Hindawi
Security and Communication Networks
Volume 2024, Article ID 9754091, 1 page
https://doi.org/10.1155/2024/9754091

Retraction

Retracted: Deconstruction of the Innovation Path of Digital Transformation Based on Network Big Data Security in the Context of Smart City

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Chen, P. Chen, and G. Chen, "Deconstruction of the Innovation Path of Digital Transformation Based on Network Big Data Security in the Context of Smart City," *Security and Communication Networks*, vol. 2022, Article ID 8800489, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8800489, 10 pages
https://doi.org/10.1155/2022/8800489

Research Article

Deconstruction of the Innovation Path of Digital Transformation Based on Network Big Data Security in the Context of Smart City

Tang Chen,[1] Pengyu Chen ,[2] and Guang Chen[3]

[1]*School of Economic and Management, Southwest Jiaotong University, Chengdu 610031, Sichuan, China*
[2]*School of Continuing Education, Sichuan Institute of Industrial Science and Technology, Deyang 618500, Sichuan, China*
[3]*School of Public Administration, Southwest Jiaotong University, Chengdu 610031, Sichuan, China*

Correspondence should be addressed to Pengyu Chen; cpy001@tch.scit.edu.cn

Received 25 August 2022; Revised 20 September 2022; Accepted 27 September 2022; Published 11 October 2022

Academic Editor: Tarni Mandal

Digital transformation means that traditional enterprises have combined commerce, administration, and manufacturing with cloud services, the use of big data, and the web to advance the modern transformation of their research and development, creation, manufacturing and assembly, administration of operations, commercial support, and more tasks. Digital transformation showed that only companies can radically and completely (or substantially and completely) redefine their business—not just IT but all aspects of organizational activities, processes, business models, and employee capabilities. Only then can success be achieved. This paper aimed to study the innovative path of digital transformation and propose a network-based big data security method. Combined with the experimental analysis, it was concluded that using network big data security to monitor computer and network security (CNS), the attack detection accuracy rate is up to 99.8%. It can be seen that this method can accurately capture the shortcomings and leaks in the process of digital transformation, help achieve targeted path innovation, and improve the technological improvement and asset income growth of enterprises in the context of smart cities.

1. Introduction

At present, as a new type of economy to replace the economic society, the digital revolution, and the agrarian industry, the digital economy is increasingly becoming a new engine for global economic expansion. Along with digitalization expanding so quickly, this series of technologies, such as AI, the Internet of things, 5 G, industrial Internet, cloud computing, blockchain, etc., has presented the growth of established sectors with a number of previously unheard-of obstacles in the world. Moreover, as economies enter a new stage of economic development, economic growth slows and traditional competition intensifies. Manufacturing is facing unprecedented challenges such as rising labor costs and declining productivity. The traditional low-cost business development system that once relied on low overhead has lost its place, the company boundary has gradually faded, and industry competition has gradually expanded in the traditional manufacturing and Internet industries. Therefore, transforming the traditional manufacturing industry improves the allocation of resources, adjusts the industrial structure, and achieves change and development. This has become a crucial duty of the current strategy.

With the advent of the new technological revolution, cities are accelerating the transition of enterprise business to digitalization. For example, banks and small and medium-sized banks must keep up with the trend of digitization to advance their retail operations. Most of the existing research on the digitization of retail business is based on joint-stock enterprises and government institutions. City commercial banks lag far behind state-owned banks and enterprises in the digital transformation of retail business. The strategy of digital transformation has also been formulated with reference to such large banks, but the feasibility of implementation is low and the transformation effect is insufficient. At present, city commercial banks are the main battlefield of digital transformation, and studying the digital transformation of the retail business of city commercial banks is crucial for various purposes.

There are two innovations in this paper. First, based on the characteristics of three components of net media manipulation are suggested for CNS regulation against the backdrop of big data, and a CNS control mechanism model is established around the three parts of security control. The other is based on whether to propose three parts of CNS control. This paper is based on a literature analysis. Through expert research and feedback, a CNS and control evaluation management system under the background of big data is constructed.

2. Related Work

The Internet in light of the current age of smart cities has won the research of many scholars. Daniel C introduced that the application of smart cities has been facilitated by technological advancements in several domains [1]. Gasco-Hernandez specialized in illustrating the lessons learned from building a smart city in Barcelona [2]. In order to comprehend and control various innovations and changes, Bygstad and Øvrelid created the idea of multiple developments [3]. Purchase et al. investigated the sequence of events and the creative pathways and trajectories that college-turncompanies eventually took [4]. Vial constructed a digital transformation framework on the basis from which a research agenda was developed that suggested examining the role of dynamic capabilities and taking ethical issues as important avenues for future digital transformation strategy IS research [5]. The disadvantage of this is that the network's big data security aspect is poorly designed.

Related research on network big data security includes the following: Jiang studied CNS and cyber protection based on big data processing and wireless technology [6]. The research by Xie had shown the efficiency of the hazard-adjusted authentication scheme [7]. Hou et al. created the divided map version table (DMVT), a new type of dataset, to facilitate signaling pathway database operations effectively [8]. SungJin and Kangseok proposed a normal network study of conduct methods based on big data analysis technology. The proposed method uses Hadoop/Hive for big data analysis and R for statistical calculation [9]. Garg et al. designed a VANET surveillance system using 5 G and cloud technologies units to communicate effectively and computing capabilities in modern smart city environments [10]. However, the above research did not reflect the introduction of network big-data security experimental methods.

3. Methods of Digital Transformation Based on Network Big Data Security

3.1. Digital Transformation Solutions. Technological progress has always been the main driver of social progress, both from a historical perspective and from a comparative research perspective. In the past three hundred years, there have been four industrial revolutions with common patterns and trends in human society. Every industrial revolution has two main lines running through it: one is the change of production conditions and the improvement of efficiency based on the development of productive forces. Second, the accumulation of social data reflects logical changes. The fourth industrial revolution has a greater and deeper involvement in the development and implementation of digital technology, which marks a new stage in the development of human society. The big data, blockchain, AI, and Internet of things technologies that support Internet technology have led to the transformation and reconstruction of the world's organizational structure, management system, and management technology [11]. For example, the digital government in smart cities, the research trend of its digital transformation, and the cognition results of each bank on digitalization are shown in Figures 1 and 2, respectively.

Digital transformation is a pervasive change encompassing technologies and systems, with various impacts on government organizations, societies, and citizens. The technological impact of this change is evident through government balance sheets, energy and efficiency improvements, regulations, and effective governance. The value structure is most evident in the values that confer principle, a high degree of understanding, reliability, low distortion, strong accountability, and responsiveness. The impact of technology and innovation plays an important role in the entire government quality system, so there is a need to re-evaluate standards under new technologies, environmental conditions, and regulatory frameworks [12, 13]. The response of government organizations to this change is particularly evident in economic development, coordination and quality, fairness and integrity, democratic trust, and effective governance.

In the process of digital transformation, the transformation of government functions must first consider the basic support for promoting social and economic development, improving the quality of government, and the observation indicators of the core quality level. While government performance, government effectiveness, and early quality assessments tend to over-rely on economic indicators, GDP-oriented approaches are considered errors and "bias" in actual implementation [14]. But this does not mean that indicators related to economic construction and development are deliberately avoided, moving from one extreme to the other.

In the context of digital transformation, the impact of government quality on the economy is not only reflected in traditional economic improvement but also in the transformation and rise of the digital economy. The transformation of data as a factor of production has promoted the transformation of the traditional economy and has also brought about new infrastructure and a new economic center of gravity [15]. From the perspective of reforming the old for the new, the quality of government plays a role in regulating, promoting, and guiding the quality of economic development. In turn, economic growth has become a new driving force for improving the quality of government.

In the process of digital transformation, the business model of technology-driven, platform-based, computerized, and database-based operations has surpassed the traditional physical space management and service model, requiring its institutional scale and functional adaptability [16]. In particular, the reform of the supporting system and mechanism

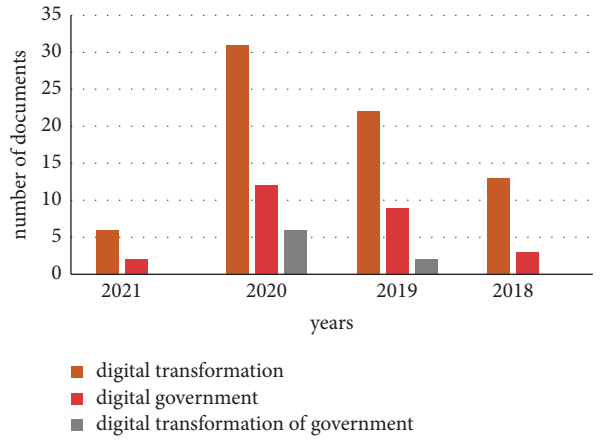

Figure 1: Digital transformation research trend figure.

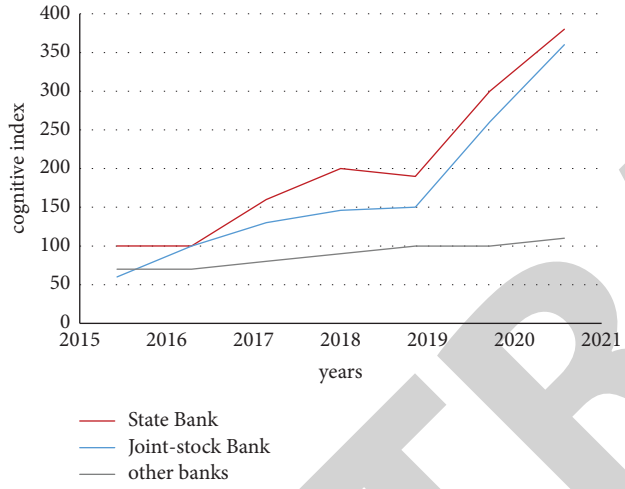

Figure 2: Banking digital awareness index.

of big data management, its structural adjustment, and its performance, as well as the obvious level changes in government scale, management cost, and government efficiency, all reflect future-oriented norms that have a broad impact on the quality of government.

In the construction of digital management for smart cities, it is necessary to improve administrative efficiency, reduce link losses, and save costs through service-oriented value process transformation and platform construction [17].

3.2. Construction of Network Big Data Security Control Mechanism. The process of building a CNS management and control mechanism in the context of big data focuses on creating CNS issues, clarifying security protection and control objects, organizing relevant managers and employees, and scientifically assigning tasks and tasks. Effectively organize the workforce, allocate security investment and other factors, set up special network information security agencies and departments, formulate network information security rules and regulations, and ensure the process of their implementation. In the evaluation of CNS management, the most effective factors must be determined, so scientific principles must be followed, which is an indispensable choice to make the evaluation results effective [18]. Due to the comprehensiveness of the current situation of CNS based on big data, the evaluation should start from a comprehensive perspective, pay attention to the effectiveness of the evaluation, simplify the evaluation procedure, and make data collection and quantification easier. The current network data and information security status is shown in Table 1.

This paper summarizes and expands the components of the regulating mechanism and extends the mouse. The extended meaning of "network control" includes CNS management objects and CNS administrators, the word "environment" best describes the management unit, and the extended meaning is network equipment, network culture, policies, and regulations. "Technology" may be summed up as the means and means of control. Its expanded definition covers four areas: avoidance, confidentiality, control, and investigation [19]. The evaluation model of the CNS control mechanism is shown in Figure 3:

The first step in any cybersecurity environment cognition process is to analyze and identify the characteristics of the cybersecurity environment [20]. Mining techniques can be divided into two types of feature enhancement methods: standard scaling and nonstandard scaling. Traditional linear regression methods include principal component analysis (PCA), linear discriminant analysis (LDA), etc. [21]. These methods basically find the best linear model under different optimization criteria. The most representative nonlinear dimensionality reduction methods include kernel methods and multiple learning methods, typically equidistant features, Laplacian features (LE), etc.

3.2.1. Principal Component Analysis. Given P features and n moments, derive the basic information matrix of the security model:

$$X = \begin{vmatrix} y_{11} L\ y_{1p} \\ MO\ \ M \\ y_{n1} L\ y_{np} \end{vmatrix}. \tag{1}$$

The fit matrix is the original model of the safety features, and the fit of the feature data is based on the mean data and variance. Adjust the original Y matrix data model, that is, perform a standard transformation on each data item. The transformation process is given as follows:

$$X_{ij} = \frac{Y_{ij} - \overline{Y_j}}{B_j} \ (i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, p). \tag{2}$$

The formula sample mean is

$$\overline{Y_i} = \frac{1}{n} \sum_{m=1}^{n} Y_{ki}. \tag{3}$$

Table 1: Status of CNS monitoring in 2009–2010.

Monitoring content	Year 2009	Year 2010	Range of change
Total number of trojan control server IPs	609436	476926	21.7% lower
Trojan controlled host IP number	2751979	10317169	274.9% increase
Total number of botnet control server IPs	22818	13782	39.6% lower
Total IPs of botnet controlled hosts	11911067	5622023	52.8% lower

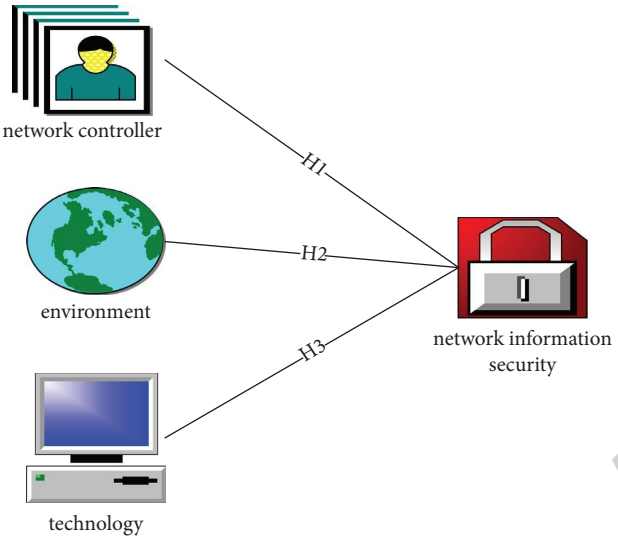

Figure 3: Network information security control evaluation model.

The sample standard deviation is

$$B_i = \sqrt{\frac{1}{n-1}\sum_{m=1}^{n}\left(Y_{ki} - \overline{Y_i}\right)^2}. \tag{4}$$

Analyze the relationship between each feature and compare the alignment of different elements of the two features. Generate a correlation matrix. For the behavior of P, the evaluation matrix can be obtained by two-way comparison,

$$P = \left(r_{ij}\right)_{p\times p}. \tag{5}$$

Among them, $r_{ij} > 0$, $r_{ji} = 1/r_{ij}$, $r_{ii} = 1$.

$$R = \frac{1}{N}\sum_{i=1}^{N} X_i X_i^T. \tag{6}$$

Assuming that R is the correlation matrix obtained by solving, its characteristic formula solving formula is

$$\lambda_i U = RU. \tag{7}$$

3.2.2. Linear Discriminant Analysis. Let the sample type be class C, there are N kinds of samples, and the number N_i is the number of samples in this class. Train a model X with a mean of m_i for class i and a mean of m for all samples.

One way to find the space separating the different classes is to maximize the rank $Z_{\max}$ of the interclass discrete matrix and minimize the rank $Z_{\min}$ of the interclass discrete matrix, calculated as follows:

$$\begin{aligned} S_{\max} &= \sum_{i=1}^{D} N_i (m_i - m)(m_i - m)^T, \\ S_{\min} &= \sum_{i=1}^{D}\sum_{j=1}^{N_i}\left(\overline{x_j}^{(i)} - m_i\right)\left(\overline{x_j}^{(i)} - m_i\right)^T. \end{aligned} \tag{8}$$

The objective function of LDA linear discrimination is

$$M_{LDA}(W) = \max_{W}\frac{W^T S_{\max} W}{W^T S_{\min} W}. \tag{9}$$

LDA optimization can be transformed into a solution to a mixed eigenvalue problem, let

$$\lambda = \frac{W^T S_{\max} W}{W^T S_{\min} W}. \tag{10}$$

It can be got

$$S_{\max} W = \lambda S_{\min} W. \tag{11}$$

This paper uses AHP to determine every index's weighting in the index system to reflect the difference in the scoring system, which is related to the importance of the value index to improve the actual operation of the evaluation system. The scoring matrix is constructed using a professional method, and the calculation method used is the total sample method [22]. The elements of each column of the evaluation matrix are normalized, and the general terms of the elements are as follows:

$$p_{ij} = \frac{p_{ij}}{\sum p_{ij}}\,(i, j = 1, 2, 3 \ldots n). \tag{12}$$

The normal case matrix for each column is added row by row as follows:

$$\sum_{W_i=j=1}^{n} b_{ij}\,(i, j = 1, 2, 3 \ldots n). \tag{13}$$

Then, the approximate solution of the desired eigenvector is

$$w = (w_1, w_2, \ldots\ldots, w_n)^T. \tag{14}$$

3.3. Dimensionality Reduction Model of Network Big Data Model. The main idea of the subspace method is to transfer large spatial data through linear or nonlinear methods. They can be transformed into low- or high-dimensional, or even

infinite, data, making the data more suitable for classification and reducing computational costs. LDA has limited ability to discriminate large amounts of data and is sensitive to sample size. In general, the samples must have a Gaussian distribution. The kernel method is a nonlinear map recognition method. By default, it consists of a kernel function and a standard learning process. It organizes the nonlinear feature data into a multidimensional feature space and uses a linear method to complete the data extraction. The advantage of the kernel method is that by choosing an appropriate kernel function, the nonlinear problem in the real space can be transformed into a linearly separable problem in the feature space. That is, the nonlinear transformation is used to introduce the X space and design in the F kernel feature space to construct a new distribution function and decrease the evaluation in processing data mapping and feature development [21]. The internal model in the kernel feature space is defined as follows:

$$k(x, y) = \langle \Phi(x), \Phi(y) \rangle. \tag{15}$$

The most important thing in the kernel method is the analysis of the kernel function, which needs to be constructed based on the kernel function related to the application problem. Commonly used kernel functions include the linear kernel function, the multiplication kernel function, the Gaussian kernel function, and the sigmoid function.

$$\begin{aligned} h(x, y) &= x^T y, \\ h(x, y) &= \left(1 + x^T y\right)^d, \\ h(x, y) &= \exp\left(-\frac{\|x - y\|^2}{2\alpha^2}\right), \\ h(x, y) &= \tanh\left(x^T y + \alpha\right). \end{aligned} \tag{16}$$

At present, the kernel methods all use a single kernel function. In real multisource heterogeneous data, people are more likely to use multi-kernel learning. Multi-kernel learning is the best linear combination of well-known kernel functions, which also subverts machine learning by providing useful methods for solving complex problems and building new kernel functions. For different data features, multi-kernel learning can be used by selecting kernel functions with different parameters or a combination of different types of kernel functions.

4. Network Big Data Security Experiment and Deconstruction

4.1. Mechanism Method Deconstruction. From the orthogonal transformation, as few total variables as practical can be extracted. The original variable occurs multiple times. Combining empirical summaries of government quality content with the impact of digital transformation, we can first identify six front-line indicators of the rating system. However, there still seem to be only a handful of 20 secondary indicators supporting the main one. This not only increases the difficulty of the calculation but also does not contribute to a comprehensive interpretation of the independent variables.

This paper investigates and compares the visual performance of different government quality information in 31 provinces (autonomous regions and municipalities), and obtains the correct rankings under various indicators through vertical comparison. However, the effectiveness of government in digital transformation is a complete and integrated process. According to the above situation, it is necessary to bridge the differences in nature and scale as much as possible [23], and scientifically evaluate the weight of each indicator to determine the above content. The horizontal list is full of corrections for different indicators. After selecting the government performance indicators as a set of indicators, it is necessary to adjust the Z-scores of 16 items in the other five categories of indicators. The total variance explanations of various types are obtained as shown in Table 2.

Combined with the eigenvalue system shown in Figure 4, it can be found that the curve converges significantly after the sixth part, so it is good to choose five factors as the result of the main analysis. Furthermore, the ever-expanding number of principal components increases statistics and complexity, deviating from the original intent of the research methodology.

4.2. Information Security Evaluation System under the Background of Network Big Data. The current big data network faces many challenges, among which security issues are the main ones. In February 2015, the monitoring equipment of a public security system failed and could not be identified. In October, the Alipay computer room network cable was cut off, and services in other areas were interrupted, making the website unavailable for 12 hours. Numbers are a problem people will face now and for a long time to come. Data leakage, Gmail's 5 million data leakage, etc. These incidents have increased people's worries about the data security of the big network, followed by worrying about the security of the main network during data transmission. Based on the perception of network data security, the results of the dimensionality reduction experiment in this paper show that in terms of time efficiency, five attacks on the Gafgyt botnet are as follows: the average reduction time is 4.0760 seconds for Single_AE, 5.3411 seconds for DeN_AE, 5.3166 seconds for SAE, 6.4456 seconds for Convol_AE, and 6.4456 seconds for K_CNN.

The average output value of the Hybrid Core Sparse Autoencoder (MK_SAE) feature extraction algorithm on the Gafgyt IoT botnet dataset is compared with the average output value on the KDD CUP99 dataset, and the comparison results are shown in Figure 5.

The results show that the feature extraction algorithms of MK_SAE all obtain the best value. The results show that the average network attack initiation rate on the KDD CUP99 dataset is 96.1%, and the average network attack initiation rate on the Gafgyt IoT botnet dataset is 97.28%.

Table 2: Various types of total variance interpretation table.

Element	Total	Initial eigenvalue variance percentage	Grand total%
1	10.34	51.72	51.72
2	3.40	16.97	68.70
3	1.90	7.45	76.16
4	0.99	4.99	81.14

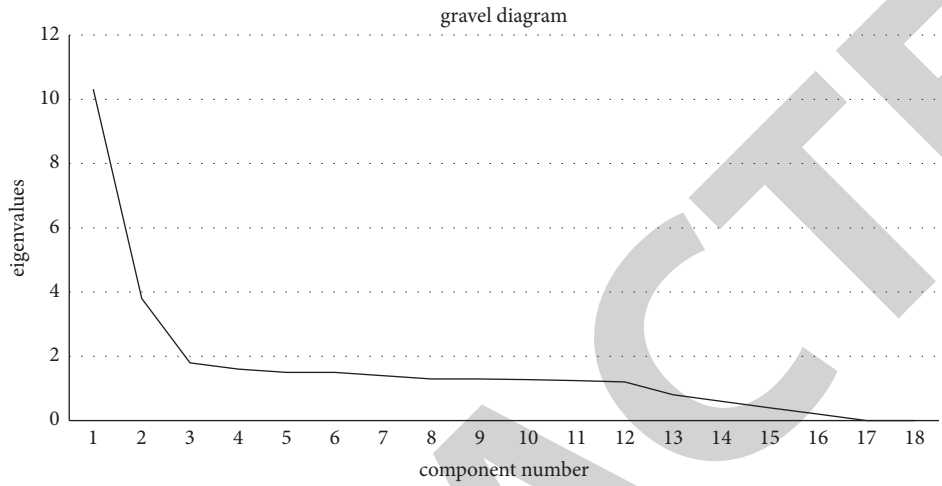

Figure 4: Judgment distribution of the number of eigenvalues.

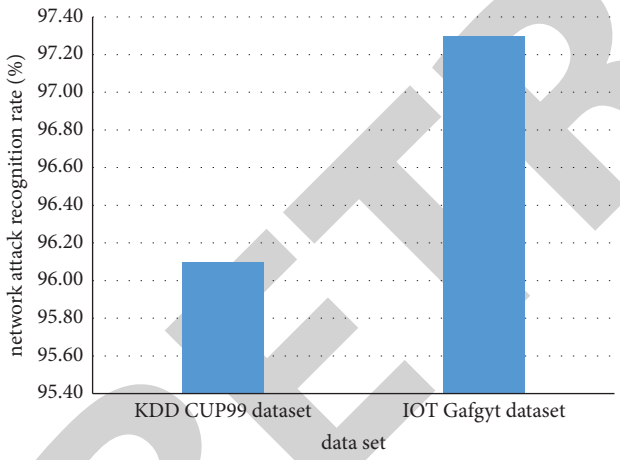

Figure 5: The average recognition rate of cyberattacks across different datasets.

In the experiments, the best experimental results were obtained when the number of layers of each 1D-TLCNN in the TLCNN-IKNN sequence was chosen to be 3, as shown in Figure 6.

The experiment shows that too many layers increase the training difficulty of the model and reduce the detection performance of the model to a certain extent. If the number of layers is too small, the learning and evolution of features would be insufficient, and the detection rate would be low.

The TLCNN-IKNN classifier uses the IKNN algorithm based on optimal Euclidean distance and inverse parameters. Figure 7 shows the impact of various remote operations on the distribution of COMBO attacks.

Figure 7(a) shows the accuracy of COMBO and JUNK attack detection, and Figure 7(b) shows the accuracy of TCP and UDP attack detection. Among them, the weighted Euclidean distance classification has the highest accuracy, the BASHLITE botnet COMBO attack detection accuracy is 99.8%, the JUNK detection accuracy rate is 97.3%, the TCP attack detection rate is 98%, and the UDP attack detection accuracy rate is 95%.

The comparison error of the evaluation results based on the traditional *D-S* evidence theory, the evaluation results based on the BP neural network, the evaluation results based on the RNN neural network, the evaluation results based on the improved evidence theory, and the evaluation results based on the expert evaluation method are shown in Figure 8.

Figure 8(a) describes the network security situation value error of the first five groups of data, and Figure 8(b) records the network security situation value error of the last five groups of data. It can be seen that the processing effect of BP on time series features is still good. The root mean square error of the IDS-NSSA (network security situation assessment) method based on the enhanced proof theory in this paper is about 0.04, which is larger than the root mean square error of DS-NSSA. It can be seen that the network security situation assessment based on the standard RNN neural network still has the problem of information loss and forgets that the input string step size is too long. The experimental results show that the network security situation assessment method based on enhanced evidence theory (IDS-NSSA) can more comprehensively, timely, and accurately characterize the network security situation.

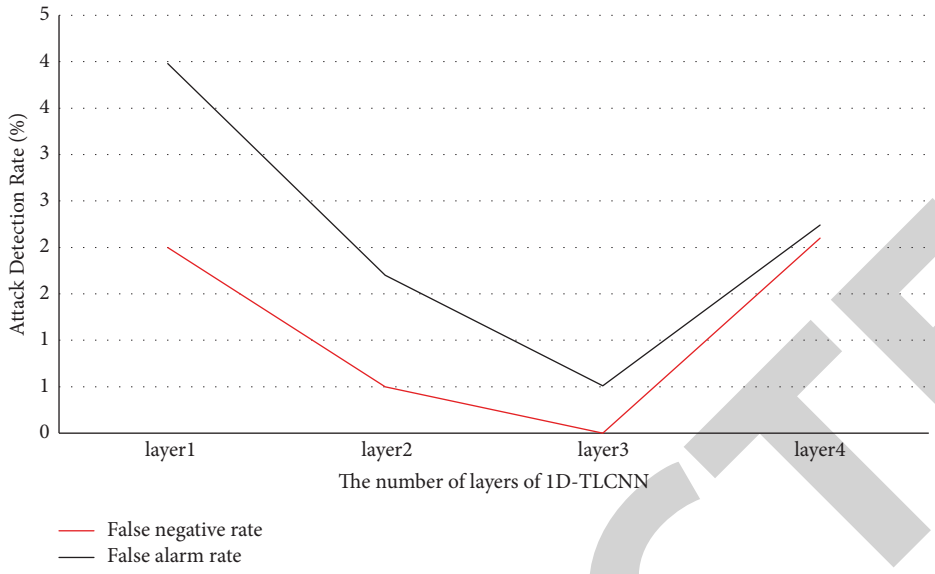

Figure 6: COMBO classification attack impact.

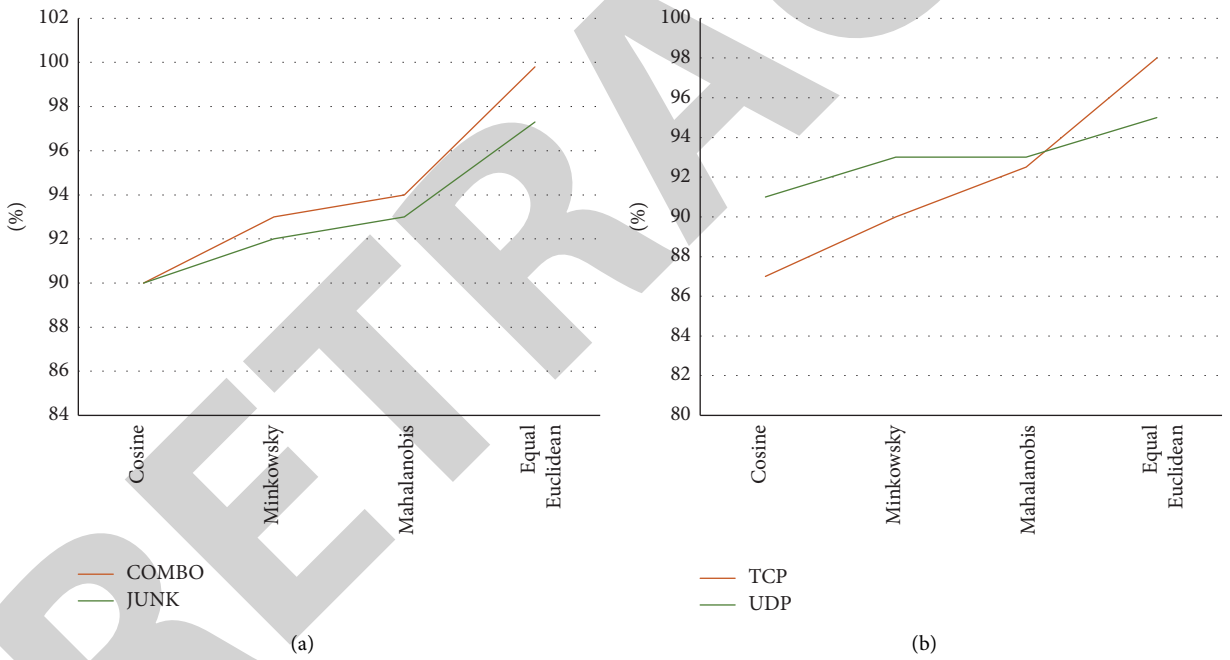

Figure 7: Different types of attack detection rates.

In terms of comprehensive technical efficiency, since the ultimate goal of an enterprise is to maximize profits, it can obtain a maximum output with as little input as possible. Operating profit is the most stable source of profit a business can make over a period of time. Only with sufficient profits, people have the ability and resources to expand production, so the growth of corporate profits is very important to the growth ability of enterprises. After the digital transformation and upgrading, the technological efficiency growth and revenue efficiency growth of enterprises are shown in Figure 9.

Figure 9(a) shows the comprehensive technology comparison results of enterprises with digital transformation, and Figure 9(b) shows the company's annual asset returns. Comprehensive analysis shows that with the advancement of technology, the better the digital development, the better the enterprise development, the more advanced the technology, and the higher the market value.

In the Internet big data environment, there are many network security data collection nodes of various types. Network security data is multidimensional, data functions are diverse, data sources are incomplete and inaccurate, and

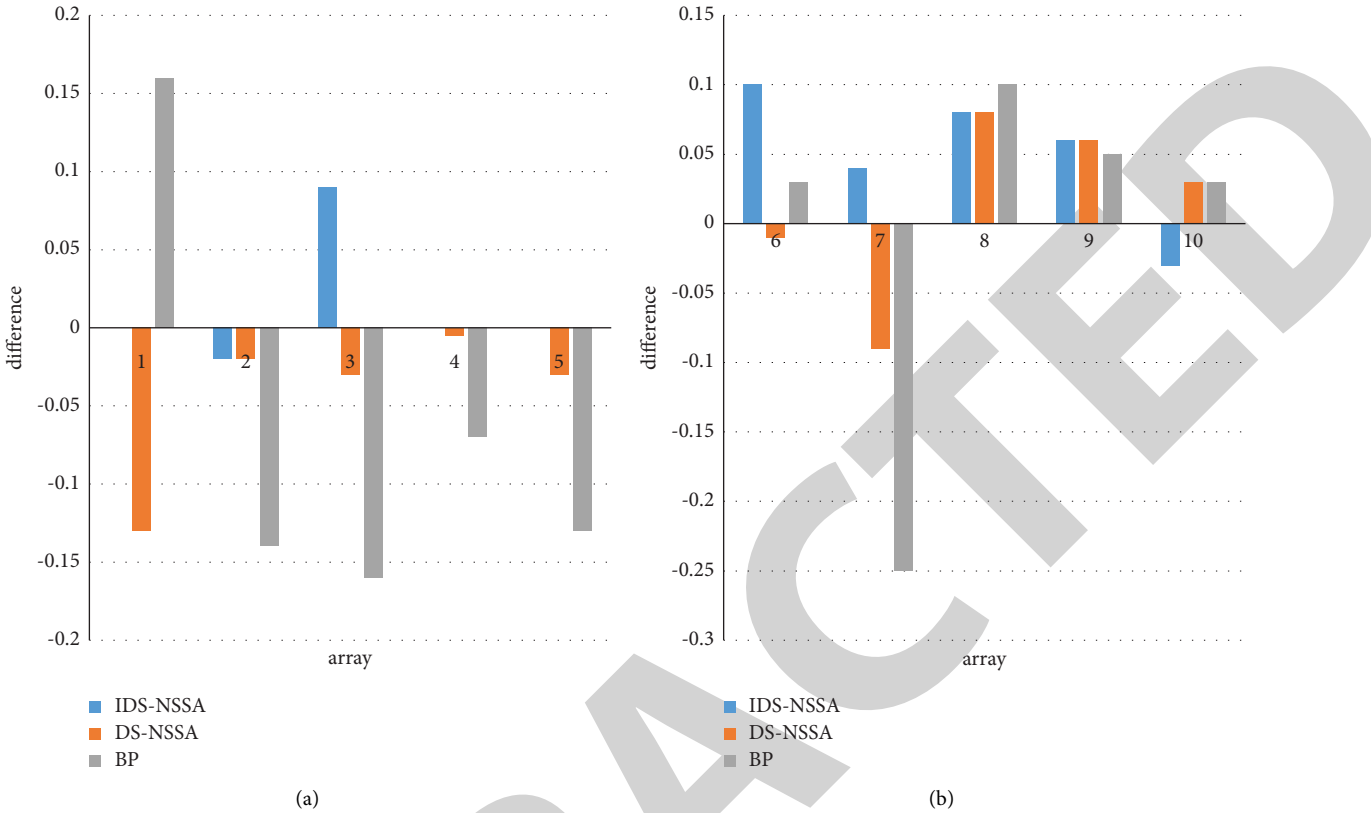

Figure 8: Comparison of errors between different security situation assessment algorithms.

Figure 9: Analysis of technical benefits and asset returns.

network security assessment indicators are difficult to determine and quantify. The assessment is based on expert knowledge, and there are many uncertainties. Therefore, this paper proposes a network security situation assessment method based on the network big data security improvement evidence theory to innovate the digital transformation and upgrading.

5. Conclusions

The smart city system was formed by the connection and functions of the intelligence of information technology and the intelligence of people and the city system, and had the function of a "smart" city system. In the process of formation and operation of the city system wisdom first combined emerging information technology with city subsystems to build smart city subsystems. Then combine human wisdom with the intelligent city subsystem to form a smart city subsystem. Various smart community systems and smart block systems can be combined to build a smart city system. High-dimensional data in the big data environment would not only increase the cost of network security data storage and computing but also increase the cost of network security data in network security situational awareness and the complexity of data mining and machine learning models. The definition, extraction, and analysis of big data network security functions and their automation process were the prerequisites for the in-depth development of the research field of network security situational awareness. The method proposed in this paper was focused on feature extraction. The feature extraction methods were used to extract various network attacks. Because big data function technology involves many methods and different data functions are applicable to different methods, feature extraction or feature selection combination methods can also be considered for different data to improve the efficiency and effectiveness of large-scale secure data processing.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] C. Daniel, C. Mario, P. Giovanni, and D. F. Cristian, "A fuzzy-based approach for sensing, coding and transmission configuration of visual sensors in smart city applications," *Sensors*, vol. 17, no. 1, pp. 1–19, 2017.

[2] M. Gasco-Hernandez, "Building a smart city: lessons from Barcelona," *Communications of the ACM*, vol. 61, no. 4, pp. 50–57, 2018.

[3] B. Bygstad and E. Øvrelid, "Managing two-speed innovation for digital transformation," *Procedia Computer Science*, vol. 181, no. 1, pp. 119–126, 2021.

[4] S. Purchase, C. Kum, and D. Olaru, "An analysis of technical and commercialization paths for an innovation trajectory," *Journal of Business & Industrial Marketing*, vol. 32, no. 6, pp. 848–863, 2017.

[5] G. Vial, "Understanding digital transformation: a review and a research agenda," *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118–144, 2019.

[6] C. Jiang, "Network security and ideological security based on wireless communication and big data analysis," *Wireless Communications and Mobile Computing*, vol. 2022, no. 3, pp. 1–6, 2022.

[7] P. S. Xie, H. J. Fan, T. Feng, Y. Yan, G. Q. Ma, and X. M. Han, "Adaptive access control model of vehicular network big data based on XACML and security risk," *International Journal on Network Security*, vol. 22, no. 2, pp. 347–357, 2020.

[8] H. Hou, Y. Jia, and H. Rong, "Provable multiple-replica dynamic data possession for big data storage in cloud computing," *International Journal on Network Security*, vol. 20, no. 3, pp. 575–584, 2018.

[9] K. SungJin and L. Kangseok, "A normal network behavior profiling method based on big data analysis techniques (Hadoop/Hive)," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 27, no. 5, pp. 1117–1127, 2017.

[10] S. Garg, A. Singh, K. Kaur et al., "Edge computing-based security framework for big data analytics in VANETs," *IEEE Network*, vol. 33, no. 2, pp. 72–81, 2019.

[11] G. Pasolini, C. Buratti, L. Feltrin et al., "Smart city pilot projects using LoRa and IEEE802.15.4 technologies," *Sensors*, vol. 18, no. 4, pp. 1118–1120, 2018.

[12] J. Liu, X. Yu, Z. Xu, K. K. R. Choo, L. Hong, and X. Cui, "A cloud-based taxi trace mining framework for smart city," *Software: Practice and Experience*, vol. 47, no. 8, pp. 1081–1094, 2017.

[13] Z. Lv, X. Li, W. Wang, B. Zhang, J. Hu, and S. Feng, "Government affairs service platform for smart city," *Future Generation Computer Systems*, vol. 81, pp. 443–451, 2018.

[14] O. Bates and A. J. Friday, "Beyond data in the smart city: repurposing existing campus IoT," *IEEE Pervasive Computing*, vol. 16, no. 2, pp. 54–60, 2017.

[15] M. J. Greeven and G. S. Yip, "Six paths to Chinese company innovation," *Asia Pacific Journal of Management*, vol. 38, no. 1, pp. 17–33, 2021.

[16] A. A. Oni, U. Musa, and S. Oni, "E-revenue adoption in state internal revenue service: interrogating the institutional factors," *Journal of Organizational and End User Computing*, vol. 32, no. 1, pp. 41–61, 2020.

[17] B. Hinings, T. Gegenhuber, and R. Greenwood, "Digital innovation and transformation: an institutional perspective," *Information and Organization*, vol. 28, no. 1, pp. 52–61, 2018.

[18] H. Ernest, "Shaping the digital enterprise: trends and use cases in digital innovation and transformation," *Computing Reviews*, vol. 58, no. 5, pp. 278–287, 2017.

[19] M. Heikkilä, H. Bouwman, and J. Heikkilä, "From strategic goals to business model innovation paths: an exploratory study," *Journal of Small Business and Enterprise Development*, vol. 25, no. 1, pp. 107–128, 2017.

[20] A. K. Singh, X. Liu, H. Wang, and H. Ko, "Recent advances in multimedia security and information hiding," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, p. e4193, 2021.

[21] D. Norris and M. Ciesielska, "Towards a framework for innovation orientation within business and management

studies: a systematic review and paths for future research," *Journal of Organizational Change Management*, vol. 32, no. 1, pp. 123–144, 2019.

[22] D. Dang-Pham, S. Pittayachawan, and V. Bruno, "Applications of social network analysis in behavioural information security research: concepts and empirical analysis," *Computers & Security*, vol. 68, no. Jul, pp. 1–15, 2017.

[23] Y. Wang, "Food information management and security strategy of computer network," *Advance Journal of Food Science and Technology*, vol. 11, no. 12, pp. 792–794, 2016.