Integrating Policy-Based Access Control with Chaotic Cryptography for Enhanced Security

Prakash Hongal[1] and Dr. Parashuram Baraki[2]
[1]*Asst. Professor, Department of CSE(AI&ML), SKSVMACET,*
Lakshmeshwar, Karnataka, INDIA
hongalpj@gmail.com / prakash.cse@agadiengcollege.com
[2] *Professor, Department of Computer Engineering, SKSVMACET,*
Lakshmeshwar, Karnataka, INDIA
parashuram.baraki@gmail.com

***Abstract*: These Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The important characteristics of chaos are its extreme sensitivity to initial conditions of the system. The policy-based cryptography allows performing of the policy enforcement while respecting the data minimization principle. Such 'privacy-aware' policy enforcement is enabled by two cryptographic primitives: policy-based encryption and policy-based signature.**

Keywords: Hybrid Cryptography, Chaotic Functions, Rule Based, Policy Based Cryptography.

I. INTRODUCTION

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the current era of information technology and proliferating computer network communications, cryptography has a special importance. Cryptography is routinely used not only to protect the data but also provides the protocols for secure communication [1], [2], [4].

A. Chaos Cryptography

The core of digital chaos-based cryptography is the selection of a good chaotic map for a given encryption scheme [1],[5],[6]. Actually, the presence of chaos does not guarantee the security of an encryption algorithm. A good digital cryptosystem based on chaos should not be just the concomitance of a chaotic map and encryption architecture, but the result of their synergic association. Indeed, the quality of a chaotic map for cryptography must be evaluated not just with considerations on its dynamic properties, but also with considerations on the needs of the sustaining encryption architecture [3][8].

There are some interesting relationship between chaos and cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems [17].

TABLE I. COMPARISON OF CHAOTIC AND CRYPTOGRAPHIC PROPERTY

Chaotic property	**Cryptographic property**	**Description**
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions/ control parameter	Diffusion with a small change in the plaintext/secret key	A small deviation in the input can cause a large change at the output
Mixing property	Diffusion with a small change in one plain-block of the whole plaintext	A small deviation in the local area can cause a large change in the whole space
Deterministic dynamics	Deterministic pseudo-random	A deterministic process can cause a random-like (pseudo-random) behaviour
Structure complexity	Algorithm(attack) complexity	A simple process has a very high complexity

The typical features of chaos include:

• **Nonlinearity**: If it is linear, it cannot be chaotic.

• **Determinism:** It has deterministic (rather than probabilistic) underlying rules every future

state of the system must follow.

• **Sensitivity to initial conditions**: Small changes in its initial state can lead to radically different behavior in its final state. This "butterfly effect" allows the possibility that even the slight perturbation of a butterfly flapping its wings can dramatically affect whether sunny or cloudy skies will predominate days later.

• **Sustained irregularity in the behaviour of the system:** Hidden order including a large or infinite number of unstable periodic patterns (or motions). This hidden order forms the infrastructure of irregular chaotic systems---order in disorder for short.

• **Long-term prediction:** (but not control!) is mostly impossible due to sensitivity to initial conditions, which can be known only to a finite degree of precision [3]-[7],[9]-[12].

PROBLEMS WITH THE SELECTION OF THE CHAOTIC SYSTEM

Problem 1. Definition of the key leading to nonchaotic behavior.

Problem 2. Non uniform probability distribution function.

Problem 3. Return map reconstruction.

Problem 4. Bad definition of the ciphertext.

Problem 5. Efficiency of the cryptosystem depending on the value of the key.

B. Policy Based Cryptography

The concept of Policy Based Cryptography allows performing cryptographic operations with respect to policies formalized as monotone boolean expressions. Such operations have interesting applications in encryption-based and proof-based authorization systems as well as in trust establishment and negotiation [8], [18].

The concept of policy-based cryptography (PBC), recently formalized in the literature, appears as a promising paradigm for the enforcement of trust establishment and authorization policies. It allows performing cryptographic operations with respect to policies formalized as monotone Boolean expressions. In PBC, a policy involves conjunctions and disjunctions of conditions, where each condition is associated to a specific credential issued by a trusted authority [18]. An entity fulfils a policy if and only if it has access to a set of credentials associated to the logical combination of conditions defined by the policy. Intuitively, a policy-based encryption scheme (PBE) allows encrypting a message according to a policy so that only entities fulfilling the policy are able to perform the decryption of the message. Symmetrically, a policy-based signature scheme (PBS) assures that only entities fulfilling a given policy are able to generate a valid signature according to the policy [19], [20].

II. DESIGN AND IMPLEMENTATIONS

A. The Proposed Policy based Chaotic System

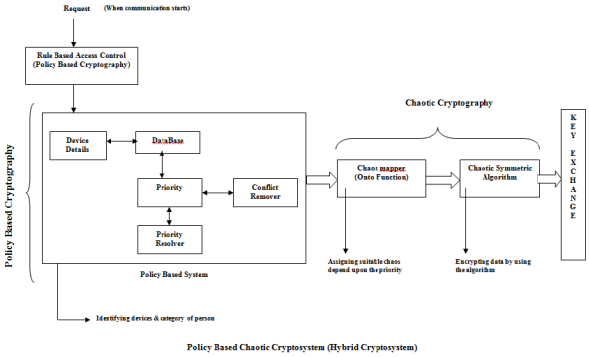

Fig. 1. Policy Based Chaotic Cryptosystem (Hybrid Cryptosystem)

1) Role Based Access Control

Here access permissions are based on the role(s) a subject is performing better scalability and ease of use. Rules are defined in the proposed systems are:

Rule 1: Mapping of the role with the corporate policy based on the device details. Hence

allot the function and the initial condition.

Rule 2: Check the destination details and decide the chaotic function to be used to be used

also decide the currently unused initial condition.

Rule 3: Decide the protocol that will be used for that communication.

Rule 4: In case of conflicts suspend or change the initial conditions.

2) Device Details

A device details includes the following information: machine name, organization/company, location of machine (city, state, and country), time frame, configuration, etc.

Database: Contain the Users information in the organization like employee id, position of the employee, category of the employee, etc.

Priority: Priority that includes priority numbers of employees in the organization. With respect to their category it is useful in generating the chaos functions to make their communication more secure.

Priority Resolver: A partial order relationship established between the employees in the organization. When communication is takes longer time between the employees that moment it checks the priority of the employees and by changing the initial condition of the function it generates some more X_{n+1} values for communication.

Conflict Remover: When the conflict occurs in the communication it will consider that one as a crisis, for that crisis it will have some chaos function for that communication. The some reasons for conflict are:

i) If communication takes longer time it changes the initial condition of the function or it takes chaos function from the crisis category.

ii) If some other employee of same category want to communicate with same category or different category employee that time chaos function can be taken out from the crisis category.

Chaos Mapper: Mapping between employees priority number and chaos function are carried out the in the chaos mapper. With respect to the category of the employee and their priority number chaos functions are mapped and they are used for communication purpose.

Chaotic Symmetric Algorithm: By making use of chaos function from chaos mapper it uses symmetric algorithm (AES) to encrypt or decrypt the messages in the communication. It makes communication more secure and prevents attacks from the eavesdroppers.

Chaos Mapper: By considering only three hierarchies are in communication channel. In this proposed work by considering that

i) **C1P1 or C1P2** – Category 1 person(s) from communication party 1(2) (high level people like Vice President of the Company or Manger or Principal of the College or Dean or Head of Department).

ii) **C2P1 or C2P2** – Category 2 person(s) from communication party 1(2) (middle level people like Programmer of the Company or Team Lead or Lecturer or Clerk).

iii) **C3P1 or C3P2** – Category 3 person(s) from communication party 1(2) (low level people like System Analyst of the Company or Supporting Staff or Attender).

TABLE II. CHAOS MAPPER TABLE WITH RANGE OF CHAOTISM AND REMARKS

Sr No.	Communicating parties	Function(s) used	Range of Chaotism	Remarks (why)
1.	C1P1,C1P2	The H´enon Map , Arnold Map	Initial values Xo=0.100000, Yo=0.200000 (Initial Conditions are itself behaves as a secret key)	With different initial values there is drastic change in the values. Here communication is must be very secure so by making use of Y_{n+1} both parties will authenticate each other.
2.	C1P1,C2P2	Two Coupled Logistic Map, Lorenz Equation	Initial condition Xo=0.234590, Y_0=0.546750 (Initial Conditions are itself behaves as a secret key)	With different initial values there is drastic change in the values. Here communication is must be very secure so by making use of Y_{n+1} both parties will authenticate each other.
3.	C1P1,C3P2	Tripled Chaotic Maps	Initial Conditions are Xo=0.100000, alpha=0.455000	With little change in the secret key values, will get the different values so that it becomes very difficult for eavesdropper to break the cipher text.
4.	C2P1,C2P2	Simple Logistic Function	with r > 3.6 falls into chaotic region.(Initial Conditions are itself behaves as a secret key)	Generated values are large.
5.	C2P1,C3P2	Quadratic Map	Initial Conditions are Xo=0.110000 (parameter C is a secret key)	With little change in the secret key values, will get the different values so that it becomes very difficult for eavesdropper to break the cipher text.
6.	C3P1,C3P2	Threshold Function	Initial Conditions are Xo=0.100100	High level security is not needed.
7.	Crisis	Tent Map	initial value of X=0.100000 and alpha=0.600000 (alpha is a secret key)	When the system is at risk state.

B. Process Flow of the Propose system (PFP):

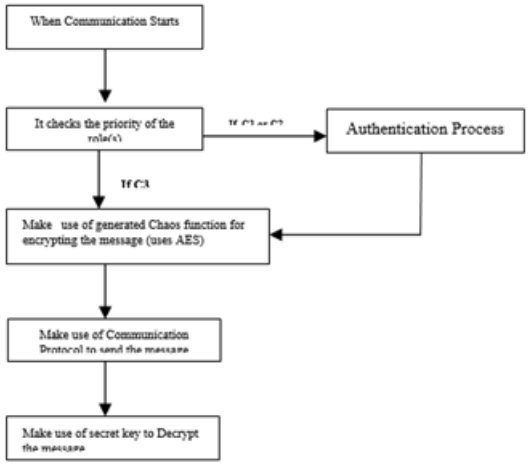

Fig. 2. Process Flow of the propose System (PFP)

C. Algorithms

1) Encryption Algorithm

Our Encryption algorithm can be seen as a kind of extension or generalization of the both Chaotic and Policy Based Cryptography. Here policies are generalized into the rules. Encryption algorithm as follows

Given message M, and rule do the following

1. Pick the chaos function with respect to the priority of the user.
2. Initial condition of the chaos function itself behaves as a secret key and that known to both the parties.
3. Compute the Cipher text by making use of S box values (by using AES algorithms).
4. Send the Cipher text to the another communication party.

2) Decryption Algorithm

Decryption algorithm is a reverse procedure of Encryption.

III. RESULT AND ANALYSIS

The listed chaotic functions are tested and taken out their values for S-box for encryption purpose and all the functions are tested according to their initial condition behaviour and chaotic nature.

A. Simple Logistic Function(SLF)

The SLF defines a discrete chaotic dynamical system by iteration as follows

$$x_{n+1} = r^{*}x_n{}^{*}(1 - x_n) \quad (1)$$

for n = 0, 1, ... it is the **SLF-based iteration**, where x0 ∈ [0, 1] is an initial value for the iteration (1) r ∈ [0, 4] is the parameter of (1). The equation (1) is a chaotic dynamical system. Before r = 3.45, this dynamical system simply shows a one-periodic attractor. Successive doublings of the period quickly occur in the approximation range 3.55 < r < 3.6.

1) When initial Condition $X_0 = 0.100000$

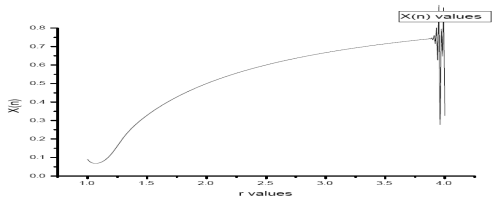

Fig. 3. Analysis of Simple Logistic Map initial Condition X0 = 0.100000

2) When Initial Condition is Xo=0.2

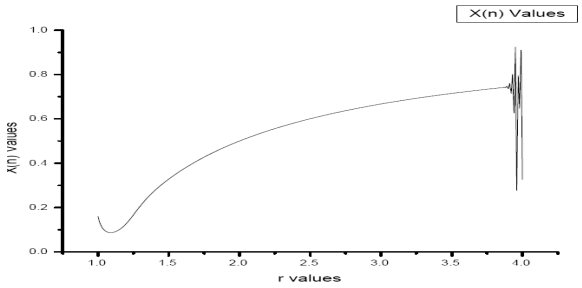

Fig. 4. Analysis of Simple Logistic Map initial Condition X0 = 0.200000

This function used for communication between the C2P1 and C2P2 because by changing the initial value it generates the different set of values for S box these values are chaos in nature. These values are unpredictable.

B. Tent Map

A tent map is one of the most popular and the simplest chaotic maps. Encryption and decryption function are described as follows

$$\mathbf{F:}\begin{cases} X_{k+1} = X_k / \alpha & (0 \le X_k \le \alpha) \\ X_{k+1} = X_k - 1 / \alpha - 1 & (\alpha \le X_k \le 1) \end{cases} \quad (2)$$

$$\mathbf{F^{-1}:}\begin{cases} X_k = \alpha X_{k+1} \\ X_k = (\alpha - 1) * X_k + 1 \end{cases} \quad (3)$$

Equation 2&3 show the tent map and the inverse map. These maps tranform an interval [0, 1] into itself and contain only one parameter α , which presents the location of the top of the tent. F is two to one map and F−1 is one to two map.

1) When initial value of X=0.100000 and alpha=0.600000

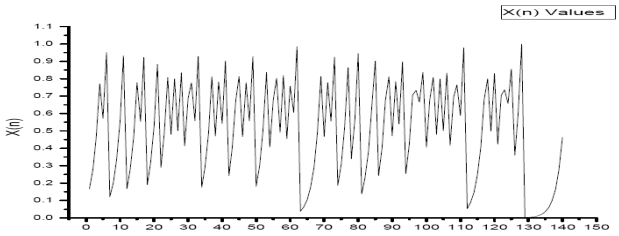

Fig. 5. Analysis of Tent Map initial Condition X=0.100000 and alpha=0.600000

2) When initial value of X=0.100000 and alpha=0.500000

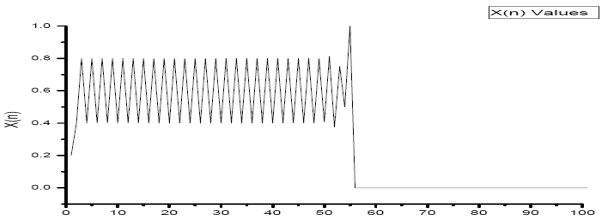

Fig. 6. Analysis of Tent Map initial Condition X=0.100000 and alpha=0.500000

3) When initial value of X=0.100100 and alpha=0.444400

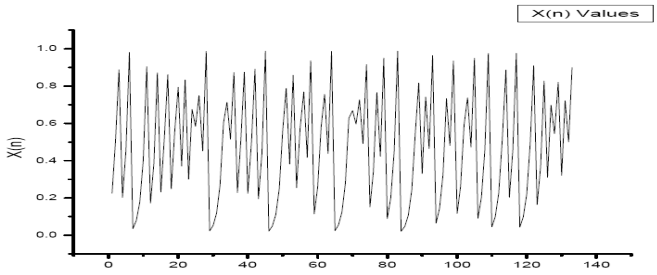

Fig. 7. Analysis of Tent Map initial Condition X=0.100100 and alpha=0.444400

This function used for communication, when there is crisis in the system. By changing the fifth or sixth decimal position values initial condition it generates the different set of values for a S box. Those values are large in numbers so it makes communication smooth and secure.

C. Lorenz Equation

The Lorenz equation has the simple form

$$\begin{aligned} X_{n+1} &= a(X_n + Y_n) \\ Y_{n+1} &= rX_n - Y_n - X_nZ_n \\ Z_{n+1} &= -bZ_n + X_nY_n \end{aligned} \quad (4)$$

Where a, r, and b are three positive parameters. We now know that the Lorenz system is a continuous-time nonlinear dynamical system, which exhibits chaos within some special parameter regime. Where r, a, r, and b are constants. The equations have chaos when a = 10, r = 28, and b = 8/3.

TABLE III. XN+1 ,YN+1 AND ZN+1VALUES OF LORENZ EQUATION

112	**150.85**	**38.75**
621.5999	**616.3498**	**16740.2**
-84.0013	**-1E+07**	**316162.2**
-1.7E+08	**36932178**	**8.7E+08**
3.25E+09	**1.45E+17**	**-6.1E+15**
2.31E+18	**1.99E+25**	**4.69E+26**
3.19E+26	**-1.1E+45**	**4.61E+43**
-1.7E+46	**-1.5E+70**	**-3.5E+71**
-2.3E+71	**-6E+117**	**2.5E+116**
-1E+119	**6E+187**	**1.4E+189**

The Lorenz equation generates Xn+1, Yn+1, Zn+1 values, all values are depend upon the initial values of Xn, Yn, and Zn. These values all not predictable until all three equations, constant values and initial conditions are known. So these values are used when there is a more secure communication is there so for that in our proposed work we using these values when there is a communication between C1P1 and C2P2.

D. Piecewise Linear Maps

The piecewise linear maps are the simplest kind of chaotic maps in practice (only several additions and one division are needed).

$$F(X, p) = \begin{cases} X/p & X \in [0, p] \\ (1 - X) / (1 - p) & X \in [p, 1] \end{cases} \quad (5)$$

Another example is the chaotic map, which is also rather simple and a little more complex than the map above:

$$F(X, p) = \begin{cases} X/p & X \in [0, p] \\ (X - p) / (0.5 - p) & X \in [p, 0.5] \\ (1 - X) / (1 - p) & X \in [p, 1] \end{cases} \quad (6)$$

Based on such a chaotic map, the improved scheme can be described as follows:

- The secret key: K = (X0, p), where X0 is the initial condition of the chaotic map.
- The input – plaintext: p1, p2, … …. pi……., where the size of pi is bi ≤ bmax.

E. Tripled Chaotic Maps

We first review the one parameter families of trigonometric chaotic maps which are used to construct the tripled chaotic maps. One-parameter families of chaotic maps of the interval [0, 1] with an invariant measure can be defined as the ratio of polynomials of degree N:

$$\Phi^{(1,2)}{}_N(X, \alpha) = (\alpha^2 * F) / (1 + (\alpha^2 - 1) * F) \quad (7)$$

Where F substitute with chebyshev polynomial of type one TN(X) for Φ(1)N(X, α) and chebyshev polynomial of type two UN(X) for Φ(2)N(X, α). As an example we give below some of these maps:

$$\Phi^{(1)}{}_2 = (\alpha^2 * (2X-1)^2) / (4X(1-X) + \alpha^2(2X-1)^2) \quad (8)$$

$$\Phi^{(2)}{}_2 = (4\alpha^2 X(1-X)) / (1+4(\alpha^2 - 1) * X*(1-X)) \quad (9)$$

1) Initial Conditions are Xo=0.100000, alpha=0.455000

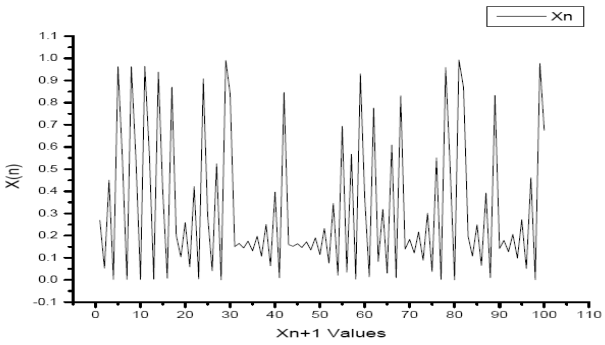

Fig. 8. Analysis of Tripled Chaotic Map initial condition Xo=0.100000, alpha=0.455000

2) Initial Conditions are Xo=0.100000, alpha=0.220000

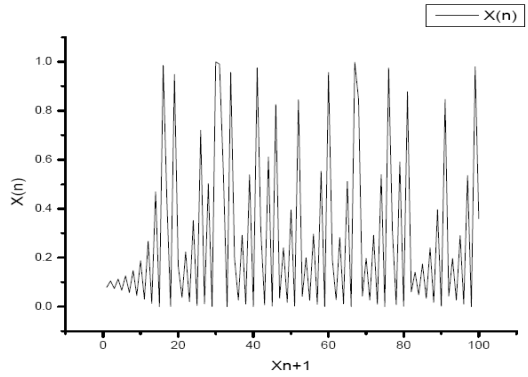

Fig. 9. Analysis of Tripled Chaotic Map initial condition Xo=0.100000, alpha=0.220000

3) Initial Conditions are Xo=0.900000, alpha=0.220000

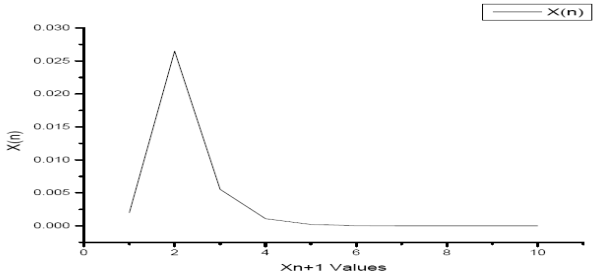

Fig. 10. Analysis of Tripled Chaotic Map initial condition Xo=0.900000, alpha=0.220000

There is always less communication between the C1 and C3 and that communication may or may not be strongly secured so for that these functions will help because these values are not so much chaos in nature compare to other functions.

F. Chaotic maps

Nonlinear and chaotic one-dimensional maps f : S→S, where S ⊂ R. The set S is S= [0, 1]. The one-dimensional dynamical system can be defined by a difference equation

$$Xk+1 = f(Xk) \qquad k=0,1,2,\ldots.. \qquad Xk \in S$$

The variable k stands for time. A dynamical system consists of a set of possible states, together with a deterministic rule, which means that the present state can be determined uniquely from the past states. The orbit of X under f is the set of points { X, f(X), f2(X),…, fn(X) }, where f2(X)= f (f (X)) and fn(X) means n times iterating of the function f(X). The starting point X for the orbit is called the initial value of the orbit. A chaotic orbit is one that forever continues to experience the unstable behavior that an orbit exhibits near a source, but that is not itself fixed or periodic.

The iterative relation of the tent map is

$$X_{k+1} = \begin{cases} X_k / p & \text{if } 0 \le X_k \le p \\ & \text{Where } X_k \in [0,1] \\ (1 - X_k) / (1 - p) & \text{if } p \le X_k \le 1 \end{cases} \quad (10)$$

Where X0 is the initial condition and p is the control parameter. The tent map is chaotic if p is in the range of (0, 1) and p≠0.5.

G. Quadratic Map

The quadratic map is defined as

$$Xn+1=Xn2+ C \qquad (11)$$

and its behaviour depends on parameter C. Most values of C beyond –1.45 left exhibit chaotic behaviours. When C is close to –2 the orbits Xn distribute within (–2, +2), i.e. Xn ∈ (-2, +2). We choose C between –1.9 to –2 for our set of quadratic maps.

1) Initial condition Xo = -1.000000

TABLE IV. XN+1 VALUES OF QUADRATIC MAP WITH INITIAL VALUE X0= -1.0

2	**8.361352**	**2.07E+29**
2.01	**67.9722**	**4.28E+58**
2.0601	**4618.291**	**1.8E+117**
2.274012	**21328606**	**3.4E+234**
3.211129	**4.55E+14**	

H. The H′enon Map

An N-dimensional discrete-time dynamical system is an iterative map

$$Xk+1 = f(Xk) \qquad (12)$$

where k = 0, 1, . . . is the discrete time and X ∈ N is the state. Starting from X0, the initial state, repeated iteration of (12) gives rise to a series of states known as an orbit.

An example is the H′enon map, a two dimensional discrete-time nonlinear dynamical system represented by the state equations.

$$Xk+1 = -\alpha X2k + Yk + 1 ,$$
$$Yk+1 = \beta Xk . \qquad (13)$$

Here, (X, Y) is the two-dimensional state of the system. The state-plane diagram for α = 1.4 and β = 0.3 for this map.

1) Initial conditions are Xo=0.100000, Yo=0.200000

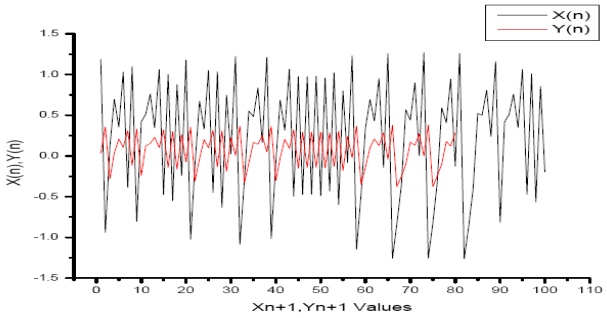

Fig. 11. Analysis of H'enon Map initial condition Xo=0.100000, Y0=0.200000

2) Initial conditions are Xo=0.200000, Yo=0.100000

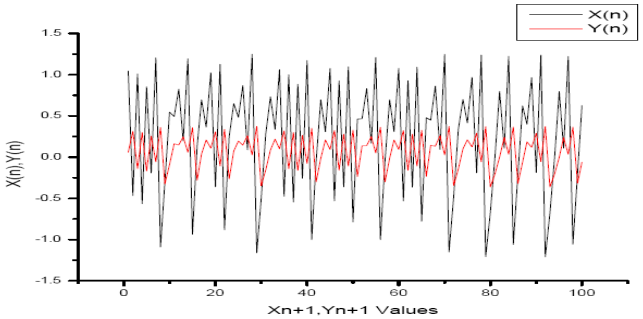

Fig. 12. Analysis of H'enon Map initial condition Xo=0.200000, Y0=0.100000

3) Initial conditions are Xo=0.100100, Yo=0.250000

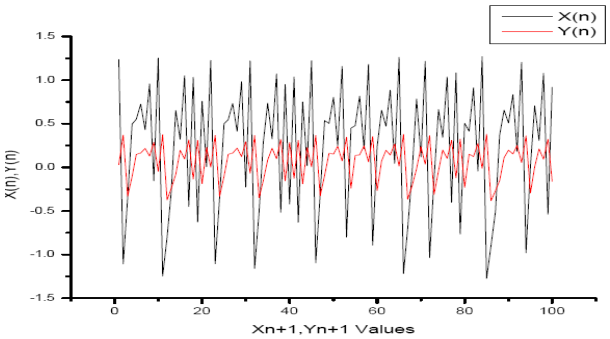

Fig. 13. Analysis of H'enon Map initial condition Xo=0.100100, Y0=0.250000

The H'enon map generates two set of values for X0 and Y0. Here in the proposed work Yn+1 it is used for authentication and Xn+1 values are for S box. The authentication is required when there is more secure channel is required for communication. By making use of H'enono

maps two set of different values are easily generated. So for that in the proposed work this function is used for when there is communication between C1 and C1.

I. Two Coupled Logistic Map

There are various functional forms of coupled Logistic equations are available

$$Xn+1 = (1- \epsilon) * f(\mu, Xn) + \epsilon * f(v, Yn)$$

$$Yn+1 = \epsilon * f(\mu, Xn) + (1- \epsilon) * f(v, Yn) \quad (14)$$

Where the map f is taken to be a one dimensional Logistic map with a strength parameter μ and

$$f(\mu, X) = \mu*X*(1-X)$$

$$f(\mu, Y) = v*Y*(1-Y)$$

Here the initial conditions X0, Y0 and parameter μ, v and € determine the dynamics of the system.

1) Initial Condition are Xo= 0.234590,Yo= 0.546750

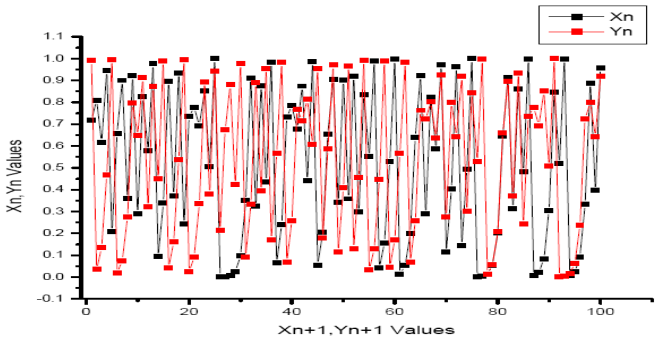

Fig. 14. Analysis of Two Coupled Logistic Equation initial condition Xo=0.234590, Y0=0.546750

2) Initial Condition are Xo= 0.234950,Yo= 0.546570

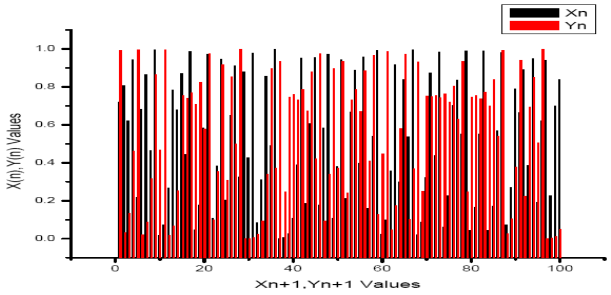

Fig. 15. Analysis of Two Coupled Logistic Equation initial condition Xo=0.234950, Y0=0.546570

The two coupled logistic equation generates Xn+1 and Yn+1 . One set of value can be used for authentication and one for S box or vice versa. Generated values are Chaotic in nature and make communication secure and strong. And also prevents the attack from the eavesdropper. So for that this function is used when there is communication between C1 and C2 in this proposed work.

J. Arnold Map

The beauty of this system is that it does not have any parameter. In fact, almost for any initial condition, the iterations of Arnold's map can quickly cover the available area of the phase space almost uniformly. In the literature, it is regarded as a strong mixing system. Here initial condition is only the secrete key. If an intruder crypt analyzes our messages, then we can use a different initial condition. Even if we change the last digit of our initial condition, we get a drastically different encrypted message for a given text. Arnold map is 2 dimensional map it is described as:

$$\mathbf{Xn+1 = Xn + Yn \ (mod\ 1)}$$

$$\mathbf{Yn+1 = Xn + 2\,Yn \ (mod\ 1)} \quad \mathbf{(15)}$$

Initial conditions are Xo= 0.234599 and Yo= 0.546756

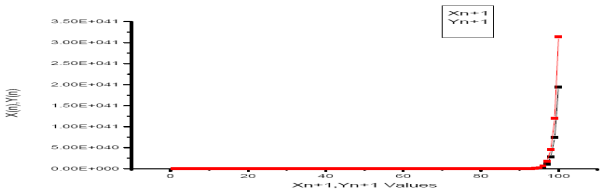

Fig. 16. Analysis of Arnold Function initial condition Xo=0.234599, Y0=0.546756

Arnold map generates the values randomly in a higher order growth. It makes system more secure and also prevents from third party attack. This function can be used when there is a more secure channel is required for communication.

K. Threshold Function

Generating the binary chaotic spreading sequences using logistic map is derived by quantizing the output of the map using the threshold function. These sequences possess truly noise-like autocorrelation properties and low cross correlations.

$$\mathbf{x_{k+1} = (1-2\,x_k^2)\,,} \qquad \mathbf{-1<x<1} \quad \mathbf{(16)}$$

1) Initial condition Xo=0.100100

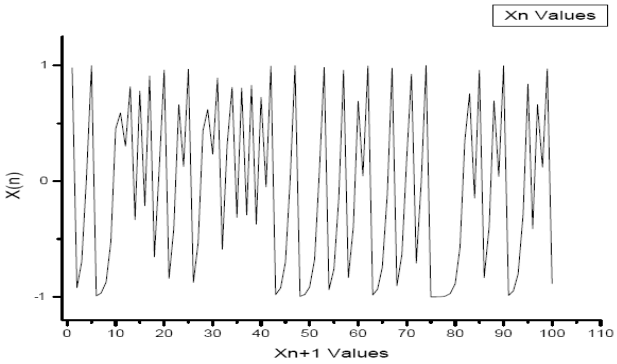

Fig. 17. Analysis of Threshold Function initial condition Xo=0.100100

2) Initial condition Xo=0.200000

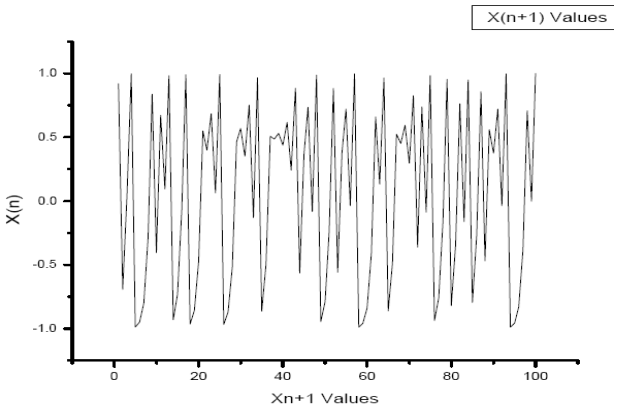

Fig. 18. Analysis of Threshold Function initial condition Xo=0.2

3) Initial condition Xo=0.900000

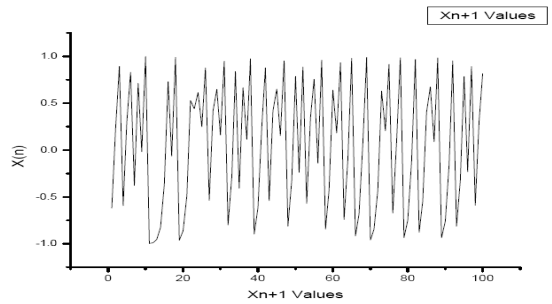

Fig. 19. Analysis of Threshold Function initial condition Xo=0.9

4) Initial condition Xo=0.950000

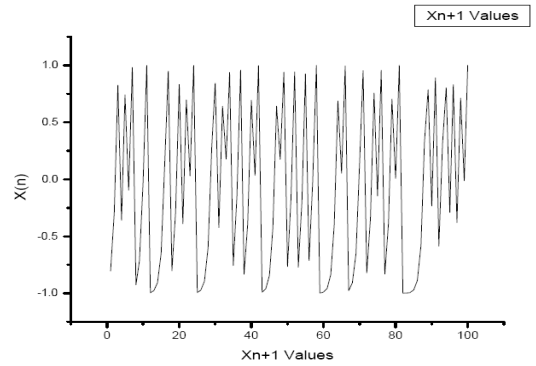

Fig. 20. Analysis of Threshold Function initial condition Xo=0.95

Threshold function generated large number of values for S box, but these values are less chaos in nature. When there is communication between C3 and C3 that time it doesn't required high level security but it required lot of values for S box, by changing the initial value of a function it generates the values in large number.

IV. CONCLUSIONS

The concept of PBC allows performing cryptographic operations with respect to policies formalized as monotone Boolean expressions. This merged with chaotic cryptography produced good results as discussed earlier

The design of the system is able to meet the following criterion

1. Behavior of the chaotic function which produces various values that are pseudo-random in nature and change in the initial condition will produce different role that can be used in policy based cryptography. This is able to solve the problem of scalability problem of key values in PBC.
2. The through study and modular testing of these chaotic functions is made for time criticalness. The policy based chaotic cryptography can produce better results as it integrates the commercial implement ability of policy based cryptography and less complex nature of chaotic function. This fusion is modularly tested in the project. It is crypt analyzed also.
3. Catetegory1 roles that are highly important have to be assigned The H′enon Map as it produces highest Chartism.
4. In the similar way the category 2 and 3 have to be assigned the function with different initial conditions. This work reduces and enhances the security and maintains the key management life cycle and avoids the conflicts while secure communication is on.
5. The system also is capable of continuing the work in case of threats also.

REFERENCES

[1] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," Mathematics, vol. 11, no. 11, p. 2585, 2023.

[2] Y. Sha, F. Bu, H. Jahanshahi, and L. Wang, "A Chaos-Based Image Encryption Scheme Using the Hamming Distance and DNA Sequence Operation," Frontiers in Physics, vol. 10, 2022.

[3] H. Zhang, W. Sun, and L. Lu, "Chaotic encryption algorithm with scrambling diffusion based on the Josephus cycle," Frontiers in Physics, vol. 11, 2023.

[4] B. Emin and Z. Musayev, "Chaos-based Image Encryption in Embedded Systems using Lorenz–Rossler System," Chaos Theory and Applications, vol. 5, no. 3, pp. 153–159, 2023.

[5] A. R. Mamat et al., "Color image encryption using chaotic-based cryptosystem," Mathematical Modeling and Computing, vol. 11, no. 3, pp. 883–892, 2024.

[6] X. Chen et al., "A novel chaotic map application in image encryption algorithm," Expert Systems with Applications, vol. 252, 2024.

[7] A. Alawida et al., "A novel chaos-based permutation for image encryption," Journal of King Saud University – Computer and Information Sciences, 2023.

[8] H. Oğraş, "A New Data Coding Algorithm for Secure Communication of Image," Chaos Theory and Applications, vol. 6, no. 4, pp. 284–293, 2024.

[9] X. Zhang et al., "Image encryption algorithm based on a new 3D chaotic system using cellular automata," Chaos, Solitons & Fractals, vol. 179, 2024.

[10] Y. Wang et al., "A novel color image encryption algorithm based on fractional-order conservative memristive hyperchaotic system," Journal of King Saud University – Computer and Information Sciences, 2025.

[11] M. Li et al., "Multi-layer image encryption framework using a chaotic system with a dynamic starting point," Digital Signal Processing, vol. 170, 2026.