Chaos coordinated neural key synchronization for enhancing security of IoT

Ahmed h. Alahmadi¹

Received: 3 June 2021 / Accepted: 26 November 2021 / Published online: 4 January 2022
© The Author(s) 2021

Abstract

The key exchange mechanism in this paper is built utilizing neural network coordination and a hyperchaotic (or chaotic) nonlinear dynamic complex system. This approach is used to send and receive sensitive data between Internet-of-Things (IoT) nodes across a public network. Using phishing, Man-In-The-Middle (MITM), or spoofing attacks, an attacker can easily target sensitive information during the exchange process. Furthermore, minimal research has been made on the exchange of input seed values for creating identical input at both ends of neural networks. The proposed method uses a 5D hyperchaotic or chaotic nonlinear complex structure to ensure the sharing of input seed value across two neural networks, resulting in the identical input on both ends. This study discusses two ways for sharing seed values for neural coordination. The first is a chaotic system with all real variables, whereas the second is a hyperchaotic system with at least one complex variable. Each neural network has its own random weight vector, and the outputs are exchanged. It achieves full coordination in some stages by altering the neuronal weights according to the mutual learning law. The coordinated weights are utilized as a key after the neural coordination technique. The network's core structure is made up of triple concealed layers. So, determining the inner configuration will be tough for the intruder. The efficiency of the suggested model is validated by simulations, and the findings reveal that the suggested strategy outperforms current equivalent techniques.

Keywords Hyperchaotic · Neural coordination · Complex anti-coordination (CAC) · Chaotic · Session key

Introduction

The power sector's automation is also transforming transportation, telecommunications, healthcare, finance, and security. Critical Energy Infrastructures (CEI) are distributed rapidly, resulting in dynamic networks that need careful security and speedy recovery in order to prevent intrusions. To connect services reliably, an intelligent energy meter in an intelligent power grid system uses an unreliable connection. Because the information is exchanged through an open channel, an attacker may present a multitude of security risks. Important attempts have been made in this regard to address privacy and security problems in IoT applications, the majority of which have focused on conventional approaches. A broad range of security considerations (secrecy, reliability, and authorization) must be resolved to protect IoT systems

from assault. Current implementations do not effectively solve the complete range of protection for IoT environments due to the peculiar features of IoT nodes. Despite the fact that a number of key agreement techniques have been illustrated so far, as seen in “Related work”, the bulk of existing approaches lack the necessary safety characteristics for IoT security. The aforementioned methods lead to the design of a stable key exchange policy which can satisfy a variety of safety standards while ignoring the safety vulnerabilities and shortcomings that presently plague IoT key swap over processes. As a consequence, for mutual key synchronization across multiple IoT devices, this paper proposes a 5D hyperchaotic or chaotic nonlinear complex system-based neural net. By sharing the input seed value through hyperchaotic or chaotic communication, an equivalent input vector for both neural networks can be created. Even though this proposed solution will control the length of the session key, it will still provide an acceptable security level for use in real-world applications.

Following are the motivations of this paper:

✉ Ahmed h. Alahmadi
aahmadio@taibahu.edu.sa

¹ Department of Computer Science and Information, Taibah University, Madinah, Saudi Arabia

1. A 5D hyperchaotic or chaotic nonlinear complex system uses chaotic synchronization to help in the sharing of same confidential seed variables at both sides. The same seed variable is used to generate the same inputs for neuronal sync.
2. Man-In-The-Middle (MITM) assault protection and resiliency should be improved. As two networks' messages are intercepted by an intruder or assailant. Since the hacker is impersonating the actual sender, it's a risky assault. The perpetrator can fool the recipient into assuming they are transmitting a true message if they have the first grasp.
3. The development of a cryptographic keys interchange system is important. So rather than sending the whole sensitive session key over such a private medium, all communications systems may use coordination over a public channel to generate a key directly.
4. With security strengthening, a chaos-guided secure communication mechanism must be developed.
5. To improve confidentiality and effectiveness, a method for coordinating the neuro key exchange process must be developed.
7. The suggested approach takes significantly less time to coordinate than current strategies for various learning rules.
8. The key exchange strategies described by Jeong et al. [12], Sarkar [31], Teodoro et al. [34], Dong and Huang [8] and Dolecki and Kozera [7] were investigated in the present study. This research focused on their weaknesses as well. To overcome the relevant problems, this article gives a TLTPM coordinating key agreement technique that results in a secret key with a flexible size.
9. The secret key is created dynamically by sharing just few variables over the public medium using the neural coordination protocol at both ends, rather than being sent individually to the other system.

The rest of the article is broken down into six sections. "Related work" provides insight into related work. In "Proposed methodology", the proposed approach is discussed. The results and interpretation are presented in "Results and analysis". Conclusions and future scope are found in "Conclusion and future scope".

This paper's various contributions are summed up as follows:

1. To address the problems given by security vulnerabilities and apparent execution costs, the goal of this study is to clarify fundamental ideas and highlight methodologies for successful 5D hyperchaotic or chaotic nonlinear complex system-based neural network-guided safety—critical applications.
2. The seed value transmitted from sender to receiver through 5D hyperchaotic or chaotic nonlinear complex system. This identical seed value will be used for generating identical input vector for neural key exchange.
3. In this article, two schemes are considered for exchanging seed values for neural synchronization. One has all real variables and exhibits chaotic behavior, while the other has at least one complex variable and exhibits hyperchaotic behavior.
4. To share the typical seed value for neural key exchange, complete Complex Anti-Coordination (CAC) of two equivalent hyperchaotic or chaotic systems is proposed.
5. The fact that the master system's state parameter synchronizes with the slave system's state parameter provides strong data sharing protection. In prior sensitive communications investigations, this section had never been identified.
6. Previously, protective connection systems relied solely on one sort of coordination. In any event, there are two types of coordination systems presented in this work (CS and AS). As a result, data transfer security will be improved.

Related work

Atan et al. [3] has proposed to develop a fuzzy set control scheme for synchronizing two non-identical hyperchaotic processes. To increase the performance of the system, fuzzy logic-based regulators are combined with strong control strategies such as sliding mode controls. The IFSMC regulator created by combining SMC and fuzzy logic-based IFLC was intended for hyperchaotic systems to take use of SMC and fuzzy logic-based IFLC. The goal of the work proposed by Tunç et al. [35] is to look at a few of the characteristics of FrRIDEs with Caputo fractional differential equations, which are nonlinear fractions delayed Volterra integro-differential equations. The reported results are also supported by the use of the Lyapunov–Razumikhin technique and the definition of an adequate Lyapunov function (LRM). Despite the fact that chaos dynamic models are predictable, long-term forecasting of their performance is difficult Casdagli [5]. Furthermore, the chaotic processes' primary features include hypersensitivity, structural blending, and orbital concentration Cho and Miyano [6], Natiq et al. [22,23]. As a result, complex systems are useful in a variety of areas, particularly computer engineering, telecommunications, physics, and technology Natiq et al. [25], Farhan et al. [10], Viet-Thanh et al. [36]. Because the features of chaos theory and the dispersion and confusing aspects of encryption Alvarez and Li [2] are comparable, a large number of chaos-based cryptography algorithms have been proposed in recent years Cao et al. [4], Moysis et al. [21]. This has necessitated the measurement of the chaotic processes' complexities Natiq et al.

Table 1 Strengths and constraints of cutting-edge techniques

Author	Strengths	Constraints
Dolecki and Kozera [7]	Suggested a tool for determining the level of coordination in specified prior coordination learning measures	It requires awhile for the two networks to entirely coordinate, and the two networks continue to learn once they are totally synced. Additional knowledge from the succeeding learning phases is revealed by the smart adversary
Liu et al. [17]	Using a hash to assess the coordination of neural networks	On the other side, network congestion might grow. If the hash functions were to be abused, a considerable quantity of data traffic would have been created
Jeong et al. [12]	Two vector-valued neural networks synchronized	This approach does not work well for group synchronization
Dong and Huang [8]	Synchronization of two complex valued neural networks	They only looked at the geometric assault; whether the CVTPM can resist a majority assault is unknown. In addition, effective group coordination is not achievable
Teodoro et al. [34]	FPGA-based TPM synchronization	No group synchronization assessment method is proposed

[24], Farhan et al. [9]. Apart from quantum key distribution, Yan et al. [38] introduced an approach called quantum-based communication that allows users to send secret messages to each other without first creating a shared secret key. With the advancement of digital technology, a wide range of cellular products and systems became accessible. The majority of methods ignored the situation of multilevel verification, a cellphone user who has completed the enrollment process at the registration center, including all authorized mobile subscribers at the registration center. Regarding virtualization, Kou et al. [15] developed a novel multilevel multi-server security mechanism. Only specific sorts of customers may effectively verify with some of these types of mobile telecommunications companies, according to the suggested protocol. Vehicle accidents, financially harmful traffic congestion, theft, pushing to incorrect paths, and economic problems for corporations and governments are all possible outcomes of cyber threats to intelligent and automated cars. Waqas et al. [37] presented a reinforcement learning method that uses the communications link's channel state information to identify malicious networks. They look at the vehicle-to-vehicle and vehicle-to-infrastructure network systems. Verification of both clients and Access points is required to establish a secured WLAN communication system, and an authenticating users technique must be used. Artificial Neural networks (ANN) are being commonly used for the cryptographic purpose Abdalrdha et al. [1]; Protic [29]; Hadke and Kale [11]. In the early 1990s, the chaos coordination mechanism was observed Pecora and Carroll [28]. Rehan [30] proposed a coordination and anti-coordination of disorderly oscillators under input saturation and disruption using basic output feedback controller. Jo et al. [13] created AAS-IoTSG, an anonymously key establishment method for the power system network. The blockchain, according to Lu et al. [18], offers multi-party cooperative secured data-

sharing technologies. By adding confidentiality federated learning, the data sharing challenge was transformed into a machine-learning challenge. Makkar et al. [19] proposed IoT device safety by detecting spamming via ML algorithms. It is recommended that the machine intelligence system are being used to identify malware in IoT to accomplish this aim. Sarkar [31], Sarkar and Mandal [32] suggested several ways for increasing TPM's weight range and therefore strengthening the symmetric keys exchange's confidentiality. Instead of a full weight vector, Shishniashvili et al. [33] suggested utilizing portions of the aligned weight vectors as an encryption key. In quantum cryptography, the cooperation of devices connected could be utilized to reduce mistakes in the key establishment method Mehic et al. [20]. The researchers of Dong and Huang [8] proposed the CVTPM, that uses complex integers for all control factors. It's unclear if the CVTPM can resist a majority threat because they only looked at the geometric threat. A VVTPM system has been proposed by Jeong et al. [12]. This approach, however, does not really give an accurate synchronization assessment. Teodoro et al. [34] suggested putting TPM structure on an FPGA to conduct key exchange by mutual training of these machines.

The merits and demerits of existing techniques are summarized in Table 1.

Proposed methodology

Applying chaotic synchronization, a 5D hyperchaotic or chaotic nonlinear complex system aids in the sharing of similar confidential seed variables at both ends. This similar seed variable is utilized to produce an equivalent inputs for neuronal sync.

Following Table 2 shows different symbols and their meanings.

Table 2 The symbols' meaning

Symbol	Meaning
$a(\text{tim})$, $b(\text{tim})$, and $g(\text{tim})$	Real-state parameters that behave in time but not uniformly
c , d , e , and v	System variable
$\dot{X}$ and $\dot{Z}$	Hyperchaotic (or chaotic) nonlinear complex system variables
Jac_{E_1}	Jacobian matrix
ψ	Eigen value
i_1	Lyapunov notation
E	Complicated error task vector
N	The quantity of input nodes that must be accessible to every node from the first concealed layer
λ	Weight range
τ_1	1st concealed layer node count
τ_2	2nd concealed layer node count
τ_3	3rd concealed layer node count
δ	The weight of neural system
γ	The input of neural system
ς	Number of input vectors
μ	Vector dimension
ξ	Output of hidden layer

Take into account the hyperchaotic (or chaotic) nonlinear complex system with the following variables:

$$\begin{aligned}\dot{X} &= FX + Q(X, Z), \\ \dot{Z} &= f(X, -X, Z),\end{aligned}\quad (1)$$

Here, $X = (a_1, a_2, \dots, a_m)^T$

$$\begin{aligned}X &= X^l + qX^p, \quad X^l = (a_1^l, a_2^l, \dots, a_m^l)^T, \\ X^p &= (a_1^p, a_2^p, \dots, a_m^p)^T, \quad q = \sqrt{-1}, \\ Q &= (u_1, u_2, \dots, u_n)^T\end{aligned}$$

Chaotic system in real form can be presented as follows:

$$\begin{aligned}\dot{a}(\text{tim}) &= ca(\text{tim}) - b(\text{tim})g(\text{tim}) - b(\text{tim}) + v, \\ \dot{b}(\text{tim}) &= -db(\text{tim}) + a(\text{tim})g(\text{tim}), \\ \dot{g}(\text{tim}) &= a(\text{tim})b(\text{tim}) - eg(\text{tim})\end{aligned}\quad (2)$$

Here $a(\text{tim})$, $b(\text{tim})$ and $g(\text{tim})$ are real-state parameters that behave in time but not uniformly, and c , d , e and v are system variables (Eq. 2). The system (Eq. 2)'s most notable feature is its ability to generate a wide range of attractors, including chaotic and unpredictable attractors. Furthermore, it has been successfully discovered that this system can also construct a chaos-based four-scroll attractor. As a generalizability of the structure (Eq. 2), this paper introduces a modern hyperchaotic (or chaotic) exhibit of complex parts in this study:

$$\begin{aligned}\dot{a}_h(\text{tim}) &= ca_h(\text{tim}) - vb_h(\text{tim})g_h(\text{tim}) - b_h(\text{tim}) + v + P_1, \\ \dot{b}_h(\text{tim}) &= -db_h(\text{tim}) + a_h(\text{tim})g_h(\text{tim}) + P_2\end{aligned}\quad (3)$$

c , d and e are positive variables, and v is a control variable that could be either complex or real. The parameters $a(\text{tim}) = a^l(\text{tim}) + qa^p(\text{tim})$, $b(\text{tim}) = b^l(\text{tim}) + qb^p(\text{tim})$ represent complex factors, $g(\text{tim})$ represent real factors, and the controlling p and l represent the imaginary and real components, respectively. This proposed system (Eq. 3) can be thought of as a variant of (Eq. 1), with $X = (a_1, a_2)^T = (a, b)^T$, and $Z = g$. The variable v has a significant impact on the system's operation (Eq. 3). System (Eq. 3) is a chaotic system if v is to be considered a real parameter. The proposed system (Eq. 3) will produce hyperchaotic behavior if $v = v^l + qv^p$ considered as a complex variable. In a sense, the method for selecting variables, either complex or real, has an impact on the system's behavior. This paper would like investigate the proposed system's behavior to clarify this previously unknown impact. The first time where the variable v is a real number, and the second time if it is indeed a complex number. In addition, this paper looking at a new form of coordination known as Complex Anti-Coordination (CAC). CAC's concept can be handled by coordinating AS and CS Rehan [30]. AS occurs when a real part of the master structure interacts with an imaginary part of a slave system, whereas CS occurs when a real part of slave system interacts with an imaginary part of master system. This paper presents a comprehensive system for considering and achieving the CAC of two equivalent chaotic dynamic nonlinear systems

are a type of (Eq. 1). This paper chooses, for example, the chaotic nonlinear complex shown in Eq. (3) with clear aim of demonstrating the effects of the proposed system of two similar structures of the type (Eq. 1).

The basic features of the structure (Eq. 3) are investigated twice: once if v is the real variable and again if v is indeed the complex variable. A structure for CAC of nonlinear systems is presented in this paper.

If v is a real variable, this proposed technique investigates the basic dynamical analysis of the system (Eq. 3). To accomplish this case, the actual type of structure (Eq. 3) is as follows:

$$\begin{aligned}\dot{a}^l(\text{tim}) &= ca^l(\text{tim}) - b^l(\text{tim})g(\text{tim}) - b^l(\text{tim}) + v, \\ \dot{a}^p(\text{tim}) &= ca^p(\text{tim}) - b^p(\text{tim})g(\text{tim}) - b^p(\text{tim}), \\ \dot{b}^l(\text{tim}) &= a^l(\text{tim})g(\text{tim}) - db^l(\text{tim}), \\ \dot{b}^p(\text{tim}) &= a^p(\text{tim})g(\text{tim}) - db^p(\text{tim}), \\ \dot{g}(\text{tim}) &= a^l(\text{tim})b^l(\text{tim}) + a^p(\text{tim})b^p(\text{tim}) - eg(\text{tim}) \quad (4)\end{aligned}$$

System (Eq. 4) seems to contain 6 quadratic nonlinear and 1 constant terms. As monitoring, the system (Eq. 4) has several key dynamical features. It is noticed that the transition is constant over time in this system (Eq. 4): $(a^l(\text{tim}), a^p(\text{tim}), b^l(\text{tim}), a^p(\text{tim}), g(\text{tim})) \Rightarrow (a^l(\text{tim}), -a^p(\text{tim}), b^l(\text{tim}), -b^l(\text{tim}), g(\text{tim}))(a^l(\text{tim}), a^p(\text{tim}), b^l(\text{tim}), a^p(\text{tim}), g(\text{tim}))$ is the elucidation of system (Eq. 4), and $(a^l(\text{tim}), -a^p(\text{tim}), b^l(\text{tim}), -b^l(\text{tim}), g(\text{tim}))$, is the resolution of the corresponding system. It is simple to locate $\nabla \cdot N = \frac{\lambda \dot{a}^l}{\lambda a^l} + \frac{\lambda \dot{a}^p}{\lambda a^p} + \frac{\lambda \dot{b}^l}{\lambda b^l} + \frac{\lambda \dot{b}^p}{\lambda b^p} + \frac{\lambda \dot{g}}{\lambda g} = 2c - 2d - e < 0$. When $2c < (2d + e)$, the structure is deformed, and it meets $\frac{dN}{d\text{tim}} = e^{-(2c-2d-e)t}$ in sort mode. It implies that at time tim, the volume element N_0 contracts to the volume section $N_0 e^{-(2c-2d-e)t}$. As $\text{tim} \rightarrow \infty$ is reached, any volume component containing the structure carrying with type rate form gathered to 0. Following that, the majority of the system aim will be limited to a 0 volume subset, and the dynamic change would be based on an attractor. Identifying the following set of parameters will help to find the system's equilibrium conditions:

$$\begin{aligned}0 &= ca^l(\text{tim}) - b^l(\text{tim})g(\text{tim}) - b^l(\text{tim}) + v, \\ 0 &= ca^p(\text{tim}) - b^p(\text{tim})g(\text{tim}) - b^p(\text{tim}), \\ 0 &= a^l(\text{tim})g(\text{tim}) - db^l(\text{tim}), \\ 0 &= a^p(\text{tim})g(\text{tim}) - db^p(\text{tim}), \\ 0 &= a^l(\text{tim})b^l(\text{tim}) + a^p(\text{tim})b^p(\text{tim}) - eg(\text{tim}). \quad (5)\end{aligned}$$

Clearly, proposed system does not have a single fixed point. The nonzero measurements are calculated as follows:

$$\begin{aligned}E_1 &= \left(-\frac{v}{c}, 0, 0, 0, 0\right), \\ E_2 &= \left(-\sqrt{de}, 0, \frac{\frac{1}{e^{\frac{1}{4}}}\left(\frac{1}{e^{\frac{1}{4}} + \delta_1}\right)}{2\sqrt{d}}, 0, -\frac{1}{2}\left(1 + \frac{\delta_1}{e^{\frac{1}{4}}}\right)\right), \\ E_3 &= \left(-\sqrt{de}, 0, \frac{\frac{1}{e^{\frac{1}{4}}}\left(\frac{1}{e^{\frac{1}{4}} - \delta_1}\right)}{2\sqrt{d}}, 0, \frac{1}{2}\left(-1 + \frac{\delta_1}{e^{\frac{1}{4}}}\right)\right), \\ E_4 &= \left(\sqrt{de}, 0, \frac{-\frac{1}{e^{\frac{1}{4}}}\left(\frac{1}{e^{\frac{1}{4}} + \delta_2}\right)}{2\sqrt{d}}, 0, -\frac{1}{2}\left(1 + \frac{\delta_2}{e^{\frac{1}{4}}}\right)\right), \\ E_5 &= \left(\sqrt{de}, 0, \frac{\frac{1}{e^{\frac{1}{4}}}\left(\frac{1}{-e^{\frac{1}{4}} - \delta_2}\right)}{2\sqrt{d}}, 0, \frac{1}{2}\left(-1 + \frac{\delta_2}{e^{\frac{1}{4}}}\right)\right), \quad (6)\end{aligned}$$

where $\delta_1 = \sqrt{(1 + 4cd)\sqrt{e} - 4\sqrt{dv}}$,

$\delta_2 = \sqrt{(1 + 4cd)\sqrt{e} + 4\sqrt{dv}}$

The Jacobian matrix of system (Eq. 4) at E_1 is used to investigate the intensity of E_1 .

$$Jac_{E_1} = \begin{pmatrix} c & 0 & -1 & 0 & 0 \\ 0 & c & 0 & -1 & 0 \\ 0 & 0 & -d & 0 & -\frac{v}{c} \\ 0 & 0 & 0 & -d & 0 \\ 0 & 0 & -\frac{v}{c} & 0 & -e \end{pmatrix}$$

The polynomial state that is most well known is:

$$(\psi - c)^2(\psi + d)\left(\psi^2 + (d + e)\psi + de - \frac{v^2}{c^2}\right) = 0 \quad (7)$$

The eigenvalues at that point are

$$\begin{aligned}\psi_1 &= \psi_2 = c, \quad \psi_3 = -d, \\ \psi_{4,5} &= \frac{1}{2c}\left[-c(d + e) \pm \sqrt{c^2(d - e)^2 + 4v^2}\right].\end{aligned}$$

If c has negative estimations and d is positive, $dc^2e < v^2$, the negotiated point $(-\frac{v}{c}, 0, 0, 0, 0)$ is e stable fixed point; otherwise, it is not.

Similarly, this paper investigated the reliability of E_2 , E_3 , E_4 , E_5

In vector information, system (Eq. 4) can be written as:

$$\dot{\alpha}(\text{tim}) = \sigma(\alpha(\text{tim}); H) \quad (8)$$

Here, $\alpha(\text{tim}) = (a^l(\text{tim}), a^p(\text{tim}), b^l(\text{tim}), b^p(\text{tim}), g(\text{tim}))^T$ represents state space vector,

$$\sigma = (\sigma_1(\text{tim}), \sigma_2(\text{tim}), \sigma_3(\text{tim}), \sigma_4(\text{tim}), \sigma_5(\text{tim}))^T$$

H is the variable configuration, and $(\dots)^T$ is the transpose. The following are the criteria for slight variations $\eta\alpha$ from the path $\alpha(\text{tim})$:

$$\eta\dot{\alpha}(\text{tim}) = \text{Jac}_{vi}(\alpha(\text{tim}); M)\eta\alpha, \quad v = D = 1, 2, 3, 4, 5 \quad (9)$$

$\text{Jac}_{vi}(\alpha(\text{tim}); H)$ denotes the Jacobian structure of the form:

$$\begin{aligned} \text{Jac}_{vi} &= \begin{pmatrix} \frac{\eta\sigma_1(\text{tim})}{\eta a^l(\text{tim})} & \frac{\eta\sigma_1(\text{tim})}{\eta a^p(\text{tim})} & \frac{\eta\sigma_1(\text{tim})}{\eta b^l(\text{tim})} & \frac{\eta\sigma_1(\text{tim})}{\eta b^p(\text{tim})} & \frac{\eta\sigma_1(\text{tim})}{\eta g(\text{tim})} \\ \frac{\eta\sigma_2(\text{tim})}{\eta a^l(\text{tim})} & \frac{\eta\sigma_2(\text{tim})}{\eta a^p(\text{tim})} & \frac{\eta\sigma_2(\text{tim})}{\eta b^l(\text{tim})} & \frac{\eta\sigma_2(\text{tim})}{\eta b^p(\text{tim})} & \frac{\eta\sigma_2(\text{tim})}{\eta g(\text{tim})} \\ \frac{\eta\sigma_3(\text{tim})}{\eta a^l(\text{tim})} & \frac{\eta\sigma_3(\text{tim})}{\eta a^p(\text{tim})} & \frac{\eta\sigma_3(\text{tim})}{\eta b^l(\text{tim})} & \frac{\eta\sigma_3(\text{tim})}{\eta b^p(\text{tim})} & \frac{\eta\sigma_3(\text{tim})}{\eta g(\text{tim})} \\ \frac{\eta\sigma_4(\text{tim})}{\eta a^l(\text{tim})} & \frac{\eta\sigma_4(\text{tim})}{\eta a^p(\text{tim})} & \frac{\eta\sigma_4(\text{tim})}{\eta b^l(\text{tim})} & \frac{\eta\sigma_4(\text{tim})}{\eta b^p(\text{tim})} & \frac{\eta\sigma_4(\text{tim})}{\eta g(\text{tim})} \\ \frac{\eta\sigma_5(\text{tim})}{\eta a^l(\text{tim})} & \frac{\eta\sigma_5(\text{tim})}{\eta a^p(\text{tim})} & \frac{\eta\sigma_5(\text{tim})}{\eta b^l(\text{tim})} & \frac{\eta\sigma_5(\text{tim})}{\eta b^p(\text{tim})} & \frac{\eta\sigma_5(\text{tim})}{\eta g(\text{tim})} \end{pmatrix} \\ &= \begin{pmatrix} c & 0 & -g-1 & 0 & -b^l \\ 0 & c & 0 & -g-1 & -b^p \\ g & 0 & -d & 0 & a^l \\ 0 & g & 0 & -d & a^p \\ b^l & b^p & a^l & a^p & -e \end{pmatrix} \end{aligned}$$

The system's Lyapunov notation i_1 is defined by:

$$i_1 = \lim_{\text{tim} \rightarrow \infty} \frac{1}{\text{tim}} \log \frac{||\lambda\alpha(\text{tim})||}{||\lambda\alpha(0)||} \quad (10)$$

Equations (8) and (9) should be mathematically determined at all times to determine i_1 . The order 4 Runge–Kutta technique is used to record i_1 . As for preliminary condition $\text{tim}_0 = 0$, $a^l(0) = 1$, $a^p(0) = 2$, $b^l(0) = 3$, $b^p(0) = 4$, $g(0) = 5$, and $c = 16.5$, $d = 24$, $e = 2$, $v = 2$. The Lyapunov coefficients are as follows: $i_1 = 4.01$, $i_2 = 0$, $i_3 = 0$, $i_4 = -10.99$, and $i_5 = -17.68$.

Since one of the Lyapunov exponents is positive, proposed structure (Eq. 4) under this option of c , d , e and v is a chaotic system.

According to guess of Kaplan–Yorke, the Lyapunov measure or the attractors of (Eq. 4)'s dimension are:

$$L = \mu + \frac{\sum_{v=1}^{\mu} i_v}{|i_{\mu+1}|} \quad (11)$$

This paper likes to highlight the effect of the variable selection approach, either complex or real, on the features and behavior of the proposed system. In the system, this paper considers $v = v^l + qv^p$ to be a complex variable. In this vein, the real form of the paradigm investigates:

$$\begin{aligned} \dot{a}^l(\text{tim}) &= ca^l(\text{tim}) - b^l(\text{tim})g(\text{tim}) - b^l(\text{tim}) + v^l, \\ \dot{a}^p(\text{tim}) &= ca^p(\text{tim}) - b^p(\text{tim})g(\text{tim}) - b^p(\text{tim}) + v^p, \\ \dot{b}^l(\text{tim}) &= a^l(\text{tim})g(\text{tim}) - db^l(\text{tim}), \\ \dot{b}^p(\text{tim}) &= a^p(\text{tim})g(\text{tim}) - db^p(\text{tim}), \\ \dot{g}(\text{tim}) &= a^l(\text{tim})b^l(\text{tim}) + a^p(\text{tim})b^p(\text{tim}) - eg(\text{tim}) \end{aligned} \quad (12)$$

System (Eq. 12) seems to have 6 quadratic nonlinear and 2 constant terms. The system's (Eq. 12) birefringent condition is the same in system (Eq. 4). Regardless, there is no modification that makes structure (Eq. 12) a symmetric system, despite the fact that this is evident in the system (Eq. 4). Situations (Eq. 12) have stabilized, indicating that they are essentially the same as other identified in the system (Eq. 4), but with a more intertwined form, as shown by the following:

$$\begin{aligned} E_1 &= \left(-\frac{v^l}{c}, -\frac{v^p}{c}, 0, 0, 0\right), \\ E_2 &= \left(-\frac{\text{dev}^l}{\delta_3}, -\frac{\text{dev}^p}{\delta_3}, \frac{v^l\delta_4}{2\delta_3}, \frac{v^p\delta_4}{2\delta_3}, -\frac{\delta_4}{2e}\right), \\ E_3 &= \left(\frac{\text{dev}^l}{\delta_3}, \frac{\text{dev}^p}{\delta_3}, \frac{v^l\delta_5}{2\delta_3}, \frac{v^p\delta_5}{2\delta_3}, \frac{\delta_5}{2e}\right), \\ E_4 &= \left(-\frac{\text{dev}^l}{\delta_3}, -\frac{\text{dev}^p}{\delta_3}, \frac{v^l\delta_6}{2\delta_3}, \frac{v^p\delta_6}{2\delta_3}, -\frac{\delta_6}{2e}\right), \\ E_5 &= \left(\frac{\text{dev}^l}{\delta_3}, \frac{\text{dev}^p}{\delta_3}, \frac{v^l\delta_7}{2\delta_3}, \frac{v^p\delta_7}{2\delta_3}, \frac{\delta_7}{2e}\right) \end{aligned} \quad (13)$$

$$\delta_3 = \sqrt{de[(v^l)^2 + (v^p)^2]},$$

$$\delta_4 = e + \sqrt{e(e + 4cde - 4\delta_3)},$$

Where $\delta_5 = -e + \sqrt{e(e + 4cde + 4\delta_3)},$

$$\delta_6 = e - \sqrt{e(e + 4cde - 4\delta_3)},$$

$$\delta_7 = -e - \sqrt{e(e + 4cde + 4\delta_3)}$$

$$\text{Jac}_{E_1} = \begin{pmatrix} c & 0 & -1 & 0 & 0 \\ 0 & c & 0 & -1 & 0 \\ 0 & 0 & -d & 0 & \frac{-v^l}{c} \\ 0 & 0 & 0 & -d & \frac{-v^p}{c} \\ 0 & 0 & \frac{-v^l}{c} & \frac{-v^p}{c} & -e \end{pmatrix}$$

Its characteristic polynomial is:

$$(\psi - c)^2 (\psi + d) \left\{ \psi^2 + (d + e)\psi + de - \frac{[(v^l)^2 + (v^p)^2]}{a^2} \right\} = 0 \quad (14)$$

The eigenvalues are:

$$\begin{aligned} \psi_1 &= \psi_2 = c, \quad \psi_3 = -d \\ \psi_{4.5} &= \frac{1}{2c} \left(-c(d + e) \pm \sqrt{c^2(d - e)^2 + 4[(v^l)^2 + (v^p)^2]} \right) \end{aligned}$$

This fixed point is stable if: $c < 0$, $d > 0$, $dc^2e < [(v^l)^2 + (v^p)^2]$

Otherwise, it is an unstable fixed point. As with E_1 , the stability of E_2 , E_3 , E_4 , E_5 can be tested.

Two equivalent chaotic (or hyperchaotic) complex nonlinear systems of the type (Eq. 1) are considered, one of which is the master system (signified by the subscript r) as follows:

$$\begin{cases} \dot{X}_r = \dot{X}_r^l + q\dot{X}_r^p = FX_r + Q(X_r) \\ \dot{Z} = f(X, -X, Z) \end{cases} \quad (15)$$

and the second is the monitored slave system (defined by the subscript h) as follows:

$$\dot{X}_h = \dot{X}_h^l + q\dot{X}_h^p = FX_h + Q(X_h) + P \quad (16)$$

Where, the added substance complicated monitor $P = (P_1, P_2, \dots, P_m)^T = P^l + qP^p$, $P^l = (P_1^l, P_2^l, \dots, P_m^l)^T$, $P^p = (P_1^p, P_2^p, \dots, P_m^p)^T$

Two combined, complex dimensional structures will display CAC in a master slave configuration if a complicated error task vector E occurs, for example:

$$E = E^l + qE^p = \lim_{\text{tim} \rightarrow \infty} \|X_h + qX_r\| = 0 \quad (17)$$

Where $E = E^l + qE^p = (s_{a_1}, s_{a_2}, \dots, s_{a_m})^T$, X_r and X_h are the master and slave's vector which are complex in nature.

$$E^l = (s_{a_1^l}, s_{a_2^l}, \dots, s_{a_m^l}) = X_h^l - X_r^p = 0 \quad (18)$$

$$E^p = (s_{a_1^p}, s_{a_2^p}, \dots, s_{a_m^p}) = X_h^p + X_r^l = 0 \quad (19)$$

Now, the meaning of CAC is applied to the systems (Eq. 15) and (Eq. 16):

$$\dot{E} = \dot{E}^l + q\dot{E}^p = X_h + qX_r \quad (20)$$

So,

$$\begin{aligned} \dot{E} &= \dot{E}^l + q\dot{E}^p = \dot{X}_h + q\dot{X}_r \\ \dot{E} &= \dot{E}^l + q\dot{E}^p = [\dot{X}_h^m - \dot{X}_r^p] + q[\dot{X}_h^p + \dot{X}_r^m] \end{aligned} \quad (21)$$

moreover, the error complex dynamical system can be derived from chaotic complex systems (Eq. 15) and (Eq. 16) as follows:

$$\begin{aligned} \dot{E} &= \dot{E}^l + q\dot{E}^p = FX_h^l + Q^l(X_h) \\ &\quad - FX_r^p - Q^p(X_r) + L^l \\ &\quad + j[FX_h^p + Q^p(X_h) + FX_r^l + Q^l(X_r) + L^p] \end{aligned} \quad (22)$$

The error complex structure, which is obtained by separating the real and imaginary parts of Eq. (22), is as follows:

$$\begin{cases} \dot{E}^l = FX_h^l + Q^l(X_h) - FX_r^p - Q^p(X_r) + L^l \\ \dot{E}^p = FX_h^p + Q^p(X_h) + FX_r^l + Q^l(X_r) + L^p \end{cases} \quad (23)$$

The positive unequivocal quantity of Lyapunov function with respect to positive parameters in the system (Eq. 23) is:

$$\begin{aligned} N(\text{tim}) &= \frac{1}{2} \left[(E^l)^T E^l + (E^p)^T E^p \right] \\ &= \frac{1}{2} \left(\sum_{i=1}^m s_{a_i^l}^2 + \sum_{i=1}^m s_{a_i^p}^2 \right) \end{aligned} \quad (24)$$

Remember some along the chaos system's path (Eq. 23), the average period derivative of $N(\text{tim})$ is as follows:

$$\begin{aligned} \dot{N}(\text{tim}) &= (\dot{E}^l)^T E^l + (\dot{E}^p)^T E^p \\ &= (FX_h^l + Q^l(X_h) - FX_r^p - Q^p(X_r) + L^l)^T E^l \\ &\quad + (FX_h^p + Q^p(X_h) + FX_r^l + Q^l(X_r) + L^p)^T E^p \end{aligned} \quad (25)$$

The main subsidiary $\dot{N}(\text{tim}) < 0$ is made by a wise strategy of the controller L^l , L^p . Thus, the ability to perform CAC is gained. As a result, the slave and master systems' requirements would be globally synced asymptotically.

Remark 1 According to Eq. (18), the difference between slave system's real part a_h^l and master system's imaginary part a_r^p goes to zero as $\text{tim} \rightarrow \infty$ (CS).

Remark 2 When $\text{tim} \rightarrow \infty$, the whole imaginary part of slave system a_h^p and the real part of master system a_r^l disappear in Eq. (19) (AS).

Remark 3 CAC combines CS and AS in Remarks 1 and 2.

Finally, this scheme is described by implementing it in “Proposed methodology” for chaotic attractors of complex nonlinear systems (Eq. 3).

This segment analyzes the CAC issue of a chaotic complex system (Eq. 3) with some parameters. As a result, the master and slave systems are described as follows:

$$\begin{aligned}\dot{a}_r(\text{tim}) &= ca_r(\text{tim}) - b_r(\text{tim})g_r(\text{tim}) - b_r(\text{tim}) + v, \\ \dot{b}_r(\text{tim}) &= -db_r(\text{tim}) + a_r(\text{tim})g_r(\text{tim}), \\ \dot{z}_r(\text{tim}) &= \frac{1}{2} [\bar{a}_r(\text{tim})b_r(\text{tim}) + a_r(\text{tim})\bar{b}_r(\text{tim})] - eg(\text{tim})\end{aligned}\quad (26)$$

and

$$\begin{aligned}\dot{a}_h(\text{tim}) &= ca_h(\text{tim}) - b_h(\text{tim})g_h(\text{tim}) - b_h(\text{tim}) + v + P_1, \\ \dot{b}_h(\text{tim}) &= -db_h(\text{tim}) + a_h(\text{tim})g_h(\text{tim}) + P_2\end{aligned}\quad (27)$$

where $a_r = a_r^l + qa_r^p$, $b_r = b_r^l + qb_r^p$, $a_h = a_h^l + qa_h^p$, $b_h = b_h^l + qb_h^p$ and $P_1 = P_1^l + qP_1^p$, $P_2 = P_2^l + qP_2^p$ are complex capacities, which is to be decided.

With the intention of achieving control signals in mind, the complex chaotic states between the supervised slave system and the supervising expert system are described as:

$$\begin{aligned}s_a &= a_h + qa_r \\ s_b &= b_h + qb_r\end{aligned}\quad (28)$$

where $s_a = s_a^m + qs_a^p$, $s_b = s_b^m + qs_b^p$, denotes the capacity for complex errors.

This paper uses condition (Eq. 26) from (Eq. 27) and using (Eq. 28) to get the complex error dynamical structure (Eq. 23):

$$\begin{aligned}\dot{s}_a &= \dot{s}_a^m + q\dot{s}_a^p = \dot{a}_e + q\dot{a}_r, \\ &= cs_a - s_b - s_b g + v + qv + P_1, \\ \dot{s}_b &= \dot{s}_b^m + q\dot{s}_b^p = \dot{b}_e + qb_r, \\ &= -ds_b + gs_a + P_2\end{aligned}\quad (29)$$

Condition (Eq. 29), on the other hand, represents a complex dynamical system in which the “errors” evolve over time.

A complex Lyapunov function can now be defined as follows for positive parameters c, d :

$$k(\text{tim}) = \frac{1}{2} ((s_a^m)^2 + (s_b^m)^2 + (s_a^p)^2 + (s_b^p)^2) \quad (30)$$

Along the framework’s arrangement (Eq. 29), the subsidiary of $\dot{N}(\text{tim})$ is:

$$\begin{aligned}\dot{N}(\text{tim}) &= s_a^m \dot{s}_a^m + s_b^m \dot{s}_b^m + s_a^p \dot{s}_a^p + s_b^p \dot{s}_b^p, \\ &= s_a^m [cs_a^m - s_b^m - s_b^m g + v + P_1^m] \\ &\quad + s_b^m [-ds_b^m + gs_a^m + P_2^m] \\ &\quad + s_a^p [cs_a^p - s_b^p - s_b^p g + v + P_1^p] \\ &\quad + s_b^p [-ds_b^p + gs_a^p + P_2^p]\end{aligned}\quad (31)$$

For the complex control capabilities, there are various options. In the event that this paper considers such controllers as:

$$\begin{aligned}P_1 &= P_1^m + qP_1^p = (1 - c)s_a + s_b + s_b g - v(1 + q), \\ P_2 &= P_2^m + qP_2^p = -gs_a\end{aligned}\quad (32)$$

The following is a true representation of the dynamic control work (Eq. 32):

$$\begin{aligned}P_1^m &= (1 - c)s_a^m + s_b^m + s_b^m g - v, \\ &= (1 - c)(a_h^m - a_r^p) + (b_h^m - b_r^p)(1 + g) - v, \\ p_1^p &= (1 - c)s_a^p + s_b^p + s_b^p g - v, \\ &= (1 - c)(a_h^p + a_r^m) + (a_h^p + a_r^m)(1 + g) - v, \\ p_2^m &= -gs_a^m = -g(a_h^m - a_r^p), \\ p_2^p &= -gs_a^p = -g(a_h^p + a_r^m)\end{aligned}\quad (33)$$

Where $s_a^m = a_h^m - a_r^p$, $s_b^m = b_h^m - b_r^p$, $s_a^p = a_r^m + a_h^p$, $s_b^p = b_r^m + b_h^p$ then Eq. (31) will be as:

$$\dot{N}(\text{tim}) = -[(s_a^m)^2 + (s_b^m)^2 + (s_a^p)^2 + (s_b^p)^2] < 0 \quad (34)$$

$\dot{N}(\text{tim})$ is a positively distinctive potential in the segment of zero organization of errors representation (Eq. 29), and its derivative is adversely different.

As a result, Lyapunov’s immediate strategy indicates that the framework’s balance purposes $s_a^m = a_h^m - a_r^p = 0$, $s_a^p = a_r^m + a_h^p = 0$, $s_b^m = b_h^m - b_r^p = 0$, $s_b^p = b_r^m + b_h^p = 0$ of the system (Eq. 29) is asymptotically stable and $s_a \rightarrow 0$, $s_b \rightarrow 0$ as $\text{tim} \rightarrow \infty$

Remark 4 As we look at the CAC issue for the framework (Eq. 3), and the variable v has a complicated system and hyperchaotic behavior ($v = v^m + Jacv^p$), we get the corresponding controller in condition (Eq. 33):

$$\begin{aligned}P_1^m &= (1 - c)s_a^m + s_b^m + s_b^m g - v^m + v^p, \\ &= (1 - c)(a_h^s - a_r^p) + (b_h^m - b_r^p)(1 + g) - v^m + v^p, \\ P_1^p &= (1 - c)s_a^p + s_b^p + s_b^p g - v^m - v^p, \\ &= (1 - c)(a_h^p + a_r^m) + (a_h^p + a_r^m)(1 + g) - v^m - v^p, \\ P_2^m &= -gs_a^m = -g(a_h^m - a_r^p), \\ P_2^p &= -gs_a^p = -g(a_h^p + a_r^m)\end{aligned}\quad (35)$$

Fig. 1 CAC communication

Fig. 2 l vs. tim

The CAC of chaotic (or hyperchaotic) dynamic system, where a parameter of the primary system coordinates with an alternative parameter of the secondary system, is a motivating type of coordination since it provides incredible protection in safe interaction. This paper considers system (Eq. 26), which is chaotic (or hyperchaotic), as a sender system, and system (Eq. 27) as a receiver, which is chaotic (or hyperchaotic). With one aspect, this paper chooses $l(tim) = 6 \cos tim + 4$ as the information movement. Suppose that $\hat{l}(tim) = l(tim) + a_h^l$ is applied to the vector $b_r^p \Rightarrow \hat{l}(tim) = \hat{l}(tim) + b_r^p = l(tim) + x_r^l + b_r^p$. The chaotic (or hyperchaotic) structure seen in Fig. 1 is used to encrypt and decrypt the data signal $l(tim)$. It shows an outline for proposed CAC communication system, in which the chaotic (or hyperchaotic) systems (Eq. 26) and (Eq. 27), including both, are the sender and receiver systems.

Figures 2, 3, 4 and 5 depict the numerical effects of application to secure communications. Figures 2 and 3 display the data signal $l(tim)$ and the transmitted signal $\hat{l}(tim)$, respectively. Figure 4 depicts the recovered information signals, which is whatever has been transmitted by $l^*(tim) = l(tim) + a_h^p - b_h^l$. Because, after completing CAC with the controller system (35) $a_r^l + a_h^p = 0$, $b_h^l - b_r^p = 0$. The failure trajectory between the original data signal and the decrypted one is depicted in Fig. 5. It is not complicated to see from Fig. 5 that the data signal $l(tim)$ is exactly retrieved after a small residual.

Fig. 3 $\hat{l}$ vs. tim Fig. 4 l^* vs. tim

1. As a result, this may concluded that safe communication in terms of CAC has the following advantages:
Strong data sharing protection attributed to the reason that the master system's state parameter synchronizes with slave system's state parameter. This portion has never been discovered in previous sensitive communications examinations.
2. Prior protection connectivity systems were based on a single type of coordination. In any case, this paper offers two types of coordination systems (CS and AS). This will result in increased data transfer protection.

Two neural networks will be involved in the coordinating procedure at any one moment. Both have a unique neural network structure known as the Triple Layer Tree Parity Machine (TLTPM). Reciprocal learning will fully coordinate all devices. The same TLTPM's weights can then be used as a session key. Let A and B are two IoT devices. Initializing, estimation, modification, assessment, and termination are the five steps of the neural coordination procedure to generate a common session key at both IoT devices.

Fig. 5 $|I - I^*|$ vs. tim

1. Initializing step: A and B both set the identical TLTPM framework in their IoT devices. The weights then are produced randomly.
2. Estimation step: For each learning phase, A and B obtain the same input vector generated from the common seed value through chaos coordination. They measure the contribution of the TLTPMs and share the results.
3. Modification step: After obtaining another party's outcomes, they compare the two outcomes to whether they are similar. A and B will make the required adjustments.
4. Assessment step: A and B must decide whether optimum coordination has been reached if the weights are efficiently updated. The method moves on to the next level if complete synchronization is achieved. Otherwise, the computation will be finished.

5. Termination strategy: A and B establish their shared key by coordinating their weights. The neural key agreement operation is approaching completion.

Once the outcomes of the both TLTPMs G and D matched, $\zeta^G = \zeta^D$ modifies the weights according to one of the rules: Using Hebbian learning algorithm, both TLTPMs will be learnt from each other (Eq. 36).

$$\delta_{v,w}^{q+} = \text{fun} \left(\delta_{v,w}^q + \gamma_{v,w}^q \zeta \Phi(\xi_v^q \zeta) \Phi(\zeta^G \zeta^D) \right) \quad (36)$$

These TLTPMs are learnt by reversing their outputs in the Anti-Hebbian direction (Eq. 37).

$$\delta_{v,w}^{q+} = \text{fun} \left(\delta_{v,w}^q - \gamma_{v,w}^q \zeta \Phi(\xi_v^q \zeta) \Phi(\zeta^G \zeta^D) \right) \quad (37)$$

The random-walk learning rule is used when the predetermined value of result isn't relevant for altering because it is the identical for the two TLTPMs (Eq. 38).

$$\delta_{v,w}^{q+} = \text{fun} \left(\delta_{v,w}^q + \gamma_{v,w}^q \Phi(\xi_v^q \zeta) \Phi(\zeta^G \zeta^D) \right) \quad (38)$$

As cryptographic keys, use these coordinated weights.

Results and analysis

The findings of the NIST test suite [26] on the synced neuronal session key are shown in Table 3. The p_Value eval-

Table 3 p_Value comparisons

Test	TLTPM's p_Value	VVTPM's p_Value Jeong et al. [12]	CVTPM's p_Value Dong and Huang [8]	p_Value of Liu et al. [17]	p_Value of Dolecki et al. Dolecki and Kozera [7]
Frequency	0.785469	0.538632	0.512374	0.516357	0.537924
Frequency within a block	0.669857	0.551571	0.538721	0.541873	0.551972
Runs	0.596873	0.508936	0.489451	0.481406	0.487329
Longest run of ones in a block	0.098573	0.061574	0.042081	0.047235	0.061287
Binary matrix rank	0.785732	0.420589	0.417393	0.427351	0.473641
Discrete Fourier transform	0.657980	0.427985	0.392762	0.397219	0.417235
Non-overlapping template matching	0.536756	0.463462	0.431759	0.447348	0.461319
Overlapping (periodic) template matching	0.387363	0.204875	0.170426	0.207321	0.181369
Maurer's "Universal Statistical"	0.836899	0.728347	0.689478	0.719872	0.701985
Linear complexity	0.757362	0.657894	0.594917	0.657410	0.631207
Serial	0.669233	0.547216	0.478902	0.482737	0.531370
Approximate entropy	0.387966	0.280699	0.204175	0.287319	0.274696
Cummulative sums	0.718369	0.640273	0.587290	0.631971	0.643780
Random excursions	0.476933	0.377634	0.299875	0.361925	0.357354
Random excursions variants	0.434782	0.249632	0.180542	0.247329	0.234691

Fig. 6 i_1, i_2, i_3, i_4, i_5 Fig. 7 $(c, a^l(\text{tim}))$

uation is carried out for the TLTPM and VVTPM Jeong et al. [12], CVTPM Huang [8], Liu et al. [17], and Dolecki and Kozera [7] methods. The TLTPM's p_Value has indeed been emerged as a promising alternative than others.

Using Eq. (10), this paper calculates $i_1, D = 1, 2, \dots, 5$ and plots the estimates of $i_1, i_2, \dots, i_5$ versus c in Fig. 6.

As seen in Fig. 6, the system (Eq. 4) has chaotic attractors if $c \in [7.6, 19.8]$. For just c lying in the intervals of time $(0, 7.6), (19.8, 30)$, the sporadic attractors of (Eq. 4) occur. This paper performs a comparative analysis of alternative variables, much as performed with variable c , and found chaotic results in each case. As a consequence, we are satisfied with the findings of variable c .

This paper finds the differentiation graphs details of the structure (Eq. 4) in Figs. 7, 8, 9, 10, and 11 as the variable a differs or changes and ensure proposed framework is chaotic. Upon on level pivot, a differentiation graph structures a system variable and on the vertical hub, a summary of the attractor's operation. As a result, differentiation graphs are c unique way to visualize how a system's behavior varies as a variable is estimated.

Differentiation graphs for $c \in [0, 30]$ are seen in Figs. 7, 8, 9, 10, and 11. Whenever $c \in [7.6, 19.8]$, system (4) has configurations that reach chaotic attractors and $c \in (0, 7.6), (19.8, 30)$ has periodic activity, it can be detected. Figures 7, 8, 9, 10, and 11 have the same dynamical behavior as Fig. 6. Following Figs. 6, 7, 8, 9, 10 and 11 are the bifurcation graphs for $c = 16.5, d = 24, e = 2, v = 2$

Fig. 8 $(c, a^p(\text{tim}))$ Fig. 9 $(c, b^l(\text{tim}))$ Fig. 10 $(c, b^p(\text{tim}))$

and the initial conditions $\text{tim}_0 = 0, a^l(0) = 1, a^p(0) = 2, b^l(0) = 3, b^p(0) = 4, g(0) = 5$.

The outcome of the frequency test in the synced neural key indicates a percentage of 1 and 0. The result is 0.785469, which is quite superior than the result 0.538632 in Jeong et al. [12], 0.512374 in Dong and Huang [8], 0.1329 in Karakaya et al. [14], 0.632558 in Patidar et al. [27], and 0.629806 in Liu et al. [16]. Table 4 shows the p_Value comparisons for the frequency strategy.

To investigate this theory mathematically (using, for example, Mathematica 7) in different parts to determine the best points. If $d = 24, e = 2$ and $v = 2$ are chosen with corresponding constraints $\text{tim}_0 = 0, a^l(0) = 1, a^p(0) = 2, b^l(0) = 3, b^p(0) = 4, g(0) = 5$, the action to take of system (4) includes chaotic attractor (Figs. 12, 13). The operation in Figs. 14 and 15 is intermittent, with $c = 22$.

Fig. 11 $(c, g \text{ (tim)})$

Table 4 Frequency test's p_Value

Methods	p_Value
TLTPM	0.785469
VVTPM Jeong et al. [12]	0.538632
CVTPM Dong and Huang [8]	0.512374
Karakaya et al. [14]	0.1329
Patidar et al. [27]	0.632558
Liu et al. [16]	0.629806

Fig. 12 $a^l \text{ vs. } g \text{ vs. } b^l$

For various learning, weight range, and constant TLTPM size, Table 5 analyzes the synchronization periods of TLTPM and CVTPM methods. When λ increases in all three rules, there is a propensity for the sync step to rise. In the λ range of 5–15, Hebbian takes fewer sync stages than other two rules, but when the λ rises, Hebbian uses more sync steps than the others.

For system (Eq. 3) with a complex parameter $v = v^l + qv^p$, the Lyapunov Exponents and bifurcation diagrams are

Fig. 13 $b^l \text{ vs. } g \text{ vs. } b^p$ Fig. 14 $b^l \text{ vs. } g \text{ vs. } a^p$

recorded and described in Figs. 16, 17, 18, 19, 20 and 21. These figures are depicted with identical parameters in the previous segment's initial conditions, $v = 2 + 3q$. As seen in Fig. 16, ignoring i_4, i_5 the system (Eq. 3) contains hyperchaotic attractor in the interval $[7.6, 19.9]$ and cyclic attractors if $c \in (0, 7.6), (19.9, 30]$. Figure 16 depicts the most remarkable perspective that could be used in this review. The chaotic activity was distorted, and a dynamic parameter was regulated in system (Eq. 3) with the replacement of one of the actual parameters. This illustrates the effect of dynamic parameters on the characteristics and performance of nonlinear dynamic systems. Following Figs. 16, 17, 18, 19, 20 and 21 are the bifurcation graphs for the bifurcation graphs for $c = 16.5, d = 24, e = 2, v = 2 + 3q$.

Fig. 15 a^p vs. b^p vs. b^l

Table 5 TLTPM and CVTPM syncing times are compared

λ Value	TLTPM Sync. period in Hebbian (in Cycle)	CVTPM Sync. period in Hebbian (in Cycle) Dong and Huang [8]
5	311.35	348.16
10	677.18	813.64
15	996.07	1769.57
20	2367.31	2971.04
25	3619.29	4186.59
30	4970.38	5982.41
35	6965.14	7310.37
40	8305.75	8953.50
45	11,013.16	11,207.26
50	14,404.91	14,952.38

Table 6 compares the TLTPM and VVTPM time synchronization approaches using the Random Walk method. The TLTPM, which uses the Random Walk learning algorithm, has a much faster coordinating period than the VVTPM.

The structure in Figs. 22 and 23 are hyperchaotic, and the cyclic attractor in Figs. 24, 25 with identical parameters in initial conditions in the preceding part with $v = 2 + 3q$.

To demonstrate and confirm the proposed scheme's estimate, we compare the CAC's amusement outcomes in two

Fig. 16 i_1, i_2, i_3 (with excluding i_4, i_5) vs. tim

Fig. 17 $(c, a^l \text{ (tim)})$

Fig. 18 $(c, a^p \text{ (tim)})$

Fig. 19 $(c, b^l \text{ (tim)})$

similar chaotic dynamic frameworks (Eq. 26) and (Eq. 27). The frameworks (Eq. 26) and (Eq. 27) with the help of system controller (Eq. 32) are numerically illuminated, and the variables are initialized to $\rho = 23$, $\mu = 6$, $v = 10$. The requirement of the master system, as well as the

Fig. 20 $(c, b^p(\text{tim}))$ Fig. 21 $(c, g(\text{tim}))$ **Table 6** TLTPM and VVTPM syncing times are compared

λ Value	TLTPM Sync. time in random walk (in cycle)	VVTPM Sync. time in random walk (in cycle) Jeong et al. [12]
5	375.81	423.58
10	667.38	729.26
15	1018.43	1158.64
20	1623.72	1789.23
25	2427.57	2598.05
30	3259.30	3364.27
35	4165.08	4847.56
40	4692.01	5398.24
45	6306.65	7389.08
50	7776.93	8784.19

basic state of the slave show ξ , τ , is taken into account.
 $(a_r(0), b_r(0), g_r(0))^T = (1 + 2q, 3 + 4q, 5)^T$,
 $(a_h(0), b_h(0), g_h(0))^T = (-1 - 2q, -3 - 4q, -5)^T$

The courses of action of (Eq. 26) and (Eq. 27) are schemed in Figs. 25, 26, 27 and 28 under different starting conditions, demonstrating that CAC is to ensure proficiency after a period tim. It can be seen by us that each $a_h^m(\text{tim})$, $b_h^m(\text{tim})$ posses a comparative symbol $a_r^p(\text{tim})$, $b_r^p(\text{tim})$ when $a_h^p(\text{tim})$, $b_h^p(\text{tim})$ have an opposite sign of $a_r^m(\text{tim})$, $b_r^m(\text{tim})$. This implies that LS bridges the gap between the hypothetical (Eq. 26) and the real (Eq. 27) framework pieces. While ALS happens among the

Fig. 22 g vs. b^l vs. a^l Fig. 23 b^l vs. g vs. b^p

real slave framework piece (Eq. 26) and the hypothetical fundamental framework part (Eq. 27). As a result, the CAC provides a higher level of unambiguous security in secure communications. CAC is adept within a short time interval, as seen in Figs. 25, 26, 27 and 28.

Figures 29, 30, 31 and 32 depict the CAC mistakes. Clearly, the CAC mistakes s_a^m , s_a^p , s_b^m , s_b^p converge to zero as $\text{tim} \rightarrow \infty$ based on the preceding exschemeatory

Fig. 24 b^l vs. g vs. a^p Fig. 25 b^l vs. a^p vs. b^p Fig. 26 a_r^l (tim) and a_h^p (tim) Fig. 27 a_r^p (tim) and a_h^l (tim) Fig. 28 b_r^l (tim) and b_h^p (tim) Fig. 29 b_r^p (tim) and b_h^l (tim)

considerations. After a small estimate of tim, the errors will approach zero.

Another phenomena are depicted in Figs. 34 and 35, but it does not appear in a wide range of synchronization in written work. In CAC, the attractors of the master and slave frameworks move in opposite or orthogonal directions with a hazy structure, as seen in Figs 34 and 35.

Figures 36, 37, 38 and 39 depict the master system's (Eq. 26) and slave system's module and step failures (Eq. 27). From Figs. 36 and 37, it has been seen that the modules errors $\beta a_r - \beta a_h$, $\beta b_r - \beta b_h$ converge to 0 as $\text{tim} \rightarrow \infty$ while

Fig. 30 e_a^l vs. tim Fig. 31 e_a^p vs. tim Fig. 32 e_b^l vs. tim Fig. 33 e_b^p vs. tim Fig. 34 $(b_r^l(tim), b_h^p(tim))$ vs. $(a_r^p(tim), a_h^l(tim))$ vs. $(a_r^l(tim), a_h^p(tim))$ Fig. 35 $(b_r^p(tim), b_h^l(tim))$ vs. $(a_r^l(tim), a_h^p(tim))$ vs. $(b_r^l(tim), b_h^p(tim))$

the phases' errors are shown in Figs. 38 and 39, which are $\phi a_r - \phi a_h$, $\phi b_r - \phi b_h$, to $\frac{\pi}{2}$ as $tim \rightarrow \infty$.

The Anti-Hebbian harmonizing durations of the TLTPM and TPM-FPGA methods are compared in Table 7. The TLTPM's sync interval is much shorter than the TPM-FPGA's, as shown by the table. The Anti-Hebbian, in com-

Fig. 36 $\beta a_r - \beta a_h$ vs. tim Fig. 37 $\beta b_r - \beta b_h$ vs. tim Fig. 38 $\phi a_r - \phi a_h$ vs. tim

pared to others, takes less time (λ value between 20 and 30).

Conclusion and future scope

The key exchange techniques proposed by Dong and Huang [8] and Jeong et al. [12] were the subject of the first part of this study. Their shortcomings were also stated in this article. Second, this paper has proposed neural network coordination using the 5D hyperchaotic (or chaotic) nonlinear dynamic

Fig. 39 $\phi b_r - \phi b_h$ vs. tim

Table 7 TLTPM and TPM-FPGA sync times are compared

λ Value	TLTPM's Sync period in anti-Hebbian (cycle)	TPM-FPGA's Sync period in anti-Hebbian (cycle) Teodoro et al. [34]
5	385.89	390.35
10	739.34	750.82
15	1085.66	1104.29
20	1623.14	1674.05
25	2393.47	2417.69
30	3152.58	3189.58
35	4412.73	4437.01
40	5728.34	5773.68
45	6690.08	6724.79
50	8725.38	8794.39

complex system to construct the key exchange mechanism to solve the current problems. Third, while there are no complex variables, the properties and components of this system were analyzed, and when there are complex variables, they were studied again. The surprise was that if all of the variables were real, the system had chaotic behavior, but if one of the variables in the complex, the behavior shifted to become hyperchaotic. Fourth, Complex Ant-Coordination (CAC) is a new kind of complex coordination that this paper implement. A definition of CAC is provided for two uncertain chaotic (or hyperchaotic) complex structures. The CAC of two unknown hyperchaotic (or chaotic) nonlinear complex systems is also investigated. CAC provides more transparent protection in secured exchanges. Via various state parameters, the attractors of the master and slaves systems shift in the opposite or anisotropic direction to one another, which is typical of a CAS. This effect did not occur and did not appear in the arrangement with any kind of coordination. Not only does the proposed strategy has the requisite security measures, but it also has a greater level of effectiveness. This article discusses the comprehensive security assessment. Fourth, the agreement's practicality is assessed, and

contemporary CVTPM, TPM-FPGA, and VVTPM methods are compared. Finally, experiments are used to assess the values for τ_1 , τ_2 , τ_3 , N and λ , which emphasize protection against an attacking network. This indicates that two approved TLTPMs would most likely share a secret key in a channel. Finally, the findings show that the proposed approach is a successful key swap over mechanism for IoT devices including both terms of effectiveness and protection. To increase the security of IoT devices in the future, a more comprehensive security review will be performed. Two main aspects would need to be changed in the future. One is to further minimize neuronal coordinating latency, and the other is to execute a fresh neuronal synchronization instead of a long one. A far more extensive investigation of the network's protection is expected in the future.

Compliance with ethical standards

Conflict of interest All authors declare that they have conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abdalrdha ZK, AL-Qinani IH, Abbas FN (2019) Subject review: key generation in different cryptography algorithm. *Int J Sci Res Sci Eng Technol* 6(5):230–240. <https://doi.org/10.32628/ijrsrset196550>
- Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurc Chaos* 16:2129–2151
- Atan Ö, Kutlu F, Castillo O (2020) Intuitionistic fuzzy sliding controller for uncertain hyperchaotic synchronization. *Int J Fuzzy Syst* 22:1430–1443. <https://doi.org/10.1007/s40815-020-00878-x>
- Cao C, Sun K, Liu W (2018) A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Process* 143:122–123
- Casdagli M (1989) Nonlinear prediction of chaotic time series. *Phys Nonlinear Phenom* 35:335–356
- Cho K, Miyano T (2014) Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution. *IEEE Trans Circ Syst Regul Pap* 62:478–487
- Dolecki M, Kozera R (2015) The impact of the TPM weights distribution on network synchronization time. *Comput Inf Syst Ind Manag* 9339:451–460
- Dong T, Huang T (2020) Neural cryptography based on complex-valued neural network. *IEEE Trans Neural Netw Learn Syst* 31(11):4999–5004. <https://doi.org/10.1109/TNNLS.2019.2955165>
- Farhan A, Al-Saidi N, Maolood A, Nazarimehr F, Hussain I (2019) Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder. *Entropy* 21:958
- Farhan A, Ali R, Natiq H, Al-Saidi N (2019) A new S-box generation algorithm based on multistability behavior of a plasma perturbation model. *IEEE Access* 7:124914–124924
- Hadke PP, Kale SG (2016) Use of neural networks in cryptography: a review. In: *Proceedings of the 2016 world conference on futuristic trends in research and innovation for social welfare (Startup Conclave)*, pp 1–4
- Jeong S, Park C, Hong D, Seo C, Jho N (2021) Neural cryptography based on generalized tree parity machine for real-life systems. *Secur Commun Netw*. <https://doi.org/10.1155/2021/6680782>
- Jo M, Jangirala S, Das AK, Li X, Khan MK (2020) Designing anonymous signature-based authenticated key exchange scheme for IoT-enabled smart grid systems. *IEEE Trans Ind Inform*. <https://doi.org/10.1109/TII.2020.3011849>
- Karakaya B, Gülden A, Frasca M (2019) A true random bit generator based on a memristive chaotic circuit: analysis, design and FPGA implementation. *Chaos Solitons Fractals* 119:143–149
- Kou J, He M, Xiong L, Ge Z, Xie G (2020) Efficient hierarchical multi-server authentication protocol for mobile cloud computing. *Comput Mater Contin* 64(1):297–312. <https://doi.org/10.32604/cmc.2020.09758>
- Liu L, Miao S, Hu H, Deng Y (2016) Pseudo-random bit generator based on non-stationary logistic maps. *IET Inf Secur* 2(10):87–94
- Liu P, Zeng Z, Wang J (2019) Global synchronization of coupled fractional-order recurrent neural networks. *IEEE Trans Neural Netw Learn Syst* 30(8):2358–2368
- Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y (2020) Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans Ind Inf* 16(6):4177–4186
- Makkar A, Garg S, Kumar N, Hossain MS, Ghoneim A, Alrashed M (2021) An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans Ind Inf* 17(2):903–912. <https://doi.org/10.1109/TII.2020.2968927>
- Mehic M, Niemiec H, Siljak M, Voznak (2020) Error reconciliation in quantum key distribution protocols. In: *Proceedings of the international conference on reversible computation*, pp 222–236
- Moysis L, Tutueva A, Volos C, Butusov D, Munoz-Pacheco J, Nistazakis H (2020) A two-parameter modified logistic map and its application to random bit generation. *Symmetry* 12:829
- Natiq H, Banerjee S, He S, Said M, Kilicman A (2018) Designing an M-dimensional nonlinear model for producing hyperchaos. *Chaos Solitons Fractals* 114:506–515
- Natiq H, Banerjee S, Ariffin M, Said M (2019) Can hyperchaotic maps with high complexity produce multistability? *Chaos Interdiscip J Nonlinear Sci* 29:011103
- Natiq H, Banerjee S, Said M (2019) Cosine chaotification technique to enhance chaos and complexity of discrete systems. *Eur Phys J Spec Top* 228:185–194
- Natiq H, Said M, Al-Saidi N, Kilicman A (2019) Dynamics and complexity of a new 4d chaotic laser system. *Entropy* 21:34
- NIST (2020) NIST statistical test. http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html
- Patidar V, Sud KK, Pareek NK (2009) A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica* 33:441–452
- Pecora LM, Carroll TL (1990) Synchronization in chaotic systems. *Phys Rev Lett* 64:8. <https://doi.org/10.1103/PhysRevLett.64.821>
- Protic D (2016) Neural cryptography. *Vojnotehnicki Glasnik* 64(2):483–495. <https://doi.org/10.5937/vojtehg64-8877>

30. Rehan M (2013) Synchronization and anti-synchronization of chaotic oscillators under input saturation. *Appl Math Modell* 37(10):6829–6837. <https://doi.org/10.1016/j.apm.2013.02.023>
31. Sarkar A (2019) Multilayer neural network synchronized secured session key based encryption in wireless communication. *Int J Artif Intell* 8(1):44–53
32. Sarkar A, Mandal J (2012) Swarm intelligence based faster public-key cryptography in wireless communication (SIFPKC). *Int J Comput Sci Eng Technol* 3(7):267–273
33. Shishniashvili E, Mamisashvili L, Mirtskhulava L (2020) Enhancing IoT security using multi-layer feedforward neural network with tree parity machine elements. *Int J Simul Syst Sci Technol* 21(2):371–383. <https://doi.org/10.5013/ijssst.a.21.02.37>
34. Teodoro A, Gomes O, Saadi M (2021) An FPGA-based performance evaluation of artificial neural network architecture algorithm for IoT. *Wirel Pers Commun*. <https://doi.org/10.1007/s11277-021-08566-1>
35. Tunç, Osman, Atan, Özkan, Tunç, Cemil, Yao, Jen-Chih (2021) Qualitative analyses of integro-fractional differential equations with caputo derivatives and retardations via the Lyapunov–Razumikhin method. *Axioms* 10:2. <https://doi.org/10.3390/axioms10020058>, <https://www.mdpi.com/2075-1680/10/2/58>
36. Viet-Thanh P, Ali D, Al-Saidi N, Rajagopal K, Alsaadi F, Jafari S (2020) A novel mega-stable chaotic circuit. *Radioengineering* 29:141
37. Waqas M, Tu S, Rehman SU, Halim Z, Anwar S, Abbas G, Abbas ZH, Rehman OU (2020) Authentication of vehicles and road side units in intelligent transportation system. *Comput Mater Contin* 64:1. <https://doi.org/10.32604/cmc.2020.09821>
38. Yan L, Zhang S, Chang Y, Sun Z, Sheng Z (2020) Quantum secure direct communication protocol with mutual authentication based on single photons and bell states. *Comput Mater Contin* 63(3):1297–1307. <https://doi.org/10.32604/cmc.2020.09873>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.