Financial Big Data Analysis and Network Security Optimization for Sustainable Development Goals

Juanjuan Wang
Department of Accounting, Yantai Vocational College, Yantai 264670, Shandong, China
Corresponding author: Juanjuan Wang (e-mail: wangjuan.999@163.com)

ABSTRACT This study investigates the theoretical foundations, practical applications, and optimization strategies of financial big data analysis and network security optimization in support of Sustainable Development Goals (SDGs). A comprehensive framework is developed to integrate sustainable financial management, environmental cost-benefit analysis, socially responsible investment decision-making, and sustainable supply chain management. The study further proposes a network security optimization architecture incorporating multi-level data encryption, access control, real-time threat monitoring, intelligent defense mechanisms, and blockchain-based data protection. The proposed framework is particularly applicable to communication-intensive environments, including wireless communication infrastructures and antenna-supported information transmission networks, where secure and reliable financial data exchange is essential. Experimental analyses demonstrate that the integration of financial big data technologies and network security mechanisms enhances data protection, operational efficiency, and sustainable decision-making capabilities. The results provide a practical reference for secure financial data governance and sustainable development in complex digital and communication-oriented systems.

INDEX TERMS financial big data, network security optimization, sustainable development goals, wireless communication infrastructure

I. INTRODUCTION

WITH the deepening global adoption of sustainable development concepts and the accelerating digital transformation, corporate financial management faces unprecedented opportunities and challenges. The United Nations Sustainable Development Goals (SDGs) provide a clear path for corporate development: demanding that enterprise pursue economic benefits while rigorously maintaining environmental protection, ethical sourcing, and corporate social responsibility. Big data advancements provide powerful analytics, enabling more accurate corporate sustainability performance assessment. The collection, storage, and analysis of massive amounts of financial data also pose serious Network Security challenges. While promoting sustainable development, enterprises must rationally utilize big data technologies to optimize financial management and ensure data security. This is a critical issue that urgently needs to be addressed. This research aims to construct a comprehensive framework that integrates sustainable development, financial big data analysis, and Network security, creating a systematic solution for enterprises to manage financial risks while pursuing ethical and environmental objectives.

II. THEORETICAL BASIS OF FINANCIAL BIG DATA ANALYSIS UNDER THE SUSTAINABLE DEVELOPMENT GOALS

A. THE INTRINSIC CONNECTION BETWEEN SUSTAINABLE DEVELOPMENT GOALS AND FINANCIAL MANAGEMENT

The Sustainable Development Goals (SDGs) are intrinsically linked to financial management, encompassing multiple aspects such as value creation, resource allocation, and risk management. From the perspective of value creation, traditional financial management focuses on maximizing shareholder value. Sustainable development, on the other hand, requires companies to create comprehensive value encompassing economic, environmental, and corporate values [1]. This shift has transformed financial management from a purely financially-focused evaluation system to a multifaceted, integrated evaluation model, integrating environmental and social costs into financial accounting. Regarding resource allocation, the SDGs encourage companies to invest in green technology innovation, clean energy development, and the development of a circular economy. Financial management requires the development of corresponding investment evaluation standards and funding allocation mechanisms. From a risk management perspective, sustainability risks such as climate change, resource shortages, and social inequality have already significantly impacted companies' long-term internal rates of return. These non-traditional risks need to be integrated into financial evaluation and risk control frameworks [2].

B. THE OPERATIONAL MECHANISM OF BIG DATA TECHNOLOGY IN SUSTAINABLE FINANCIAL ANALYSIS

The integrated nature of sustainable finance, particularly the necessity of embedding non-traditional risks (e.g., climate change impact, ethical sourcing compliance, and resource scarcity) into financial models, presents an insurmountable challenge for conventional financial management tools. These risks are quantified using massive, heterogeneous, and high-velocity datasets—such as real-time supply chain sensor data, social media sentiment, and global climate reports—that far exceed the capacity of standard databases and reporting systems. Consequently, big data technology is not merely an optional enhancement but the essential methodological foundation required to bridge the gap between abstract SDG objectives and actionable, measurable financial risk assessment, allowing for the comprehensive, integrated evaluation model demanded by modern sustainability mandates. Big data technology plays a key role in sustainable financial analysis, primarily through data collection, processing, analysis, and application. In terms of data collection, big data technology can realize the real-time collection of massive heterogeneous data inside and outside the enterprise, including financial data, production data, energy data, supply chain data, market data, etc., and provide comprehensive data support for sustainable financial analysis [3]. In data processing, methods such as data cleaning, integration, and standardization are used to transform the originally scattered data in different formats into consistent data sets that can be used for analysis, thereby solving the problem of traditional financial analysis data silos. In the data analysis link, by applying advanced algorithms such as machine learning, deep learning, and predictive modeling, we can find the deep connections between data, identify the main driving force for sustainable development, and predict future development trends. In the data application link, visualization tools, intelligent reports, decision support systems and other tools are used to convert analysis results into a basis for management decisions [4].

C. THE IMPORTANCE OF NETWORK SECURITY FOR SUSTAINABLE FINANCIAL DATA MANAGEMENT

Network security occupies a fundamental and strategic position in sustainable financial management. Its significance lies in data protection, business continuity, compliance with laws and regulations, and credit maintenance. Sustainable financial data covers sensitive data such as the company's core financial information, environmental monitoring data, and social responsibility fulfillment. The leakage or tampering of this data will not only cause economic losses but also damage the company's image and affect the trust of stakeholders [5]. Network security incidents can cause financial system collapse, data loss or business interruption, seriously hindering the normal operation of the company and the achievement of sustainable development goals. In terms of compliance requirements, governments and international organizations have become increasingly stringent in terms of data protection regulations. Companies need to ensure that the management of their financial data complies with the requirements of relevant laws and regulations to avoid legal risks and corresponding penalties caused by data security issues. Network security is also the cornerstone of building stakeholder trust. Investors, customers, suppliers and other stakeholders have paid more and more attention to the data security capabilities of companies, and regard it as an important indicator to measure the sustainable development capabilities of companies [6].

III. APPLICATION OF FINANCIAL BIG DATA ANALYSIS IN SUSTAINABLE DEVELOPMENT

A. CONSTRUCTION OF AN ENVIRONMENTAL COST-BENEFIT BIG DATA ANALYSIS MODEL

Environmental cost-benefit analysis is a core component of sustainable development financial management. Big data technology provides strong support for building a comprehensive and accurate environmental cost-benefit analysis model. Creating this model requires establishing a comprehensive environmental cost accounting system that incorporates direct, indirect, implicit, and external environmental costs. Using IoT sensors and intelligent monitoring equipment, real-time data on energy consumption, waste emissions, and resource utilization during production and process flow is collected.

To ensure the trustworthiness of this multi-source, heterogeneous data, rigorous data governance protocols are enforced at the data processing stage. This includes metadata management, data lineage tracking, and automated validation checks to guarantee data quality and auditability across sensors and operational databases.

Big data analytics techniques are then used to conduct in-depth mining and correlation analysis of this data. The model utilizes a life cycle assessment approach to track and calculate the environmental impacts of each stage, from raw material procurement, production and processing, transportation and sales, to end-of-life disposal, to measure the environmental costs incurred at each stage [7]. Crucially, the raw environmental data (e.g., cubic meters of water, kilograms of CO2 emissions) is financialized by applying established monetary valuation methods (such as carbon pricing mechanisms or shadow pricing) to accurately translate physical environmental impact into financial liabilities or assets for inclusion in the cost accounting system. Regarding benefit evaluation, the model not only calculates direct economic benefits, such as savings from energy and electricity savings, but also quantifies indirect benefits, such as enhanced brand image, expanded market share, and reduced financing costs. With the help of machine learning algorithm models, specifically utilizing Time Series Forecasting (for predicting future resource prices and consumption) and Classification/Clustering algorithms (for segmenting products by environmental performance), we can discover the main factors affecting environmental cost-benefit and predict the results of different environmental investment projects to provide data support for enterprises to make environmental management decisions. The model also establishes an environmental performance indicator system to achieve dynamic monitoring and evaluation of environmental management effects. In order to more clearly illustrate the complete process of environmental cost-benefit analysis, the figure (Figure 1) below shows a systematic analysis model from data collection to decision support [8].

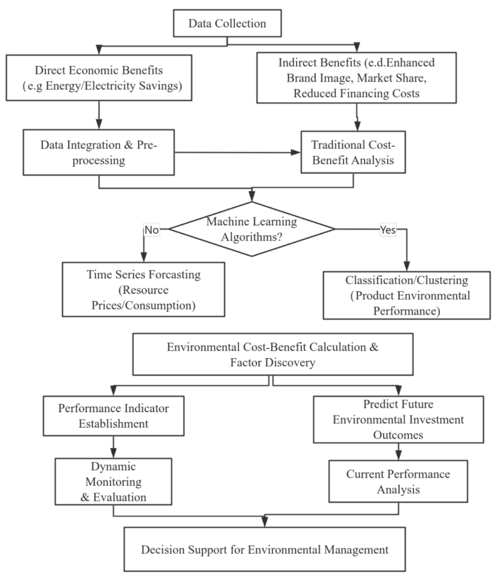

FIGURE 1. Flowchart of building an environmental cost-benefit big data analysis model

B. DATA-DRIVEN SOCIALLY RESPONSIBLE INVESTMENT DECISION SUPPORT

Socially responsible investment decisions must balance financial returns and social impact. Big data analysis provides powerful data support and analytical tools for this complex decision-making process. The data-driven socially responsible investment decision support system pioneered a multi-dimensional investment evaluation indicator system. In addition to traditional financial indicators, it also includes environmental impact, social contribution, and corporate governance metrics. Specifically, this system is structured around four main pillars, with the innovation lying in the granular, big-data-driven metrics:

Financial & Risk: Includes traditional metrics (e.g., Return on Assets) but integrates non-compliance financial risks (e.g., regulatory fines and penalties for environmental breaches).

Environmental (E): Features specific, industry-relevant metrics like Water Use Intensity (cubic meters per unit of production), Carbon Emissions per Revenue, and Waste Recycling Rate.

Social (S): Employs auditable metrics such as Labor Rights Compliance Audit Pass Rate across the supply chain, Employee Training Investment per Capita, and Community Investment Index.

Governance (G): Focuses on Board Independence Score and the Transparency Index of ESG Reporting. This system's innovative point is its structure which assigns dynamic weightings based on the real-time material impact of each metric to the company's long-term financial stability, a process made possible by the continuous data ingestion and analytical capabilities of the platform.

It integrates data from multiple sources, including corporate financial statements, sustainability reports, news media reports, social media comments, and data from third-party rating agencies.

Similar to the environmental model, data governance is paramount. Cross-source data trustworthiness is established through automated consistency checking, anomaly detection, and a weighting mechanism that factors in the credibility and real-time nature of each source (e.g., prioritizing audited reports over unverified social media data).

Using natural language processing and sentiment analysis, it extracts and quantifies the social value of companies. Specifically, machine learning Classification algorithms (such as support vector machines or neural networks) are trained to assign proprietary ESG scores based on textual and quantitative inputs, thereby financializing the social and governance data for use in portfolio optimization. By constructing an investment portfolio optimization model, it maximizes the social and environmental benefits of investments while maintaining a balanced risk-return balance. The system uses scenario analysis and stress testing to analyze portfolio performance under different economic, social, and environmental contexts [9], identifying potential risks and opportunities. Big data analysis can be used to track the social impact of investment projects, continuously optimizing investment strategies by comparing projected outcomes with actual results. The system also incorporates real-time monitoring and early warning capabilities, providing timely warnings when significant social responsibility risks arise in investment targets, safeguarding investor interests. Through continuous data accumulation and model optimization, the system enables better decision-making, ensuring the scientific and accurate nature of socially responsible investment. The operating mechanism of the socially responsible investment decision support system is shown in the figure (Figure 2) below. The system provides a scientific basis for investment decisions through multi-source data integration and intelligent analysis [10].

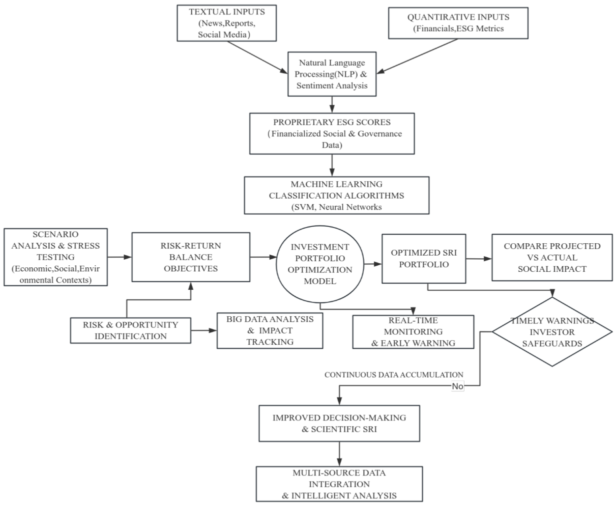

FIGURE 2. Data-Driven socially responsible investment decision support system flow chart

C. SUSTAINABLE SUPPLY CHAIN FINANCIAL DATA INTEGRATION AND ANALYSIS

Sustainable supply chain management requires companies to comprehensively consider and manage the financial, environmental, and social performance of upstream and downstream enterprises in the supply chain. Big data technology enables efficient integration and in-depth analysis of supply chain financial information. The integrated analysis platform must first establish supply chain data standards and interface specifications to ensure smooth data integration and sharing across different enterprises and systems. The platform collects data covering supplier financial status, production costs, logistics costs, inventory levels, on-time delivery, quality, environmental compliance, and labor rights protection. Data integration technologies are used to aggregate data from various nodes into a unified analysis platform, generating a comprehensive view of the supply chain. Network analysis methods are used to identify key nodes and potential risk points in the supply chain and assess its stability and resilience [11]. A supplier sustainability scoring model has been developed to comprehensively evaluate suppliers' financial health, environmental performance, and commitment to social responsibility, serving as a key basis for supplier selection and management.

To provide methodological rigor, the model utilizes a weighted aggregation approach, where the final Supplier Sustainability Score (S_{score}) is determined by the three main component scores (Financial F, Environmental E, and Social S) and their respective system-defined weights (ω_f, ω_e, ω_s).

$$S_{score} = \omega_f F + \omega_e E + \omega_s S$$

This structure ensures $\omega_f + \omega_e + \omega_s = 1$, allowing for dynamic adjustment based on market and regulatory priorities.

The component scores are defined as follows:

Financial Score (F): Derived from real-time analysis of metrics like D/E (Debt-to-Equity Ratio), liquidity ratios, and compliance fine history.

Environmental Score (E): Determined by performance indicators such as waste-water discharge per unit of output (collected via IoT) and the percentage of renewable energy use in production.

Social Score (S): Quantified using inputs from automated ethical auditing reports (e.g., labor hours compliance) and social media sentiment analysis (e.g., brand reputation risk).

The threshold for S_{score} is automatically adjusted based on the inherent sustainability risk category of the supplied material, ensuring stricter standards for high-impact raw materials.

Using predictive analytics, the platform can forecast supply chain cost trends, identify cost optimization opportunities, and assess the financial impact of sustainable procurement strategies. The full process architecture for integrated analysis of sustainable supply chain financial data is shown in the figure (Figure 3) below. The platform achieves end-to-end integration from data source to decision output [12].

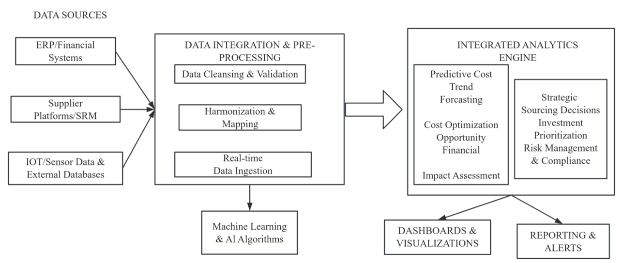

FIGURE 3. Flowchart of the Sustainable Supply Chain Financial Data Integration and Analysis Platform

IV. NETWORK SECURITY OPTIMIZATION STRATEGY FOR FINANCIAL BIG DATA SYSTEMS

A. RESEARCH ON MULTI-LEVEL DATA ENCRYPTION AND ACCESS CONTROL MECHANISMS

Multi-level data encryption and access control mechanisms are the first line of defense for ensuring the security of financial big data systems. A comprehensive security system must be established to provide comprehensive protection at all levels, including data storage, transmission, processing, and use. At the data storage level, high-strength encryption algorithms are used to encrypt static data, including database encryption, file system encryption, and backup data encryption. This ensures that even if the storage media is stolen, the data cannot be directly read [13]. Field-level encryption is implemented for sensitive financial data, allowing only authorized users to decrypt and view it. During data transmission, secure transmission channels are established, using the SSL/TLS protocol to encrypt data in transit to prevent interception or tampering during network transmission. An end-to-end encryption strategy is implemented to ensure that data remains encrypted and protected from the source to the destination. For access control, a role-based access control system should be established to assign fine-grained data access rights based on user responsibilities and business needs. Implement the principle of least privilege: users can only access the minimum amount of data necessary to complete their work, use multi-factor authentication methods such as passwords, fingerprints, dynamic tokens, etc. to improve the reliability of identity authentication, establish an access behavior audit system, record all data access operations, and promptly detect abnormal access behavior.

1) Addressing the Security-Performance Conflict

While technologies like Homomorphic Encryption (HE) and Quantum-safe Encryption are recognized for their advanced cryptographic strength, their significantly high resource consumption and low processing efficiency (as evidenced by HE's high Average Latency and Peak CPU Utilization) present a critical performance conflict in real-time financial big data processing. To resolve this trade-off, the system employs a pragmatic, risk-based tiered approach:

Tiered Security Deployment: High-efficiency algorithms, such as AES-256 (high Key Operation Throughput), are prioritized for high-volume, low-latency tasks (e.g., bulk data transmission). Conversely, low-efficiency, high-security algorithms like Homomorphic Encryption are reserved for non-real-time or highly sensitive analytical tasks where data must remain encrypted during computation (e.g., specific risk model calculation on confidential external data), ensuring computational integrity without sacrificing the security of the underlying data.

Acceptable Latency Thresholds: The system defines differentiated latency thresholds based on the business process. These thresholds are used during the architectural design phase to proactively assign the appropriate, pre-selected encryption scheme to the data pipeline. For real-time financial transactions, the acceptable latency threshold is stringent ($\leq$ 100 milliseconds), mandating the application of the pre-selected, high-throughput scheme (e.g., Hybrid Encryption) for that specific data type or process. For daily batch processing or complex risk modeling (where HE may be used), the acceptable latency can be relaxed to several seconds or minutes, acknowledging the security gain justifies the performance cost.

Resource Allocation Strategy: The security management platform dynamically allocates dedicated, high-performance computing clusters (e.g., GPU acceleration) to process data encrypted with high-cost schemes like HE, effectively mitigating the resource consumption impact on the primary real-time business processes. Based on a detailed analysis of multi-level data encryption technology, Table 1 presents a comparative evaluation of the security and performance characteristics of different encryption algorithms, synthesized from an extensive review of existing cryptographic and performance literature, with performance metrics anchored to standard industry benchmark results.

TABLE 1. Research on multi-level data encryption and access control mechanisms [14]

Encryption technology type	Key Length (bits)	Key Operation Throughput (ops/s)	Average Latency (ms)	Peak CPU Utilization (%)	Implementation Complexity (Relative)
RSA-2048 asymmetric encryption	2048	500	15.2	75	Medium
ECC elliptic curve cryptography	256	2100	5.5	40	Medium
Hybrid encryption scheme	Variable	8200	2.1	55	High
Homomorphic encryption technology	Variable	50	150.0	95	Very High
Quantum-safe encryption	Variable	200	45	85	Very High

The performance data (Latency and CPU Utilization) is based on results from a simulated environment typical for financial backend systems. Testing environment parameters include: CPU: Intel Xeon E5-2699 v4; Memory:

256GB RAM; OS: Linux; Implementation Library: OpenSSL v1.1.1 (for standard ciphers) and equivalent reference implementations for HE/Quantum-safe. While the overall test data size for throughput assessment was a 1MB plaintext block, the reported Latency values for asymmetric algorithms (RSA/ECC) specifically reflect the cryptographic operation time within a hybrid encryption context (e.g., key encapsulation/exchange), rather than direct encryption of the entire block. The test data size was a 1MB plaintext block, and metrics reflect the average of 1,000 encryption/decryption cycles for non-HE schemes. For symmetric and homomorphic schemes, Latency is measured as $T_{\text{encryption}} + T_{\text{decryption}}$ for the test block; however, for RSA and ECC, Latency reflects the time required for key establishment and digital envelope processing within the hybrid framework.

B. REAL-TIME THREAT MONITORING AND INTELLIGENT DEFENSE SYSTEM CONSTRUCTION

A real-time threat monitoring and intelligent defense system is the core guarantee of the financial big data security network. It leverages advanced detection technologies and intelligent analysis methods to proactively detect and respond to network security vulnerabilities. The system utilizes a distributed architecture and is deployed at multiple monitoring points, forming a comprehensive monitoring network that covers the network perimeter, intranet, endpoints, and various application systems. Using big data analytics, it collects and analyzes large amounts of network traffic, system logs, and security events in real time to establish a baseline of normal operation. Anomaly detection algorithms then identify potential security threats. The system utilizes a variety of security tools, including intrusion detection systems, firewalls, and antivirus software, to centrally collect and analyze threat information. By applying machine learning and artificial intelligence technologies, a threat identification model is constructed that automatically detects both unknown and known threats, including zero-day attacks and advanced persistent threats. A threat intelligence sharing mechanism has been established to access external threat intelligence in a timely manner, improving the accuracy and timeliness of threat identification. The system automates the threat response process, automatically executing defensive measures such as isolation, blocking, and removal based on threat severity and type. A security operations center has been established, staffed with a professional security team, to conduct manual analysis and response to major security incidents. Based on an in-depth investigation and effect analysis of current mainstream network security threat detection technologies, Table 2 systematically compares the actual application effects of various threat detection technologies, with data generated from a controlled, simulated environment. The testbed was configured to emulate a financial transaction processing network (Hardware: Intel Xeon Gold 6248R; OS: CentOS 8; Key Software: ELK Stack for log aggregation). Testing utilized a hybrid dataset of network traffic, comprising 70% anonymized proprietary enterprise financial logs and 30% publicly available security datasets (specifically the CICIDS2017 corpus) to ensure comprehensive representation. A standard, commercially available rule-based Security Information and Event Management (SIEM) system served as the baseline comparison benchmark for all reported metrics. Furthermore, the reported accuracy and false alarm rates were subjected to a month-long expert evaluation process, where three certified security analysts manually validated all flagged incidents to confirm the operational efficacy of each technology. Detection Accuracy is calculated as (True Positives + True Negatives) / Total Samples, while the Zero-Day Attack Detection Rate specifically measures the ratio of previously unknown malicious patterns correctly flagged to the total number of unknown attack samples tested. It is critical to note that Signature-based IDS relies solely on pre-existing pattern databases. Therefore, it possesses no true capability to detect novel, unknown zero-day attacks. Any non-zero result would typically represent a false positive or the detection of a known attack variant, not a genuine zero-day threat. For practical deployment, advanced detection methods with inherently higher potential False Alarm Rates (like User Behavior Analysis) must undergo further refinement, such as adaptive thresholding and behavioral profiling, to ensure the False Alarm Rate is operationally sustainable for the Security Operations Center (SOC).

TABLE 2. Real-Time threat monitoring and intelligent defense system construction [15]

Threat Detection Technology	Detection accuracy (%)	False alarm rate (%)	Avg. Response Time (ms)	Zero-Day Attack Detection Rate (%)	Resource utilization (%)	Deployment Cost (Relative)
Signature-based IDS	94.2	2.8	50	0.0	15	Low
Abnormal behavior detection	87.6	8.2	120	68.5	35	Medium
Machine Learning Detection	91.8	5.1	210	85.2	42	High
Deep Packet Inspection (DPI)	89.3	4.7	80	22.0	28	High
Threat Intelligence Correlation	92.5	3.6	150	45.0	22	Medium
Sandbox dynamic analysis	95.7	2.1	1530	92.1	68	Very High
User behavior analysis	86.4	4.5	370	35.0	31	Medium

C. RESEARCH ON THE APPLICATION OF BLOCKCHAIN TECHNOLOGY IN THE FIELD OF FINANCIAL DATA SECURITY

Due to its decentralized, tamper-proof, and traceable nature, blockchain technology offers innovative solutions for financial data security, playing a crucial role in data integrity protection, audit tracking, and identity authentication. To protect data integrity, hash values of key financial data are stored on the blockchain, creating an unalterable data fingerprint. Changes to the original data are immediately detected. Building a distributed ledger system using blockchain enables real-time synchronization and confirmation of financial transactions, ensuring consistent and accurate billing. Smart contract technology enforces predefined financial management rules and processes, eliminating the risk of manual errors and fraud. Regarding audit tracking, blockchain records all financial data operations—such as creation, modification, and query— to form a complete audit chain. Auditors can use blockchain to quickly verify the authenticity and integrity of financial information, significantly improving audit efficiency and credibility. Regarding identity authentication and authorization management, a blockchain-based distributed identity authentication system is established, storing user identity and permission information on the blockchain, enabling unified identity authentication across systems and organizations. Adopting the consensus mechanism of blockchain to complete the authorization decision-making of multiple parties, increase the credibility and fairness of authorization. In terms of data sharing, blockchain technology is used to create a credible data sharing platform, and under the premise of ensuring data privacy and security, it enables upstream and downstream supply chain companies to share financial data safely.

V. CONCLUSION

Big data financial analysis and Network Security Optimization focused on achieving Sustainable Development Goals are the paths that enterprises across all sectors, must take to successfully achieve digital transformation and ensure long-term sustainable development. Implementing these strategies allows to use advanced analytics to track ethical sourcing and water consumption financially, while robust network security protects the integrity of sensitive global supply chain and ESG reporting data from threats . Through a systematic analysis of the inherent connection between sustainable development indicators and financial management, this paper explores the mechanism of big data in sustainable financial management, the elements of network security, and proposes a theoretical framework. At the application practice level, this paper proposes an environmental cost-benefit analysis model, a socially responsible investment decision support system, and a sustainable supply chain financial data integration and analysis platform, providing a specific application practice path for enterprises. For network security optimization, the study has designed a multi-level data encryption and access control mechanism, realtime threat monitoring, and an intelligent defense system. At the same time, the study explores the innovative application of blockchain technology to form a relatively complete security assurance system, which is vital for verifying the ethical sourcing, material provenance, and supply chain transparency required. This integration allows for immutable digital records that enhance trust and accountability across every stage of production. In the future, with technological advancement and the deepening of sustainable development concepts, the combination of financial big data analysis and network security optimization will become even closer. This convergence will allow for real-time risk assessment of environmentally and socially non-compliant suppliers, while fortified Network Security will be essential to protect the sensitive, proprietary data streams driving this complex sustainable financial oversight.

AUTHOR CONTRIBUTIONS

Juanjuan Wang designed, collected and analyzed the data, and drafted the manuscript. Juanjuan Wang conducted the study, critically revised the manuscript for important intellectual content, and gave final approval of the version to be published. Juanjuan Wang participated fully in the work, take public responsibility for appropriate portions of the content, and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] T. Liu, "A Secure Storage Method for Enterprise Financial Data Based on Cloud Computing Technology," Computer Informatization and Mechanical System, vol. 8, no. 2, 2025, doi: 10.12250/JPCIAMS2025090415.

[2] Y. Lin, "An Exploration on the Creative Application of Big Data Analysis to the Practice Teaching of Financial Management," Exploration of Educational Management, vol. 3, no. 2, 2025, doi: 10.12417/3029-2328.25.02.016.

[3] K. Ungar and C. Oprean Stan, "Optimizing Financial Data Analysis: A Comparative Study of Preprocessing Techniques for Regression Modeling of Apple Inc.'S Net Income and Stock Prices," Studia Universitatis, Vasile Goldis" Arad – Economics Series, vol. 35, no. 1, 2025, doi: 10.2478/SUES-2025-0004.

[4] J. O. Imoniana, W. L. Silva, V. G. Slomski, and V. Slomski, "IT auditing in assurance of financial statement: what characterizes Cybersecurity data breach disclosure by Brazilian filers of NYSE?" Procedia Computer Science, vol. 257, 2025, doi: 10.1016/J.PROCS.2025.03.137.

[5] X. Yang, "Enterprise Financial Decision Support and Data Analysis," Academic Journal of Business & Management, vol. 6, no. 8, 2024, doi: 10.25236/AJBM.2024.060812.

[6] X. Lun, X. Zhang, Y. Wang, and T. Wang, "Abnormal recognition of corporate financial data based on deep belief network," International Journal of Industrial and Systems Engineering, vol. 45, no. 2, 2023, doi: 10.1504/IJISE.2023.134371.

[7] Y. Chu, "A fast encryption method of large enterprise financial data based on adversarial neural network," International Journal of Industrial and Systems Engineering, vol. 44, no. 3, 2023, doi: 10.1504/IJISE.2023.132269.

[8] K. Wang, W. Qian, X. Yang, X. Li, C. Yang, Yue, and S. et al, "Intelligent Data Analysis System Based on Edge Computing," 2022, doi: 10.1007/978-3-031-06788-4_7.

[9] L. Wang, "Judgement method of enterprise financial data abnormality based on high-order dynamic Bayesian network," International Journal of Industrial and Systems Engineering, vol. 44, no. 3, 2023, doi: 10.1504/IJISE.2023.132270.

[10] P. Rosati and T. Lynn, "A dataset for accounting, finance and economics research on US data breaches," Data in Brief, pp. 35, 2021, doi: 10.1016/J.DIB.2021.106924.

[11] M. Liang, "Optimization of Quantitative Financial Data Analysis System Based on Deep Learning," Complexity, pp. 2021, 2021, doi: 10.1155/2021/5527615.

[12] J. F. Ebert, L. Huibers, B. Christensen, and M. B. Christensen, "Paper-or Web-Based Questionnaire Invitations as a Method for Data Collection: Cross-Sectional Comparative Study of Differences in Response Rate, Completeness of Data, and Financial Cost," Journal of Medical Internet Research, vol. 20, no. 1, 2018, doi: 10.2196/jmir.8353.

[13] H. Yu and X. He, "Corporate Data Sharing, Leakage, and Supervision Mechanism Research," Sustainability, pp. 13, 2021, doi: 10.3390/su13020931.

[14] J. S. P. Tyoso, A. Amaludin, T. I. Hendriana, and Y. Radnan, "The Influence of Strategic Decision Making, Business Performance, and Employee Development on Big Data Technology in HR: A Case Study of a FinTech Company in Jakarta," West Science Journal Economic and Entrepreneurship, vol. 2, no. 02, pp. 123-135, 2024, doi: 10.58812/wsjee.v2i02.879.

[15] Y. Zhang and H. Zhang, "Construction of Financial Big Data Analysis Platform in Universities under Big Data Technology," Proceedings of the 2nd International Conference on Information, Control and Automation, ICICA 2022; December 2-4, pp. Chongqing, China. 2023, 2022, doi: 10.4108/eai.2-12-2022.2328061.