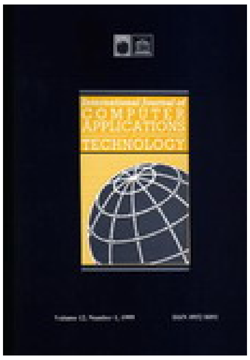


International Journal of Computer Applications in Technology

ISSN online: 1741-5047 - ISSN print: 0952-8091
https://www.inderscience.com/ijcat

Cloud computing based construction and empirical evaluation of the security risk early warning evaluation system of digital economy

Yanan Wu

DOI: 10.1504/IJCAT.2025.10075047

Article History:

Received:	27 May 2025
Last revised:	17 September 2025
Accepted:	20 October 2025
Published online:	17 February 2026

Cloud computing based construction and empirical evaluation of the security risk early warning evaluation system of digital economy

Yanan Wu

Saxo Fintech Business School,
Sanya University,
Sanya, Hainan, China
Email: yananwu@sanyau.edu.cn

Abstract: Traditional static risk assessment methods struggle to meet real-time processing demands for large-scale, multi-source heterogeneous data, showing sluggish responsiveness to emergencies and abnormal transactions. These approaches often suffer from poor early-warning accuracy and frequent false or missed alerts. To address these challenges, this study proposes a cloud-based security risk warning evaluation system for the digital economy. The system first establishes a multi-level risk indicator framework, utilising fuzzy hierarchical analysis and information entropy to calculate weighted metrics that integrate qualitative and quantitative indicators. It then employs grey prediction algorithms for short-term risk trend forecasting. Through a cloud computing distributed architecture, the system achieves real-time collection, processing and risk assessment of multi-source heterogeneous data, ensuring instant precision in warnings. Experimental results demonstrate that this method consistently outperforms existing approaches in both warning accuracy and recall metrics, with significantly reduced average response time, while maintaining reasonable control over false alarm rates and resource consumption. This research provides a practical technical solution for digital economy security risk management, offering both theoretical value and practical significance.

Keywords: risk early warning; evaluation system construction; digital economy; economic security.

Reference to this paper should be made as follows: Wu, Y. (2026) ‘Cloud computing based construction and empirical evaluation of the security risk early warning evaluation system of digital economy’, *Int. J. Computer Applications in Technology*, Vol. 78, No. 2, pp.135–143.

Biographical notes: Yanan Wu is an Associate Professor at Sanya University. She received the Bachelor’s degree from Zhengzhou University of Aeronautical Industry Management and Master’s degree from Hainan University. Her research interests include international trade and digital economy.

1 Introduction

The digital economy is booming, business models such as electronic transactions and mobile payments are widely popularised, platform operation and data processing are becoming more and more complex and security risks are becoming more and more diverse. Traditional security risk assessment methods mostly use stand-alone static analysis or simple threshold judgment, which is difficult to process multi-source heterogeneous data in real time, slow response to emergencies and abnormal transactions and unable to meet the needs of dynamic security management in the digital economy. In addition, the platform’s data is massive and growing rapidly. It has the characteristics of high volatility of small samples and incomplete information. Relying solely on traditional machine learning models for risk prediction and early warning has limitations, and it is ineffective in short-term trend prediction and real-time dynamic early warning. In order to solve these problems, this paper proposes a cloud-based security risk early warning and evaluation system for the digital economy. The system integrates a multi-dimensional risk index system, Fuzzy Analytic Hierarchy Process (F-AHP) weight distribution and grey prediction model and can dynamically monitor and warn key risk indicators such as data security and transaction security. With the help of cloud computing distributed architecture, the system can efficiently process large-scale multi-source data to ensure the real-time and accuracy of data collection, pre-processing and risk prediction. This paper also takes a regional digital economy platform as the experimental object, uses transaction logs, network access records and other data for empirical research and verifies the good performance of the system in terms of early warning accuracy, risk response speed and resource utilisation and provides an effective solution for digital economy security risk management.

This article mainly has two core contributions. At the methodological construction level, a multi-dimensional dynamic early warning system of risk indicators based on cloud computing has been created, key indicators such as data security and transaction security have been incorporated into a unified evaluation framework, and F-AHP and information entropy weighting method have been used to scientifically integrate qualitative and quantitative indicators to make the weight distribution of indicators more objective and reasonable. In terms of algorithm application, the innovative introduction of grey prediction models, dynamic modelling of short-term risk trends, accurate prediction of small samples, high volatility data, combined with cloud computing distributed architecture, achieves real-time collection, processing and prediction of multi-source heterogeneous data, significantly improving the real-time and accuracy of system early warning.

2 Related work

Many scholars have studied Digital Economy (DE) security. McKinnon (2019) believed that in more developed economies, the social and economic challenges of transition to DE with changes in the labour market were often manifested as increasingly unstable risks. McKinnon's (2019) research aimed to reveal the increasing employment instability and socioeconomic risks caused by changes in the labour market in developed economies during their transition to a digital economy, and advocates building a governance framework for 'managing transformation' through reforming social security, strengthening skills training and adjusting labour laws to achieve more inclusive and sustainable digital economic development. Viriyasitavat (2019) analysed DE in the Internet of Things (IoT) era, and optimising system performance was becoming a huge challenge for the growing large-scale distributed application system. Khitskov (2017) analysed the concept of DE, selected the best quotations from scientific circles and public figures, and expounded the necessity of social digital transformation. His work emphasises that digital transformation is a systemic societal shift, implying that its risks are not only technical but also social and institutional, thus highlighting the need for a comprehensive risk early warning system. Sturgeon (2021) sorted out the new and old characteristics of DE, summarised the three major business strategies of platform embedding, digital capability improvement and differentiated market positioning, and summarised social welfare and risks, mainly from two aspects of innovation and market positioning, and made strategic and policy choices for enterprises and decision-makers in economically backward regions. Banalieva and Dhanaraj (2019) mainly discussed the internationalisation of digital service multinational enterprises, focusing on how digitalisation would change the characteristics of the company's unique assets and explore its management options in cross-border trade. Zaloznova and Trushkina (2019) believed that under the condition of today's dynamic development, DE has realised the management of enterprise logistics activities, including effective utilisation of material resources, improvement of warehouse economy, production and commodity inventory, management of transportation flow and marketing activities and improvement of logistics service quality. Tan (2017) focused on big data applications that support operational decision-making, including advanced research on DE decision-making models and tools, and has collected many high-quality articles. The above research has achieved good results, but with the continuous updating of technology, there are still some problems.

How to use economic risk early warning has been analysed at different levels by many scholars. Zeng (2022) believed that service preloading can improve the response speed of enterprise financial risk early warning to a certain extent. This exploration provided a reference for the research of enterprise financial risk early warning model based on Multi-access Edge Computing (MEC) and the Internet of Things. Kou (2019) believed that financial system risk was an important issue in economics and the financial system. In order to detect and cope with the systematic risk of the increasing amount of data generated in financial markets and systems, many researchers have increasingly adopted machine learning methods. Ma (2020) found that internet finance has developed rapidly, and various Peer-to-Peer (P2P) lending platforms have been launched. Peer-to-Peer (P2P) platforms are internet-based financial models that directly connect borrowers and lenders through digital platforms, bypassing traditional financial institutions to facilitate lending. While they offer advantages such as high efficiency and low barriers to entry, they also present issues such as credit, compliance and technical risks, particularly in the context of inadequate regulation, which can easily lead to financial risks. Fallah (2022) assessed the credit risk of individual and corporate customers in the banking system and believed that without accurate credit scores of customers, it would be impossible to estimate the credit risk of banks, financial institutions and insurance companies. Fendi (2017) believed that the stability of the financial system is an important factor for the stability of the entire economy. As an intermediary flow of funds, it is the main source of funds for most investments, as well as the deposit of surplus funds from households and enterprises. Wang (2022) used T-S neural network model to build a farmer credit risk early warning system. The institution can timely predict the occurrence and change of farmer credit risk and quickly take countermeasures to reduce losses. Lin et al. (2018) focused on system risk analysis to understand the dynamics of volatility, interdependence and risk during the recent financial crisis. Then, the time series dynamics and cross-sectional ranking of these system risk measures were reported. The above research shows that the application of economic risk early warning has a positive effect, but there are still some problems.

This paper studies the construction and empirical analysis of DE safety risk early warning evaluation system. First, it analyses the principle of DE and risk early warning, and then gives an analysis of the mature period of application, the replacement of old and new economies, and the point of economic development. It also subdivides the content of DE in safety risk early warning evaluation, and studies it through the methods of early warning evaluation system construction and empirical analysis. Finally, the relationship between DE and electric energy system is explained, which is a reference for this kind of research.

3 Design of security risk early warning system for cloud-based digital economy

3.1 Related theories

(1) *Background of DE*: The global economy is now becoming increasingly digital, and human society has entered a new era characterised by digital. DE plays an important role in the global economy and promotes economic and social development.DE is a new economic form, which comes into being with the arrival of the global digital era. It takes the use of digital knowledge and information as the core production factors, modern information network as the main carrier and the use of information and communication technology to improve efficiency and economic structure as the main driving force.

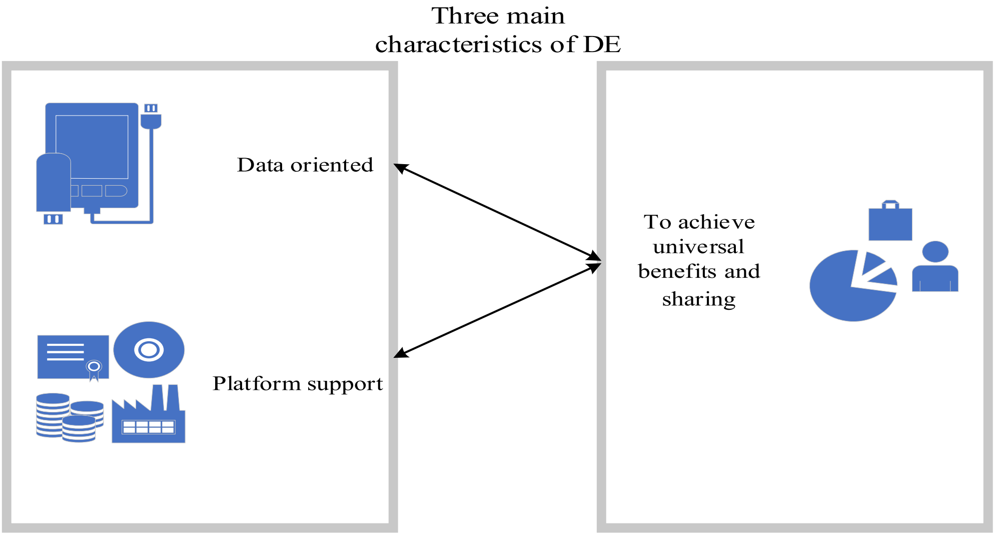
DE mainly has the following three characteristics, as shown in Figure 1.

With the emergence of the platform, the affordable infrastructure has emerged, which has enabled people to give full play to their potential and greatly reduced the cost of social information. Owing to the high digitalisation of business processes, enterprise data can be efficiently collected and stored, so that its business can be found all over the world. Now, with the continuous emergence of AI and other emerging technologies, the mining depth and speed are constantly improving and the traditional mining mode is gradually replaced by a new business ecology.

(2) *Cloud computing*: Cloud computing is a demand-based service that allows users and companies to easily obtain the required computing, storage and network resources without purchasing expensive software, hardware and network equipment. Based on online credit, a credit evaluation model based on big data has been established to adapt to more personal risk characteristics, so that all trading entities can participate in and benefit from it, thus promoting fair and equitable international trade.

(3) *Definition of risk warning*: As a comprehensive social initiative spanning economics, technology, management and organisational frameworks, the enterprise risk early warning system operates under inherent uncertainties across multiple dimensions. By establishing a risk assessment framework to predict potential hazards, this system serves as an effective mechanism for mitigating operational risks. Functioning as a vital safeguard for maintaining business continuity and maximising corporate value, the system identifies and manages commercial activities through risk analysis and control measures. Through proactive risk mitigation strategies, it prevents and resolves latent threats while minimising potential losses to the greatest extent possible.

Figure 1 Three main features of DE (see online version for colours)


Three main characteristics of DE
Data oriented
Platform support
To achieve universal benefits and sharing

3.2 Data acquisition and processing module

In the digital economy security risk early warning and evaluation system, the data collection and processing module is the foundation and core.It leverages the high concurrency and distributed characteristics of cloud computing architecture to collect, standardise and store heterogeneous data from multiple sources in real time, and provides high-quality data support for subsequent risk modelling and intelligent early warning. Digital economic activities cover multiple dimensions such as transactions and communications, and risk information presents high-dimensional, unstructured and dynamically changing characteristics. Traditional methods that rely on a single database and static sampling are difficult to meet real-time and global needs. To this end, in the module design, this paper integrates the cloud computing big data processing framework and intelligent preprocessing methods to achieve data governance throughout the life cycle.

In terms of data collection, the module uses a hierarchical and multi-channel collection mechanism. There are four types of data sources: first, user transaction data, such as online payment flows, order records, etc., can reflect the compliance of economic entities and transaction risks; second, network log data, such as server access records, can detect potential network attacks and abnormal traffic; third, public opinion data, from news, social media, etc., can monitor external risk signals and changes in user trust; fourth, third-party risk information, such as government early warning notices, etc. The collection uses message queuing (Kafka), distributed crawler technology and cloud load balancing strategies to ensure stable data throughput in a high concurrency environment.

In the data preprocessing link, the module adopts Extract, Transform, Load (ETL) process and big data cleaning technology for the redundancy, deletion and heterogeneity of data from different sources. First, in the data extraction stage, raw data is obtained from relational databases, log files and streaming interfaces; then in the data conversion stage, regular expression analysis, feature normalisation, timestamp alignment and other methods are used to achieve consistent data structure and timing synchronisation; finally, in the data loading stage, distributed storage and in-memory computing are used to achieve efficient write queries and ensure fast access to downstream modelling. When the data is cleaned, the mean interpolation and standard deviation test methods are used to deal with outlier and missing values.

After completing the data cleaning, the module also needs to standardise the risk factors of different dimensions to solve the problem of inconsistent dimensions. The transaction amount is usually in ‘yuan’, while the traffic in the network log is in Megabyte (MB). If directly entered into the model, the contribution of the indicator will be unbalanced. Therefore, the interval normalisation method is adopted to map the index data x_i to the range of [0, 1], and the formula is as follows:

$$x_i^{'} = \frac{x_i - \min(X)}{\max(X) - \min(X)} \tag{1}$$

$\min(X)$ and $\max(X)$ represent the minimum and maximum values of the indicator samples, respectively. Given the dynamic nature of digital economy risks, the system incorporates a streaming computing framework in cloud environments to perform window-based computation and real-time updates on data streams. For instance, when network traffic experiences sudden spikes accompanied by abnormal transactions, the system utilises a sliding window mechanism to promptly calculate the latest risk index and issue alerts, thereby enhancing both real-time responsiveness and warning accuracy.

3.3 Construction of risk index system

In the cloud-based digital economic security risk early warning and evaluation system, a scientific and reasonable risk index system is essential for accurate early warning and dynamic evaluation. The operation of the digital economy has the characteristics of multi-dimensional, multi-subject and high complexity. Risks are often intertwined in a chain reaction, and it is difficult for a single-dimensional measurement to fully reflect potential threats. This paper constructs a multi-level and quantifiable risk index system from the four dimensions of data security, transaction security, network security and platform reputation. It combines the expert scoring method and the information entropy weighting method to ensure that the index selection and weight distribution are scientific and objective. The data security dimension focuses on the security of the whole process of platform data, with indicators such as data encryption rate; the transaction security dimension focuses on the payment and settlement risks of economic entities, including indicators such as the proportion of abnormal transactions; the network security dimension covers system defense and operational stability, such as Distributed Denial of Service (DDoS) attack detection rate, etc.; The platform reputation dimension focuses on external trust and user perception, including user satisfaction. The four dimensions complement each other to form a point-line-surface combined risk monitoring pattern, which can not only reflect the internal operating conditions, but also take into account the external trust environment, and provide comprehensive and effective support for the early warning and assessment of security risks in the digital economy.

When selecting indicators, first use the expert scoring method for preliminary screening. Invite experts in the fields of network security, financial technology and big data governance to score based on the relevance, operability and availability of indicators, and set thresholds to eliminate low-weight or redundant indicators. The process can be expressed in a specific mathematical form.

$$S_j = \frac{1}{m}\sum_{i=1}^{m} s_{ij} \tag{2}$$

S_j represents the average score for the j-th indicator, s_{ij} is the score given by the i-th expert to indicator j and m is the total number of experts participating in the scoring.

When $S_j < 0$, the indicator is excluded, typically set within the range of 0.6 to 0.7, to ensure the simplicity and representativeness of the indicator system.

However, relying solely on expert experience tends to introduce subjectivity. Therefore, the Entropy Weight Method is introduced in the final weight allocation process to reflect the uncertainty of indicators' own information and their differences and importance. Let the standardised value of indicator *j* in sample *i* be q_{ij}, then the formula for calculating the information entropy of this indicator is:

$$E_j = -k\sum_{i=1}^{n} q_{ij} \ln\left(q_{ij}\right), \quad k = \frac{1}{\ln(n)}$$

where n represents the sample size and k denotes the normalisation constant to ensure entropy values E_j within the [0, 1] range. A higher entropy value indicates greater information content for a metric, suggesting its weight should be increased accordingly. This method retains expert qualitative judgment while using objective data to adjust weight distribution, enhancing the scientific rigor and adaptability of the indicator system. In practical implementation, our risk indicator framework comprises primary dimensions (e.g., data security) and multiple secondary indicators, each assessed through expert scoring and entropy weighting. For instance, in the data security dimension, if 'sensitive information leakage rate' shows significant variation in actual samples with low information entropy, its weight surpasses 'compliance inspection pass rate,' emphasising its critical role in risk alerts. This mechanism ensures both comprehensive coverage and adaptive weight adjustments according to data dynamics, thereby improving the system's adaptability to emerging risk scenarios and providing robust support for digital economy security early warning.

3.4 Risk modelling and intelligent warning algorithm

In the digital economy security risk early warning system, risk modelling and intelligent alerts form the core of platform protection. Within this ecosystem, platform operational data exhibits complex characteristics – heterogeneous multi-source data with temporal variations – which traditional static evaluation methods struggle to handle sudden incidents or incomplete data sets. This study employs the Grey Prediction Model (GM) (1, 1) for risk prediction and anomaly detection, leveraging cloud computing infrastructure to enable real-time dynamic alerts that provide scientific decision-making support for platform administrators. The grey system approaches stochastic processes as regular time series through modelling and forecasting, requiring minimal computational resources and information input. The calculation formula is:

$$x^0(k) + az^{(1)}(k) = b \tag{4}$$

Among them, *a* and *b* are constants, which reflect the law of change and predict the future development trend. The value of the next stage is calculated iteratively with the current value, and the calculation formulas are as follows:

$$\hat{x}^{(1)}\left(k+1\right) = \left[x^{(1)}(0) - \frac{b}{a}\right]e^{-ak} + \frac{b}{a} \tag{5}$$

$$\hat{x}^{(0)}\left(k+1\right) = \hat{x}^{(1)}\left(k+1\right) - \hat{x}^{(1)}(k) \tag{6}$$

Formula (2) is the discrete response to the grey differential formula. $x^{(1)}$ is reduced once to restore it to a grey prediction model formula (3), namely $x^{(0)}$.

The calculation formulas of residual error ε and precision p^0 are:

$$\varepsilon(k) = \frac{x^{(0)}(k) - \hat{x}^{(0)}(k)}{x^{(0)}(k)} \times 100\% \tag{7}$$

$$\varepsilon(avg) = \frac{1}{n-1}\sum_{k=2}^{n} |\, \varepsilon(k)\, | \tag{8}$$

$$p^0 = \left(1 - \varepsilon\left(avg\right)\right) \div 100\% \tag{9}$$

Among them: $x^{(0)}(k)$ is the actual value and $\hat{x}^{(0)}(k)$ is the model value; accuracy can determine the level of grey model.

In practical application, the system combines the multidimensional risk index system constructed in the early stage and the weights of F-AHP or information entropy method to form a comprehensive risk index:

$$R_t = \sum_{i=1}^{n} w_i \hat{x}_i^{(0)}\left(t\right) \tag{9}$$

The Comprehensive Risk Index dynamically visualises weighted trends of various risk indicators across the platform, triggering real-time alerts when thresholds are exceeded. The cloud computing environment provides efficient data processing and storage capabilities, supporting parallel computation and streaming processing of large-scale multi-source data to ensure timely and accurate warnings. The system incorporates a rolling update mechanism to enhance risk prediction accuracy and anomaly detection precision. By dynamically adjusting grey prediction model parameters with newly collected data, it continuously updates predictions over time, improving short-term forecasting accuracy and sensitivity to emergencies. During anomaly detection, the system calculates deviations between predicted values and actual observations. When thresholds are exceeded, anomalies are identified and risk levels adjusted based on the Comprehensive Risk Index, enabling multi-dimensional dynamic alerts. This solution is applicable to scenarios such as abnormal trading activities and cyber-attack outbreaks, significantly reducing risk response times.

The deep integration of grey prediction algorithms with cloud computing distributed architecture constitutes a key advantage in the digital economy risk early warning system. Leveraging the Spark Streaming framework, the system processes real-time data streams including transaction records, network logs, public sentiment analysis and third-party risk indicators into the GM (1, 1) model for sliding window-based dynamic prediction. Real-time weighting of risk metric predictions updates the composite risk index, enabling comprehensive platform-wide risk monitoring. The cloud's elastic computing capabilities ensure low-latency predictions with high accuracy even under high-concurrency and large-data scenarios. This algorithm demonstrates distinct advantages: accurately predicting risk trend patterns in small-sample, highly volatile data environments; integrating with distributed cloud processing to achieve real-time data stream handling and sliding window prediction. After weighting through F-AHP or information entropy methods to generate the composite risk index, the system performs dynamic risk assessment, anomaly detection and real-time alerts, providing scientific and actionable technical support for secure digital economy platform operations.

4 Simulation experiment of DE safety risk early warning evaluation system construction

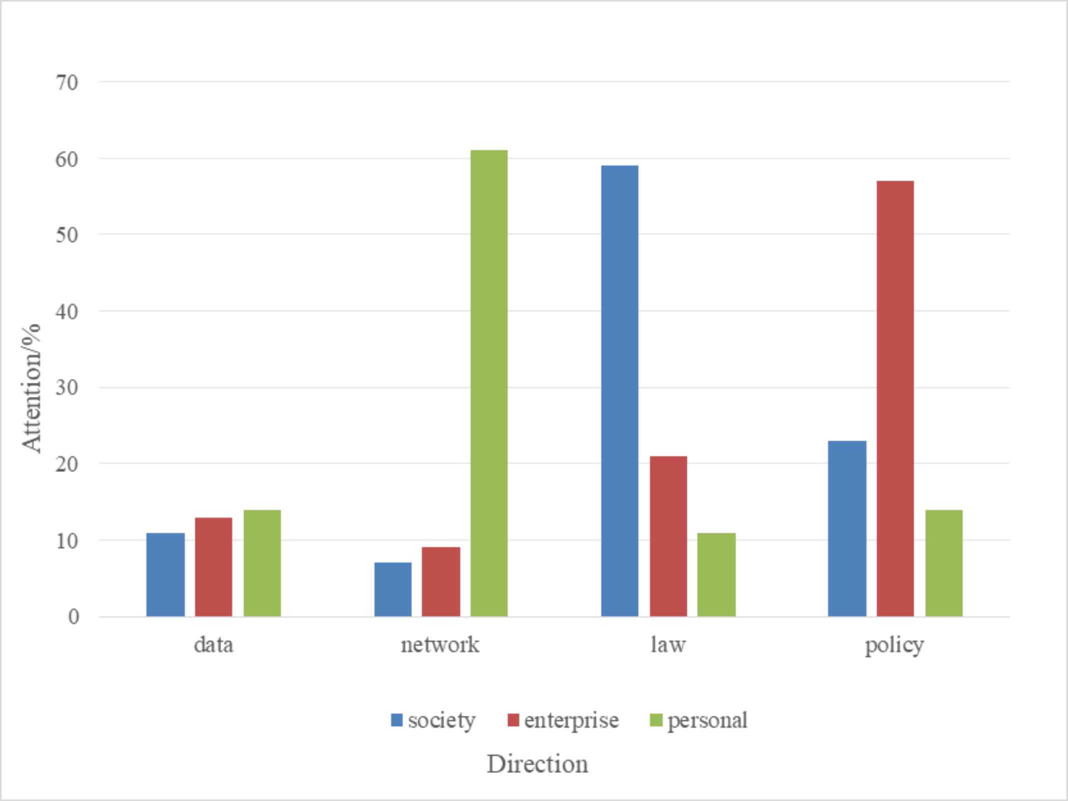
This empirical study selected a regional digital economy service platform as the experimental subject, collecting multi-source data including transaction logs and network access records over six months. First, we utilised cloud computing-based data collection and pre-processing modules to standardise raw data, fill in missing values, and handle outliers, thereby constructing a data set compliant with the risk indicator system. Subsequently, we applied F-AHP algorithm to determine indicator weights and employed GM (1, 1) grey prediction algorithm for dynamic risk index forecasting, generating a comprehensive risk index with threshold-based early warning mechanisms. During validation, the system was compared with traditional single-machine static evaluation methods through metrics including prediction accuracy, response latency and anomaly detection rate to assess the performance of the early warning system. Table 1 shows the analysis of the digital economy scale and the proportion of Gross Domestic Product (GDP) in the region in 2017–2022.

Economic security risk analysis is conducted at three levels: society, enterprise and individual, as shown in Figure 2.

Table 1 Analysis of the proportion of digital economy scale and GDP in this region from 2017 to 2022

	2017	*2018*	*2019*	*2020*	*2021*	*2022*
Economic scale/100 million yuan	359730	378920	412900	469830	491030	587900
Proportion of GDP/%	28.3	33.5	37.6	39.7	40.8	42.3

Figure 2 Attention analysis of economic and security risks (see online version for colours)



It can be seen from Figure 2 that society, enterprises and individuals paid different attention to the possible risks of economic security at different levels. It can also be clearly seen that in addition to data, the network, law and policy were highly concerned in the three levels. Among them, the social attention to the law was 59%, so all economic activities need to be carried out within the scope allowed by the law; enterprises payed 57% attention to policies, because policies may bring financial fluctuations to enterprises, and they need to change their own business methods according to policies; the personal attention to the network was 61%. In this era of the internet, most of the information that people knew comes from the internet, so the personal attention to the network is high. The average attention of the data in the three levels was 12.7%; the average attention of the network in the three levels was 25.7%; the average attention of law in the three levels was 30.3%; the average attention of the policy in the three levels was 31.3%. It can be seen that the average concern of the policy was the highest. Therefore, when discussing DE security risks, people should focus on the policy direction.

In this experiment, to verify the effectiveness of cloud-based grey prediction methods in digital economy security risk early warning, we compared them with three commonly used machine learning approaches –: Random Forest (RF), Support Vector Machine (SVM) and Convolutional Neural Network (CNN). The experiments utilised the same data set encompassing transaction logs, network access records, system operation data and public sentiment information. A unified preprocessing and standardisation process was implemented to ensure fairness. Each method underwent 10 independent trials under identical conditions, with the prediction accuracy rates recorded for each trial. The results are specifically illustrated in Figure 3.

As shown in Figure 3, the digital economy security risk early warning system developed by this study using grey prediction and cloud computing demonstrates significant advantages in accuracy. Through 10 experimental runs, the proposed method maintained an accuracy rate between 0.90 and 0.92 with minimal fluctuations, exhibiting high stability and reliability. Traditional machine learning methods like RF achieved 0.84–0.85 accuracy, CNN 0.85–0.87, while SVM only reached 0.80–0.82. These conventional approaches face limitations when handling small sample sizes, high volatility and multi-source heterogeneous data, often being susceptible to abnormal data impacts that lead to unstable or low prediction accuracy. By employing grey prediction algorithms for short-term trend modelling, our method effectively captures risk indicator patterns, making it particularly suitable for digital economies with limited data volumes or frequent updates. Furthermore, cloud computing’s distributed processing and elastic scheduling capabilities enable rapid handling of multidimensional risk indicators in high-concurrency scenarios, ensuring real-time dynamic alerts. Experimental results conclusively demonstrate that our method outperforms traditional machine learning approaches in precision, stability and real-time responsiveness, showcasing both technical advantages and practical applicability.

To evaluate the performance of the digital economy security risk early warning system in incident response, comparative experiments were conducted between the grey prediction and cloud computing-based method and three commonly used machine learning approaches – Random Forest (RF), Support Vector Machines (SVM) and Convolutional Neural Networks (CNN). The experiments utilised the same data set containing transaction logs, network access records and system operation information to ensure consistent operational conditions for all methods. Each method underwent 10 experimental runs, with recorded average latency from risk event occurrence to complete detection and resolution. The results are specifically illustrated in Figure 4.

Figure 3 Comparison of early warning accuracy across methods (see online version for colours)

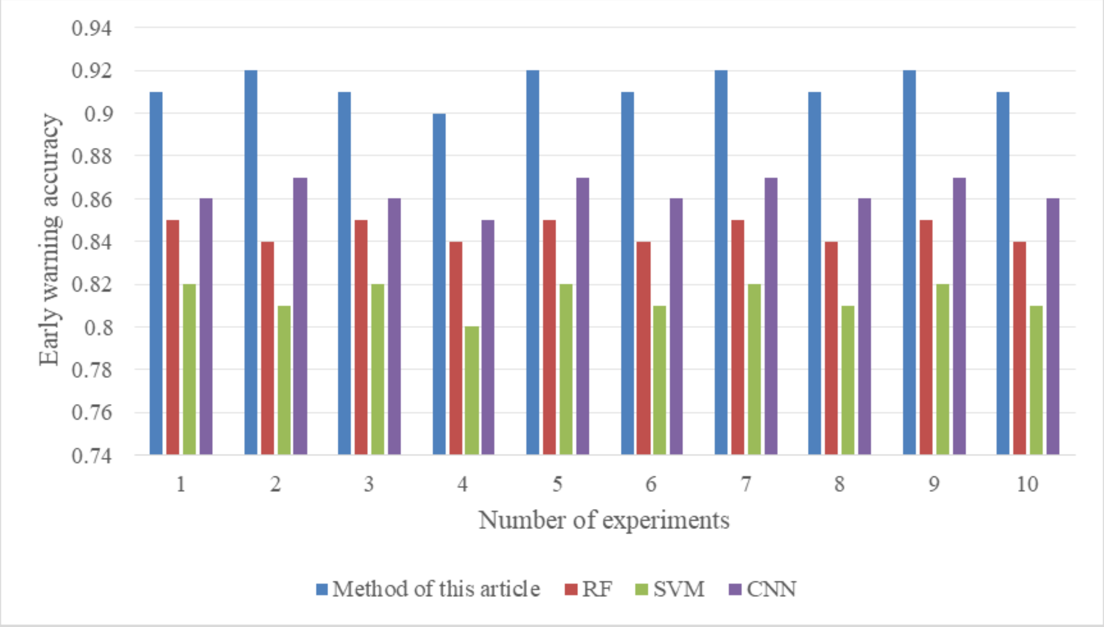
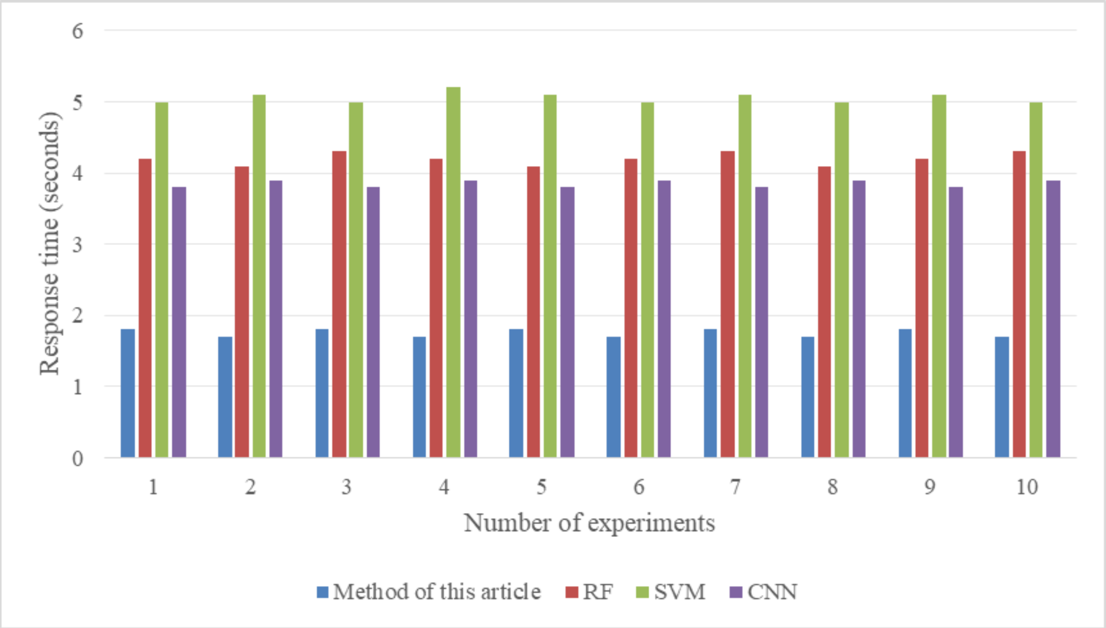


Figure 4 Comparison of risk response speed among different methods (see online version for colours)



As shown in Figure 4, the risk early-warning system developed in this study demonstrates significant advantages in response speed. In 10 experimental runs, the average response time of our method remained stable at 1.7–1.8 seconds, showing exceptional stability and real-time performance when processing multi-source heterogeneous data and high-concurrency risk events. In contrast, the random forest method averaged 4.1–4.3 seconds, CNN 3.8–3.9 seconds, while Support Vector Machine (SVM) lagged behind with 5.0–5.2 seconds, highlighting the inefficiency of traditional machine learning methods when handling dynamic high-frequency data. Our approach excels through three key aspects: 1) Dynamic modelling of short-term risk trends using grey prediction algorithms; 2) Cloud computing-based distributed processing enabling rapid computation and real-time updates, allowing swift generation of alerts and reduced response latency; 3) Comprehensive analysis of multidimensional risk indicators through dynamic weighting and rolling update mechanisms, ensuring fast, accurate and comprehensive early-warning responses. Overall, this method enhances platform security incident handling efficiency, strengthens digital economy platforms' adaptability in complex environments and provides reliable technical support for real-time dynamic alerts and scientific decision-making.

In this experiment, to comprehensively evaluate the performance of the digital economy security risk early warning system, evaluation indicators including Recall and False Positive Rate, resource utilisation efficiency and other multidimensional metrics were adopted to holistically assess the system's performance in real-time dynamic alerts, computational efficiency, stability and resource scheduling. Specific experimental details are shown in Table 2.

Table 2 Multidimensional indicator results of the digital economy platform risk early warning system

Evaluation index	*Method of this article*	*RF*	*SVM*	*CNN*
False positive rate (%)	5	12	15	10
System throughput (bar/s)	1500	900	800	1200
Recall (%)	94	89	88	90
CPU (Central Processing Unit) utilisation (%)	65	70	60	75

As shown in Table 2, the proposed method demonstrates a significant advantage with a false positive rate of only 5%, compared to 12% for random forest, 15% for SVM and 10% for CNN. This indicates that through comprehensive multidimensional analysis and dynamic modelling using grey prediction, the proposed method effectively reduces false positives and enhances early warning credibility. In terms of system throughput, the proposed method achieves 1500 packets/second, far exceeding RF's 900 packets/second and SVM's 800 packets/second, while slightly surpassing CNN's 1200 packets/second. This highlights the efficient processing capabilities of cloud computing distributed systems in handling multi-source heterogeneous data. The Recall metric shows that the proposed method identifies 94% of actual risk events, outperforming the other three methods in detecting true risks more reliably. Additionally, the proposed method maintains a CPU utilisation rate of 65%, lower than the peak occupancy of CNN and RF, demonstrating high resource scheduling efficiency. In summary, the proposed method exhibits significant advantages across multiple aspects, fully validating the practicality and technical superiority of the grey prediction-based cloud computing early warning system in real-time dynamic alert scenarios.

5 Conclusion

The development of digital economy has become the engine of high-quality economic development. How to enhance the risk prevention of digital economy while promoting the development of digital economy has become a major challenge in the development of digital economy in China. This paper establishes a digital economy security risk early-warning and assessment system within cloud computing environments. By leveraging a multi-dimensional risk indicator framework, F-AHP weighting allocation and grey prediction algorithms, the system conducts comprehensive monitoring and dynamic alerts for data security, transactional integrity, network vulnerabilities and platform credibility. The distributed architecture of cloud computing endows the system with robust capabilities, featuring high throughput and elastic resource scheduling that ensures stable and efficient operation even under heavy concurrent data processing and large-scale platform operations. Moreover, this architecture effectively reduces peak CPU and memory consumption, demonstrating excellent resource utilisation efficiency and scalability. Overall, the system developed in this study theoretically refines the risk early-warning methodology for the digital economy while providing practical tools for platform risk prevention and security management. It facilitates enhanced security assurance and intelligent risk management in future digital economic environments, thereby laying a solid foundation for the secure development of the digital economy.

Acknowledgement

This study is supported by Financial Innovation and Multi-Asset Intelligent Trading Laboratory of the Key Laboratory of Philosophy and Social Sciences in Hainan Province of University of Sanya.

Declarations

All authors declare that they have no conflicts of interest.

References

Banalieva, E.R. and Dhanaraj, C. (2019) ‘Internalization theory for the digital economy’, *Journal of International Business Studies*, Vol. 50, No. 8, pp.1372–1387.

Fallah Shams, M. (2022) ‘Designing credit risk early-warning system for individual and corporate customers of the bank using multiple logit comparison model and survival function’, *International Journal of Finance and Managerial Accounting*, Vol. 7, No. 25, pp.163–177.

Fendi, U. (2017) ‘Early warning indicators for monitoring non-performing loans in Jordanian banking system’, *International Journal of Business and Social Science*, Vol. 8, No. 6, pp.104–114.

Khitskov, E.A. (2017) ‘Digital transformation of society: problems entering in the digital economy’, *Eurasian Journal of Analytical Chemistry*, Vol. 12, No. 5, pp.855–873.

Kou, G. (2019) ‘Machine learning methods for systemic risk analysis in financial sectors’, *Technological and Economic Development of Economy*, Vol. 25, No. 5, pp.716–742.

Lin, E.M.H, Sun, E.W. and Yu, M-T. (2018) ‘Systemic risk, financial markets, and performance of financial institutions’, *Annals of Operations Research*, Vol. 262, No. 2, pp.579–603.

Ma, L. (2020) ‘Early warning for internet finance industry risk: an empirical investigation of the P2P companies in the coastal regions of China’, *Journal of Coastal Research*, Vol. 106, No. SI, pp.295–299.

McKinnon, R. (2019) ‘Introduction: social security and the digital economy-managing transformation’, *International Social Security Review*, Vol. 72, No. 3, pp.5–16.

Sturgeon, T.J. (2021) ‘Upgrading strategies for the digital economy’, *Global Strategy Journal*, Vol. 11, No. 1, pp.34–57.

Tan, K.H. (2017) ‘Using big data to make better decisions in the digital economy’, *International Journal of Production Research*, Vol. 55, No. 17, pp.4998–5000.

Viriyasitavat, W. (2019) ‘Blockchain and internet of things for modern business process in digital economy – the state of the art’, *IEEE Transactions on Computational Social Systems*, Vol. 6, No. 6, pp.1420–1432.

Wang, H. (2022) ‘Model and application of farmers’ credit risk early warning system based on TS fuzzy neural network application’, *Mathematical Biosciences and Engineering*, Vol. 19, No. 8, pp.7886–7898.

Zaloznova, Y. and Trushkina, N. (2019) ‘Management of logistic activities as a mechanism for providing sustainable development of enterprises in the digital economy’, *Virtual Economics*, Vol. 2, No. 1, pp.64–81.

Zeng, H. (2022) ‘Influences of mobile edge computing-based service preloading on the early-warning of financial risks’, *The Journal of Supercomputing*, Vol. 78, No. 9, pp.11621–11639.