Heliyon 10 (2024) e32639

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Enterprise financial sharing and risk identification model combining recurrent neural networks with transformer model supported by blockchain

Yang Wu

Accounting School, Tongling University, Tongling City, Anhui Province 244000, China

ARTICLE INFO

Keywords:
Blockchain
Recurrent neural networks
Enterprise financial sharing
Transformer
Risk identification
BiLSTM

ABSTRACT

The objective of this study is to investigate methodologies concerning enterprise financial sharing and risk identification to mitigate concerns associated with the sharing and safeguarding of financial data. Initially, the analysis examines security vulnerabilities inherent in conventional financial information sharing practices. Subsequently, blockchain technology is introduced to transition various entity nodes within centralized enterprise financial networks into a decentralized blockchain framework, culminating in the formulation of a blockchain-based model for enterprise financial data sharing. Concurrently, the study integrates the Bi-directional Long Short-Term Memory (BiLSTM) algorithm with the transformer model, presenting an enterprise financial risk identification model referred to as the BiLSTM-fused transformer model. This model amalgamates multimodal sequence modeling with comprehensive understanding of both textual and visual data. It stratifies financial values into levels 1 to 5, where level 1 signifies the most favorable financial condition, followed by relatively good (level 2), average (level 3), high risk (level 4), and severe risk (level 5). Subsequent to model construction, experimental analysis is conducted, revealing that, in comparison to the Byzantine Fault Tolerance (BFT) algorithm mechanism, the proposed model achieves a throughput exceeding 80 with a node count of 146. Both data message leakage and average packet loss rates remain below 10 %. Moreover, when juxtaposed with the recurrent neural networks (RNNs) algorithm, this model demonstrates a risk identification accuracy surpassing 94 %, an AUC value exceeding 0.95, and a reduction in the time required for risk identification by approximately 10 s. Consequently, this study facilitates the more precise and efficient identification of potential risks, thereby furnishing crucial support for enterprise risk management and strategic decision-making endeavors.

1. Introduction

In the contemporary digital economy, conventional financial models encounter challenges in meeting the developmental requisites of medium to large enterprises. Financial sharing services have emerged as pivotal tools in mitigating operational costs and augmenting financial accounting efficiency, thereby enhancing the financial management capacities of enterprises [1–3]. Nonetheless, traditional financial information-sharing services are beset with myriad potential security vulnerabilities, encompassing data leakage, tampering, opacity, and data disparities [4]. Consequently, the resolution of issues pertaining to financial information sharing and

E-mail address: isabel@tlu.edu.cn.

https://doi.org/10.1016/j.heliyon.2024.e32639
Received 22 January 2024; Received in revised form 29 May 2024; Accepted 6 June 2024
Available online 13 June 2024

security within traditional financial systems constitutes a substantial challenge. Against the backdrop of burgeoning trends in deep learning, blockchain, big data, and the Internet of Things (IoT), scholars in pertinent domains are directing their attention towards the application of these technologies in the realm of enterprise finance to fortify security and efficacy.

Within the contemporary business milieu, financial information sharing and security have perennially constituted critical imperatives in enterprise management and the financial sector. Emerging technologies such as deep learning, blockchain, big data, and the IoT have ushered in new prospects for enterprise financial sharing services [5,6]. Big data analytics methodologies have the capacity to unveil latent value within extensive datasets, furnishing clientele with precise product information to cater to diverse requirements [7]. Blockchain technology, characterized by its decentralization, immutability, and heightened transparency attributes, stands poised to effectively mitigate trust issues among enterprises amidst escalating inter-company transactions with substantial trust costs. This engenders dependable transactions, enhanced business efficiency, and cost-effectiveness [8,9]. Furthermore, the integration of deep learning holds the potential to autonomously extract features from data within financial sharing service centers, offering considerable promise in bolstering financial business process efficiency, fortifying risk management, and refining data analysis [10].

The aim of this study is to explore a methodology for enterprise financial sharing and risk identification by amalgamating recurrent neural networks (RNNs) and Transformer models with the backing of blockchain technology. This approach endeavors to enhance the security and precision of financial information sharing among enterprises. The innovative utilization of blockchain technology has precipitated the conception of a blockchain-based model for enterprise financial data sharing. Additionally, this study proffers the Bidirectional Long Short-Term Memory (BiLSTM)-fused transformer model for enterprise financial risk identification. Subsequently, the efficacy of these models will be assessed through experimental analysis to enhance the meticulous identification of financial risks, fortify enterprise risk management, and refine strategic decision-making.

The structure of this study unfolds as follows: Initially, section 2 furnishes a literature review, elucidating background and theoretical underpinnings by scrutinizing pertinent papers and technological advancements. Subsequently, section 3 expounds upon the study methodologies, encompassing the application of blockchain technology and the fusion of RNNs and Transformer models, culminating in the construction of the financial sharing and risk identification model. Section 4 delineates experimental results and discussions, offering an intricate analysis of model performance and experimental outcomes. Ultimately, section 5 encapsulates the principal findings of the study and delineates future research trajectories.

2. Literature review

2.1. Current research status on financial information sharing and risk identification

Currently, a plethora of scholars have engaged in research pertaining to enterprise financial information sharing and risk identification. For instance, Levytska et al. (2022) [11] proposed a risk-oriented internal auditing methodology tailored for financial monitoring entities. This methodology adeptly discerns and manages potential financial risks, furnishing robust backing for financial monitoring endeavors. Gao (2022) [12] delved into the realm of enterprise financial accounting information management through the lens of big data, offering profound insights for a comprehensive comprehension of the role of financial information processing in enterprise governance. Xu et al. (2022) [13] introduced a differential game model grounded in blockchain technology for facilitating supply chain financial information sharing, positing the potential to bolster the efficiency and transparency of supply chain finance mechanisms. Alrawad et al. (2023) [14] employed the analytic hierarchy process to scrutinize managers' perceptions and attitudes towards financial risks within small and medium-sized enterprises. The study unveiled diverse managerial perspectives on various financial risks, thereby furnishing invaluable insights for the enhanced management and sustenance of small and medium-sized enterprises. Cornwell et al. (2023) [15] delved into the role of data analysis within operational risk management, drawing insights from the financial services and energy sectors. The study underscored the pivotal role of data analysis in risk management practices, rendering it immensely consequential for the refinement of risk management strategies.

Blockchain technology has garnered significant attention in the realm of information sharing, attracting scholarly inquiry from researchers such as Yang et al. (2023) [16]. From the perspective of evolutionary game theory, the issue of ensuring the authenticity of initial information in agricultural supply chains based on blockchain technology was investigated. They focused on leveraging blockchain technology to enhance the transparency and authenticity of information within the supply chain, and evaluated the effectiveness of different strategies through simulating the process of evolutionary game theory. The key aspect of this technology lies in its novel approach to the authenticity of information in supply chain management, as well as the potential of blockchain technology to improve information quality. Lee et al. (2023) [17] evaluated the prioritization factors for public-sector blockchain application services. This helps the public sector better understand how to leverage blockchain technology to enhance service quality. Some scholars have also applied blockchain to risk prediction, such as Wang et al. (2023) [18]. They focused on the risk prediction and credibility detection of public opinion in video networks based on blockchain technology. By analyzing public opinion in network videos, they ensured data immutability using blockchain technology and combined specific algorithms to predict the risk level and credibility of public opinion. The strength of this technology lies in its in-depth analysis of video content and the application of blockchain technology, thereby enhancing the accuracy of risk prediction and the security of data. Xie et al. (2023) [19] focused on credit risk, emphasizing the application of models in practical credit risk assessment, which aligns with the purpose of the model proposed in this study to support enterprise risk management and strategic decision-making. Additionally, a random forest weighted naive Bayes model was designed, which demonstrates good interpretability and generalization capability. The BiLSTM-fused Transformer integrated model proposed in this study is also aimed at enhancing the accuracy and efficiency of risk assessment, indicating that both studies are exploring how to leverage advanced algorithm models to improve the effectiveness of risk management.2.2

Current Application of Deep Learning in Information Risk Identification.

Deep learning exhibits remarkable performance across diverse domains, particularly in handling large-scale and intricate datasets. Its application in information risk identification garners considerable attention. Zhang et al. (2020) [20] combined deep belief networks and support vector machines to achieve real-time and comprehensive detection of network attacks. The findings demonstrated that this approach effectively enhanced network security performance. Lv et al. (2023) [21] addressed security concerns associated with deep learning in digital twin systems and proposed a security defense mechanism for deep learning service computing systems. The results indicated that this mechanism contributed to fortifying the data and information protection of digital twin systems. Wu et al. (2023) [22] introduced an automated lane-change trajectory planning method for autonomous vehicles, which enhanced the safety of autonomous driving vehicles through instantaneous risk identification. Li et al. (2023) [23] conducted risk prediction in the financial management domain of listed companies and introduced an optimized method based on a backpropagation neural network, facilitating more precise financial risk prediction. Dhingra et al. (2023) [24] proposed a machine learning-based method for identifying financial loss risk factors in railway accidents. This method collected railway accident data, extracted key risk factors using feature selection techniques, and ranked these factors using machine learning algorithms to identify the risks most likely to result in financial losses. The core of this technology lay in its ability to analyze a large amount of accident data and comprehensively assess risk factors through machine learning algorithms. Chen et al. (2023) [25] proposed a financial risk prediction model for e-commerce enterprises based on RNNs. The results indicate that this model helps e-commerce companies to manage financial risks. Dong et al. (2023) [26] utilized artificial intelligence technology to predict abnormal patterns in corporate financial statements, which was similar to the goal of the enterprise financial risk identification model proposed in this study, i.e., predicting potential risks through the analysis of financial data. They used decision trees, neural networks, and deep learning among other machine learning and data mining techniques to analyze historical financial data, learn patterns and trends within it, and predict future anomalies. Similarly, this study employed deep learning techniques (BiLSTM and Transformer models) to identify and predict enterprise financial risks, demonstrating the commonality of technical applications between the two studies. Sasaki et al. (2023) [27] analyzed risk chains and extracted implicit information from publicly disclosed documents, which was similar to the goal of the enterprise financial risk identification model proposed in this study, i.e., identifying potential risks through the analysis of financial data. By constructing risk chain diagrams to understand and categorize risks, this study identified and evaluated risks through the design of a blockchain-based financial data sharing model and a BiLSTM-fused transformer model, both of which employed graphical methods to represent and process risk information. Gunjal et al. (2023) [28] explored the various integrations of machine learning technology in the financial domain, which shared similarities in technical application with the method proposed in this study to improve enterprise financial sharing and risk identification using blockchain and deep learning technologies. This study emphasized the role of machine learning in accurate predictive model construction, similarly employing BiLSTM and Transformer models to enhance the accuracy of financial risk prediction.

2.2. *Summary*

Upon analyzing the works of the aforementioned scholars, it becomes apparent that the present study on financial information sharing and risk identification encompasses diverse domains, spanning internal audit methodologies, big data analysis, supply chain financial information sharing, and managerial perceptions concerning financial risks. Furthermore, the literature review highlights the contributions of blockchain technology towards augmenting the security and transparency of information sharing, as evidenced by the studies of literatures [16,17]. Additionally, deep learning has demonstrated remarkable efficacy in information risk identification. Nevertheless, the amalgamation of blockchain and deep learning technologies for information risk identification and analysis within the domain of corporate finance remains an underexplored territory. The sharing and management of corporate financial information are crucial for industries. With the development of the digital economy, enterprises are facing increasingly complex financial environments and ever-changing market demands. Effective sharing of financial information can reduce operating costs, enhance financial accounting efficiency, and thereby improve the financial management capabilities of enterprises. At the same time, accurate risk identification and management are of significant importance for safeguarding corporate assets, maintaining investor confidence, and ensuring sustainable development of enterprises. This study aims to enhance the security of financial information sharing and the accuracy of risk identification by combining blockchain technology and deep learning models. This has significant value for enterprises to maintain competitiveness and achieve sound operations in complex and dynamic markets. Henceforth, an innovative methodology has been introduced, merging blockchain technology and deep learning models, thereby furnishing a framework to bolster financial information sharing and risk identification. This offers substantial reinforcement for addressing real-world financial risk management challenges.

3. Methods for enterprise financial sharing and risk identification

3.1. *Analysis of enterprise financial information security issues*

Throughout the enterprise development process, financial information stands as a cornerstone for decision-making among management, investors, creditors, and other stakeholders. Offering insights into the financial standing of the enterprise, financial information facilitates strategic and operational decision-making for all involved parties [29]. Concurrently, financial information sharing not only fosters investor and shareholder confidence, enabling enterprises to secure financing and support, but also dismantles information silos, thereby enhancing the accuracy of accounting information [30]. Hence, the sharing of financial information is indispensable for enterprise operations. Nonetheless, financial information sharing also introduces certain security concerns, as depicted in Fig. 1.

In Fig. 1, When sharing enterprise financial information, unauthorized access may lead to data leakage to unauthorized individuals or competitors, while data tampering can result in inaccurate or misleading financial information for the enterprise. Unauthorized access may lead to the leakage or tampering of sensitive financial information. Simultaneously, external attacks, such as hackers and malicious software, can cause data loss, system interruptions, and service unavailability, thereby negatively impacting the enterprise's normal operation. Furthermore, physical or cloud storage devices used to store financial information may face threats of theft, damage, or data leakage, posing risks to data storage.

Comprehending the security issues associated with enterprise financial information sharing underscores the importance of enhancing and optimizing financial information-sharing services and risk identification. Hence, this study delves into the precise identification of risks in enterprise financial information-sharing services by introducing blockchain technology and deep learning algorithms, thereby bolstering security and advocating for continuous optimization of financial risk management mechanisms within enterprises.

3.2. Design of a model for applying blockchain to enterprise financial information sharing

A blockchain is a chain-like data structure capable of sequentially linking a series of transaction records to form a blockchain. Each block contains a specific amount of transaction data and a block header information associated with the preceding block [31,32]. The architecture of blockchain is depicted in Fig. 2.

In Fig. 2, the blockchain architecture consists of multiple layers, each of which serves different functions and roles. From bottom to top, the first layer is the data layer, which is the core of the blockchain, composed of a series of data blocks sorted by timestamp, forming the chain-like structure of the blockchain. Each data block contains a certain amount of transaction data and ensures data security through encryption algorithms (such as asymmetric encryption). The design of the data layer ensures the immutability and traceability of data, providing a solid data foundation for the entire blockchain system. Above the data layer is the network layer, which establishes a decentralized communication mechanism through a peer-to-peer (P2P) network. The validation mechanism of the network layer ensures that data transmission between nodes is secure and reliable, with each node participating in the validation and propagation process, enhancing the robustness of the entire network. Moving further up is the consensus layer, which is responsible for achieving consensus in a decentralized network. The consensus layer employs various consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated PoS (DPoS), and Practical Byzantine Fault Tolerance (PBFT) to ensure that all nodes in the network unanimously recognize the data. The incentive layer provides incentives to participants in the network through issuance and distribution mechanisms, encouraging nodes to participate in the maintenance and data validation of the blockchain, thus maintaining the vitality and security of the network. The smart contract layer enables the automation of transaction execution through smart contract scripts, where the algorithmic mechanisms in the contract can automatically handle transactions that meet predetermined conditions, thereby improving efficiency and reducing human errors. At the topmost layer is the application layer, which provides functions such as data management and permission management, allowing users to interact with the blockchain conveniently and develop and deploy various blockchain applications [33]. When applying blockchain to financial information-sharing services, its underlying logic is congruent, as illustrated in Fig. 3.

In Fig. 3, the underlying logic of blockchain technology and its compatibility with enterprise financial information sharing services is reflected in several key characteristics. Firstly, privacy protection is ensured through encryption technology and authorization access mechanisms, safeguarding the security and privacy of financial information to ensure that only authorized users can access sensitive

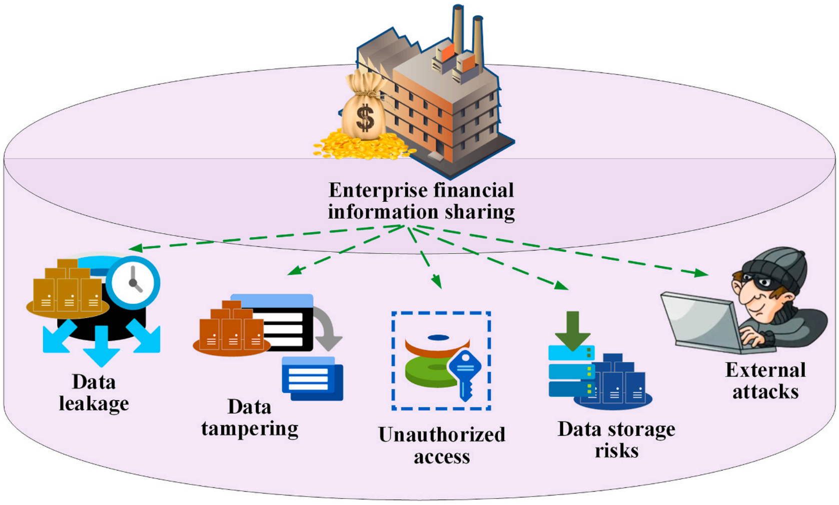


Fig. 1. Schematic representation of financial information sharing security issues.

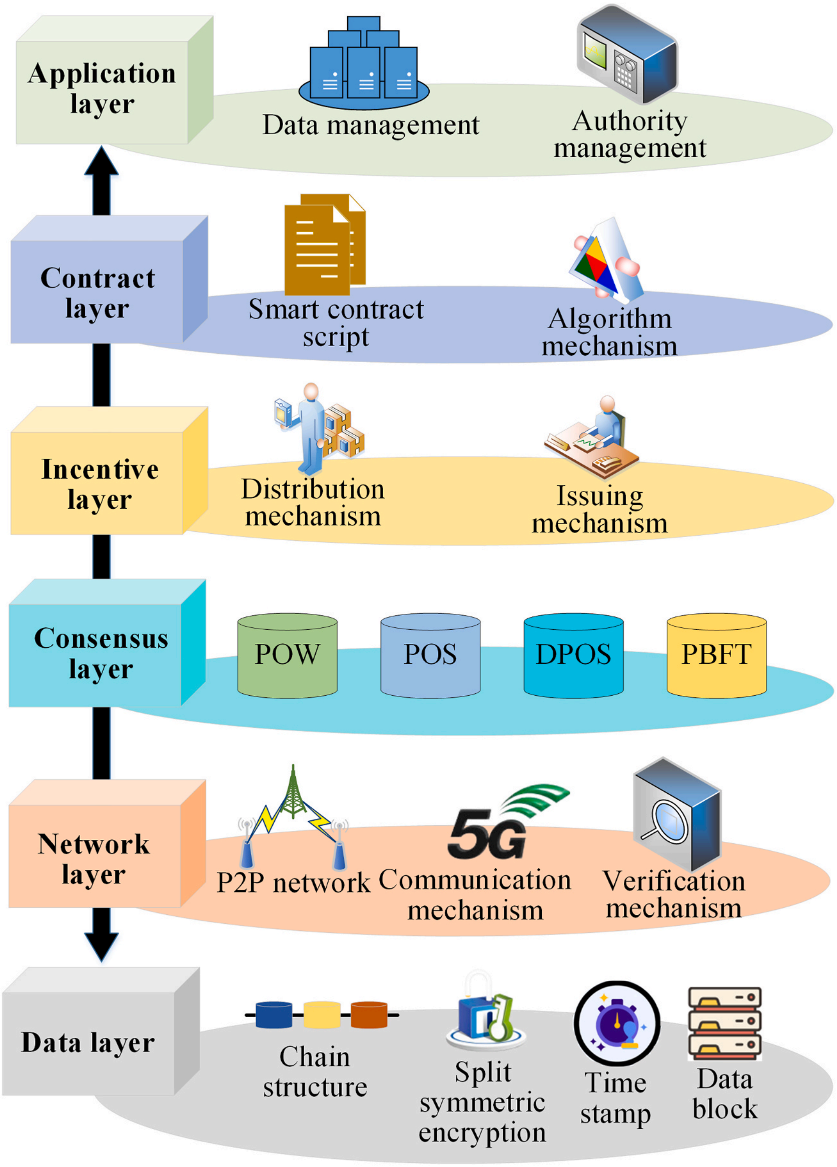


Fig. 2. Schematic representation of blockchain architecture.

financial data. Secondly, decentralization provides enterprises with an open, transparent, trustworthy, and traceable environment for financial information sharing, enhancing the transparency and trustworthiness of data sharing. Furthermore, the consensus mechanism offers consensus algorithms to ensure the consistency and credibility of financial information changes, enabling all parties to reach a consensus on the recognition of financial data. Lastly, blockchain technology ensures the immutability of financial information, preventing data tampering and fraudulent activities, thereby safeguarding the integrity and reliability of data. Addressing the imperative of efficient storage for enterprise financial data and the pertinent challenges concerning data sharing and privacy protection among employees, business units, financial institutions, and regulatory authorities, this study presents a meticulously crafted blockchain-based enterprise financial data sharing model, elucidated in Fig. 4.

In Fig. 4, in the blockchain-based enterprise financial data sharing model, various stakeholders such as regulatory authorities, enterprises, financial institutions, and employees interact through a blockchain network. Enterprises store financial data on cloud servers and utilize smart contracts of the blockchain to automate financial transactions, such as executing contract terms and processing payments and settlements. The encrypted data in smart contracts is protected by private keys, ensuring the security and privacy of the data. Simultaneously, the distributed ledger of the blockchain ensures data availability, enabling all authorized participants to access and verify financial information in real-time, thereby enhancing the efficiency and transparency of data sharing. Additionally, the immutability and anti-tampering mechanisms of the blockchain guarantee the integrity and reliability of financial data, preventing illegal tampering and fraudulent activities, thus providing enterprises with a secure and efficient platform for financial information

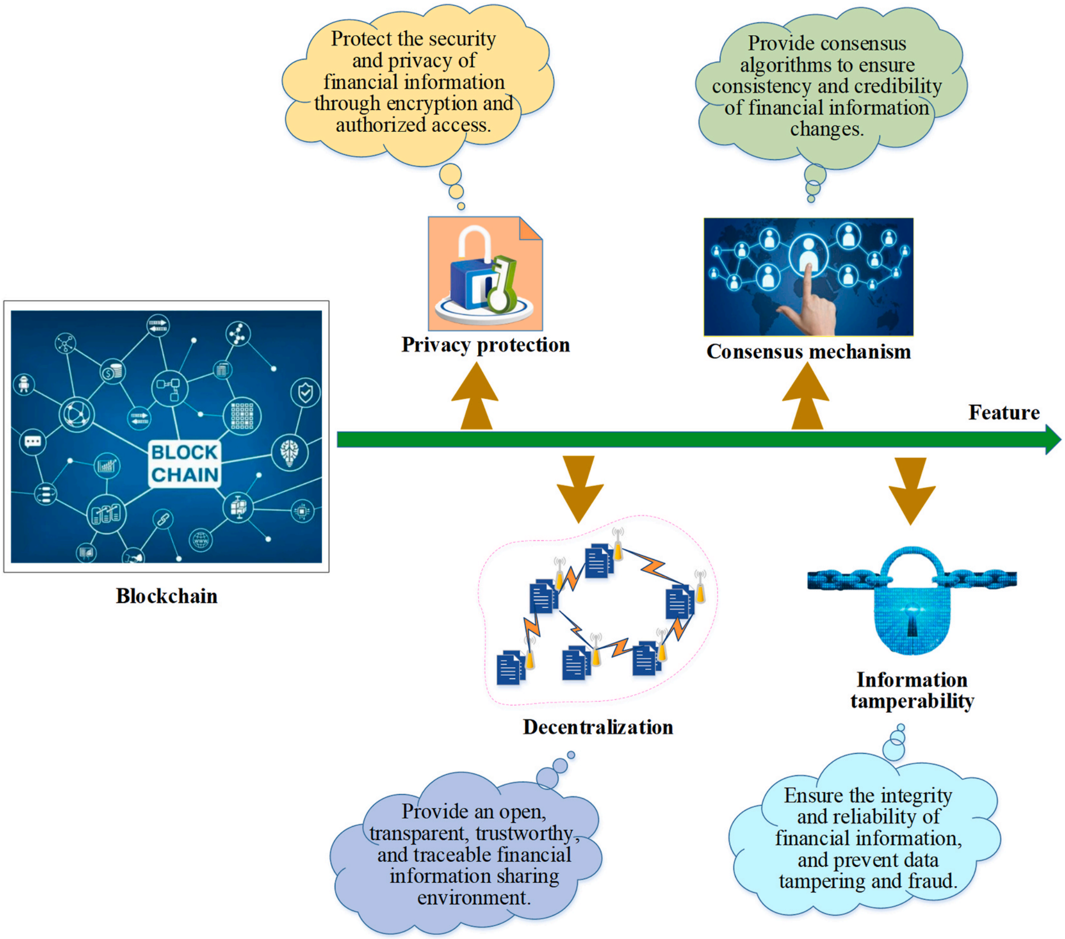

Protect the security and privacy of financial information through encryption and authorized access.
Provide consensus algorithms to ensure consistency and credibility of financial information changes.
Privacy protection
Consensus mechanism
BLOCK CHAIN
Blockchain
Feature
Decentralization
Information tamperability
Provide an open, transparent, trustworthy, and traceable financial information sharing environment.
Ensure the integrity and reliability of financial information, and prevent data tampering and fraud.

Fig. 3. Schematic representation of the underlying logic compatibility between blockchain technology and enterprise financial information sharing services.

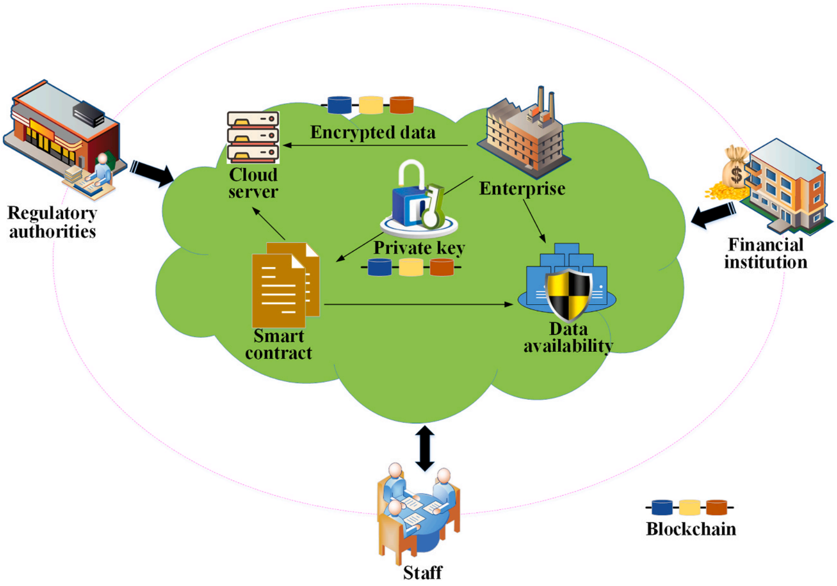


Fig. 4. Schematic representation of the blockchain-based enterprise financial data sharing model.

sharing and management. This model initiates the process by orchestrating the mapping of various entity nodes from the centralized network of enterprise finance onto the blockchain network, thereby facilitating decentralization. Subsequently, it leverages fully homomorphic encryption contract algorithms to encrypt shared financial data sources. This encryption serves the critical purpose of safeguarding the transmitted data exchanged among the nodes of participating entities, ensuring paramount principles of privacy and security regarding enterprise financial data, data authorization distribution, and secure data transmission. In the context of sharing enterprise financial information, the utilization of the PoW mechanism [34] is paramount. In situations of conflicting information, this model prioritizes the blockchain branch with the highest block count. Consequently, potential malicious attackers are compelled to ensure that the length of their attack chain surpasses that of the primary chain to acquire the capability to manipulate the entirety of the blockchain's dataset. The calculation of probability P_n is shown in Eq. (1):

$$P_n = \begin{cases} 1, q_F \geq p_T \\ (q_F/p_T)^n, q_F < p_T \end{cases} \tag{1}$$

In Eq. (1), p_T represents the probability that the next block belongs to an honest node, q_F represents the probability that the next block belongs to a malicious node, and P_n represents the probability of a malicious attacker tampering with n blocks. Therefore, the potential progress of malicious nodes should follow a Poisson distribution. The calculation of its expected value λ is shown in Eq. (2):

$$\lambda = nq_F/p_T \tag{2}$$

When the number of blocks published by malicious nodes exceeds the number of blocks published by honest nodes, the malicious nodes successfully complete the attack. The probability P of this scenario should be calculated by multiplying the probability density of the Poisson distribution for the number of blocks already published by malicious nodes k and the probability that malicious nodes can still complete the attack at that point. The specific calculation results are shown in Eq. (3):

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q_F/p_T)^{n-k} & k \leq n \\ 1 \quad k > n \end{cases} \tag{3}$$

The occurrence probability P is simplified, and the calculation result is as shown in Eq. (4):

$$P = 1 - \sum_{k=0}^{n} \frac{\lambda^k e^{-\lambda}}{k!} \left[1 - (q_F/p_T)^{n-k}\right] \tag{4}$$

After calculation, it is observed that as the number of block generations (n) increases, the probability of a successful attack decreases when the computing power of the malicious node is less than 50 %. In this study, a value of n is set to 6 for the application in enterprise financial data information-sharing services. This implies that information contained in a new block is deemed secure and effective only after undergoing six block generations.

3.3. Construction of an enterprise financial risk identification model based on the BiLSTM fusion transformer

During enterprise financial sharing services, the prediction of risks can significantly enhance the organization's ability to respond to potential threats. Financial risk prediction inherently constitutes a classification problem. Additionally, enterprise financial data manifests temporal continuity, wherein financial statements mutually influence each other, and data from preceding fiscal periods can exert an impact on subsequent years, particularly in terms of ratio information such as year-over-year growth rates and growth rates compared to the beginning of the period, which are pivotal financial metrics. RNNs are adept at capturing temporal dependencies in data, rendering them suitable for enterprise financial risk identification tasks. However, issues such as vanishing gradients and exploding gradients necessitate the introduction of a variant of RNNs, namely BiLSTM. BiLSTM comprises two independent Long Short-Term Memory (LSTM) layers—one initialized from the forward sequence and the other from the backward sequence—whose outputs are subsequently merged. This architecture enables BiLSTM to simultaneously consider past and future contextual information in both financial videos and text data, thereby capturing long-range dependencies in video and text sequences more effectively [35,36].

When the BiLSTM algorithm is applied to extract enterprise financial data information for a given sequence $S = \{w_1, w_2, \cdots, w_n\}$, the input information is first embedded and represented as $e_1, e_2, \cdots, e_n$. The forward LSTM encodes the text, as shown in Eq. (5):

$$\begin{cases} f_t = \sigma(W_f[h_{t-1}, e_i]) \\ i_t = \sigma(W_i[h_{t-1}, e_i]) \\ \widetilde{C}_t = \tanh(W_C[h_{t-1}, e_i]) \\ C_t = f_t \times C_{t-1} + i_t \times \widetilde{C}_t \\ o_t = \sigma(W_o[h_{t-1}, e_i]) \\ h_t = o_t \times \tanh(C_t) \end{cases} \tag{5}$$

In Eq. (5), σ and tanh are activation functions, with the former being the sigmoid function. W_f, W_i, W_C, W_o represents the weight parameters, h_{t-1} refers to the output of the previous neuron, C_t represents the cell state at time t, and h_t signifies the hidden layer output at time t.

Furthermore, the experiment feeds the financial data features x_t and h_{t-1} into the BiLSTM model, obtaining coefficients f_t, i_t through a sigmoid function applied to the financial data. The input is then processed through an activation function, resulting in a temporary cell variable $\widetilde{c}_t$. The computation process is illustrated in Eqs. (6)–(8):

$$f_t = \delta\left(\left[w_f \cdot [h_{t-1}, x_t] + b_f, w'_f \cdot \left[h'_{t-1}, x_t\right] + b'_f\right]\right) \tag{6}$$

$$i_t = \delta\left(\left[w_i \cdot [h_{t-1}, x_t] + b_i, w'_i \cdot \left[h'_{t-1}, x_t\right] + b'_i\right]\right) \tag{7}$$

$$\widetilde{c}_t = \tanh\left(\left[w_c \cdot [h_{t-1}, x_t] + b_c, w'_c \cdot \left[h'_{t-1}, x_t\right] + b'_c\right]\right) \tag{8}$$

In Eqs. (6)–(8), w denotes the weight matrix, and b represents the bias vector. Therefore, the hidden state h_t at time t can be expressed as shown in Eqs. (9) and (10):

$$h_t = \left[\overrightarrow{h}_t, \overleftarrow{h}_t\right] \tag{9}$$

$$\begin{cases} \overrightarrow{h}_t = \overrightarrow{LSTM}\left(\overrightarrow{w}_t, \overrightarrow{h}_{t-1}, \overrightarrow{b}_t, \overrightarrow{c}_{t-1}\right) \\ \overleftarrow{h}_t = \overleftarrow{LSTM}\left(\overleftarrow{w}_t, \overleftarrow{h}_{t-1}, \overleftarrow{b}_t, \overleftarrow{c}_{t+1}\right) \end{cases} \tag{10}$$

In Eqs. (9) and (10), W and b respectively denote the relevant weights for the gate units and memory cells, and c_t and h_t represent the

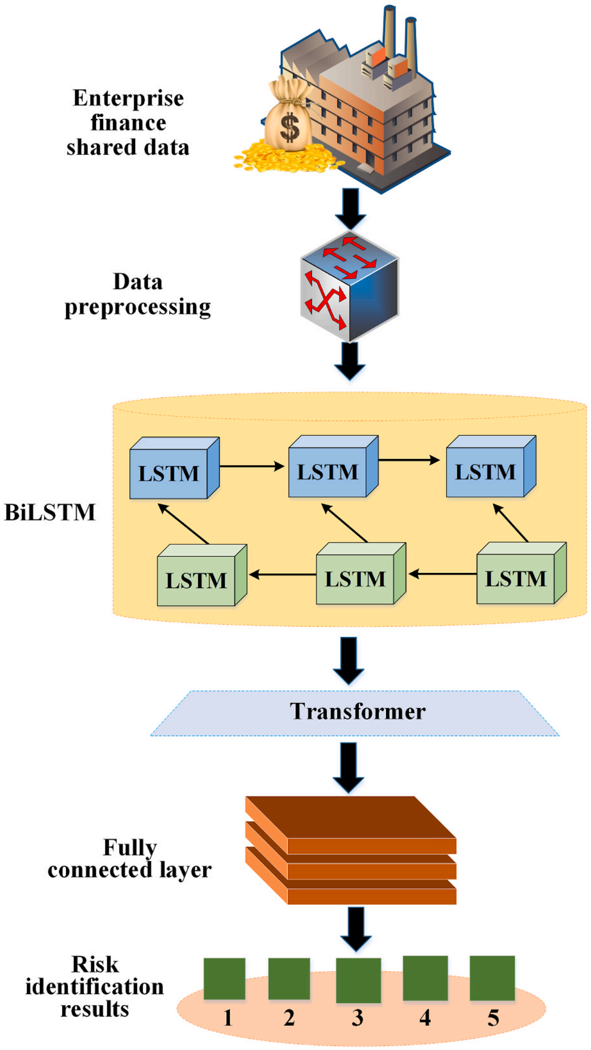


Fig. 5. Schematic representation of the enterprise financial management risk identification model integrating BiLSTM and transformer.

state of the memory cell and the value of the LSTM's hidden state at time t. In this context, the calculation of $\overrightarrow{h}_t$, $\overleftarrow{h}_t$ is defined in Eq. (10), where → and ← symbolize forward and backward financial data information.

However, it is crucial to acknowledge that each word may contribute differently to the semantics based on the diverse contexts of financial video and text data. The multi-head attention mechanism (AM) stands as a pivotal element within the Transformer architecture. It is specifically engineered to compute multiple attention weight matrices, thereby facilitating the learning of distinct attention patterns across various subspaces of financial video and text representations. This study introduces the Transformer model algorithm, thereby enabling the model to effectively integrate features originating from different subspaces [37]. This advancement lays the groundwork for the development of an enterprise financial risk identification model that combines both BiLSTM and Transformer, as depicted in Fig. 5.

In Fig. 5, the initial step within this model encompasses the preprocessing of input samples, encompassing both enterprise financial video and text data. This preprocessing phase entails various tasks such as text tokenization, elimination of stopwords and special characters, as well as denoising, image enhancement, and color correction for images. Following this preprocessing stage, the preprocessed enterprise financial video and text sequence data, adeptly processed using BiLSTM, becomes capable of capturing the intricate interdependencies inherent within the data. Subsequently, the experiment leverages the multi-head AM inherent within the Transformer model. This mechanism concurrently computes multiple attention weight matrices, facilitating the learning of distinct attention patterns from diverse subspaces. Consequently, the system gains the ability to simultaneously direct attention across different levels of information within enterprise financial video and text data samples, thereby effectively capturing semantic correlations present in various subspaces. To make practical use of the multi-head AM for capturing the actual dependencies in enterprise financial video and text data, the context vector q_{avg} is integrated as a feature into the sequence generated by the multi-head AM, denoted as h_i^U. This yields α_i value to measure the importance of the i-th word in the sentence, as computed in Eqs. (11)–(14):

$$\alpha_i = \frac{\exp\left(\gamma\left(h_i^U, q_{avg}\right)\right)}{\sum_{j=1}^{n} \exp\left(\gamma\left(h_i^U, q_{avg}\right)\right)} \tag{11}$$

$$\gamma\left(h_i^U, q_{avg}\right) = \tanh\left(h_i^U W_\alpha q_{avg}^T + b_w\right) \tag{12}$$

$$U = \sum_{i=1}^{n} \alpha_i h_i \tag{13}$$

$$p(y) = soft\max(WU + b) \tag{14}$$

In Eqs. (11)–(14), γ represents the scoring function, W_α refers to the attention parameter matrix, and b_w indicates the bias values. Subsequently, the attention scores are used to obtain the final context representation of enterprise financial video and text data. U is input into a softmax classifier to obtain the probability distribution for each relationship. The results of risk classification are labeled on a scale of 1–5, as shown in Table 1.

In this model, the precise pseudocode detailing the application of the BiLSTM integrated with the Transformer algorithm for enterprise financial management risk identification is depicted in Fig. 6.

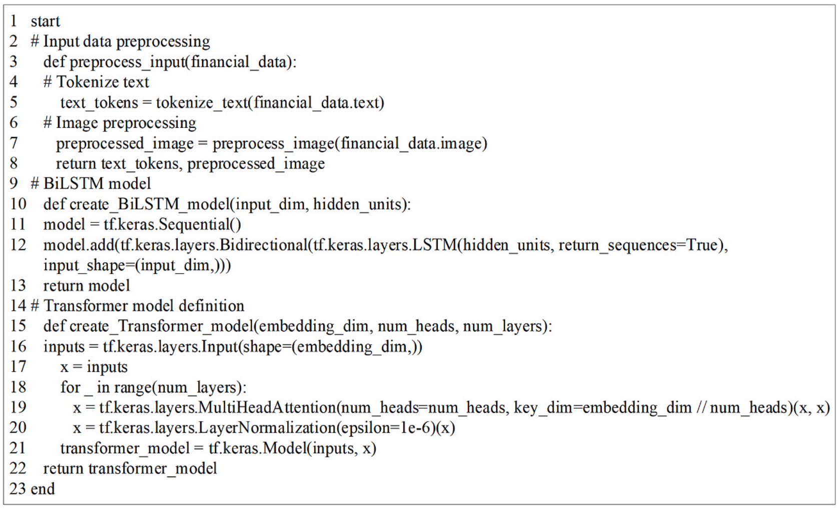
3.4. Experimental evaluation

To evaluate the performance and efficacy of the enterprise financial sharing model and the risk identification model elucidated in this study, data are meticulously acquired from the Wind database, accessible at the web address www.wind.com.cn/. The selection of datasets is conducted with a focus on including sample enterprises, particularly targeting small and medium-sized entities among A-share listed companies, chosen for their accessibility and relevance to the study's objectives. To safeguard individual privacy, measures are implemented to anonymize the obtained data, such as removing personal identifiers or aggregating data. Additionally, ethical considerations are prioritized, with the data undergoing review by an ethical committee to ensure adherence to ethical principles and regulations. Subsequently, the dataset is divided into a training set and a test set in an 8:2 ratio. An example of financial data input into Wind database is shown in Table 2.

Video-format financial data may include events such as corporate financial report releases and investor briefings. The application of video analysis technology can extract key financial information from videos, such as corporate strategic directions, summaries of financial conditions, and future plans. These pieces of information can be combined with textual data to provide more comprehensive inputs for the model. The experiment first preprocesses these video and text data, including tokenization of text, removal of stopwords and special characters, as well as denoising, image enhancement, and color correction for videos. Before constructing the enterprise

Table 1
Risk severity classification.

Numerical value	1	2	3	4	5
Corporate financial status	Excellent	Good	Fair	High Risk	Very High Risk



```
start
# Input data preprocessing
  def preprocess_input(financial_data):
  # Tokenize text
     text_tokens = tokenize_text(financial_data.text)
  # Image preprocessing
    preprocessed_image = preprocess_image(financial_data.image)
    return text_tokens, preprocessed_image
# BiLSTM model
  def create_BiLSTM_model(input_dim, hidden_units):
  model = tf.keras.Sequential()
  model.add(tf.keras.layers.Bidirectional(tf.keras.layers.LSTM(hidden_units, return_sequences=True),
  input_shape=(input_dim,)))
  return model
# Transformer model definition
  def create_Transformer_model(embedding_dim, num_heads, num_layers):
  inputs = tf.keras.layers.Input(shape=(embedding_dim,))
     x = inputs
     for _ in range(num_layers):
       x = tf.keras.layers.MultiHeadAttention(num_heads=num_heads, key_dim=embedding_dim // num_heads)(x, x)
       x = tf.keras.layers.LayerNormalization(epsilon=1e-6)(x)
     transformer_model = tf.keras.Model(inputs, x)
  return transformer_model
end
```

Fig. 6. Pseudocode flow chart of applying BiLSTM fusion transformer algorithm to enterprise financial management risk identification.

Table 2
Financial data input example of wind database.

Hundsun Technologies Inc.			
Item	2023 Annual Report	2022 Annual Report	Increase
Total Operating Income (yuan)	7.281 billion	6.502 billion	11.98 %
Net Profit Attributable to Owners of the Parent Company (yuan)	1.424 billion	1.091 billion	30.50 %
Non-Recurring Net Profit (yuan)	1.448 billion	1.145 billion	26.51 %
Monetary Funds (yuan)	2.422 billion	2.873 billion	−15.69 %
Accounts Receivable (yuan)	1.068 billion	0.923 billion	15.77 %
Interest-Bearing Debt (yuan)	0.501 billion	0.226 billion	121.52 %
Gross Profit Margin	74.84 %	73.56 %	1.74 %
Net Profit Margin	19.82 %	17.23 %	15.06 %
Proportion of Three Expenses to Operating Income	21.00 %	23.12 %	−9.17 %
Net Assets per Share (yuan)	4.23	3.59	17.86 %
Earnings per Share (yuan)	0.75	0.57	31.58 %
Operating Cash Flow per Share (yuan)	0.66	0.6	10.82 %

financial risk identification model, preprocessing the collected video and text data is a crucial step. Text data preprocessing involves tokenization of text using natural language processing tools to break continuous text into meaningful words or lexical units. Common but irrelevant words are removed as they are not crucial for model training. Words are converted into their base forms to reduce data dimensions and improve model generalization. Besides numerical information in financial data, other special characters and digits are removed from the text to avoid interference with the model. Video data preprocessing involves reducing noise in videos using image processing techniques to improve picture quality. Adjusting video colors ensures color authenticity and consistency, aiding subsequent feature extraction. Keyframes are extracted from the video, which may contain critical information from financial reports. Fusion of images and text data involves extracting term frequency-inverse document frequency (TF-IDF) features from text data and extracting visual features such as edges, textures, etc., from image data. Extracted features are converted into numerical vectors for input into machine learning models. Data augmentation techniques such as rotation, scaling, cropping, etc., are applied to video data to enhance model robustness. For text data, data augmentation involves methods like synonym replacement and sentence reconstruction to increase training diversity. Standardization is applied to numerical features such as financial indicators to conform to the numerical range for model training. For risk identification tasks, financial data is annotated based on risk levels, ranging from 1 (best financial condition) to 5 (serious risk). Preprocessed data is then processed through BiLSTM and Transformer models to identify and predict enterprise financial risks.

In the financial data-sharing model constructed, the Hyperledger Fabric blockchain platform is employed as the foundational framework. To meticulously assess the performance of this model, a systematic process of experimentation and optimization is conducted. Key configuration parameters included a block size of 2 megabytes, a block confirmation time interval of 15 min, adoption of the PoW consensus algorithm, a bandwidth constraint set at 100 megabits per second, initiation of 1000 requests by clients, and a network composition comprising a total of 150 nodes. To comprehensively evaluate the effectiveness of the financial sharing model algorithm proposed in this study, comparative analyses are conducted against alternative model algorithms, specifically the Delegated Byzantine Fault Tolerance (DBFT) [38], the model suggested by literature [16], and the model introduced by literature [18]. These comparisons are based on a suite of performance metrics, including throughput and security parameters such as the evaluation of average leakage rate and packet loss rate.

Regarding the enterprise financial management risk identification model based on BiLSTM integrated with Transformer developed in this study, simulation and modeling are performed using the TensorFlow platform, along with various Python modules. Specific hyperparameter settings include a batch size of 100, 100 iterations, and optimization of the loss function using the stochastic gradient descent algorithm with an initial learning rate of 0.001. The performance of the model proposed in this study, with BiLSTM integrated with the Transformer algorithm, is compared with BiLSTM, RNNs [39], Transformer, and the model algorithm suggested by literature [24], based on metrics such as accuracy, AUC value, and computation time for risk prediction.

4. Results and discussion

4.1. Analysis of comparative results for data transmission with different algorithms

The financial sharing model algorithm proposed in this study is evaluated against the DBFT, literature [16], and literature [18] model algorithms based on metrics such as throughput and security (average leakage rate, packet loss rate), as illustrated in Figs. 7–9.

In Fig. 7, the throughput analysis of various algorithms indicates a decrease in throughput with an increase in the number of nodes. Remarkably, when the number of nodes reaches 146, the throughput of the enterprise intelligent financial sharing and privacy security model proposed in this study reaches 88.51, showcasing superior performance compared to other model algorithms such as DBFT. The order of throughput for each model, from highest to lowest, is as follows: the algorithm proposed in this study, literature [18], literature [16], DBFT. Thus, the blockchain-based enterprise financial data-sharing model suggested in this study demonstrates enhanced efficiency, enabling the handling of a larger volume of data within the same time frame.

Figs. 8 and 9 present a comparison of the average leakage rate and packet loss rate in data transmission for different algorithms under varying data volumes. As the volume of network data transmission increases, the average data leakage rate for the model algorithm proposed in this study decreases, significantly lower than other model algorithms. This could be attributed to the gradual performance stabilization of the model algorithm as data transmission volume increases. At a data volume of 1000 records, the data leakage rate does not exceed 10 % (Fig. 8). Regarding the mean packet loss rate, as the volume of system data transmission increases, the loss rate of data associated with the proposed model algorithm exhibits a marginal increment, remaining below the 10 % threshold, as illustrated in Fig. 9. In direct comparison to alternative algorithmic mechanisms, this study's model showcases superior performance in terms of data leakage and packet loss rates. Consequently, when assessed across various data volumes, the data transmission within the financial sharing model elucidated in this study consistently manifests a significantly reduced average leakage rate and upholds a diminished packet loss rate. This outcome underscores the model's robust network data security transmission capabilities.

4.2. Analysis of risk identification results with different algorithms

Further evaluation of the risk prediction performance of the model proposed in this study, incorporating the BiLSTM integrated with Transformer algorithm, is conducted in comparison to BiLSTM, RNNs, Transformer, and the model algorithm suggested by literature [24]. This assessment is based on metrics such as accuracy, AUC value, and computation time, as depicted in Figs. 10 and 11.

In Fig. 10, an analysis of the accuracy of the algorithmic model proposed in this study, in comparison to RNNs, BiLSTM, Transformer, and the model algorithm suggested by literature [24], demonstrates significantly higher accuracy for the model proposed in this study. The accuracy of enterprise risk identification consistently exceeds 94.5 % across all cases, representing a minimum of 4.28

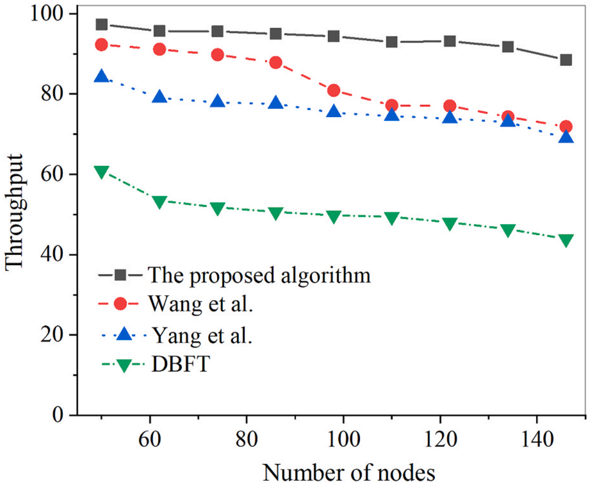


Fig. 7. Throughput results for different node counts under various algorithms.

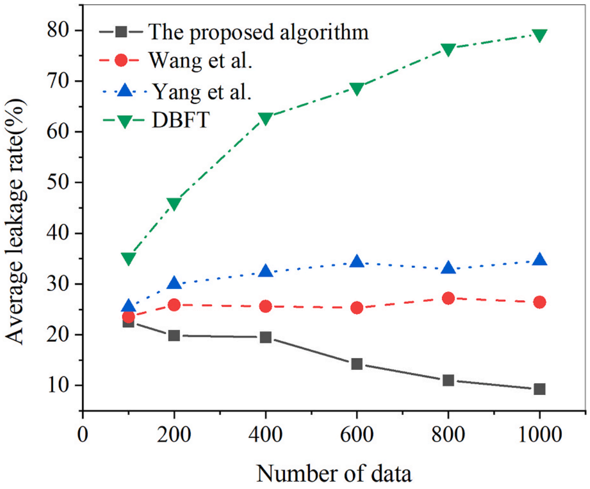


Fig. 8. Average leakage rate results for different algorithms under various data volumes.

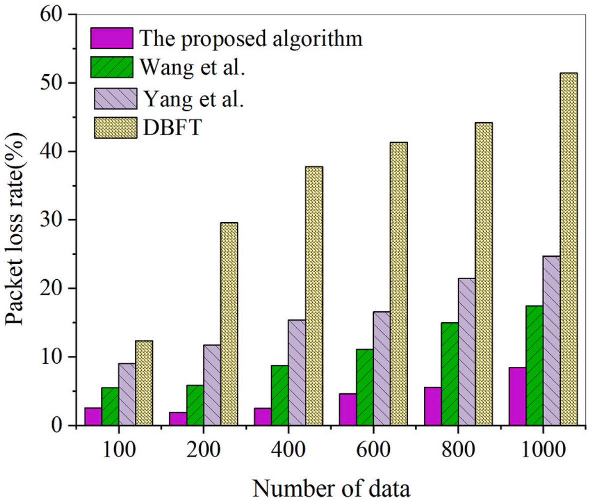


Fig. 9. Packet loss rate results for different algorithms under various data volumes.

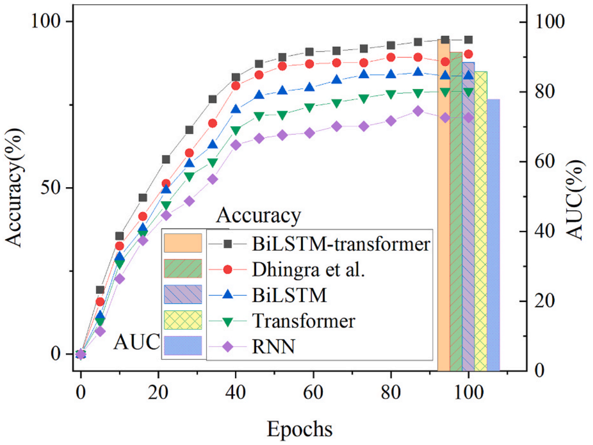


Fig. 10. Accuracy of Different Algorithms in Enterprise Financial Risk Identification ((A) is Accuracy; (B) is AUC value).

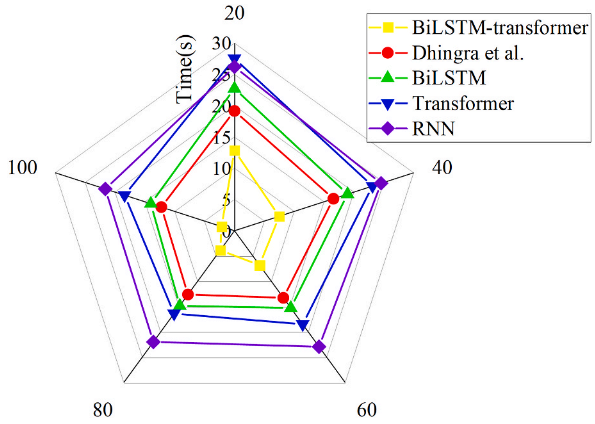


Fig. 11. Recognition time results for different algorithms in enterprise financial risk.

% higher accuracy compared to algorithms employed by other researchers (e.g., RNNs, BiLSTM, etc.). The order of accuracy for the algorithms, from highest to lowest, is as follows: the model proposed in this study, the model algorithm suggested by literature [24], BiLSTM, Transformer, RNNs. Furthermore, the AUC value for the model proposed in this study is 95.13 %. Consequently, in comparison to algorithms utilized by other researchers, the enterprise financial management risk identification model based on BiLSTM integrated with Transformer, as proposed in this study, demonstrates a heightened level of accuracy in risk identification. This enhances the model's capacity to predict financial risks effectively, thereby furnishing more precise support for the intelligent evolution of enterprises.

In Fig. 11, as the number of iterations increases, the required time initially decreases and then stabilizes, indicating a convergence trend. In comparison to other models, the algorithmic model proposed in this study maintains a stable required time of approximately 2.16 s. Contrasted with the models introduced by fellow researchers, the algorithmic model presented in this study surpasses the model proposed by literature [24] by reducing the requisite time by 10.06 s. Furthermore, this time efficiency exceeds that of other existing model algorithms. Consequently, the model algorithm provided in this study has the capacity to expedite the process of enterprise financial risk recognition, achieving notably swifter results.

The BiLSTM integrated with Transformer algorithm proposed in this study is compared with the techniques of Dhingra, Wang, and Yang in terms of accuracy, AUC value, and computation time for risk prediction. Comparative analysis demonstrates that the proposed algorithm achieves an accuracy exceeding 94.5 % in enterprise financial risk identification, with an AUC value reaching 95.13 %. Moreover, it exhibits advantages in time efficiency for risk identification, with an average identification time of approximately 2.16 s, representing a reduction of 10.06 s compared to the model proposed by Dhingra et al.

5. Conclusion

The blockchain-based enterprise intelligent financial sharing and privacy security model demonstrates outstanding throughput performance. With 146 nodes, the model achieves a throughput of 88.51, and the data leakage rate and packet loss rate during data transmission remain below 10 %. In terms of risk prediction and recognition, the proposed BiLSTM integrated with the Transformer algorithm achieves an accuracy of over 94.5 % in identifying enterprise financial risks. It serves as a powerful tool for supporting subsequent intelligent and efficient financial decision-making for enterprises.

The results of this study hold significant practical application value for the industry. Enterprises can utilize the proposed financial sharing model to enhance the security and efficiency of financial data sharing through blockchain technology, thereby reducing financial risks. Additionally, by employing the risk identification model integrated with BiLSTM and Transformer, enterprises can more accurately predict and manage potential financial risks, enabling them to make wiser strategic decisions. In terms of academic research, this study provides new perspectives and methodologies for the fields of financial information sharing and risk identification. The introduction of blockchain technology and the fusion of deep learning models offer novel avenues for future research. Furthermore, the experimental analysis and results discussion of this study provide empirical evidence and references for similar research in academia. However, this study also has certain limitations. Firstly, the generalization ability of the model has not been validated on a broader dataset. Secondly, despite demonstrating high accuracy in experiments, the model may be influenced by various factors in practical applications, such as data quality and model parameter adjustments. Moreover, the interpretability of the model needs to be further improved to provide clearer risk identification guidelines for enterprise decision-makers. Addressing the limitations of the current study, several future research directions are proposed: 1. Validate the generalization ability and robustness of the model on a broader range of enterprise financial datasets, including different industries and scales of enterprises. 2. Apply the model to actual enterprise financial risk management processes, evaluate its performance in real-world complex environments, and optimize it based on feedback. 3. Research and develop new technical means to enhance the interpretability of the model, aiding enterprises in better understanding the results of risk identification. 4. Further optimize the structure and parameters of the BiLSTM and Transformer models to improve the operational efficiency and accuracy of the model. 5. Integrate multidisciplinary knowledge including financial management, blockchain technology, and deep learning to explore more comprehensive and in-depth enterprise financial risk management strategies. This study is expected to inspire further research on the application of blockchain technology in enterprise financial management and the exploration of deep learning models in risk identification tasks.

Data availability statement

All data generated or analyzed during this study are included in this published article [and its supplementary information files].

Ethics statement

All submissions which include human or animal participation must have an ethics and consent section in the manuscript.

CRediT authorship contribution statement

Yang Wu: Writing – review & editing, Writing – original draft, Visualization, Methodology, Investigation, Formal analysis, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] B. Bustani, M. Khaddafi, R.N. Ilham, Regional financial management system of regency/city regional original income in aceh province period year 2016-2020, International Journal of Educational Review, Law And Social Sciences (IJERLAS) 2 (3) (2022) 459–468.

[2] T. Polzer, I.M. Nolte, J. Seiwald, Gender budgeting in public financial management: a literature review and research agenda, Int. Rev. Adm. Sci. 89 (2) (2023) 450–466.

[3] A.Y. Ha, H. Luo, W. Shang, Supplier encroachment, information sharing, and channel structure in online retail platforms, Prod. Oper. Manag. 31 (3) (2022) 1235–1251.

[4] C. Baah, D. Opoku Agyeman, I.S.K. Acquah, et al., Effect of information sharing in supply chains: understanding the roles of supply chain visibility, agility, collaboration on supply chain performance, Benchmark Int. J. 29 (2) (2022) 434–455.

[5] R. Durga, E. Poovammal, Fled-block: federated learning ensembled deep learning blockchain model for covid-19 prediction, Front. Public Health 10 (2022) 892499.

[6] R. Kumar, P. Kumar, R. Tripathi, et al., Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems, IEEE Trans. Ind. Inf. 18 (11) (2022) 8065–8073.

[7] D.K. Nguyen, G. Sermpinis, C. Stasinakis, Big data, artificial intelligence and machine learning: a transformative symbiosis in favour of financial technology, Eur. Financ. Manag. 29 (2) (2023) 517–548.

[8] J. Gao, Research on the corporate financial transformation with big data technologies, International Journal of Progressive Sciences and Technologies 32 (2) (2022) 8–12.

[9] H. Liu, B. Yang, X. Xiong, et al., A financial management platform based on the integration of blockchain and supply chain, Sensors 23 (3) (2023) 1497.

[10] C. Li, X. Wang, Y. Hu, et al., Forecasting shipping index using CEEMD-PSO-BiLSTM model, PLoS One 18 (2) (2023) e0280504.

[11] S. Levytska, L. Pershko, L. Akimova, et al., A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring, International Journal of Applied Economics, Finance and Accounting 14 (2) (2022) 194–206.

[12] J. Gao, Analysis of enterprise financial accounting information management from the perspective of big data, Int. J. Sci. Res. 11 (5) (2022) 1272–1276.

[13] M. Xu, S. Ma, G. Wang, Differential game model of information sharing among supply chain finance based on blockchain technology, Sustainability 14 (12) (2022) 7139.

[14] M. Alrawad, A. Lutfi, M.A. Almaiah, et al., Managers' perception and attitude toward financial risks associated with SMEs: analytic hierarchy process approach, J. Risk Financ. Manag. 16 (2) (2023) 86.

[15] N. Cornwell, C. Bilson, A. Gepp, et al., The role of data analytics within operational risk management: a systematic review from the financial services and energy sectors, J. Oper. Res. Soc. 74 (1) (2023) 374–402.

[16] W. Yang, C. Xie, L. Ma, Dose blockchain-based agri-food supply chain guarantee the initial information authenticity? An evolutionary game perspective, PLoS One 18 (6) (2023) e0286886.

[17] J. Lee, B. Kim, A.R. Lee, Priority evaluation factors for blockchain application services in public sectors, PLoS One 18 (3) (2023) e0279445.

[18] Z. Wang, S. Zhang, Y. Zhao, et al., Risk prediction and credibility detection of network public opinion using blockchain technology, Technol. Forecast. Soc. Change 187 (2023) 122177.

[19] X. Xie, J. Zhang, Y. Luo, et al., Enterprise credit risk portrait and evaluation from the perspective of the supply chain, Int. Trans. Oper. Res. 31 (4) (2024) 2765–2795.

[20] H. Zhang, Y. Li, Z. Lv, et al., A real-time and ubiquitous network attack detection based on deep belief network and support vector machine, IEEE/CAA Journal of Automatica Sinica 7 (3) (2020) 790–799.

[21] Z. Lv, D. Chen, B. Cao, et al., Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins, IEEE Trans. Comput. (2023), https://doi.org/10.1109/TC.2021.3077687.

[22] J. Wu, X. Chen, Y. Bie, et al., A co-evolutionary lane-changing trajectory planning method for automated vehicles based on the instantaneous risk identification, Accid. Anal. Prev. 180 (2023) 106907.

[23] X. Li, J. Wang, C. Yang, Risk prediction in financial management of listed companies based on optimized BP neural network under digital economy, Neural Comput. Appl. 35 (3) (2023) 2045–2058.

[24] N. Dhingra, R. Bridgelall, P. Lu, et al., Ranking risk factors in financial losses from railroad incidents: a machine learning approach, Transport. Res. Rec. 2677 (2) (2023) 299–309.

[25] X. Chen, Z. Long, E-commerce enterprises financial risk prediction based on FA-PSO-LSTM neural network deep learning model, Sustainability 15 (7) (2023) 5882.

[26] X. Dong, B. Dang, H. Zang, et al., The prediction trend of enterprise financial risk based on machine learning arima model, Journal of Theory and Practice of Engineering Science 4 (1) (2024) 65–71.

[27] H. Sasaki, M. Fujii, H. Sakaji, et al., Enhancing risk analysis with GNN: edge classification in risk causality from securities reports, International Journal of Information Management Data Insights 4 (1) (2024) 100217.

[28] S.N. Gunjal, S. Shiyamala, P.D. Halle, et al., Enhancing financial insights: integration of various machine learning techniques, International Journal of Intelligent Systems and Applications in Engineering 12 (17s) (2024) 644–650.

[29] A.P. Monteiro, J. Vale, E. Leite, et al., The impact of information systems and non-financial information on company success, Int. J. Account. Inf. Syst. 45 (2022) 100557.

[30] L. Machfuzh, H. Setiyawati, The impact of the quality of financial statements on institution performance accountability, IJO-International Journal of Business Management (ISSN 2811-2504) 5 (1) (2022) 1–18.

[31] S.B. Far, A.I. Rad, M.R. Asaar, Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse, Data Science and Management 6 (3) (2023) 183–197.

[32] W. Xiong, D. Wan, Financial investment trust mechanism based on smart contract, PLoS One 18 (7) (2023) e0287706.

[33] F. Nemeczek, D. Weiss, Insights on crypto investors from a German personal finance management app, J. Risk Financ. Manag. 16 (4) (2023) 248.

[34] N. Sapra, I. Shaikh, A. Dash, Impact of proof of work (PoW)-Based blockchain applications on the environment: a systematic review and research agenda, J. Risk Financ. Manag. 16 (4) (2023) 218.

[35] G. Ni, X. Zhang, X. Ni, et al., A WOA-CNN-BiLSTM-based multi-feature classification prediction model for smart grid financial markets, Front. Energy Res. 11 (2023) 1198855.

[36] D. Zhou, X. Zhuang, H. Zuo, et al., A model fusion strategy for identifying aircraft risk using CNN and Att-BiLSTM, Reliab. Eng. Syst. Saf. 228 (2022) 108750.

[37] M. Zhong, Y. Wang, J. Yan, et al., Transformer-based comparative multi-view illegal transaction detection, PLoS One 18 (1) (2023) e0276495.

[38] A.A. Khan, A.A. Laghari, P. Li, et al., The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises, Sci. Rep. 13 (1) (2023) 1656.

[39] G. Mu, Z. Liao, J. Li, et al., IPSO-LSTM hybrid model for predicting online public opinion trends in emergencies, PLoS One 18 (10) (2023) e0292677.