthcare, and industrial automation. As these devices often handle sensitive personal data, establishing robust mutual authentication remains a primary security challenge. Most contemporary authentication frameworks rely on linear One-Time Password (OTP) or Multi-Factor Authentication (MFA) protocols or static lookup tables.

These traditional mechanisms suffer from several critical limitations in the face of modern cryptanalysis:

(1) Predictability and Linearity: an attacker captures a sufficient sequence of any token, then the linear relationship between states may be mathematically modeled and predicted.
(2) Susceptibility to Differential Attacks: small variations in input signals often produce predictable output shifts in linear systems, rendering them vulnerable to template-matching or cloning attacks.
(3) Key Management Overhead: Static keys require secure storage on the device, which is susceptible to physical probing or side-channel leakage in resource-constrained environments.

However, this proliferation has rushed the development of robust security protocols, leaving terminal devices vulnerable to sophisticated cyber-attacks. Mutual authentication, where both the user and the secured system verifying each other, remains the important criteria for securing such systems [1].

To minimize authentication processing power, time or even required memory to conduct a task, many authentication architectures based hardware were proposed, such as; In a linear architecture, the relationship between input and output is proportional and mathematically transparent. This weakness of complexity introduces significant risks; if an attacker intercepts a series of tokens, they can use algebraic regression to predict future keys [2]. small changes in user identifiers result in similar output tokens, making the system vulnerable to attacks [3]. linear systems often lack Avalanche effect needed to discriminate a legitimate hardware token from an unauthorized device with replicated original data [4].

This research integrates deterministic chaos to address these weaknesses. In contrast to linear systems, chaotic maps are characterized by their extreme sensitivity to initial conditions. By utilizing the Logistic Map, the system transforms static user identifiers into a high-entropy chaotic stream.

This paper introduces a resilient mutual authentication protocol designed for resource-restricted Arduino environments. Three key contributions may fix previous mentioned weaknesses; maximizing generated key entropy may reduces the predictability of nonlinear key generation, such method performed via high iteration of chaotic engine; Multi-Level Factor Authentication (MLFA) process as mutual

handshaking architecture ensures, user's mobile (software token) and the Radio Frequency Identification (RFID) reader (hardware token), dual-end validation; chaos system stability proving with statistical validation using Monte Carlo simulations.

The following sections are as follows: related works detailed in section 2, one time password extraction proposed in section 3, system performance analysis presented in section 4, Avalanche effect presented in section 5, results and discussion applied in section 6, finally, conclusion produced in section 7.

2. RELATED WORKS

Many previous related works concerned different algorithms based software tokens with or without hardware tokens to generate OTP; Synchronized timing and cryptographic hashing may be effective at heavy duty computing infrastructure when generating secure OTP, but they still present challenges for limited IoT terminals for example. Three primary methodologies are categorized for the following related works:

2.1 Software-based and time-synchronized One-Time Password frameworks

Early OTP technology focused on seed exchanging performed via software token verifying authentication process and correctness of OTP [5]. Time based OTP algorithm produced with compatibility to payment services and customer authentication purposes, in this approach three steps produced to get secure connection between client and bank, but with some disadvantages which are; need to additional devices; physical accessibility to tokens, and authority blockage when token damaged [6]. To enhance security, mathematical calculation, as intermediate layer, added between a user (waiting an OTP) and a system (generating an OTP), is to be solved by user to obtain that OTP [7]. Infinite OTP generation is constructed rather than finite one, where multiple short hash chains proposed instead of long chain improving Lamport's OTP and addressing its weaknesses, this procedure eliminated the request of pre-sharing secret between any two authentication entities [8].

2.2 Multi-factor and hybrid authentication systems

To reduce the risks of single-factor compromise, diverse security layers were integarted. A secure MLFA based hashing algorithm-256 developed for mobile finance applications by combining Personal Identification Number (PIN), OTP, fingerprint biometric and quick response code as an additional security when providing authentication within mobile money apps with high performance comparing with other available apps [9]. Integration of three authentication methods (Edwards-curve digital signal algorithm, quick response, and cryptographically secure pseudorandom number generator) is proposed for remotely document authentication using digital signatures, providing 76.27% improvement for all parameters under assessment [10]. Multi-factor authentication system proposed based graphical passwords as a security level against key logging and screen capturing attacks [11]. Three layer authentication system proposed for securing E-Health records based 16-bit XOR cryptography for data storage, the system enhances security effectively depending on block chain management system [12]. Periodic sequences replaced with real random data in order to enhance the security of cryptography in information technology systems and generate OTPs using quantum true random number generator exceeding post processing requirements and generating unpredictable secure keys [13]. Keyed hash message authentication code protocol proposed for secure communication between wireless body area network sensor nodes in order to share secure patient information remotely with efficient energy and memory utilization [14]. Two factor authentication protocol proposed for IoT securing devices, the first factor serves as mutual secrete identifier, and channel based random characteristics parameters as second factor for high security against attacks [15]. Traditional multi-factor authentication frameworks, such as the three-level system proposed by the study [1], established a solid foundation for securing RFID and GSM-based access. However, many of these systems rely on linear or additive algorithms for key generation, it still required for more robust and secured algorithms for generating OTP.

2.3 Chaotic and non-linear key generation

For more secure authentication and OTP generation, many modifications performed with previous researches depending on, either software token or hardware token or both of them, one of which is the utilization of chaos theory for OTP generation.

A combination of chaotic theory with OTP technology proposed for attacks resistance via hash functions combined with chaotic hash function based Hénon-like mapping [16]. Based logistic map with predetermined initial and control parameters, OTP generated utilizing Android software for authentication purposes, the proposed method characterized with well resistant to keylogging software and attacks [17]. Complex key generation based logistic maps performed for, IoT sensors security purpose and advanced encryption standard improvement; the technique utilizes the 3-dimensional key generation matrix to generate alphanumeric initial key as a matrix form, then two more steps performed to generate a second and third keys via 8-bit linear feedback shift register and then an X-or operation performed to get the last key [18]. Six digits OTP, generated based B-exponential chaotic map, with 120 times high security comparing to 4-digit OTP, this OTP generated according to correct data entered from a user, then OTP generated and sent to user's mobile [19].

Table 1. Comparative analysis of authentication methodologies

Methodology	Ref.	Security Mechanism	Main Limitation
Software/Time-Based	[5-8]	Linear counters/Hash chains	Predictable if logic is exposed
Hybrid/Multi-Factor	[9-12]	Biometrics/XOR/Blockchain	High computational/Hardware cost
Quantum/Hardware	[13, 14]	Physical Randomness	Integration complexity for IoT
Chaotic (Single Key)	[17-19]	Non-linear mapping	Often uses static parameters
Proposed Work	This study	Dual-Parametric Chaos	N/A

In this research, a simple modification as an improvement performed on the previous framework published by the study [1]., which used linear methods to generate an OTP with a possible vulnerability to modern cryptanalysis, addressing this gap with utilizing non-linear logistic map chaotic engine for OTP generation and mutual authentication purpose.

Table 1 presents a comparative analysis of authentication methodologies.

3. ONE-TIME PASSWORD EXTRACTION

The proposed authentication protocol which is based on OTP extraction is defined as a transformation function F which maps physical and user-specific variables into a high-entropy token space, Eq. (1):

$$OTP = F(UID, M, i) \tag{1}$$

where, UID represent a hardware identifier as input space, and M is the mobile suffix as input space, for i iterations, and the OTP represents the output space.

The system assumes the mapping function $f(M)$ remains private and the non-linearity of chaotic map prevents internal state x_n reconstruction from the observed outputs.

Robustness of this OTP generator evaluated via the following assumptions with an assumed attacker model:

(1) An attacker can intercept a generated OTP during transmission over any local network.
(2) An attacker may get physically a lost RFID tag, so knowing the UID.
(3) An attacker may have access to previous pairs of UIDs and their corresponding OTPs.

Conventional and traditional OTP extracting systems suffer some security issues, which my needed to be solved by using chaotic mapping properties, one of which is the chaotic logistic mapping properties as shown in Eq. (2) to be integrated with traditional process suggested in the study [1] to attain more random and secure characteristics for a generated key, Eq. (2) represents the internal state of the chaotic mapping as a recurrence relation.

$$x_{n+1} = r x_n (1 - x_n) \tag{2}$$

where, x_n is the current state with range (0 to 1) in decimal, r is the control parameter with best range (3.57 to 3.99), x_{n+1} is the next state. If the control parameter is out of this range, the system approaches a fixed point [20-22].

In this proposed system, a terminal device verifies the user's physical token represented by RFID Unique Identifier (UID). Concurrently, session validation performed by server to generate a time sensitive chaotic token based user's mobile number as a shared information. This two-way verification guarantees that even if any unauthorized party emulates any RFID card, they cannot break the system without the synchronized generated chaotic response from the server.

The proposed modified scheme utilizes a mutual authentication handshake through three stages is illustrated in Figure 1 for OTP generation.

Stage1: a unique UID utilized, after its validation in a database, to define the initial seed x_0 for the chaotic logistic map. This seeding process ensures that the entropy of the resulting OTP is linked to the hardware token (RFID card), providing sensitive process to the specific user's identity. The initial seed acts as non-stochastic input to the chaotic engine that produces the final OTP, this initial seed leads to a different PIN if different RFID card is used, since any change in the UID leads to different x_0 and a different path. Since UIDs are very big integers, they need to be normalized to the range (0 and 1) using Eq. (3):

$$x_0 = \frac{UID_{int}\ (mod\ M)}{M} \tag{3}$$

where, x_0 is the inital seedfor the choitic logistic map, UID_{int} represents the RFID UID converted from hexadecimal to integer, M represents scaling constant to achieve best resolution to the initial seed, setting $M = 10^6$ is recommended to provide six decimal places as precision to x_0.

At same time, each UID is related to a unique mobile number belongs to a specific user in that database; a mobile number here behaves as a coordinator to the chaotic engine since the control parameter r is determined from it using a linear mapping technique, this means that each user has its own r as a unique chaotic environment for every authentication attempt.

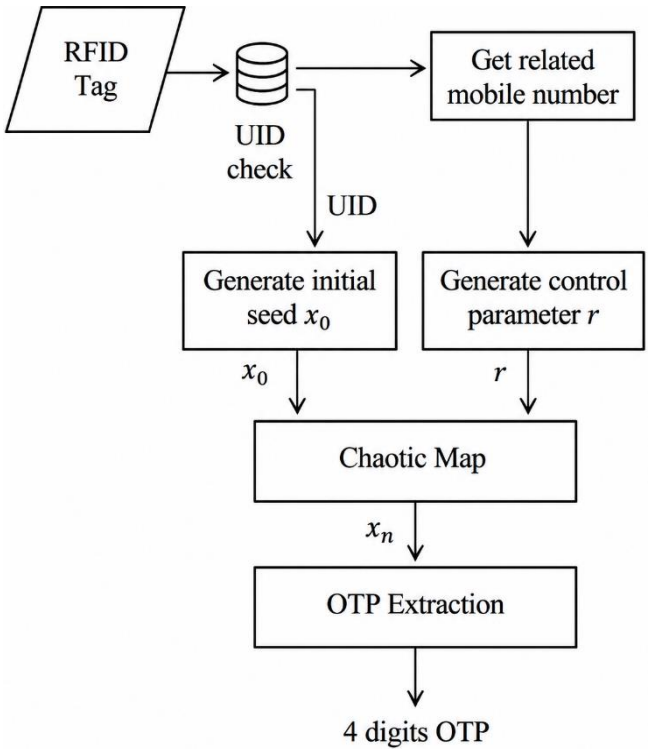


Figure 1. Block diagram of the proposed system

Figure 1 illustrates that the proposed system architecture follows these layers:

(1) Normalization Layer: Converts the hex-encoded UID into the initial seed x_0.
(2) Parametric Mapping Layer: Derives the structural key r from the mobile suffix, ensuring each user operates on a unique chaotic trajectory.
(3) Chaotic Engine: Executes i iterations to eliminate any linear correlation from the inputs.
(4) Quantization Layer: Maps the final chaotic state x_i into the decimal OTP format.

Most users in Iraqi mobile network providers share same prefix with two, three or more digits (like 077, 07701, 079, 07901 …etc.), so this unique redundant part is isolated in this proposed scheme, and the last six digits are taken, for example: if a mobile number is (07702xxxxxx) then the part (07702) is neglected and the part (xxxxxx) is taken for manipulation. These six (xxxxxx) digits are normalized within the range (3.57 and 3.99) to maintain the system within chaotic zone. The normalization formula is given in Eq. (4):

$$r = r_{min} + (\frac{xxxxxx}{999999} \times (r_{max} - r_{min})) \quad (4)$$

where, r is the control parameter, r_{min} is the minimum value of the control parameter (3.57), r_{max} is the maximum value of the control parameter (3.99), and the $\frac{xxxxxx}{999999}$ part of the equation represents normalization to the six digits ($xxxxxx$) to the range (0 to 1) as decimal number.

Stage2: chaotic transformation is performed utilizing both extracted parameters x_0 and r in a recursive calculation where the system runs the logistic mapping formula for 100 loops to transform a linear input to non-linear chaotic state x_n obtaining Avalanche effect. In this phase, the user's identity is effectively hidden through 100 iterations of the chaotic map.

Stage3: PIN quantization and final preparation is performed by transforming the final state x_{100} into readable PIN by multiplying the decimal last value by 10000 to attain integer range, and then a quantization performed to discard the decimal part with a truncation process, finally, 4-digit PIN extracted by processing with (mod 10000).

This stage provides a range-reduction by transforming a chaotic decimal with high-entropy properties into a standard 4-digit integer OTP, keeping the non-linear properties of the OTP generator. In addition, modulo 10000 step turns the system to one way function that prevents an attacker to reverse the PIN and get user information (as mobile number).

4. SYSTEM PERFORMANCE ANALYSIS

Comparing the above non-linear proposed chaotic system based, with the original traditional system, the proposed system has directionality security metric, where the system generates an OTP from an identity, but it is computationally infeasible to reverse the operation to get the identity from the generated OTP mathematically, unlike the original system where an attacker can guess the UID if he sees the OTP. The proposed system is resistive to reverse engineering.

In addition, the probability of a collision is statistically negligible, since any two different users can't get same generated OTP in this proposed system, since it generates 4-digit OTP and this ranges from 0000 to 9999, so the probability to get same OTP from two different users in 1/10000. Table 2 presents a comparison of the system presented in the study [1] with this proposed chaotic based system.

From Table 2, the cryptographic robustness of the system is significantly bolstered by transitioning from a linear model to a chaotic map. As the original work in the study [1] provided three level authentication framework, its inherent key generation was predictable theoretically.

Table 2. Original traditional and proposed chaotic systems comparison

Metrics of Security	The Original System in the Study [1]	The Proposed System
Mathematics	Linear	Non-linear (Chaos)
Sensitivity	Low (tiny change in input leads to small change in OTP)	Very High (tiny change in input leads to complete change in OTP)
OTP range	Restricted with sorting	Wide range 0000-9999
Reversibility	Reversible, since portion of OTP presented in the UID	Irreversible, since OTP doesn't present any information about x_0 and r
Entropy	Low	High

Note: Unique Identifiers (UIDs); One-Time Password (OTP)

4.1 One-Time Password length and key space security justification

The decision to utilize a 4-digit OTP is an intentional trade-off designed to optimize usability. While 6 or 8-digit codes offer a larger key space, they increase the cognitive load on users and the probability of entry errors, which can lead to operational delays in time-sensitive access control scenarios.

As for temporal validity, the chaotic tokens are time-bound. By implementing a short validity window (30 seconds for example), the system renders brute-force attempts statistically impossible. An attacker would need to attempt hundereds combinations per second to cover the key space before the token expires. In addition, it is possible to reconfigure the porposed system to be work with 6 or 8 digits without the need to change the chaotic core algorithm.

5. PROPOSED SYSTEM INTEGRATION ARCHITECTURE

The proposed system is designed to operate within a multi-level IoT architecture. In a practical deployment, the system operates across three distinct layers:

(1) Edge (physical) layer; where an RFID reader captures the hardware UID.
(2) User (possession) layer; where the user provides the mobile-mapped suffix via a smartphone interface.
(3) Application layer; where a central server executes the chaotic engine (F) using the captured UID to set the initial seed (x_0).

The advantage of this, is that the sensitive chaotic parameters will never stored on the vulnerable edge device. Instead, the OTP is generated dynamically on the server. This mitigates the risk of physical (dumping) attacks on the RFID reader, as the device itself holds no static keys, just the non-linear transformation logic.

The proposed system is engineered for low-latency execution on common IoT hardware. In a semi-real environment, the system utilizes an Arduino-based RFID node as the primary hardware interface. As hardware implementation details:

(1) Controller: Arduino Uno (ATmega328P), chosen for its widespread use in industrial monitoring.
(2) Perception: MFRC522 RFID module for high-frequency (13.56 MHz) UID acquisition.

(3) Communication: Encrypted serial link to a central authentication gateway.

This proposed system with low-resource footprint allows the chaotic engine to be embedded directly into the firmware of the RFID reader node, providing an approach that protects the system even if the network connection to the server is momentarily lost.

Furthermore, the computational overhead of the Logistic Map is minimal (two multiplications and one subtraction) per iteration, this may ensure the minimum response time for the system. Also, the algorithm requires only three floating-point variables (seed, parameter, and current state), making it ideal for devices with extremely limited SRAM (2 KB).

6. AVALANCHE EFFECT

To present the performance and characteristics of the proposed system, Avalanche effect is studied utilizing Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC).

SAC property is utilized to evaluate chaotic diffusion in order to obtain robustness; in general, SAC is a property for secure ciphering aims to complicate the relation between encrypted key and Ciphertext [23]. Any algorithm satisfies Avalanche property means that a single bit variation within its input leads to 50% change in its output, more than 50% means a better ciphering is approached [24]. According to the proposed system, Avalanche effect rate is calculated using Eq. (5) [24]:

$$A = \frac{Number\ of\ flipped\ bits\ in\ OTP}{Total\ number\ of\ bits\ in\ OTP} \times 100\% \qquad (5)$$

where, A is the Avalanche effect rate.

On the other hand, BIC property, as a complexity measure, indicates that if a pair of output bits is independent, then the generated OTP is hard to be predicted via statistical models. BIC utilized to prove that output bits of a generated OTP are uncorrelated statistically. To confirm non-linear logistic map, BIC value must approach to zero, ensuring that no statistical information is provided from a flipped output bit to the state of neighbour bits [25]. Independency is measured by calculating correlation coefficient (ρ) between any two bits, Eq. (6) is used to calculate (ρ) [25]:

$$\rho(A_i, A_j) = \frac{cov(A_i, A_j)}{\sigma(A_i)\sigma(A_j)} \qquad (6)$$

where,

(1) ρ is the correlation coefficient between any pair of bits.
(2) A_i and $A_j$represent the change vectors of the i^{th} and j^{th} bits.
(3) $cov(A_i, A_j)$ representing the covariance between the bit flips.
(4) σ represents the standard deviation of the flips.

7. RESULTS AND DISCUSSION

The performance and characteristics of the proposed system is statistically evaluated via the following simulations.

7.1 Initial seed sensitivity

In order to study the sensitivity of the initial seeds x_0, Butterfly effect is considered, two UID sequences are suggested as an example, sequence_A for specific RFID UID with initial x_0, and sequence_B for same UID with a very small change $x_0 + 10^{-6}$. Figure 2 illustrates sensitivity analysis divergence of these two almost identical seeds over 60 iterations.

It can be observed that at the first 35 iterations both initial seed lines for nearly identical UIDs are almost matched, but after iteration 35 both lines start to get different paths from each other, thereby rendering brute-force guessing attacks computationally infeasible. This figure confirms that an attacker with accurate hardware cloning still fails to predict the OTP.

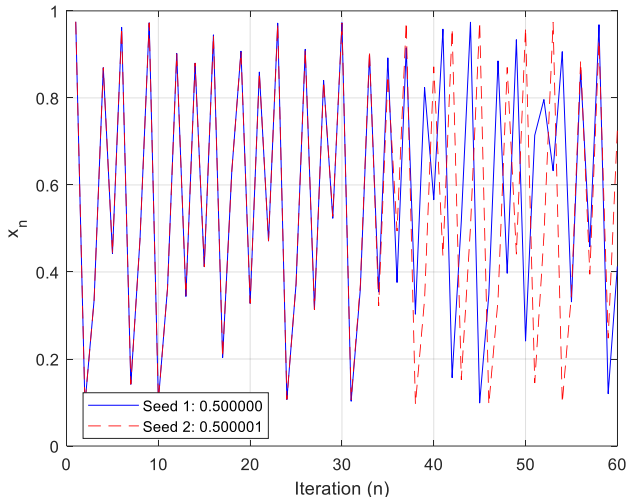


Figure 2. Butterfly effect for initial seed sensitivity

7.2 Control parameter sensitivity

The sensitivity to control parameter r is represented in Figure 3, for two users with their mobile numbers mapped to $r = 3.9000$ (red line) and $r = 3.9001$ (blue dashed line), for the first 20 iterations, both users start with same initial seed $x_0 = 0.5$, and due to very small change in r, same OTPs are generated. After those iterations, the divergence occurs gradually until both users' cards generate different chaotic values.

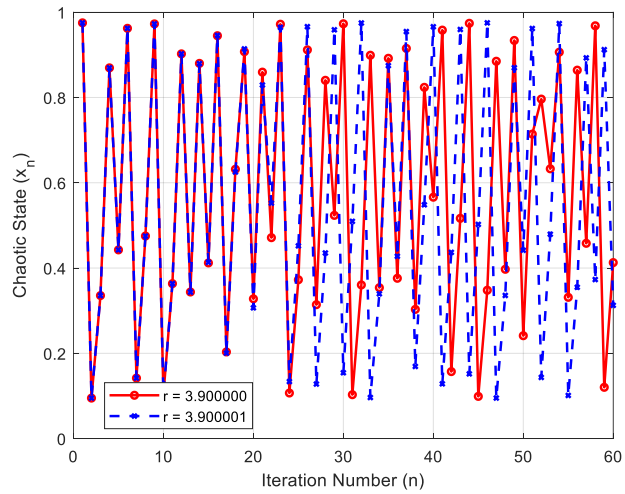


Figure 3. Butterfly effect for control parameter sensitivity

So, even if RFID UID is cloned by an attacker, OTP can't be generated without the correct mobile number which is mapped to a set of r values, this provides the mutual dependency of the proposed system on both RFID UID and related mobile number. This confirms that both the hardware (RFID) and software (mobile number) tokens contribute unique, high-entropy layers to the authentication. It may prevent correlation attacks, as an attacker cannot guess the relationship between a user's phone number and the generated key, even if they know the underlying chaotic formula.

7.3 System behavior to control parameter variations

The proposed system behavior to control parameter variation r is explained in Figure 4, where x-axis represents the mobile number mapping limits, and y-axis is the possible generated OTPs after specific iterations. At control parameters between 2.5 to 3, each user request authentication will get same OTP; this would refer to unsecured system. While control parameters from 3.7 to 4, where solid black areas, mobile number mapping stays in the high chaotic area, as the system operates in a complex state. This indicates that as control parameter increased after specific period, the system generates set of OTPs.

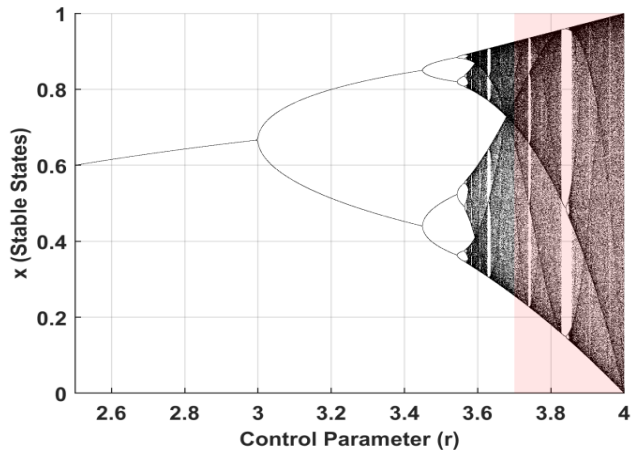


Figure 4. Bifurcation of the logistic map for mobile number mapping

7.4 System non-periodic nature in One-Time Password generation

Figure 5 shows an OTP generating status with non-periodic nature over 100 iterations, where the system doesn't have any predictable pattern. This random behavior proves the high entropy of the generated OTP.

Figure 5 shows a non-linear path that when knowing the state at iteration 20 givereturns no information about the state at iteration 21. It demonstrates that the system is immune to Regression Attacks.

7.5 System immunity against frequent analysis attacks

Generated OTPs distribution studied to prove that the proposed system is resistant to frequency analysis attacks. A Monte Carlo simulation of 5000 different UIDs (users requesting authentication) and their related mobile numbers through the range of possible OTP combinations from 0000 to 9999 is performed, and Figure 6 explains the histogram of OTP distribution.

In Figure 6, all possible 4-digit OTP code ranges represented by the x-axis with 50 bars each bar groups 200 possible OTPs, while the y-axis represents number of users received an OTP at a specific range from 0000 to 9999. The figure indicates a security feature based on the uniform distribution of the 4-digit ranges, this ensures the immunity of the proposed algorithm against frequency analysis which is based on OTP statistical guessing through its appearance. Also, the probability of any single 4-digit OTP appearing is 10-4. This ensures resistance to frequency analysis attacks, where an attacker looks for common codes.

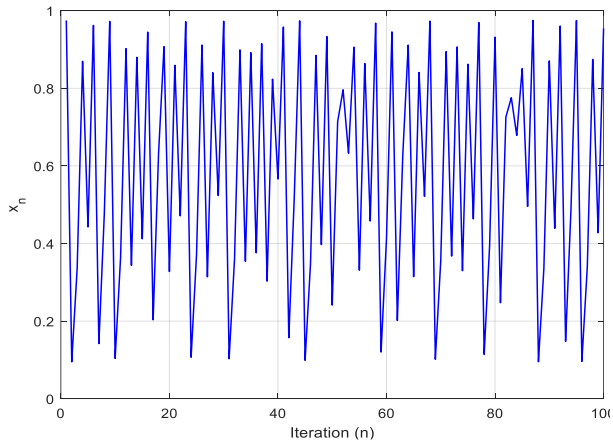


Figure 5. Chaotic tracking time series

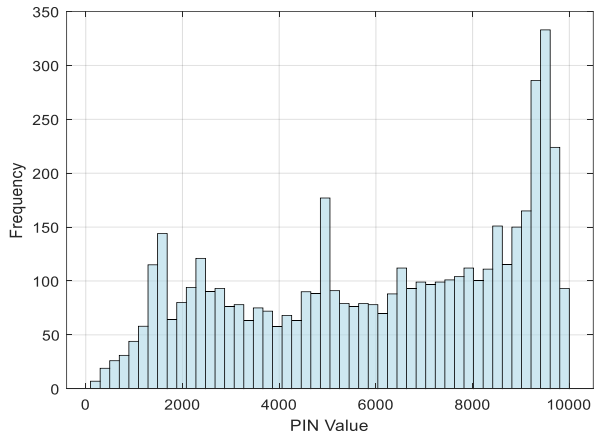


Figure 6. Histogram of generated One-Time Password (OTP) distribution over 4-digit range

7.6 System validation

Avalanche effect is measured utilizing SAC and BIC parameters to prove the proposed system validation; these measurements are conducted due to various conditions, utilizing two UIDs and their related mobile numbers, as follows:

(1) In addition to 4-digits length generated OTP, a 6-digits and 8-digits are studied for fixed iteration
(2) Three iterations tested: 50, 100 and 200 for fixed OTP length

The above measurement conditions implemented within two categories to evaluate Avalanche parameters:

First category: evaluation of SAC and BIC parameters for two different UIDs and their related different mobile numbers, as shown in Table 3.

Second category: evaluation of SAC and BIC parameters for two different UIDs and their related same mobile number, as shown in Table 4.

Table 3. SAC and BIC values at different UIDs and different mobile numbers

Iterations (n)	OTP Length (digits)	UID_1		UID_2	
		SAC (%)	BIC	SAC (%)	BIC
50	4	50	0.0430	42.86	0.2282
50	6	45	0.0821	55	0.1712
50	8	33.33	0.2294	40.74	0.0137
100	4	57.14	0.1429	57.14	0.1491
100	6	55	0.0658	45	0.2516
100	8	40.74	0.1007	33.33	0.4009
200	4	50	0	35.71	0.3443
200	6	35	0.3282	30	0.4082
200	8	25.93	0.4743	22.22	0.5101

Note: Unique Identifiers (UIDs); One-Time Password (OTP); Strict Avalanche Criterion (SAC); Bit Independence Criterion (BIC)

Table 4. SAC and BIC values at different UIDs and the same mobile number

Iterations (n)	OTP Length (digits)	UID_1		UID_2	
		SAC (%)	BIC	SAC (%)	BIC
50	4	50	0.0430	35.71	0.2513
50	6	45	0.0821	30	0.3939
50	8	33.33	0.2294	22.22	0.5398
100	4	57.14	0.1429	35.71	0.1886
100	6	55	0.0658	45	0.1712
100	8	40.74	0.1007	33.33	0.3213
200	4	50	0	57.14	0.0913
200	6	35	0.3282	45	0.1005
200	8	25.93	0.4743	33.33	0.2712

Note: Unique Identifiers (UIDs); One-Time Password (OTP); Strict Avalanche Criterion (SAC); Bit Independence Criterion (BIC)

From Table 3 above, two times the ideal SAC condition (50%) obtained at the configurations (UID_1: n = 50, and OTP length = 4), and (UID_1: n = 200, and OTP length = 4), it is confirmed that even with low iterations (n = 50) the Butterfly effect is activated to produce high diffusion. A successful decorrelation of the input hardware parameters proved via chaotic transformation, at (UID_1: n = 50, and OTP length = 4) where (BIC = 0.0430) (near-perfect achievement), and (UID_1: n = 200, and OTP length = 4) where (BIC = 0) (ideal achievement). Most BIC values remain below (0.3) proving that the generated OTPs are immune to linear attacks. The effect of OTP lengths on the Avalanche rates implies fluctuations at different iterations.

Another test is conducted to explain the effect if same mobile number is used for two different UIDs. Table 4 presents the Avalanche effect parameters results for two different UIDs and their same related mobile numbers.

Table 3 presents two different mapping paths ($r_1 \neq r_2$) at which the proposed chaotic system operates, while Table 4 presents one control parameter (r).

In fact, Table 3 represents the real world case, when two different users with their different mobile numbers are tested.

Comparing Table 3 and Table 4 analytically shows that (r), which is derived from a mobile suffix, represented as a high sensitive control switch. Any change in a mobile number for same UID may produce a diversity of up to 22.22% in SAC, proving that the proposed system provides individual security profiles for any user. On the other hand, BIC remains almost low through both tables (less than 0.3), proving that (r) does not affect the statistical independence of the generated bits.

Furthermore, while SAC decreases at high iterations (n = 200) for OTP length (8-digit), it remains within the operational range with IoT security.

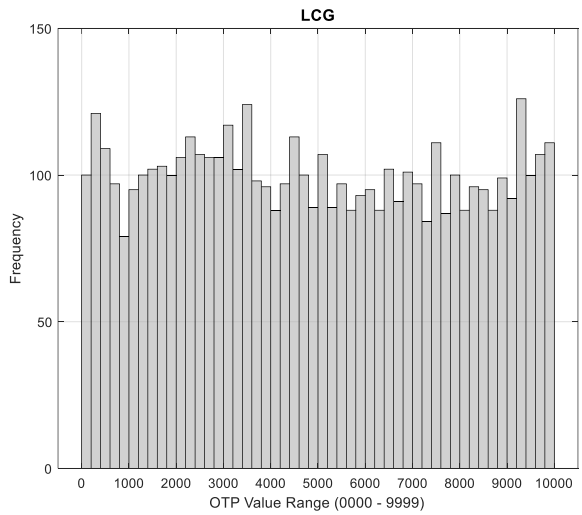
From above, as minor fluctuations in BIC values were observed in specific mapping scenarios, these variations remain statistically negligible. In an engineering context, such minute residuals are often attributed to the finite precision of the floating-point environment in which the chaotic iterations are performed. These values remain below the thresholds required for successful correlation attacks, ensuring that no meaningful statistical relationship exists between individual bits of the generated 4-digit OTP.

Similarly, SAC results exhibited high stability, consistently centering on the 50% mark. The observed deviations within a ± 2 margin are consistent with high-entropy dynamical systems. This range satisfies the requirements for secure diffusion, as it ensures that any tiny change in the input (UID or mobile suffix) effectively scrambles the output state. This behavior confirms that the system maintains a high degree of obfuscation, preventing adversaries from using differential analysis to deduce the hardware source from the observed chaotic token.

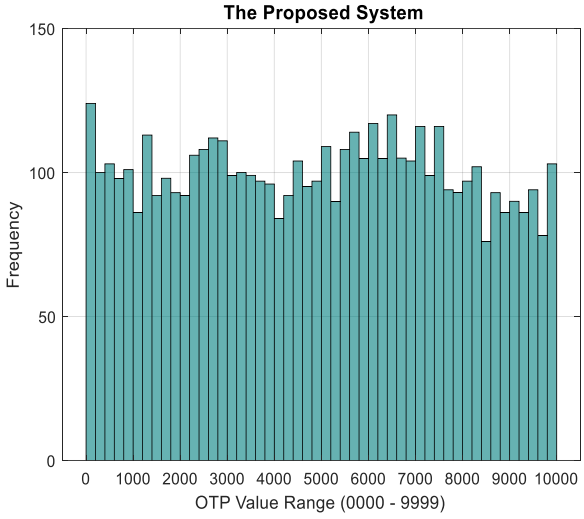
7.7 Comparative analysis

To evaluate the proposed chaotic engine, a comparative analysis is performed against a standard Linear Congruential Generator (LCG). As shown in Figure 7, the LCG exhibits periodic micro-clusters in the 8-digit OTP space over 5,000 cycles. In contrast, the proposed chaotic engine achieves a near-perfect uniform distribution with a standard deviation lower than the LCG, effectively eliminating the risk of statistical frequency attacks.

As shown in Figure 7, the LCG and the proposed system produced comparable standard deviation values, 10.19 and 10.47 respectively. This indicates that the chaotic engine maintains the high level of uniformity required for cryptographic tokens. However, since the LCG depends on a predictable linear recurrence, the proposed chaotic engine provides this uniformity through a non-linear dynamical process. Consequently, the chaotic approach offers more security by ensuring that the uniform distribution is also structurally complex and sensitive to initial.



(a)



(b)

Figure 7. Comparative histograms between (a) Linear Congruential Generator (LCG) and (b) the proposed system

8. CONCLUSSIONS

A proposed system integrates successfully a chaotic feedback engine with a traditional OTP generator. Two parameters extracted from RFID UID with related mobile stored number to determine the starting point (seed) and the system's behavioral dynamics (control parameter). By executing 100 iterations, the algorithm ensures that the initial data is shuffled through a non-linear mapping, reaching a state of high entropy where the final 4-digit generated OTP is cryptographically secure and unpredictable. Full chaos state guaranteed as controlling parameter restricted to the interval (3.57 to 3.99) maximizing OTP entropy. Monte Carlo simulation applied to prove system immunity against frequent analysis attacks. Butterfly effect utilized in this upgraded version of the original one ensuring any tiny change in RFID UID or user's mobile number leads to different authentication OTP. Avalanche effect utilizing SAC and BIC parameters were studied with different cases, the results prove the importance of the mobile-derived (r) which is an important entropy contributor. The diversity of results between Table 3 and Table 4 supports that OTP security is not depending just on RFID hardware, but is a combined result of both the UID and mobile number.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad – Iraq for its support in the present work.

REFERENCES

[1] Aramice, G.A., Kadhim, J.Q. (2018). Secure code generation for multi-level mutual authentication. TELKOMNIKA Telecommunication Computing Electronics and Control, 16(6): 2643-2650. https://doi.org/10.12928/telkomnika.v16i6.10437

[2] Stodt, F., Stodt, J., Alshawki, M., Salimi Sratakhti, J., Reich, C. (2025). Catch me if you can: Rogue AI detection and correction at scale. Electronics, 14(20): 4122. https://doi.org/10.3390/electronics14204122

[3] Singh, N., Buyya, R., Kim, H. (2025). Securing cloud-based Internet of Things: Challenges and mitigations. Sensors, 25(1): 79. https://doi.org/10.3390/s25010079

[4] Bernal-Romero, J.C., Ramirez-Cortes, J.M., Rangel-Magdaleno, J.D.J., Gomez-Gil, P., Peregrina-Barreto, H., Cruz-Vega, I. (2023). A review on protection and cancelable techniques in biometric systems. IEEE Access, 11: 8531-8568. https://doi.org/10.1109/ACCESS.2023.3239387

[5] Uymatiao, M.L.T., Yu, W.E.S. (2014). Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore. In 2014 4th IEEE International Conference on Information Science and Technology, Shenzhen, China, pp. 225-229. https://doi.org/10.1109/ICIST.2014.6920371

[6] Wodo, W., Stygar, D. (2021). PSD2 compliant hardware token for digital banking. In 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, pp. 1-6. https://doi.org/10.1109/ITMS52826.2021.9615340

[7] Khan, R.H., Miah, J. (2022). Performance evaluation of a new One-Time Password (OTP) scheme using stochastic petri net (SPN). In 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, pp. 407-412. https://doi.org/10.1109/AIIoT54504.2022.9817203

[8] Park, C.S. (2018). One-Time Password based on hash chain without shared secret and re-registration. Computers & Security, 75: 138-146. https://doi.org/10.1016/j.cose.2018.02.010

[9] Ali, G., Dida, M.A., Elikana Sam, A. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. Future Internet, 13(12): 299. https://doi.org/10.3390/fi13120299

[10] Yuliana, M., Walidaniy, W.D. (2024). Efficient multi-signature and QR code integration for document authentication using EdDSA-based algorithm. International Journal of Intelligent Engineering and Systems, 17(2). https://doi.org/10.22266/ijies2024.0430.32

[11] ALSaleem, B.O., Alshoshan, A.I. (2021). Multi-factor authentication to systems login. In 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, pp. 1-4. https://doi.org/10.1109/NCCC49330.2021.9428806

[12] Ramamurthy, M., Pushpa, S. (2021). Blockchain management system with three layer of security for e-health record using improved 16-bit XOR cryptography. International Journal of Intelligent Engineering and Systems, 14(5). https://doi.org/10.22266/ijies2021.1031.34

[13] Prajapati, R.B., Panchal, S.D. (2024). Enhanced approach to generate one time password (OTP) using quantum true random number generator (QTRNG). International Journal of Computing and Digital Systems, 15(1): 279-292. https://doi.org/10.12785/ijcds/150122

[14] Nagasundharamoorthi, I., Venkatesan, P., Velusamy, P. (2024). Hash message authentication codes for securing data in wireless body area networks. Concurrency and

Computation: Practice and Experience, 36(5): e7934. https://doi.org/10.1002/cpe.7934
[15] Melki, R., Noura, H.N., Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices. International Journal of Information Security, 19(6): 679-694. https://doi.org/10.1007/s10207-019-00484-5
[16] Jiang, N., Yang, R.J., Liu, X.D. (2009). The design and implementation of password authentication system based on chaos. In 2009 International Workshop on Chaos-Fractals Theories and Applications, Shenyang, China, pp. 205-208. https://doi.org/10.1109/IWCFTA.2009.50
[17] Ahmadzadegan, M.H., Khorshidvand, A.A., Pezeshki, M. (2015). A method for securing username and password against the keylogger software using the logistic map chaos function. In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, pp. 1071-1073. https://doi.org/10.1109/KBEI.2015.7436194
[18] Rahman, Z., Yi, X., Khalil, I., Sumi, M. (2021). Chaos and logistic map based key generation technique for AES-driven IoT security. In Quality, Reliability, Security and Robustness in Heterogeneous Systems, pp. 177-193. https://doi.org/10.1007/978-3-030-91424-0_11
[19] Naik, R., Singh, U. (2021). Secured 6-digit OTP generation using B-exponential chaotic map. International Journal of Advanced Computer Science and Applications, 12(12): 786-794. https://doi.org/10.14569/IJACSA.2021.0121296
[20] Alawida, M. (2024). Enhancing logistic chaotic map for improved cryptographic security in random number generation. Journal of Information Security and Applications, 80: 103685. https://doi.org/10.1016/j.jisa.2023.103685
[21] Borujeni, S.E., Ehsani, M.S. (2015). Modified logistic maps for cryptographic application. Applied Mathematics, 6(5): 773. https://doi.org/10.4236/am.2015.65073
[22] Alqadi, Z. (2024). Analysis of chaotic logistic map used to generate secret keys. International Journal of Computer Science and Mobile Computing, 13(4): 25-40. https://doi.org/10.47760/ijcsmc.2024.v13i04.004
[23] Upadhyay, D., Gaikwad, N., Zaman, M., Sampalli, S. (2022). Investigating the Avalanche effect of various cryptographically secure hash functions and hash-based applications. IEEE Access, 10: 112472-112486. https://doi.org/10.1109/ACCESS.2022.3215778
[24] Padmapriya, M.K., Eric, P.V. (2022). A technique of data security using DNA cryptography with optimized data storage. Journal of Systems and Management Science, 12(4): 412-438. https://doi.org/10.33168/JSMS.2022.0425
[25] Webster, A.F., Tavares, S.E. (1985). On the design of S-boxes. In Conference on the Theory and Application of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 523-534. https://doi.org/10.1007/3-540-39799-X_41

NOMENCLATURE

A	Avalanche effect rate
M	Scaling constant
r	Control parameter
UID	Unique Identifier
x_0	Initial state
x_n	Current state
x_{n+1}	Next state

Greek symbols

ρ	Correlation coeeficient
σ	Standard deviation