A Method for Four-Property Detection of Electronic Financial Archive Data Based on Dynamic Particle Swarm Algorithm

Liang Chen*
Information Centre, Guangdong Power Grid Corporation, China
chenliang@gdxx.csg.cn

You Wen
Information Centre, Guangdong Power Grid Corporation, China
13531002273@139.com

Huaquan Su
Information Centre, Guangdong Power Grid Corporation, China
suhuaquan@foxmai.com

Abstract: *The detection of the four properties Authenticity, Integrity, Usability, and Security (AIUS) of Electronic Financial Archive Data (EFAD) data involves multiple technical aspects, such as data encryption, integrity verification, and access control. This complexity prevents the static Particle Swarm Algorithm (PSA) from iteratively adapting to the dynamic changes in financial data, leading to high detection deviations and an elevated risk rate for electronic financial archive data. In order to ensure the reliability of financial data storage, a method for detecting the four properties of electronic financial file data based on a Dynamic Particle Swarm Algorithm (DPSA) is proposed to promote the standardization of intelligent financial management. The authenticity, integrity, usability and security requirements of Electronic Financial File Data (EFFD) are analyzed in depth. The SM2 algorithm in Digital Signature Algorithm (DSA) is used to encrypt and process the initial electronic financial file data to optimize the security of electronic financial file data. The four-property detection index of electronic financial file data is iteratively optimized based on the dynamic particle swarm algorithm, and the Fitness Value (FV) of the four-property detection index of electronic financial file data is calculated. The abnormality of electronic financial file data is judged based on the fitness value, so as to realize the Four-Property Detection (FPD) of electronic financial file data. Experimental verification shows that this method achieves good results in the four-propertyistic detection of electronic financial file data. The data encryption results are random, effectively improving the security of electronic financial file data. The detection deviation is less than 1%, and the risk rate of electronic financial file data is less than 1.5%. The detection results can be intuitively displayed on a visual page, proving that this method effectively ensures the quality of electronic financial file data and promotes intelligent management of electronic financial file data.*

Keywords: *Dynamic particle swarm algorithm, electronic financial archive data, four properties detection, authenticity, integrity, availability, security, digital signature algorithm.*

Received May 28, 2025; accepted April 01, 2026
https://doi.org/10.34028/iajit/23/5/13

1. Introduction

Electronic Financial Archive Data (EFAD) refers to various types of financial information stored electronically during an enterprise's financial management process. It includes critical enterprise information and provides comprehensive, accurate data support for financial decision-making [24]. Due to the significance of EFAD, it is highly vulnerable to malicious attacks, which may result in data leakage, loss, or tampering, the electronic financial file data for Authenticity, Integrity, Usability, and Security (AIUS) of the four nature of the test, can be found in a timely manner in the electronic financial file data in the problem [25], to ensure that the content of the electronic financial file data, the structure and the background information is complete, and can be normally retrieved, presented to protect the long-term preservation and effective use of financial information.

Gomez *et al*. [11] applied an autonomous algorithm to optimize data storage based on the edge computing approach. Training samples with large prediction errors are intelligently identified and prioritized for retention, thus effectively improving system performance with little additional memory burden. A self-commissioning state monitoring system is chosen to effectively realize e-file data detection by self-learning to distinguish between normal and abnormal through minimal a priori knowledge. However, too little a priori knowledge in this method may lead to low learning efficiency of the algorithm in the initial stage, and may even fall into the local optimal solution, which affects the final realization of the accuracy of the results of e-file data detection. Kumar *et al*. [17] comprehensively collects the relevant attribute information of the devices in the enterprise network, deploys an endpoint detection and response system, and combines the tactical intelligence analysis, the threshold cryptography and the reputation management mechanism to construct trust assessment algorithms, continuous tracking and recording of data, dynamic assessment of the subject's trust, and synchronized in-depth analysis against the known threat

signature library, which in turn provides strong support for conditional access control policies. In order to improve the accuracy of electronic file data detection, the use of tactical intelligence analysis and information theory principles for optimization. The structure of this method is more complex, resulting in the inability to adapt to the dynamic changes in data, affecting the data risk rate. Grossi *et al*. [13] used a comprehensive protection strategy that combines an intrusion prevention system with an intrusion detection system to monitor and identify potential security risks in the e-file data stream. In order to improve the performance of the defense and detection system in high-speed data transmission scenarios, a dedicated hardware platform is designed to implement the functions of the intrusion prevention system and intrusion detection system to provide a more robust detection of e-file data. However, in the high-speed electronic file data transmission environment, server-based software intrusion prevention system and intrusion detection system may be due to the problem of processing power and performance degradation, unable to respond to threats in real time, and the method relies on the processing speed of the Central Processing Unit (CPU), to achieve the applicability of the electronic file data detection is poor. Nagamani *et al*. [20] by comprehensively evaluating the electronic file data management of the incoming and outgoing data processing processes, considered suspicious activities as potential security threats and employed an innovative interference-distinguishing proof structure to enhance the security design of the framework. Emphasis is placed on the use of the special case distinction proof technique to identify and disclose violations, in-depth analysis of the feature recognition mechanism in the system database, focusing on several key components, and training through real data sets to achieve more accurate detection of e-finance file data. The in-depth analysis of the feature recognition mechanism in the system database in this method helps to understand the behavioral patterns of the data more accurately, but the accuracy of feature recognition is highly dependent on the quality and completeness of the data, if the initial data quality is poor, it can lead to poor detection of the final e-file data.

In the actual electronic financial file data, the data storage environment has large differences, the scale and complexity are different, so the realization of electronic financial file data four-property detection process is more complex. Based on the Dynamic Particle Swarm Algorithm to achieve electronic financial file data four-property detection can effectively solve the above problems, the algorithm has a strong versatility and adaptability, well adapted to the changing detection environment, through the simulation of group behavior, the use of group intelligence to cooperate to find the optimal solution to the problem, can significantly improve the efficiency of the four-property detection, shorten the detection time Chang *et al*. [7]. Therefore, we propose a dynamic particle swarm algorithm based on the electronic financial file data four-property detection method, can achieve a better effect of electronic financial file data four-property detection, effectively ensure the safety of financial information, help enterprises make more scientific and reasonable financial decision-making.

2. Four Properties Detection Method for Electronic Financial Archive Data

2.1. Model for Four Properties Detection of Electronic Financial Archive Data

The four-properties detection of electronic financial file data, i.e., AIUS detection, plays a crucial role in financial management and file preservation Gokila and Kannan [10]. Among these, integrity is an important guarantee of the value of electronic financial archives and can comprehensively record the financial activities of an enterprise. Availability is the basis for the existence of electronic financial archives and ensures that they can be used. Security can maintain the value and legal effectiveness of electronic financial archives and protect the business secrets and legitimate rights and interests of an enterprise. In the process of managing the preservation of electronic financial archives, the four-property test is the key to ensuring the value of electronic financial archives Dubey and Choubey [9]. In view of the above research, a four-property test model for electronic financial archives data is constructed, as shown in Figure 1.

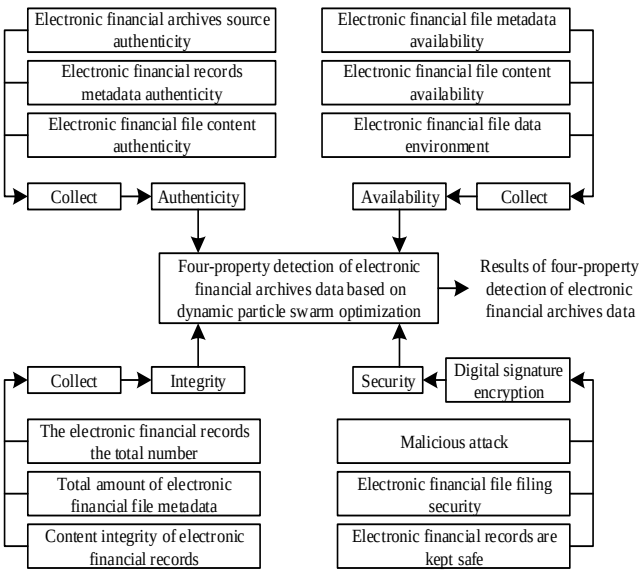


Figure 1. Four-property detection model for electronic financial file data.

As shown in Figure 1, for the actual electronic financial file data, the electronic financial file data is first encrypted using digital signature technology to ensure that the electronic financial file data is not tampered with or destroyed during transmission and storage. The EFAD is aggregated as required, and a dynamic particle swarm

algorithm is then applied to test its four properties to test the AIUS of the electronic financial file data, thereby identifying anomalies and potential risks in the electronic financial file data.

2.2. Encryption of Electronic Financial Archives Based on Digital Signature Technology

Electronic financial archives usually contain a large amount of financial information, and the integrity of this information is crucial for financial audits and decision-making. During the process of generation, transmission and storage, they may face the risk of being tampered with or forged, resulting in partial loss or damage of the data. This may lead to the leakage or illegal access of electronic financial archives, which will cause serious economic losses and reputational damage to the enterprise [26]. Digital signature technology can generate a unique digital signature for electronic financial file data through hash operations and private key encryption, ensuring that only legitimate users can sign and verify electronic financial file data, and effectively ensuring the authenticity and accuracy of electronic financial file data [8].

EFAD data using the SM2 Digital Signature Algorithm (DSA) in digital signatures, constructing the SM2 DSA elliptic curve Bagchi *et al.* [3], which is defined over a prime field ψ_{ς} or a binary extension field $\psi_2{}^n$, represented in affine coordinates through Weierstrass function, regarding any point *P* on the elliptic curve, the coordinates of that point (*X*, *Y*, *Z*), The affine coordinate point corresponding to *P* is (*X*, *Y*), and the equation of the curve at this point is expressed as Equation (1):

$$\lambda: Y^2 = X^3 + \varsigma XZ^4 + \xi Z^6 \, mod \, \upsilon \tag{1}$$

Here, ς, ξ represents a constant, $4\varsigma^3+27\xi^2\neq 0$ mod () denotes the modulus function, υ is prime and $\upsilon>3$. *Let a* be a positive integer, C be a point on the elliptic curve, and the scalar product $[a]C$ be defined by repeated addition at the same point on the elliptic curve as Equation (2):

$$[a]C = C + \overset{a}{\overbrace{C + \cdots}} + C \tag{2}$$

Based on the above process for constructing the elliptic curve of the SM2 DSA, an algebraic structure with closure, associativity, and commutativity is obtained, thus providing a solid theoretical foundation for the SM2 DSA [15]. The flow of the SM2 DSA is shown in Figure 2.

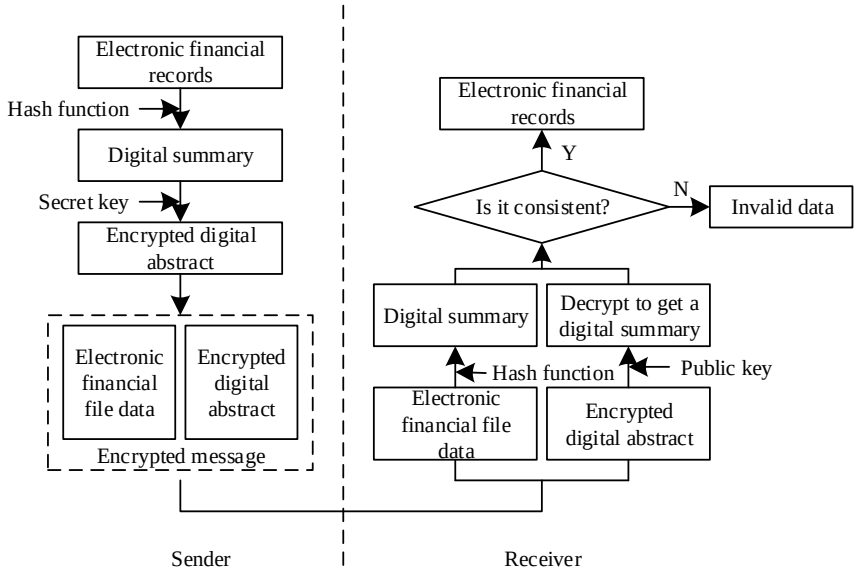


Figure 2. Flowchart of SM2 digital signature algorithm.

The SM2 DSA includes the key generation algorithm, signature generation algorithm, and signature verification algorithm for EFAD. First, the system generates the Private Key (skD) and Public Key (pkD) for the EFAD using the key generation algorithm. Then, the signer uses the key skD to run the signature generation algorithm to create the signature pair (g, h) for the EFAD D and sends it to the verifier, where g and h represent the encrypted EFAD and the encrypted digital digest, respectively. Finally, after the verifier receives the signature pair (g, h), they use the signer's public key pkD to run the signature verification algorithm to check whether the signature is valid, thus achieving the encryption and decryption process of the EFAD.

Let E represent the base point of the elliptic curve SM2, and l represents the order of the base point E. The specific calculation process is as follows:

1) EFAD Key Generation Algorithm.
Input the security parameters to obtain the key skD, then the public key is represented as Equation (3):

$$pk_D = [sk_D]E \tag{3}$$

Where, $sk_D \in [1, l\text{-}2]$.

2) Signature Generation Algorithm.
Calculate the hash value of the EFAD *D* using a hash function, represented as Equation (4):

$$\tau = hash(D) \tag{4}$$

Here, hash () represents the hash function.
Generate a random number $a \in [1, l\text{-}1]$, for the base point *E* of the SM2 elliptic curve, let its corresponding affine coordinate point be (x_E, y_E), and calculate its scalar multiplication, represented as Equation. (5):

$$[a]E = (x_E, y_E) \tag{5}$$

For the signature pair (*g*, *h*) of the EFAD D, calculate the encrypted EFAD g, represented as Equation (6):

$$g = (\tau + x_E) \, mod \, l \tag{6}$$

When g =0 or $g+a$ =l, regenerate the random number *a*, Otherwise, continue calculating the signature of the electronic financial file data *D* against the encrypted digital digest *h* in (*g*, *h*), expressed as Equation (7):

$$h = [(1 + sk_D)^{-1} \cdot (a - g \cdot sk_D)] \, mod \, l \tag{7}$$

Where, when $h = 0$, regenerate the random number *a*, otherwise end the calculation and output the signature pair *(g,h)* of the EFAD *D* .

Verify the signature pair *(g,h)* obtained from the EFAD *D* if valid, the satisfied condition is represented Equation (8):

$$\begin{cases} g' \in [1, l-1] \\ h' \in [1, l-1] \end{cases} \tag{8}$$

Receiving encrypted EFAD *D'* the hash value is calculated through a hash algorithm, represented as Equation. (9):

$$\tau' = hash(D') \tag{9}$$

Performing the decryption process of EFAD, represented as Equations (10), (11) and (12):

$$\gamma = (g' + h') \, mod \, l \tag{10}$$

$$(x_E, y_E) = [h']E + [\gamma]pk_D \tag{11}$$

$$G = (\tau' + x_E') \, mod \, l \tag{12}$$

When $\gamma = 0$, the signature verification fails, and the decryption of EFAD fails, resulting in invalid information. When $G \neq g'$, the signature verification fails.

2.3. Detection of the Four Properties of electronic financial archive data Based on Dynamic Particle Swarm Algorithm

Electronic Financial Files (EFF), as important corporate assets, need to be well managed. In section 2.2, EFF can be encrypted and protected using SM2 digital signature technology. However, encrypted EFF may be subject to malicious attacks during transmission and storage. The combination of dynamic particle swarm algorithm and SM2 digital signature technology can ensure the confidentiality and integrity of EFF during transmission [18], and can detect whether the files have been tampered with during storage to ensure the authenticity of the data.

The idea of the particle swarm algorithm is based on the foraging process of a flock of birds. It is an optimization algorithm that uses the cooperation and competition among particles in the group to generate the optimal solution Ajmera and Tewari [1]. Dynamic Particle Swarm Optimization (PSO) has been demonstrated to improve global search capability and optimization performance in complex data-processing tasks, providing methodological support for its application in four-property detection of EFAD [16]. Let the particle swarm size be *M*, that is, all the four-property detection indicators in the electronic financial file data, and let the target search space dimension be *Q*. The *Q* dimensional spatial position vector of the*i*-th electronic financial file data four-property detection indicator is expressed as: $s_i = (s_{i1}, s_{i2}, \cdots, s_{iQ})$, where each$s_i$ represents a solution in the solution space. All the four-property detection indicators in the electronic financial file data can be judged according to the Fitness Value (FV) calculated by the objective function to see if they are in an optimal state. The *Q* -dimensional spatial velocity vector of the *i*- th electronic financial file data four-property detection index is expressed as $v_i=(v_{i1}, v_{i2}, \cdots, v_{iQ})$, the individual optimal position of the i-th electronic financial file data four-property detection index is expressed as $PB_i=(PB_{i1}, PB_{i2}, \cdots, PB_{iQ})$, and the optimal position of all four-property detection indexes in the electronic financial file data is expressed as $GB_i=(GB_{i1}, GB_{i2}, \cdots, GB_{iQ})$. If k=1,2, …, *Q*, the iterative formula is expressed as Equations (13), (14) and (15):

$$PB_{i,t+1}{}^k = \begin{cases} s_{i,t+1}{}^k, fit(s_{i,t+1}) < fit(PB_{i,t}) \\ PB_{i,t}{}^k, else \end{cases} \tag{13}$$

$$v_{i,t+1}{}^k = \omega v_{i,t}{}^k + \mu_1 \sigma_1 (PB_{i,t}{}^k - s_{i,t}{}^k) + \mu_2 \sigma_2 (GB_{i,t}{}^k - s_{i,t}{}^k) \tag{14}$$

$$s_{i,t+1}{}^k = s_{i,t}{}^k + v_{i,t+1}{}^k \tag{15}$$

Where, μ_1 represents the cognitive acceleration factor that adjusts the optimal particle direction flight step length of the electronic financial file data quadruple property detection index, and μ_2 represents the social acceleration factor that adjusts the optimal particle direction flight step length of the electronic financial file data quadruple property detection index [14]. Σ1 σ_1 σ_2 all represent random numbers within the [0,1] range, and $v_{i,t+1}{}^k$,$s_{i,t+1}{}^k$ respectively represent the speed and position of the *i* th EFAD four property detection indicator in the $t+1$ th iteration in the *k* th dimension. $PB_{i,t}{}^k$, $GB_{i,t}{}^k$ respectively represent the positions of the individual and global extremum points of the *i* th EFAD four property detection indicator in the *t* th iteration in the *k* th dimension. ω represents the inertia factor, which can control the search speed, quickly converge to the local area, and then perform a local search to obtain the final solution. The update formula for the inertia factor

ω is expressed as Equation (16):

$$\omega = \omega(\omega min_{max} t/T_{max})_{max} \quad (16)$$

Among them, ω_{max} and ω_{min} represent the maximum and minimum inertia factors, respectively, and T_{max} indicates the maximum number of iterations.

Let the set of positions for the four property detection indicators of electronic financial archives data be represented as $S = \{s_1, s_2, \cdots, s_z\}$, z, which denotes the number of four property detection indicators of electronic financial archives data. A region with a radius of R is defined around each four property detection indicator of electronic financial archives data. Due to the varying Euclidean distances between the four property detection indicators of electronic financial archives data [23], there is a possibility of overlap between regions. Each four property detection indicator of electronic financial archives data not only represents itself but also represents the region it is in. If the total number of four property detection indicators of electronic financial archives data is M, then the global region can be divided into M different sub-regions. $s_i = (s_{i1}, s_{i2}, \cdots, s_{iQ})$, where Q represents the dimension. If $Q = 1$, then the divided regions are one-dimensional, and each region is a line segment, allowing for overlap; if $Q = 2$, then the divided regions are two-dimensional, and each region is a circle, allowing for overlap.

Each e-finance file data quadruple test index represents a subregion and is the current optimal solution in that region [4]. To obtain the optimal solution for the region, each e-finance file data quadruple test index evolves within its region and updates the optimal solution for the region. The evolutionary process is expressed as Equation (17):

$$s_i = \vartheta(s_i, R) \quad (17)$$

Here, $\vartheta(s_i,R)$ represents the Gaussian distribution random function. If s_i falls outside the region, evolutionary computation is restarted, keeping it within the region. During the setting process of radius R, if it is too large, the regions overlap severely; if it is too small, the individual regions cannot cover the entire spatial area, making it easy to fall into local optima and unable to find the global optimum solution [12]. Therefore, R is set as a dynamic variable, represented as Equation (18):

$$R = R\, exp\left[\rho(0,1)/Q^{\frac{1}{2}}\right] \quad (18)$$

Here, Q represents the dimension, and ρ (0,1) is a random number within the range of [0,1].

To ensure that the EFAD's four property detection indicators are free from local extrema, and that local optimal value information is not disrupted by extreme value disturbances, the path and area of particle search have been expanded to better discover the optimal state [6, 22]. A random disturbance factor is introduced, represented as Equation. (19) and (20):

$$\varphi_1 = \begin{cases} {r_1}^{t_0 > T_0}, if \rho(0,1) \geq 0.5 \\ 1, else \end{cases} \quad (19)$$

$$\varphi_2 = \begin{cases} {r_1}^{t_{GB} > T_{GB}}, if \rho(0,1) \geq 0.5 \\ 1, else \end{cases} \quad (20)$$

Here, t_0 and t_{GB}, T_0 and T_{GB} represent the number of iterations for optimizing the four property detection indicators of electronic financial records data and the threshold for random disturbance factors, respectively. Due to the randomness of the evolutionary mechanism, the solution for the four property detection indicators of electronic financial records data may deviate, making it impossible to find the optimal state location Nayak *et al*. [21].

In this case, a fallback factor is used; if at any moment the optimal solution for the four property detection indicators of electronic financial records data has not improved or has regressed, the particle needs to retreat based on its current position, meaning that the original addition becomes subtraction, effectively increasing the probability of finding the optimal state for the four property detection indicators of electronic financial records data. Through the above analysis, introducing a dynamic process into the traditional particle swarm algorithm helps enhance the ability to optimize the optimal solution, thus Equations (14) and (15) can be updated as Equations (21) and (22):

$$\begin{aligned} {v_{i,t+1}}^{k'} = \omega {v_{i,t}}^{k} + \mu_1 \sigma_1 \left(\varphi_1 {PB_{i,t}}^{k} - {s_{i,t}}^{k}\right) \\ + \mu_2 \sigma_2 \left(\varphi_2 {GB_{i,t}}^{k} - {s_{i,t}}^{k}\right) \end{aligned} \quad (21)$$

$${s_{i,t+1}}^{k'} = {s_{i,t}}^{k} \pm {v_{i,t+1}}^{k'} \quad (22)$$

Based on the above analysis, in the process of detecting the four properties of EFAD using the dynamic particle swarm algorithm [2, 5, 19], let κ represent the relationship containing M EFAD detection indicators for the four properties S_1, S_2, $\cdots$, S_M, θ indicates that κ contains the projection of the electronic financial data index of S_i, S_{i+1}, $\cdots$, S_j, which is expressed as Equation. (23):

$$\theta = \prod_{S_i, S_{i+1}, \cdots, S_j}(\kappa) \quad (23)$$

The support of tuples θ on the same ι is represented as $sup(\iota)$, which equals the number of tuples in the relationship κ that contain the same values of the EFAD four property detection indicators S_i,S_{i+1},$\cdots$,S_j. Let the tuple be $\iota = S_i, S_{i+1}, \cdots, S_j$, and the target EFAD four property detection indicator be represented as S_j. The neighbors of S_j are represented as $\beta(S_j,\iota)=\langle S_i,\cdots,S_{j-1}\rangle$, which are the items on ι that do not contain S_j. For the tuple $\iota = S_i, S_{i+1}, \cdots, S_j$, if the target EFAD four property detection indicator is represented as S_j, then the fitness of S_j is represented as Equation. (24):

$$fit(S_j, \iota) = \sum_{i=1}^{j-1} sup[\beta(S_i, \iota)] \,/\, sup[\beta(S_j, \iota)] \quad (24)$$

Among them, $sup[\beta(S_i,\iota)]$ and $sup[\beta(S_j,\iota)]$ represent the support levels of $\beta(S_i,\iota)$ and $\beta(S_j,\iota)$, respectively. Based

on the above calculations, the smaller the value of $fit(S_j,t)$, the more likely it is that the corresponding EFAD's four property detection index value is abnormal, thus enabling the detection of the four characteristics of EFAD.

3. Experimental Analysis

To verify the effectiveness of the proposed four-property detection method for EFAD based on the dynamic PSO algorithm, a medium-sized machinery manufacturing enterprise was selected as the test subject for the study. Founded in 2010, the company has over 500 employees and an annual output value of 200 million yuan. Its business covers multiple areas, including the production, assembly, and sales of mechanical components. During daily operations, the company generates a large volume of EFAD, such as procurement contracts, sales invoices, and financial statements. The management status of its EFAD is illustrated in Figure 3.

Figure 3. Data management of enterprise electronic financial archives.

The experimental data were sourced from the EFAD generated during the company's actual operations. The data collection methods were as follows: First, the data export interface provided by the EFAD management system was used to export nearly three years of EFAD in Extensible Markup Language (XML) format, totaling approximately 8 Million records, covering various business segments such as procurement, sales, and financial accounting. Second, by analyzing system log files, user operation records for EFAD were extracted, including login times, operation types (e.g., query, modify, delete), and operation objects, among other key information. A total of about 1.5 Million operation log entries were collected to comprehensively understand data usage patterns and potential risk points.

As shown in Figure 3, the experimental enterprise's EFAD is managed and stored via a dedicated archive management system, and the detailed parameters of which are statistically analyzed, and the results obtained are shown in Table 1.

Table 1. Data management parameters of electronic financial archives.

Parameters	Actual value
Database type	MySQL/Oracle/SQL server
Storage capacity	10TB
Data backup strategy	Daily automatic backup,weekly full backup
User interface support device	PC,tablet computer,mobile phone,etc
User rights management	Multi-level permission settings to ensure data security
File entry	Supports manual input, batch import,OCR identification and other modes
File query	Support keyword,date range,classification and other search conditions
File classification and labeling	Customize categories and labels for easy management
Approval process management	Customize the approval process and support multi-level approval
Report generation and export	Generate all kinds of financial statements and export them in Excel, PDF and other formats

As shown in Table 1, the system adopts a hybrid database architecture, with database types including MySQL (for storing daily business data, accounting for about 60%), Oracle (for storing core financial data, accounting for about 30%), and SQL Server (for storing some report data, accounting for about 10%) to meet diverse data storage and processing needs across different business functions. The storage capacity reaches 10TB, with approximately 6.5TB currently in use, leaving sufficient space to accommodate data growth for the next 3-5 years. The data backup strategy combines daily automatic backups with weekly full backups. Daily incremental backups are performed at 2:00 AM, with an average backup size of about 50GB, while weekly full backups are conducted at 1:00 AM on Saturdays, averaging around 300GB. Backup data is stored in an off-site data center to ensure data security and recoverability. The user interface supports multiple devices, including PCs (about 70%), tablets (about 20%), and smartphones (about 10%), enabling users in different roles to access the system anytime, anywhere. User permission management employs a multi-level permission system, with 15 distinct permission levels assigned based on user roles (e.g., financial managers, accountants, cashiers) and departmental divisions to strictly safeguard data security. File entry supports multiple modes, including manual input (about 30%), batch import (about 50%), and OCR recognition (about 20%), improving data entry efficiency. File queries support various search conditions, such as keywords (up to three keywords for combined queries), date ranges (accurate to the day), and categories (e.g., procurement, sales, expenses), allowing users to quickly locate the required data. File classification and labeling are customizable, with the company setting up 8 first-level categories and 30 second-level categories based on its business characteristics, along with customizable tags for easier data management. Approval workflow management supports customizable multi-level approval processes, with each workflow involving an average of 3-5 approval nodes to ensure business

compliance. Report generation and export functions enable the creation of various financial statements, such as balance sheets, income statements, and cash flow statements, with support for export in formats like Excel and Portable Document Format (PDF). On average, about 50 reports are generated monthly.

In the experiment, 100 sets of simulated electronic financial record data were collected, covering financial information of enterprises of different sizes, including financial statements, transaction records, etc. Firstly, the SM2 algorithm is used to encrypt the initial electronic financial record data to ensure data security. Then, set the relevant parameters of the dynamic particle swarm algorithm, iteratively optimize the four property detection indicators of electronic financial record data, calculate the FV, and judge whether there are abnormal situations in the data based on the FV. In this experiment, the hyperparameters of the dynamic particle swarm algorithm were configured as follows: after multiple trials and adjustments, the maximum inertia weight was set to 0.9, the minimum value was set to 0.4, the maximum number of iterations was set to 200, the number of particles was set to 30, and the learning factor was set to 2.0. This simulated experimental environment was used to evaluate the performance of the method. As shown in Table 2.

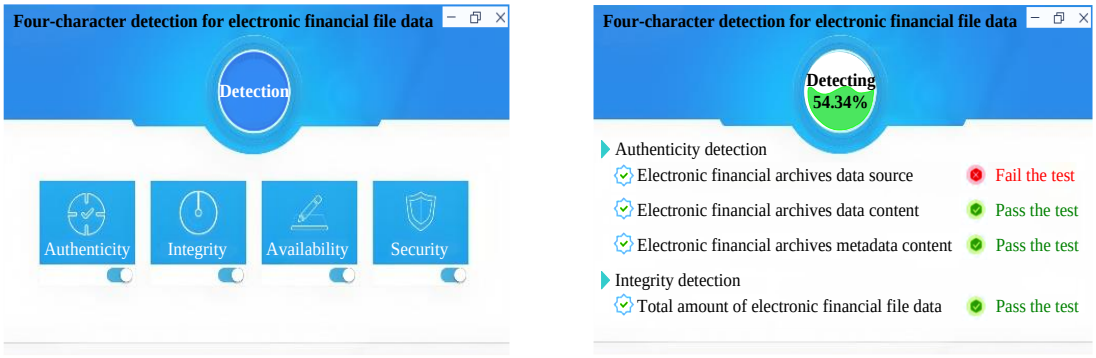
Table 2. Superparameter experimental results.

Data ID	Authenticity testing results (0 normal, 1 abnormal)	Integrity testing results (0 normal, 1 abnormal)	Usability testing results (0 normal, 1 abnormal)	Security testing results (0 normal, 1 abnormal)	Fitness value
1	0	0	0	0	0.85
2	0	0	0	0	0.82
3	1	0	0	0	0.45
4	0	1	0	0	0.52
5	0	0	1	0	0.60
6	0	0	0	1	0.38
...	...	...	...	...	...
100	0	0	0	0	0.88

According to Table 2, in terms of the accuracy of the detection results, most of the data in the table, such as data numbered 1, 2, and 100, have normal four property detection results (with a value of 0), indicating that this method can accurately judge whether the characteristics of normal data meet the requirements. However, data with abnormalities such as data numbered 3, 4, 5, and 6 have been detected as problems in different characteristics, indicating that it can effectively identify abnormal situations in electronic financial record data and has a positive effect on ensuring the reliability of financial data; In terms of the relationship between FV and detection results, FV to some extent reflect the comprehensive situation of the four property of the data. Normal data FV are generally high, such as 0.85 for number 1 and 0.88 for number 100, while abnormal data are relatively low, such as 0.45 for number 3 and 0.38 for number 6. It can be seen that FV can be an important reference indicator for judging whether data is abnormal, and the lower the value, the greater the possibility of abnormal data; In terms of the impact of parameter settings, when the inertia weight set in this experiment is between 0.4-0.9, the learning factor is set to 2.0, the number of particles is 30, and the maximum iteration is 200 times, the dynamic particle swarm algorithm can complete the detection task well, with good convergence and the ability to accurately judge data anomalies by finding optimal detection indicators in a reasonable time. This highlights the key role of reasonable parameter settings in algorithm performance and detection result accuracy. Subsequent research can further explore the impact of different parameter combinations on algorithm performance to optimize detection methods.

Through the electronic financial file data management related parameters shown in Table 1, combined with the method of this paper on the electronic financial file data shown in Figure 3 of the experimental enterprises for the detection of the Four-Property. Based on the characteristics of EFAD and practical application requirements, specific thresholds for the four-property detection indicators were established: The authenticity threshold was set at 0.95. If the detection value fell below this threshold, the data's authenticity was considered potentially compromised. The integrity threshold was set at 0.98 to ensure data completeness and accuracy. The usability threshold was set at 0.92 to guarantee timely and accurate access to data when needed. The security threshold was set at 0.99 to strictly safeguard data security.

The FV was calculated to determine whether anomalies existed in the data-the lower the FV, the higher the likelihood of data anomalies. Finally, the detection results were clearly presented through a visualization interface, which displayed the scores of each detection indicator, the distribution of anomalous data, and an overall assessment of the four properties of the data in the form of charts and reports. This allowed users to intuitively evaluate the four-property status of the company's EFAD. Specific electronic financial file data four-property detection is shown in Figure 4.

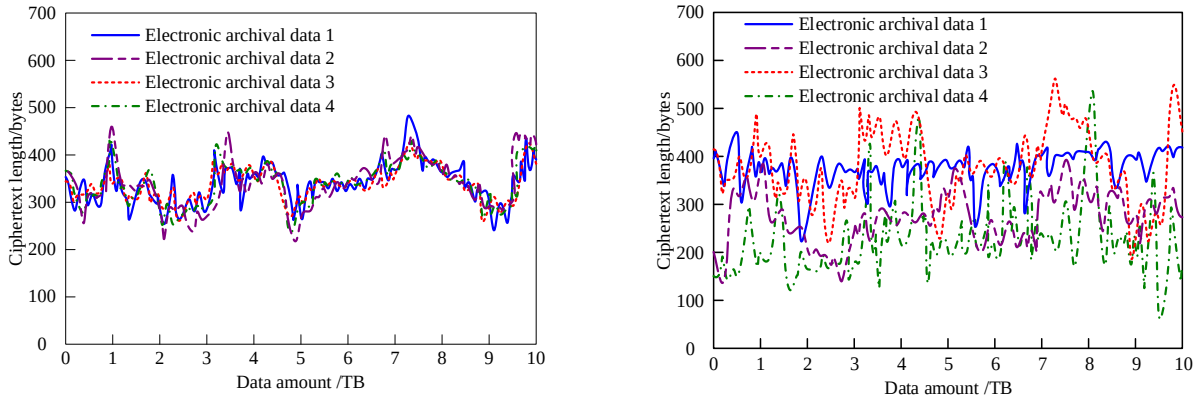


a) Electronic financial archives data four-sex detection start page. b) Electronic financial archives data four-sex detection page.

Figure 4. Four-property detection for electronic financial file data.

As shown in Figure 4, the method can realize a better electronic financial file data four-property detection. By combining the method, the final electronic financial file data four test results can be displayed through the interface. According to Figure 4 a) shows that, according to the method can effectively achieve the authenticity of electronic financial file data, integrity, usability, security of the overall detection and single detection, select the items that need to be detected after the corresponding detection can be achieved. As shown in Figure 4 b), the detection process, can effectively realize the different detection projects in different indicators for detection, and ultimately through the method to give a clearer electronic financial archives data four test results, to provide an intuitive basis for the relevant personnel, can be found in a timely manner in the electronic financial archives data problems.

In order to verify the effectiveness of this paper's method to realize the EFAD four-property detection, the method through the digital signature for EFAD processing to test the effect of randomly selected four electronic archive data, through the method of this paper's digital signature technology for encryption processing. The ciphertext length of the test data in different data volume cases is counted to verify the significance of this method for ensuring the security of EFAD, and the results of encryption processing realized by this method are compared with those of encryption with symmetric key encryption algorithm, as shown in Figure 5.



a) Symmetric key encryption algorithm on the encryption of electronic financial file data. b) Effect of the method on the encryption of electronic financial file data.

Figure 5. Effect of electronic financial archives data encryption processing.

As shown in Figure 5, the method proposed in this article has significant advantages in ensuring the security of electronic financial records data. The symmetric key encryption algorithm (such as the AES algorithm in Figure 5 a)) exhibits a certain regularity in the ciphertext length as the data volume increases from 0 to 10TB. For example, in certain data intervals, the ciphertext length shows an approximately linear relationship with the data volume. The predictability of ciphertext length poses a potential security risk, as attackers may infer partial plaintext information or encryption keys by analyzing ciphertext patterns, thereby threatening data confidentiality [26].

In contrast, the SM2 DSA used in this article is a national security standard asymmetric encryption algorithm based on elliptic curve cryptography. From Figure 5 b), it can be seen that under the same 4 electronic archive data samples, as the data volume changes, there is no obvious pattern in the ciphertext length, and the trends of each curve are chaotic and have

no pattern of change. This good randomness originates from the closed, associative, and commutative algebraic structure formed by the SM2 algorithm during its construction process, which provides a solid theoretical basis for its security [3]. This randomness significantly enhances the anti-cryptanalysis ability of ciphertext, making it difficult for attackers to infer the original data information through ciphertext length or statistical features, thereby effectively improving the confidentiality and integrity of electronic financial record data during transmission and storage.

In the framework of anomaly detection, the security of encryption algorithms directly affects the reliability of detection models. Traditional symmetric encryption algorithms, due to the regularity of their ciphertext characteristics, may interfere with anomaly detection models when dealing with complex network attacks, resulting in insensitivity to real data anomalies caused by the pattern of the encrypted data itself. The SM2 algorithm used in this article generates randomized ciphertext, which enables anomaly detection based on more unpredictable and discriminative data features. This helps the dynamic particle swarm algorithm to more accurately identify real anomalies caused by malicious tampering or destruction, thereby improving the overall accuracy and robustness of the four property detection [15].

In order to further validate the effect of this paper's method to realize the four-nature detection of electronic financial file data, for the AIUS of electronic financial file data detection projects under different data volumes, the actual four-nature detection of electronic financial file data is carried out by the method, and the detection deviation is statistically calculated based on the detection results, and the risk rate statistics are carried out at the same time. This paper's method of electronic financial file data four-property detection results and electronic financial file data four-property detection commonly used in text mining technology, Convolutional Neural Network (CNN) method, random forest method to achieve the electronic financial file data four-property detection results for comparison, the results obtained as shown in Table 3.

Table 3. Results of the four property testing of electronic financial archives data.

Parameters		Textual method		Text mining technology		Convolutional neural network		Random forest method	
Test item	Data amount/TB	Deviation/%	Risk rate/%	Deviation/%	Risk rate/%	Deviation/%	Risk rate/%	Deviation/%	Risk rate/%
Authenticity	0.5	0.75	0.11	5.7	2.18	2.41	6.95	6.73	3.42
	1	0.34	0.67	4.94	3.21	1.53	5.11	5.39	2.2
	2	0.95	0.63	3.9	5.09	1.5	6.32	8.24	4.86
	5	0.52	1.03	5.12	4.85	1.26	4.06	4.63	3.3
Integrity	0.5	0.04	0.15	5.8	2.15	2.89	3.7	8.63	2.15
	1	0.39	0.4	5.51	6.37	3.04	4.77	8.38	4.49
	2	0.29	0.47	5.92	4.09	1.16	5.97	6.9	3.69
	5	0.42	0.37	5.6	5.61	3.26	6.85	4.05	3.41
Availability	0.5	0.66	0.1	3.96	4.49	2.24	4.66	8.26	2.18
	1	0.91	0.23	3.3	6.54	2.67	3.64	7.28	3.37
	2	0.84	0.36	3.67	5.3	1.83	5.56	6.78	5.64
	5	0.14	0.74	4.84	6.67	2.95	6.48	6.44	4.44
Security	0.5	0.15	0.41	4.65	5.11	2.8	5.53	6.11	3.97
	1	0.31	0.08	3.56	3.91	2.45	4.79	7.34	5.42
	2	0.16	0.12	4.39	5.93	2.83	6.75	4.59	4.39
	5	0.48	0.62	4.65	4.96	1.29	5.74	6.86	3.77

As shown in Table 3, the method can realize the better effect of electronic financial file data four-property detection. Electronic financial file data authenticity, integrity, availability, security testing, in different data volumes, compared with text mining technology, CNN method, random forest method to achieve the electronic financial file data four-property detection results, this method to achieve the electronic financial file data four-property detection deviation is less than 1%, so as to be able to timely find the electronic financial file data in the existing problems The risk rate of electronic financial file data is effectively reduced to less than 1.5% after the detection realized by the method, which proves that the method has outstanding ability and advantage in improving the quality of electronic financial file data management, ensuring the truthfulness and reliability of data and maintaining data security.

To compare the performance of the proposed method, text mining techniques, CNN methods, and random forest methods in detecting the four properties AIUS of EFAD, experiments were conducted using a one-year dataset of electronic financial records from a selected enterprise. The dataset included various types of documents such as procurement contracts, sales invoices, and financial statements, with a total volume of approximately 500GB. To ensure fairness in the experiments, the dataset was divided into training and testing sets in a 7:3 ratios for model training and performance evaluation, respectively. By comparing the four methods in terms of accuracy, recall, F1-score, and other metrics for the four-property detection, the strengths and weaknesses of each approach in evaluating EFAD were analyzed. The results are presented in Table 4.

Table 4. Comprehensive performance analysis.

Method	Authenticity			Integrity			Usability			Safety		
	Accuracy	Recall	F1 value	Accuracy	Recall	F1 value	Accuracy	Recall	F1 value	Accuracy	Recall	F1 value
Proposed method	0.96	0.95	0.955	0.97	0.96	0.965	0.98	0.97	0.975	0.99	0.98	0.985
Text mining technology	0.88	0.85	0.865	0.89	0.87	0.88	0.9	0.88	0.89	0.91	0.89	0.9
Convolutional neural network method	0.92	0.9	0.91	0.93	0.91	0.92	0.94	0.92	0.93	0.95	0.93	0.94
Random forest method	0.9	0.88	0.89	0.91	0.89	0.9	0.92	0.9	0.91	0.93	0.91	0.92

According to Table 4, the proposed method demonstrates the best performance in the four-aspect detection of EFAD. In terms of authenticity detection, the accuracy, recall, and F1-score all exceed 0.95, indicating that this method can effectively verify the authenticity of EFAD, ensuring reliable sources and accurate content. For completeness detection, the metrics are equally outstanding, enabling precise identification of data integrity and mitigating business risks caused by missing or corrupted data. In usability detection, the proposed method ensures that EFAD can be efficiently retrieved, presented, and understood, meeting the daily operational needs of enterprises. As for security detection, the high accuracy and recall rates confirm its effectiveness in preventing security threats such as data tampering and leakage, thereby safeguarding corporate financial data.

Text mining techniques show relatively weaker performance in the four-aspect detection. While they can analyze and process textual data to some extent, they struggle to accurately capture the four key characteristics when handling complex EFAD. For example, in authenticity detection, text mining primarily relies on content analysis and lacks robust capabilities for source verification, resulting in lower accuracy and recall rates. In completeness detection, it may fail to identify hidden data gaps or structural damage. CNNs achieve moderate results in the four-aspect detection but still fall short compared to the proposed method. Although CNNs excel in fields like image recognition, processing EFAD requires converting it into a model-friendly format, which may lead to information loss.

Moreover, CNNs primarily extract features based on spatial structures and are less effective in capturing logical relationships and business rules within financial data, thereby limiting detection performance.

The Random Forest method exhibits stable but overall inferior performance compared to the proposed approach. By constructing multiple decision trees for ensemble learning, Random Forest reduces overfitting risks but may struggle to distinguish subtle feature differences in complex financial archive data. Additionally, its performance heavily depends on feature selection and parameter tuning, requiring extensive optimization in practical applications. In conclusion, the proposed method demonstrates significant advantages in the four-aspect detection of EFAD, providing enterprises with more reliable and secure financial data management.

4. Extended Analysis

To evaluate the generalizability of the proposed method, we extended the experiments to include 300 sets of electronic financial record data from three distinct sectors: finance, manufacturing, and retail. These data cover financial statements, transaction records, etc. of enterprises of different sizes, and are stored on local servers and cloud storage in different archiving systems. At the same time, to compensate for the lack of strict comparison between evaluation indicators and baselines, the experiment not only calculated the FV, but also calculated the false positive rate, false negative rate, accuracy rate, recall rate, F1 value, and Receiver Operating Characteristic /Area Under the Curve (ROC/AUC) standard detection performance indicators. The Dynamic PSO algorithm was compared with three established anomaly detection baseline methods: One-Class Support Vector Machine (OCSVM), isolation forest, and Robust Principal Component Analysis (RPCA). In the experiment, the SM2 algorithm was used to encrypt the initial electronic financial record data. The inertia weight of the dynamic particle swarm algorithm was adjusted between 0.4-0.9, the learning factor was set to 2.0, the number of particles was 30, and the maximum number of iterations was 200. The results are shown in Table 5.

According to Table 5, the detection method based on dynamic PSO algorithm exhibits good characteristics: in terms of method generality, this method can obtain relatively stable FV when applied to electronic financial record data in different fields such as finance, manufacturing, and retail, with an average between 0.81-0.84, indicating that it can adapt to the financial data characteristics of enterprises in different fields and is not limited to a single enterprise environment; In terms of comparing evaluation indicators, the PSO method had an average false positive rate of 8%, an average false negative rate of 6%, an average accuracy rate of 91%, an average recall rate of 94%, an average F1 value of 0.92, and an average ROC/AUC value of 0.93 in the three experiments. All indicators were superior to the three baseline methods of OCSVM, Isolation Forest, and RPCA, indicating that it can more accurately identify normal and abnormal data when detecting anomalies in electronic financial records, reducing misjudgments and omissions; By comparing

with three baseline methods, the PSO method performs well in various standard detection performance indicators, demonstrating the relative effectiveness of the proposed dynamic particle swarm algorithm based electronic financial record data four property detection method, which can provide reliable anomaly detection support for intelligent financial management. In the future, algorithm parameters can be further optimized and different complex scenario applications can be explored to improve performance and universality.

Table 5. Analysis of universality and effectiveness.

Experimental grouping	Data field	Data volume	Detection method	Average fitness value	False alarm rate/%	Leakage rate/%	Accuracy /%	Recall rate/%	F1 value	ROC/AUC
Group 1	Finance	100	PSO	0.83	8	6	91	94	0.92	0.93
			OCSVM	-	12	10	88	90	0.89	0.90
			Isolation Forest	-	10	8	90	92	0.91	0.91
			RPCA	-	15	12	85	88	0.86	0.87
Group 2	Manufacture		PSO	0.81	9	7	90	93	0.91	0.92
			OCSVM	-	14	11	86	89	0.87	0.88
			Isolation Forest	-	11	9	89	91	0.90	0.90
			RPCA	-	16	13	84	87	0.85	0.86
Group 3	Retail		PSO	0.84	7	5	92	95	0.93	0.94
			OCSVM	-	13	9	87	91	0.89	0.90
			Isolation Forest	-	9	7	91	93	0.92	0.92
			RPCA	-	17	14	83	86	0.84	0.85

5. Conclusions

The electronic financial file data for the four test, mainly including electronic financial file authenticity, integrity, availability and security testing, to ensure the quality of electronic financial file data has an important role in the electronic financial file data based on the electronic financial file data four test, can effectively verify the authenticity of the electronic financial file data to ensure that the source of the data is reliable, the content of the data is accurate, timely detection and repair of the data in the lack of data, optimize the data storage format and reading mode, to ensure the security of the data. This paper proposes a dynamic particle swarm algorithm based on the electronic financial file data detection method, by combining digital signature technology and dynamic particle swarm algorithm, to achieve a more effective electronic financial file data detection of the four, which helps to improve the level of financial management, to protect the information security of enterprises.

References

[1] Ajmera K. and Tewari T., "SR-PSO: Server Residual Efficiency-Aware Particle Swarm Optimization for Dynamic Virtual Machine Scheduling," *The Journal of Supercomputing*, vol. 76, no. 3, pp. 15459-15495, 2023. https://doi.org/10.1007/s11227-023-05270-8

[2] Amal M. and Napitupulu H., "Particle Swarm Optimization Algorithm for Determining Global Optima of Investment Portfolio Weight Using Mean-Value-at-Risk Model in Banking Sector Stocks," *Mathematics*, vol. 12, no. 24, pp. 1-33, 2024. https://doi.org/10.3390/math12243920

[3] Bagchi P., Bera B., Das A., Shetty S., and et al, "Post Quantum Lattice-Based Secure Framework using Aggregate Signature for Ambient Intelligence Assisted Blockchain-Based IoT Applications," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 52-58, 2023. DOI: 10.1109/IOTM.001.2100215

[4] Bi Y., Lam A., Quan H., Liu H., and Wang C., "RETRACTED ARTICLE: A Comprehensively Improved Particle Swarm Optimization Algorithm to Guarantee Particle Activity," *Russian Physics Journal*, vol. 64, no. 5, pp. 866-875, 2022. https://doi.org/10.1007/s11182-021-02403-5

[5] Cansu T., Kolemen E., Karahasan O., Bas E., and Egrioglu E., "A New Training Algorithm for Long Short-Term Memory Artificial Neural Network Based on Particle Swarm Optimization," *Granular Computing*, vol. 8, no. 6, pp. 1645-1658, 2023. https://doi.org/10.1007/s41066-023-00389-8

[6] Cerini C. and Aglietti G., "Estimation of a Craig-Bampton Equivalent Model Using a Hybrid Particle Swarm Optimization for DCLA Purposes," *Acta Astronautica*, vol. 210, pp. 564-575, 2023. https://doi.org/10.1016/j.actaastro.2023.05.002

[7] Chang W., Soma P., Chen H., Chang H., and Tsai C., "A Hybrid Firefly with Dynamic Multi-Swarm Particle Swarm Optimization for WSN Deployment," *Journal of Internet Technology*, vol. 24, no. 4, pp. 825-836, 2023. https://jit.ndhu.edu.tw/article/view/2926

[8] Diwan P., Kashyap R., and Khandelwal B., "Blockchain Assisted Encryption Scheme for Intellectual Share Estimation Using Medical Research Data," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 2, pp. e7896.1-e7896.19, 2024. https://doi.org/10.1002/cpe.7896

[9] Dubey A. and Choubey S., "Blockchain and Machine Learning for Data Analytics, Privacy Preserving, and Security in Fraud Detection," *I-Manager's Journal on Software Engineering*, vol. 18, no. 1, pp. 45-55, 2023.

https://api.semanticscholar.org/CorpusID:265573005

[10] Gokila R. and Kannan S., "A Novel Machine Learning-Based Model for Network Attack Detection in Cyber Security Using Big Data," *Journal of Environmental Protection and Ecology*, vol. 24, no. 4, pp. 1401-1412, 2023. https://scibulcom.net/en/article/Um8crAKfgY4xpMJcbotO

[11] Gomez P., Gajardo M., Mijatovic N., and Dragicevic T., "A Self-Commissioning Edge Computing Method for Data-Driven Anomaly Detection in Power Electronic Systems," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 10, pp. 13319-13330, 2023. DOI: 10.1109/TIE.2023.3347839

[12] Goyal G. and Bisht D., "Adaptive Hybrid Fuzzy Time Series Forecasting Technique Based on Particle Swarm Optimization," *Granular Computing*, vol. 8, no. 2, pp. 373-390, 2023. https://doi.org/10.1007/s41066-022-00331-4

[13] Grossi M., Alfonsi F., Prandini M., and Gabrielli A., "A High Throughput Intrusion Detection System (IDS) to Enhance the Security of Data Transmission Among Research Centers," *Journal of Instrumentation*, vol. 18, no. 12, pp. C12017.1-C12017.12, 2023. DOI: 10.1088/1748-0221/18/12/C12017

[14] Ilyas L., Fathallah R., Ahmed E., Nacer S., and Abdelmajid B., "Robust LQR Control Based on Multidimensional Particle Swarm Optimization for Enhancing the Dynamic Performance of Poultry House System," *International Journal of Dynamics and Control*, vol. 11, no. 4, pp. 1593-1608, 2023. https://doi.org/10.1007/s40435-022-01082-5

[15] Kakkar L., Gupta D, Tanwar S, Saxena S, and et al., "A Secure and Efficient Signature Scheme for IoT in Healthcare," *Computers, Materials and Continua*, vol. 73, no. 3, pp. 6151-6168, 2022. http://doi.org/10.32604/cmc.2022.023769

[16] Karima K. and Nacera B., "A Dynamic Particle Swarm Optimisation and Fuzzy Clustering Means Algorithm for Segmentation of Multimodal Brain Magnetic Resonance Image Data," *The International Arab Journal of Information Technology*, vol. 17, no. 6, pp. 976-983, 2020. https://doi.org/10.34028/iajit/17/6/16

[17] Kumar N., Kasbekar G., and Manjunath D., "Application of Data Collected by Endpoint Detection and Response Systems for Implementation of a Network Security System based on Zero Trust Principles and the EigenTrust Algorithm," *ACM SIGMETRICS Performance Evaluation Review*, vol. 50, no. 4, pp. 5-7, 2022. https://doi.org/10.1145/3595244.3595247

[18] Lin W. and Zhang A., "Research on the Dynamic Early Warning Law for Confidential Information Security in Large-Scale Communication Networks," *Computer Simulation*, vol. 40, no. 11, pp. 370-374, 2023. https://d.wanfangdata.com.cn/periodical/jsjfz202311070

[19] Ma X., "RETRACTED ARTICLE: Enterprise Financial Early Warning Based on Improved Particle Swarm Optimization Algorithm and Data Mining," *Soft Computing*, vol. 28, no. 2, pp. 611-611, 2024. https://doi.org/10.1007/s00500-023-08518-w

[20] Nagamani C. and Chittineni S., "Network Database Security with Intellectual Access Supervision Using Outlier Detection Techniques," *International Journal of Advanced Intelligence Paradigms*, vol. 22, no. 3-4, pp. 348-361, 2022. https://doi.org/10.1504/IJAIP.2022.124318

[21] Nayak J., Swapnarekha H., Naik B., Dhiman G., and Vimal S., "25 Years of Particle Swarm Optimization: Flourishing Voyage of Two Decades," *Archives of Computational Methods in Engineering*, vol. 30, no. 3, pp. 1663-1725, 2023. https://doi.org/10.1007/s11831-022-09849-x

[22] Nemati Z., Mohammadi A., Bayat A., and Mirzaei A., "Fraud Risk Prediction in Financial Statements through Comparative Analysis of Genetic Algorithm, Grey Wolf Optimization, and Particle Swarm Optimization, grey wolf optimization, and particle swarm optimization," *Iranian Journal of Finance*, vol. 8, no. 1, pp. 98-130, 2024. DOI: 10.61186/ijf.2024.384462.1401

[23] Pak Y., Kong Y., and Ri J., "Robust PID Optimal Tuning of a Delta Parallel Robot Based on a Hybrid Optimization Algorithm of Particle Swarm Optimization and Differential Evolution," *Robotica*, vol. 41, no. 4, pp. 1159-1178, 2023. https://doi.org/10.1017/S0263574722001606

[24] Raj B. and Venugopalachar S., "Multi-data Multi-user End to End Encryption for Electronic Health Records Data Security in Cloud," *Wireless Personal Communications*, vol. 125, no. 3, pp. 2413-2441, 2022. https://doi.org/10.1007/s11277-022-09666-2

[25] Sonya A. and Kavitha G., "An Effective Blockchain-Based Smart Contract System for Securing Electronic Medical Data in Smart Healthcare Application," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 28, pp. e7363.1-e7363.17, 2022. https://doi.org/10.1002/cpe.7363

[26] Srivastava A. and Gupta J., "Attack Resistant Blockchain-Based Healthcare Record System Using Modified RSA Algorithm," *International Journal of Information Technology*, vol. 16, no. 1, pp. 417-424, 2023. https://doi.org/10.1007/s41870-023-01588-x

Liang Chen is currently a Member of the Application Management Department of the Digital Intelligence Operation Center, Guangdong Power Grid Co., Ltd. He received his M.S. degree in Software Engineering from South China University of Technology, China. His main research interests include Software Modeling and Natural Language Processing.

You Wen is currently a Member of the Application Management Department of the Digital Intelligence Operation Center, Guangdong Power Grid Co., Ltd. He received his B.S. degree in Software Engineering from South China Agricultural University, China. His main research interests Include Information Technology and its Applications.

Huaquan Su is currently a Member of the Application Management Department of the Digital Intelligence Operation Center, Guangdong Power Grid Co., Ltd. He received his B.S. degree in Information Engineering from South China University of Technology, China. His main research interests include Informatization and Big Data Analysis.