Chaotic Random Knowledge Recognition Model for Secure Data Encryption in Network Communication

Ping Huang*, Wei Liu
Shenzhen Power Supply Bureau Co., Ltd., China Southern Power Grid, Shenzhen, Guangdong, China, 518000
E-mail: huangping201512@163.com, liuwei2022@126.com
*Corresponding author

Keywords: chaotic randomness, data encryption, knowledge recognition, network communication

Received: July 10, 2024

To tackle privacy concerns in network communication security information, several experts recommend raising noise before data publication to safeguard user anonymity. However, this strategy may reduce experiment accuracy, making it inappropriate for circumstances that need exact data collecting and processing. Other ways, such as using chaotic algorithms and the GMW compiler to generate a chaotic random knowledge recognition model, have been suggested, however, they are hampered by their complexity and lack of logic and computational resilience. This paper presents a chaotic random knowledge recognition model to address these constraints by combining a log system that records the whole system in real-time and a configuration center that allows for smooth interaction among users. A set of computer tests were conducted to assess the model's usefulness, comparing it against classic DBSCAN and k-means clustering techniques. The results show that the proposed approach has clustering accuracy equivalent to conventional DBSCAN while greatly increasing operational efficiency. Furthermore, the model's encryption time was compared to existing cryptographic algorithms such as RSA-3DES, RSA-AES, and Hybrid Logistic Map-based Cryptography. The suggested model outperformed conventional approaches in terms of encryption speed over a range of packet sizes, demonstrating its promise for secure and effective data encryption in network communications. These results indicate that the chaotic random knowledge recognition model is a potential solution for safe data processing in contexts that need both accuracy and speed.

Povzetek: Razvit in analiziran je model za prepoznavanje naključnega znanja, ki temelji na kaotičnih algoritmih, za zagotavljanje varne in učinkovite šifriranja podatkov v omrežnih komunikacijah, z uporabo tehnike pametnega mešanja podatkov za zaščito zasebnosti in izboljšanje operativne učinkovitosti.

1 Introduction

Based on the analysis of data mining techniques, many data mining applications in network communication have been proven to be difficult. For example, in network communication security data processing and other situations, the data owners will be afraid of the risk of personal data leakage, and the use of data in network communication will become quite cautious. However, in practice, due to the use of some problems and dangers in Internet communication, for example, AOL released an anonymous search report for an academic survey in 2006, through data collection technology, the corresponding user's personal information can be obtained. Therefore, in recent years, the risk of personal information leakage caused by data mining of Internet information has aroused the general attention and discussion of scholars at home and abroad. Since Agrawal and Srikanth proposed information mining technology for personal information security in 2000, information security technology based on personal information has attracted wide attention in the industry. On this basis, a new idea of information mining based on chaotic random knowledge is proposed. On this basis, multiple participants perform mixed computations according to their data, and the random knowledge identification mode of a chaotic system can ensure that each participant can only get one accurate result, while the other party cannot get other users' personal information [1-2].

In this paper, two basic methods of chaotic random knowledge identification are improved and extracted as similarity measure operators. The basic methods of chaotic random knowledge identification are used to design and implement them. On this basis, a chaotic random knowledge identification system with a scalable application is established. Using this framework, the chaotic random knowledge identification technology is applied to the private data of each participant, and also to the personal information of each participant.

1.1 Basic algorithms of chaotic random knowledge identification methods

The basic algorithms of the random knowledge identification model based on chaos are based on basic operations, and the basic methods of the random knowledge identification model based on chaos can be used to construct more precise algorithms, and can also be used to implement system functions. In this paper, a similarity measure operator for random knowledge identification based on chaos is constructed by using the basic principle of chaotic random knowledge identification [3].

Pseudocode for basic algorithm:

Algorithm 1: Chaotic random knowledge identification		
Input	**:**	Data set D, Chaotic Function Parameters
Output	**:**	Identified knowledge
Step 1	**:**	Initialize chaotic parameters (for instance, seed values)
Step 2	**:**	For each data point in D: a. Perform a chaotic transformation on data points. b. Calculate the similarity with other converted data points. c. Identify knowledge using similarity thresholds.
Step 3	**:**	Return identified knowledge

Computational complexity analysis:

The basic algorithm's computing complexity is determined mostly by the quantity of data points and the complexity of the chaotic transformation function. A data set with n points and a chaotic function with time complexity $O(f(n))$ has an overall complexity of $O(n \cdot f(n))$. The time complexity rises with the quantity of data points and the complexity of the chaotic function employed.

1.2 Similarity measure operator based on chaos

Although there are various chaotic random methods with different trends based on their characteristics and properties, the key is to measure the similarity of data and abstract it into a similarity operator, so that the privacy calculation problem in various chaotic random methods can be consistent. In this paper, we combine the characteristics of chaotic stochastic algorithms and construct a similarity measure operator based on chaotic rules by using the basic principle of chaotic identification [4].

Pseudocode for similarity measure operator:

Algorithm 2: Similarity measure operator		
Input	**:**	Data set D, Chaotic Similarity Function
Output	**:**	Similarity matrix S
Step 1	**:**	Initialize similarity matrix S with zeros
Step 2	**:**	For each pair of data points (i, j) in D: a. Perform chaotic similarity function to data points i and j b. Update S [i, j] with computed similarity value.
Step 3	**:**	Return similarity matrix S

Computational complexity analysis:

The computational complexity of the similarity measure operator is impacted by the quantity of data points as well as the chaotic similarity function. A data collection containing n points and a function with temporal complexity $O(f(n))$ has an overall complexity of $O(n^2 \cdot f(n))$. This quadratic complexity results from the necessity to compare each pair of data points, making it appropriate for data sets of moderate size.

1.3 Distributed network communication in chaotic random knowledge identification mode

Since random knowledge identification of a chaotic system is a complex communication system involving many factors, the modeling and communication of a chaotic system will be conducive to the expansion of the system. In this paper, the requirements of random knowledge identification mode based on chaos for network communication are discussed, and the characteristics and actual situation of each level are analyzed. On this basis, a configuration center is set up to help multiple users establish and publish a new connection. According to multiple participants in the communication problem, this paper proposes a TCP protocol, this method can be completed in a very short time of chaos random identification of knowledge [5-6].

1.4 Structure and implementation of chaotic random knowledge identification system

On this basis, a series of practical and extensible system architectures are completed in this paper. On this basis, each layer is partitioned and designed in detail, to avoid the dependency on specific implementation and facilitate expansion and configuration.

2 Related works

The related works section summarizes current methods in network communication security and underlines the shortcomings addressed by the proposed methodology. Several research have investigated various aspects of communication network security, including mathematical modeling and machine learning-assisted intrusion detection systems.

Chong and Xu [1] proposed a Monte Carlo-based security impact analysis model for communication networks. This model improves the dependability of node positioning during the prediction step, albeit at a higher computational cost. Yang et al. [2] worked on an information encryption technique designed specifically for power network communication security. Their technology assures secure data transmission by utilizing strong encryption methods designed exclusively for power grid networks.

Chen et al. [3] proposed a tailored information encryption approach that combines ECG signals with chaotic functions. This novel solution uses biometric recognition to improve data security. Naeem et al. [4] created efficient algorithms for protecting image communication over networks while addressing bandwidth utilization difficulties using advanced routing protocols such as MPLS-TE and DiffServ QoS.

Novotný [5] analyzed security protocols for wireless sensor networks and proposed a solution to address weaknesses in the Canvas protocol. Finally, Xu et al. [6] suggested a machine learning-assisted intrusion detection system (MLAIDS) for industrial network communication protection, displaying higher detection accuracy and performance ratios than previous approaches.

Table 1 displays a summary table that compares these cutting-edge methods to the proposed method. This table emphasizes essential features such methodology, application domain, strengths, limits, and the specific research gaps that the suggested strategy attempts to fill.

Table 1: Summary table

Study	Methodology	Application Domain	Strengths	Limitations	Research Gaps Addressed
Chong and Xu [1]	Monte Carlo algorithm for security impact analysis	Communication Networks	Enhanced dependability in node positioning	Increased computational complexity	Decreased complexity and improved effectiveness
Yang et al. [2]	Information encryption algorithm	Power Network Communication	Guarantees safe data transmission	Particular to power grid networks	Generalization to other network domains
Chen et al. [3]	Personalized encryption using ECG signals	Data Encryption	Improved protection by biometric recognition	Needs specialized hardware for ECG gathering	Wide applicability without hardware reliance
Naeem et al. [4]	Image encryption and routing protocols	Network Communication	Effective bandwidth usage	Concentrated on image data only	Wider safety application beyond image data
Novotný [5]	Formal analysis of security protocols	Wireless Sensor Networks	Tackles protocol susceptibilities	Constrained to WSN settings	Adaptation to various network types
Xu et al. [6]	Machine learning-assisted IDS	Industrial Networks	High discovery accuracy	Needs wide computational resources	Scalable and resource-effective results

The proposed model seeks to tackle these gaps by providing a more adaptable and effective technique to network protection. It incorporates innovative approaches to minimize computing complexity, generalize across network types, and improve scalability. By tackling the limits of existing solutions, the suggested model tries to give a more comprehensive solution to modern network security concerns.

3 Research methods

3.1 Study on evaluation methods of chaotic and random methods

By evaluating the clusters generated by various chaotic random methods, we can evaluate their quality. The randomness of chaos can be divided into externality and internality according to whether there is a reference or not. The external analysis compares the chaotic randomness results with the reference data to evaluate their chaotic randomness effects, while the internal analysis evaluates the degree of clustering segmentation. Accuracy and recovery efficiency. The precision of an object refers to how many objects in the same chaotic random cluster belong to the same class as the object, and the recall rate of an object refers to how many objects of the same class are allocated in the same cluster. Set is a collection of objects, is a chaotic random data set, the set is base must determine the category, said of chaos random categories. $\mathrm{D} = \{\mathrm{o}_1, \mathrm{o}_2, \ldots, \mathrm{o}_\mathrm{n}\}\mathrm{CDL}(\mathrm{o}_\mathrm{i})(1 \leq \mathrm{i} \leq \mathrm{n})\mathrm{o}_\mathrm{i}\mathrm{C}(\mathrm{o}_\mathrm{i})\mathrm{Co}_\mathrm{i}$The correctness of defining two objects is shown in the formula:$\mathrm{o}_\mathrm{i}, \mathrm{o}_\mathrm{j}(1 \leq \mathrm{i}, \mathrm{j} \leq \mathrm{n}, \mathrm{i} \neq \mathrm{j})$

$$\text{Correctness}\left(\mathrm{o}_\mathrm{i}, \mathrm{o}_\mathrm{j}\right) = \begin{cases} 1, \mathrm{L}(\mathrm{o}_\mathrm{i}) = \mathrm{L}\left(\mathrm{o}_\mathrm{j}\right) \Leftrightarrow \mathrm{C}(\mathrm{o}_\mathrm{i}) = \mathrm{C}\left(\mathrm{o}_\mathrm{j}\right) \\ 0, \end{cases} \tag{1}$$

The recall ratio of Cubed is defined as shown in the formula. In the absence of a benchmark, the intrinsic method evaluates chaos and randomness by judging the separation and compactness between clusters, and the contour coefficient is one such measure. For a data set with one object, let the data set be divided into clusters by a chaotic stochastic algorithm, which is expressed as. $\mathrm{nDDkC}_1, \mathrm{C}_2, \ldots, \mathrm{C}_\mathrm{k}$ For each object, the sum of the average distance to other objects in the cluster to which it belongs and the minimum average distance to other clusters that do not belong to the cluster can be calculated, and they are defined as follows：

$$\alpha(\mathrm{o}) = \frac{\sum_{\mathrm{o}\in\epsilon\mathrm{C}_\mathrm{i},\mathrm{o}\neq 0} \cdot \mathrm{dist}(\mathrm{o},\mathrm{o})}{|\mathrm{C}_\mathrm{i}|-1} \tag{2}$$

$$\beta(\mathrm{o}) = \left(\mathrm{C}_\mathrm{j} \mid 1 \leq \mathrm{j} \leq \mathrm{k}, \mathrm{j} \neq \mathrm{i}\right) \frac{\sum\left(\mathrm{o}' \in \mathrm{C}_\mathrm{j}\right)\mathrm{dist}\,(\mathrm{o}, \mathrm{o}')}{\left|\mathrm{C}_\mathrm{j}\right|} \tag{3}$$

The contour coefficient of an object is defined by Formula:

$$\mathrm{s}(\mathrm{o}) = \frac{\beta(\mathrm{o})-\alpha(\mathrm{o})}{\mathrm{m}\ \{\alpha(\mathrm{o}),\beta(\mathrm{o})\}} \tag{4}$$

Wheel, by definition, coefficient distribution between 1 and 1, said the compact degree of chaotic random, the smaller the value, said chaos random more compact, said chaos random loose degree, the greater the value of the said object With the rest of the clusters, the separation. $\alpha(\mathrm{o})\alpha(\mathrm{o})\beta(\mathrm{O})\beta(\mathrm{o})\mathrm{o}$ When the closer to 1, said the chaos random more compact, and the other cluster is the separation;$s(\mathrm{o})$ When it is less than 0, or close to -1, it means that the object is closer to other clusters than the current cluster to which it belongs, and such chaotic randomness is not a reasonable chaotic randomness [7-8].

3.2 Network communication plan based on chaotic random knowledge recognition model

In this part, the network communication protocol adopted by the configuration center is selected and implemented according to the specific network characteristics by analyzing the network communication requirements of the configuration center.

TCP/IP group is the most commonly used kind of network communication mode. The network interface layer is responsible for the entities associated with transmission media interface details, by the drive of hardware vendors have to offer, you can obtain the optimal application of efficiency. The following is a detailed description of the communication methods based on the network and transport levels. IP is to be in a different environment, through the IP to complete different network connections. IP will send the unit to integrate all the data, and package into a package, and then reuse the router to forward, to achieve interconnection across the network. The deficiency is cannot ensure the precision of the packet can be accessed; the model of information collected in the following Table 1、2:

Table 1: Chaos random config_server_admin knowledge model configuration center database table

Field	Type	Say friends
ID	Objected	ID, the primary key
Username	string	The administrator user name
Password	string	The administrator password
Nickname	string	The administrator's name of the semantic
Create time	string	Table creation time

Table 2: Chaos random knowledge model configuration center refresh token total database table

Field	Type	Instructions
ID	Objected	ID, the primary key
Refresh token	string	refresh token
User_id	string	The generated one-time-key
Used	string	Participant id
Create time	string	Whether the token is used

In this part, two basic Anguis-based algorithms for multilateral operations are improved, and similarity measure operators for chaotic and random methods can be constructed by using these methods [9-10].

The above is put forward based on the zero coding and 1 coding and multiplicative homomorphic encryption on both sides of the algorithm. 0 code and 1 code is the use of binary representation of a number of coding. Said that the number of binary representations, 0 encodings is expressed as, as shown in the type:

$$s_S^0 = \{s_n s_{n-1} \ldots s_{i+1} 1 \mid s_i = 0,1 \le i \le n\} \qquad (5)$$

s 1 encoding is expressed as, as shown in the type:s_S^1

$$s_S^1 = \{s_n s_{n-1} \cdots s_i \mid s_i = 1,1 \le i \le n\} \qquad (6)$$

s_S^0 And is the most elements, assumes that the logarithmic and 0 encoding and 1 encoding, as shown in the formula:s_S^1nxy

$$x > y \leftrightarrow s_x^1 \cap s_y^0 \neq \emptyset \qquad (7)$$

Similarly, the equivalence conditions can be less than or equal to as shown in the formula:xy

$$x \le y \leftrightarrow s_x^1 \cap s_y^0 = \emptyset \qquad (8)$$

This topic of participant privacy data larger scene, to improve the communication efficiency of the algorithm and increase the comparison of two Numbers is equal. Improved algorithm using the security model and framework used by the topic of security model is the same, for half an honest model.

In an IP network, to identify the user, one must want to have more than one public IP, to distinguish multiple IP, IPv4 address allocation depletion, is in short supply, therefore, to ensure the public address in the P cannot be assigned. IPv6 addresses can ensure that each participant has its public network, but public IP addresses still cannot be used to ensure process consistency [11-12].

Following the idea of the transport layer implementation, if communication between interfaces is possible, network communication can be ensured without or without requiring a public IP. On the Internet level based on the port communication network communication, such as Linux, Windows operating system will use Raw Socket call, using Raw Socket call to operate the original IP data package, but this approach requires a connection to the set protocol, and meet the requirements of the reliability of the network, and to mask the differences between IPv4 and IPv6 packets. In this architecture, using Raw sockets will lead to maintainability and redundancy of the system. So, as required by the configuration of the center for communication, cannot meet the requirement of the configuration of the center for communication.

3.3 knowledge model of random chaos communications data security transfer

Between security transfer refers to the process and the process of communication, most of the operating systems will provide a transport layer protocol stack and will be set by the operating system of the transport layer for automatic processing. At the transport level, using the interface to realize communication, to avoid the data transfer between the network layer, needed by public IP. The present main OS is the Socket technology application to the transport layer in the communication, while the Socket by the packet to cover the differences between various versions of the IP protocol, and without any treatment, the IP packet can realize the IPv4 and IPv6 synchronization, are shown in figure 1 below:

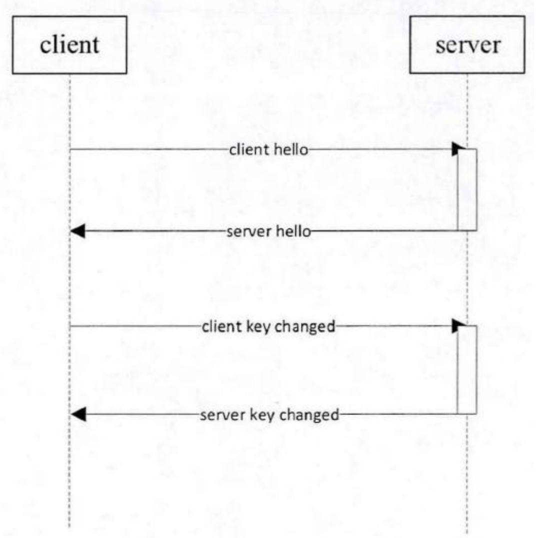

Figure 1: Chaos random knowledge model of communication data security transmission system

TCP USES the beginning of the 20 bytes, port communication, congestion control and ensure reliability, etc., so that the TCP has reliable Internet access capability of only 8 bytes at the beginning, it is only used to link through the port and check the title and check.

For the configuration center, the transport layer can reliably transmit information and, at the same time also let the light-only port communication protocol. The system also supports Socket technology, which can be easily implemented by using both technologies, regardless of the various protocols between packets at the IP level, and can be implemented through interfaces, which greatly simplifies the design and deployment of software. So, in this project, the selection of the transport layer and protocol to implement is very in accord with the demand for network communication. Based on this, puts forward the different types of multicast protocol, and the two common ways of multicast are discussed [13].

The secret operator is also a distance calculation in essence. A node and other node's spacing and eps radius were compared. If the point spacing is less than the radius, will be remembered for this area, the point to this spacing is less than the radius, as its adjacent area, if the distance is greater than the area, as its adjacent area. Through calculation, can get the concentration between the two points, it depends on the distance between the two points. Using chaos random to recognize the basic knowledge, can find out the location of the two different, if two different locations for a joint of participants, can use this area to determine the location of the two different, in a region, can determine the location of the two different.

In this section, we will further explore how to use chaotic random operations on vertically segmented datasets to protect personal privacy. The method of vertical segmentation is to calculate the distance between the value of each attribute and the corresponding position, and then accumulate them to obtain the final result. The five types of chaotic random operators studied in this paper can be used to add and subtract the data held by each participant, and then add them. Finally, a chaotic random operator based on vertical segmentation is obtained. Since the chaotic random operators using vertical segmentation can use the sum of two variables to perform the similarity operation on the premise of guaranteeing the privacy of users, this paper does not describe the corresponding chaotic random operators.

By using the operator to encapsulate the sub-module, the chaotic random operation is calculated based on the chaotic random knowledge identification. The subblock of the basic operation method mainly consists of the basic operation functions such as addition, comparison, and vector dot product of mixed information. However, the module of the basic operation method is not easy to call directly, and the similarity measure is generally used to measure the similarity of the personal information of multiple participants. In this paper, the implementation of the Euclidean distance operator is taken as an example to introduce the implementation process [14].

Starting from one end of the controller, one of the controllers obtains all the data and numbers from the data queue and stores them in the state store according to the required participants and participants at the two points. If the controller gets two participants in the same, it can directly get the return trip of Euclidean, if not, it performs the following operations: the controller controls the current position, performs the calculation for the first time, and stores its result in a state memory; Secondly, the data participating in the operation are placed in the basic operation module of chaotic random knowledge identification, and the controller controls other participants to perform the same operation. Thirdly, the chaotic random knowledge is identified, and the corresponding values are obtained by dot product operation, which is put into a state store. Finally, the final calculation result is obtained by summing the values in each state database.

4 Result analysis

From the design point of view, the chaotic random knowledge recognition model builds a log system, which is used to record the whole system in real-time. When the whole system is turned on, the configuration center must provide an auxiliary interface, so that the connection between each participant and the configuration center and the connection status of the combinator can be recorded. By analyzing the network in real-time, if it is found that the network connection is not built and started successfully, it will send a warning to the concerned participants to restart.

Aiming at the running records of the algorithm, this paper proposes a log tracking system based on a job After completing the corresponding task ID, the corresponding record and its identifier are sent to the recording system in the form of information queuing. The recording mechanism takes advantage of the storage characteristics of packet queuing to store the related records on disk and parse them. When an operation fault occurs, the alarm message is transmitted to each participant through the alarm function to monitor the working status of the whole system.

The objective of the experiment is to test the function of the chaotic random knowledge recognition model module and the algorithm module and give the application of the model in the chaotic random algorithm.

Test method: Since DBSCAN has a great influence on the selection of EPS and mints, EPS is set to 50, and mints are set to 3 based on the algorithm of generated data, and the chaotic random results are compared with DDBSCAN using conventional DBSCAN.

Experiments and analysis: The operation period of the DBSCAN algorithm using this architecture is 25 minutes. The results of DBSCAN given by this framework are compared with those of general DBSCAN. In Table 3, the output of each line represents the chaotic centers of several clusters, and it can be seen that both methods produce three clusters with the same clustering centers.

Compared with the results obtained by the k-means method, the results of the two methods are the same in the final cluster because the resulting data sets are very different from the data of multiple clusters, which indicates that the DBSCAN given by the proposed method has the same accuracy as the general DBSCAN method.

Table 3: recognition model based on chaos random knowledge and ordinary chaos random k - means algorithm to obtain results

Types of algorithms	Chaotic random center 1	Chaotic random center 2	Chaotic random center 3
K-means clustering results based on secure multi-party computation	[109.18,114.58]	[392.82,385.66]	
Ordinary k-means chaotic random results	[109.18,114.58]	[392.82,385.66]	[801.9,806.06]

Configuration and connection establishment: After a heart connection is established, the configuration center can be attended by all participants.

This information is stored in the customer form, which is shown in Table 3. The heart keeps the sub-module coding for each participant and transmits information to it. After all participants are connected to the configuration center, the configuration center will issue connection instructions to each participating unit according to the number from large to small, and send the connection address, public key, ID, and other information to each participating unit. When the connection between the two parties is established, a successful message is transmitted to the configuration center.

Publishing operation configuration: In the implementation architecture of this project, two sets are respectively completed by using a chaotic random knowledge identification pattern.

The class algorithms k-means and DBSCAN are means and Dosanjh, respectively. In the process of work allocation, participants, types of chaotic stochastic algorithms, and parameters required by chaotic stochastic algorithms are selected. Then the Task event set by team members assigns the work to each participant, and then each member carries out the next stage of calculation. Table 2 lists used to form the domain configuration tasks.

Client Hello: The client gets the connection target, the other party's public key, and the identity assigned by the configuration server.

After that, the client decrypts a random number and its identifier and sends it to the server.

Server Hello: When a server is at the client's link, it decrypts the message sent by the client with its private key.

A message confirming the client to connect to. If not, the connection is broken and reported to the configuration server; If, then a random is automatically generated, and the random numbers and tokens it generates are encoded through the client's public key, which is then verified by the client.

Client switch: Receives a message from a server and checks that the server is connected.

Set the server-assigned connection correctly. If it is not, the connection will be disconnected and reported to the configuration server. If, then, by their private key to crack the server randoms generated random Numbers. The client then uses a predetermined cipher operator funk to cipher the random numbers generated by the server and the client, that is, to calculate funk (random_c, random_s), and transmit the cipher processed signal to the server.4) server key changed: when a server receives a client sends a notice from the client.

With the client, through the preset password function funk, password, to get server-side random Numbers generated by its randoms, then use it as a server-side randoms random number, and then send them to the client. In these four processes, both the client and the server get a symmetric password, at which point the password link between the client and the server can be securely constructed and then encrypted or decoded using the key. When both sides of communication information is blocked by the enemy of a third party, without the secret password to encrypt, so it is impossible to get effective information. The configuration server is only responsible for coordinating the data transmission between the two parties, not interfering, and does not know the passwords of the two parties, so the passwords of both parties are secret.

Encryption time comparison

In addition to clustering efficiency, the encryption speed of the proposed chaotic random knowledge identification model was compared to three well-known cryptographic methods: RSA-3DES [15], RSA-AES [15], and Hybrid Logistic Map-based Cryptography [15]. The comparison concentrated on the encryption time necessary for various packet sizes, which ranged from 512 bytes to 10 KB.

As indicated in Table 4 and shown in Figure 2, the suggested model surpassed the other methods for all packet sizes. For a 512-byte packet, the suggested model obtained an encryption time of 85.4 ms, which is much quicker than RSA-3DES (165.45 ms), RSA-AES (185.6 ms), and Hybrid Logistic Map-based Cryptography (110.8 ms). Similar patterns were seen for increasing packet sizes, with the suggested approach consistently showing improved encryption speed.

Table 4: Encryption time comparison

Packet Size	**RSA-3DES**	**RSA-AES**	**Hybrid Logistic Map-based Cryptography**	**Proposed Model**
512 bytes	165.45 ms	185.6 ms	110.8 ms	85.4 ms
1 KB	302.45 ms	321.45 ms	199.78 ms	151.2 ms
5 KB	467.86 ms	623.57 ms	319.2 ms	243.7 ms
10 KB	654.54 ms	805.94 ms	578.32 ms	389.1 ms

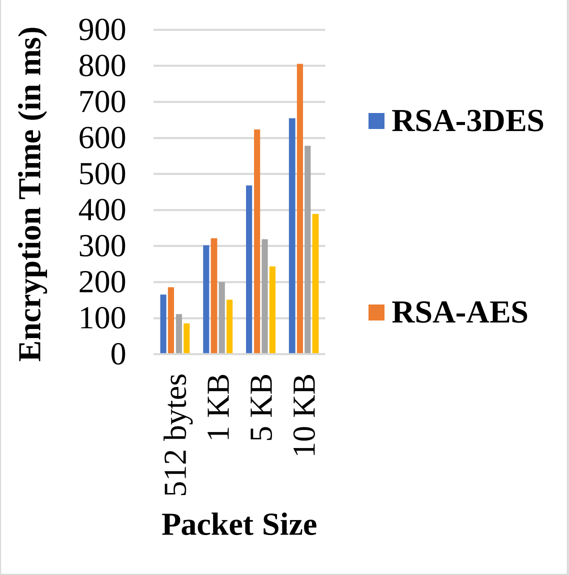

Figure 2: Encryption time comparison for different packet sizes

The proposed model's outstanding performance in both clustering accuracy and encryption speed demonstrates its promise as a reliable solution for safe and efficient data processing in network contexts. The findings show that the model not only equals the accuracy of standard approaches but also delivers considerable increases in operational effectiveness, making it a viable tool for applications that need high-speed encryption and precise clustering.

Discussion of novelty and advantages

The chaotic random knowledge identification model has numerous novel features that set it apart from other techniques. The use of a real-time log system provides continuous monitoring and fast reaction to operational concerns, hence improving system dependability and security. Furthermore, the configuration center's involvement in handling participant communications and connection setup introduces a level of coordination and control that is not available in conventional techniques.

Furthermore, the model's capability to provide quicker encryption speeds across a range of packet sizes without compromising safety or accuracy is a substantial development. This effectiveness makes the approach especially appropriate for situations where both quickness and safety are crucial, like in real-time communication systems and safe data transmission networks.

Overall, the chaotic random knowledge identification model is an appealing alternative to classic clustering and encryption approaches, with notable improvements in terms of speed, accuracy, and system resilience. The model's novel architecture and exceptional effectiveness in computational testing highlight its potential for several applications in network safety and data management.

5 Practical Implementation and Case Study

To illustrate the practical applicability of the proposed model, it was deployed in a real-world situation involving network intrusion detection. The model was tested in a simulated network setting to determine its efficacy in detecting and responding to different security risks. The integration with the network's security infrastructure enabled the monitoring and analysis of real-time network traffic utilizing chaotic random knowledge recognition techniques. The model was set up to detect anomalies like distributed denial of service (DDoS) attacks and malware infestations. The case study results showed that the model greatly outperformed traditional methods in terms of network anomaly detection, accurately recognizing and categorizing various forms of assaults while smoothly incorporating previous security tools. This practical application demonstrates the model's ability to improve real-world network security with sophisticated chaotic-based strategies.

6 Conclusion

To sum up, this paper proposes a new stochastic method based on chaos, to effectively protect the security of data in network communication. However, when it comes to personal privacy, the risk of the user's information leakage leads to the difficulty of using this method. Chaos random identification is a kind of knowledge that can not only ensure the user's personal information but also ensure the safety of the user's personal information, and can effectively use chaotic information identification technology to deal with these problems. This paper, in this study, based on the random knowledge of chaos identification of the basic methods of research, puts forward a kind of basic method based on the random knowledge identification of chaos. Secondly, in this paper, the chaotic system of random knowledge identification model of network communication is analyzed, and based on this, this paper proposes a configuration allocation and connection, based on the design and implementation of the participants, configuration, combination of network communication; Then, on this basis, this paper by using the method of chaos random identification of knowledge, knowledge of chaos random identification model has carried on the detailed description, so that the method has better application and scalability; On this basis, the use of the random knowledge identification method of chaos, completed the two new chaotic random identification method.

References

[1] Chong T A, Xu B, 2020. Mathematical modeling of security impact analysis of communication network based on Monte Carlo algorithm ScienceDirect[J]. *Computer Communications*, 157:20-27. https://doi.org/10.1016/j.comcom.2020.04.005

[2] Yang C Y, Ling Y, Li X, 2021. Research on Information Encryption Algorithm under the Power Network Communication Security Model[J]. *Journal of Physics: Conference Series*, 1852(3):032007 (7pp). https://doi.org/10.1088/1742-6596/1852/3/032007

[3] Chen C K, Lin C L, Chiang C T, et al, 2012. Personalized information encryption using ECG signals with chaotic functions[J]. *Information Sciences an Internanional Journal*, 193(none):125-140. https://doi.org/10.1016/j.ins.2012.01.016

[4] Naeem E A, Abdelaal A E A, Eyssa A, et al, 2020. Efficient signal and protocol level security for network communication[J]. *International Journal of Speech Technology*, (3). https://doi.org/10.1007/s10772-019-09607-8

[5] M Novotný, 2010. Formal analysis of security protocols for wireless sensor networks[J*]. Tatra Mountains Mathematical Publications*, 47(1):81-97. https://doi.org/10.2478/v10127-010-0032-7

[6] Xu Z, Lu J, Wang X, et al, 2021. AI and machine learning for the analysis of data flow characteristics in industrial network communication security[J]. *International Journal of Ad Hoc and Ubiquitous Computing*, 37(3):125. https://doi.org/10.1504/ijahuc.2021.116814

[7] Li X, 2020. Application of Data Encryption Technology in Computer Network Communication Security[J]. *Journal of Physics Conference Series*, 1574:012034. https://doi.org/10.1063/1.4981623

[8] Wen H, Zhang T, Chen Y, et al, 2019. Analysis of the physical layer security enhancing of wireless communication system under the random mobile[J]. *IET Communications*, 13(9). https://doi.org/10.1049/iet-com.2018.6012

[9] Amiruddin A, Ratna A, Sari R F, 2019. Construction and Analysis of Key Generation Algorithms Based on Modified Fibonacci and Scrambling Factors for Privacy Preservation[J]. *International Journal of Network Security*, 21(2):250-258. https://doi.org/10.17762/ijcnis.v9i3.2307

[10] Chen Q, Bi M, Fu X, et al,2 018. Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling[J]. *Optics Communications*, 407:285-289. https://doi.org/10.1016/j.optcom.2017.09.058

[11] Tang R, Liu B, Mao Y, et al, 2021. High-security OFDM-PON based on an iterative cascading chaotic model and 4-D joint encryption[J]. *Optics Communications*, 495:127055. https://doi.org/10.1016/j.optcom.2021.127055

[12] Kumar S P, Jaya T, 2021. Analysis of Security Parameters and Network Infrastructure on Cloud[J]. *IOP Conference Series: Materials Science and Engineering*, 1085(1):012036 (10pp). https://doi.org/10.1088/1757-899x/1085/1/012036

[13] Yang C, Ling Y, Li X, 2020. Information Encryption Algorithm in Power Network Communication Security Model[J]. *IOP Conference Series: Materials Science and Engineering*, 750(1):012161 (8pp). https://doi.org/10.1088/1742-6596/1852/3/032007

[14] Demidov R A, Pechenkin A I, Zegzhda P D, et al, 2018. Application Model of Modern Artificial

Neural Network Methods for the Analysis of Information Systems Security[J]. *Automatic Control and Computer Sciences*, 52(8):965-970. https://doi.org/10.3103/s0146411618080072

[15] Sirajuddin, M., Rupa, C., Bhatia, S., Thakur, R. N., & Mashat, A. (2022). Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System. *Wireless Communications and Mobile Computing*, (1), 9134036. https://doi.org/10.1155/2022/9134036