Interdisciplinary Research perspective

Article

A Cloud Computing Communication Network Security Transmission Control Method Based on Long Short-Term Memory Networks

Kun Ma[*1,2], Chuangyue Hu[1] and Yuzhi Zhang[2]

[1] Jiaxing Yangtze Delta Region Blockchain Technology, Jiaxing, China

[2] College of software, Nankai University, Tianjin, China;

***** Correspondence: makuning@foxmail.com

https://doi.org/10.63138/irp010101

Abstract: With the rapid development of cloud computing communication networks, issues such as limited resources and insufficient processing capabilities make it difficult to ensure the security of data transmission. This paper proposes a novel secure transmission control method based on Long Short-Term Memory networks (LSTM). In response to potential security threats during data transmission, three key technologies are designed: data encryption and transmission, intrusion detection and response, and access control and privilege management. By applying LSTM technology, this method significantly improves data processing speed, enhances the accuracy of intrusion detection, and increases the adaptability of privilege configuration. Experimental results show that the LSTM-based method outperforms traditional methods in key performance indicators, verifying its effectiveness and feasibility in practical applications.

Keywords: Long Short-Term Memory networks (LSTM); Cloud Computing; Network Security; Data Encryption; Intrusion Detection; Access Control

1. Introduction

Against the backdrop of rapid development in information technology, cloud computing has become an integral part of modern communication networks and is widely applied across various industries. However, as the scale of cloud computing communication networks expands and their complexity increases, security issues are becoming increasingly prominent1. Traditional security technologies, such as firewalls, intrusion detection systems, and static access control strategies, are struggling to cope with the current complex and variable network attacks, especially with the emergence of new attack methods like Advanced Persistent Threats (APT), making the network security situation even more severe.

Long Short-Term Memory networks (LSTM), a special type of recurrent neural network in the field of deep learning, possess the ability to process time-series data and capture long-distance dependency relationships3. LSTM has achieved significant results in areas such as natural language processing, speech recognition, and financial forecasting, and its powerful learning and generalization capabilities offer new insights into solving security issues in communication networks. Applying LSTM technology to the security protection of cloud computing

communication networks can identify abnormal behaviors in massive data in real-time, improving the accuracy and response speed of intrusion detection.

Cloud computing, through virtualization technology, distributed computing, and big data processing, has achieved efficient utilization and dynamic expansion of computing resources, providing users with flexible computing services. However, data transmission in cloud computing environments involves a complex network architecture with multiple tenants, nodes, and cross-regions, facing more diversified and complex data security threats. For example, data may be subjected to eavesdropping, tampering, replay attacks, and other threats during transmission, making traditional encryption and authentication mechanisms unable to effectively guarantee the confidentiality and integrity of the data in a timely manner.

In response to the issues, this paper proposes a cloud computing communication network security transmission control technology based on LSTM, aiming to enhance the security of data transmission and the overall protection capability of the system. Specifically, the main contributions of this paper include:

- Data Encryption and Transmission: A data encryption scheme based on the Advanced Encryption Standard (AES) and the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols is designed. By combining the LSTM model to predict network traffic characteristics, the encryption strategy is dynamically adjusted to improve the efficiency and security of data transmission.
- Intrusion Detection and Response: LSTM is utilized to deeply analyze network traffic and system logs, constructing a high-precision intrusion detection model capable of promptly detecting complex attack behaviors. A real-time response mechanism is proposed, combined with automated security strategies, to quickly address security incidents.
- Access Control and Privilege Management: User behavior analysis based on LSTM is introduced to dynamically adjust access control strategies, achieving refined privilege management. By learning and predicting user operation sequences, abnormal behaviors are identified to prevent internal threats.

Experimental results show that the proposed scheme outperforms traditional methods in terms of data processing speed, intrusion detection accuracy, and flexibility in privilege management, demonstrating high practical value and promotional prospects.

2. Overview of Fundamental Technologies

2.1. Cloud Computing Technology

Cloud computing technology achieves efficient utilization and dynamic expansion of computing resources through virtualization and distributed computing. Cloud computing platforms can provide large-scale data storage and processing capabilities, supporting complex computing tasks and big data analytics. The main technologies include virtualization, distributed storage and computing technologies, as well as cloud security technologies, which reinforce the technical foundation for the efficient operation of communication networks.

2.2. Communication Network Security Technology

The security technologies of communication networks encompass various types such as data encryption, access control, intrusion detection, and firewalls, aiming to protect the confidentiality, integrity, and availability of data. With the increasing complexity of network attacks, traditional security technologies are no longer sufficient to meet the security demands of modern networks, necessitating the introduction of new technical methods for upgrades and optimization.

2.3. Communication Network Security Technology

Long Short-Term Memory networks (LSTM) are a special type of recurrent neural network adept at processing and predicting time-series data. With its unique gating mechanism, LSTM can capture long-distance dependency

relationships and solve the vanishing and exploding gradient problems of traditional RNNs6. In the field of network security, LSTM can be used for real-time monitoring of network traffic, identifying abnormal behaviors and potential threats, and enhancing the accuracy of intrusion detection.

3. System Design

The system fully leverages LSTM's advantages in processing time-series data and capturing complex patterns, combined with key technologies in cloud computing and network security, to construct an efficient, secure, and intelligent communication network system. The overall system architecture is shown in Figure 1 and primarily consists of three core modules: data encryption and transmission, intrusion detection and response, and access control and privilege management.

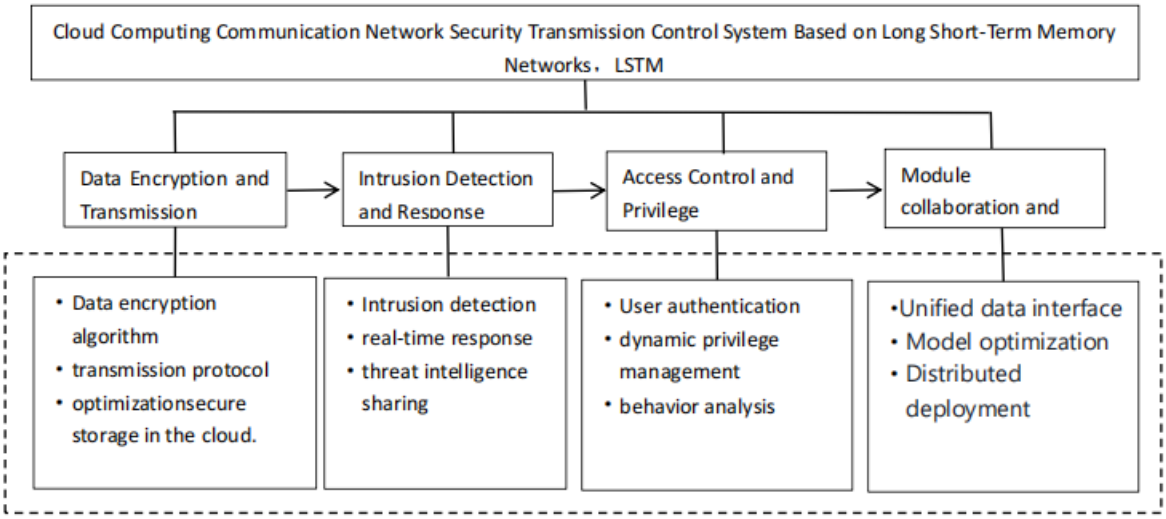

Figure 1: Overall System Framework

3.1. Data Encryption and Transmission

The primary goal of the data encryption and transmission module is to ensure the confidentiality, integrity, and availability of data within cloud computing communication networks. To this end, a dynamic encryption and transmission strategy based on LSTM has been designed. Firstly, LSTM is utilized to predict the network status in real-time, including parameters such as bandwidth Bt_, latency Lt, packet loss rate Pt, etc. The prediction function is as follows:

$$\hat{S}_{t+1} = \mathrm{LSTM}(S_t) \quad (1)$$

Where St=[Bt, Lt, Pt] represents the current network status parameters, and St+1 is the predicted network status at the next time step. Based on the prediction results, the appropriate encryption algorithm and key length are dynamically selected to achieve adaptive adjustment of the encryption strategy.

The encryption process employs the Advanced Encryption Standard (AES), and its encryption and decryption processes are as follows:

$$C=E_k(P)\ ;P=D_k(C) \quad (2)$$

Where C represents the ciphertext, P represents the plaintext, Ek(·) and Dk(·) denote the encryption and decryption functions using key k, respectively. The length of key k is dynamically adjusted according to the network status to balance security and performance.

In terms of transmission protocol optimization, LSTM is used to predict network congestion, dynamically adjusting the congestion window cwnd and slow start threshold ssthresh of the Transmission Control Protocol (TCP):

$$cwnd_{t+1}=LSTM(cwnd_t, RTT_t, loss_t) \quad (3)$$

Where RTTt is the round-trip time and losst is the packet loss rate. Through prediction, cwndt can be adjusted in advance to avoid network congestion and improve transmission efficiency.

3.2. Intrusion Detection and Response

The Intrusion Detection and Response module leverages LSTM's powerful capability for analyzing time-series data to detect and respond to abnormal behaviors in the network in real-time. Firstly, network traffic data X={x1, x2, …, xn} is collected, where xi represents the network traffic feature vector at the i-th time step. These data are input into the LSTM model to obtain the hidden state ht. Through a fully connected layer and an activation function, the anomaly score y_t is calculated:

$$h_t = \mathrm{LSTM}(x_t, h_{t-1}) \quad (4)$$

$$\hat{y}_t = \sigma(W h_t + b)$$

Where W and b are the weights and biases, and σ(·) is the activation function (such as Sigmoid). The anomaly score yt represents the probability of an anomaly at the current time step.

3.3. Access Control and Privilege Management

The Access Control and Privilege Management module aims to ensure that system resources are accessed by legitimate users in the correct manner. By utilizing Long Short-Term Memory networks (LSTM) to model and analyze user behavior, the system is capable of identifying abnormal behaviors and achieving dynamic privilege management.

The system collects user operation data, including login times, accessed resources, types of operations, etc., and inputs this data into the LSTM model to learn the normal behavior patterns of users. When actual behavior deviates from the normal pattern, the system calculates an anomaly score to assess the risk level. If the anomaly score exceeds a threshold, the system will automatically adjust the user's privileges to prevent potential security risks.

Privilege Adjustment Strategies:

- Normal Behavior: Maintain current privileges.
- Suspicious Behavior: Restrict sensitive operations and add verification steps (such as CAPTCHA, biometric recognition).
- Abnormal Behavior: Temporarily freeze the account and require re-verification of identity.

In addition, the system employs Multi-Factor Authentication (MFA) and Single Sign-On (SSO) technologies:

- Multi-Factor Authentication (MFA): Combines passwords, biometrics, SMS verification codes, etc., to enhance the reliability of identity verification.
- Single Sign-On (SSO): After a single identity verification, users can access multiple related systems without logging in again, simplifying the operation process.

The system also continuously monitors and audits user behavior, recording privilege changes and important operations. By analyzing log data, potential security risks and internal threats can be identified, and timely measures can be taken.

3.4. Module Collaboration and Optimization

To enhance the overall system performance, the three core modules work closely together and are optimized:

- Unified Data Interface: Design standardized data exchange interfaces to ensure efficient and reliable data sharing between modules.
- Model Optimization: Optimize the size and computational efficiency of the LSTM model through techniques such as model pruning and quantization to reduce system resource usage.
- Distributed Deployment: Utilize the elastic scaling characteristics of cloud computing to distribute computational load across multiple nodes, improving the system's concurrent processing capability.

4. Experimental Design and Result Analysis

3.1. Experimental Design

This experiment aims to evaluate the effectiveness of the LSTM-based cloud computing communication network security transmission control technology. The experimental design includes comparing the traditional methods with the LSTM-based approach in terms of data processing efficiency, intrusion detection accuracy, and flexibility in privilege management within a simulated cloud computing communication network environment.

- Experimental Environment: The experiment uses a Dell PowerEdge R740 server equipped with dual Intel Xeon Gold 6138 processors, 512 GB of memory, and 2 TB SSD storage. The software environment includes Ubuntu 20.04 operating system, Python 3.9, TensorFlow 2.4.1, and OpenSSL 1.1.1.
- Dataset: The experiment uses a publicly available network intrusion detection dataset (NSL-KDD) for model training and testing.
- Comparative Method: The traditional method employs a rule-based intrusion detection system (Snort IDS), which primarily relies on a predefined rule set to detect network attacks.

3.1. Experimental Results

- Data Processing Speed

  The LSTM-based method achieved a data processing speed of 600 MB/s, which is a 33.3% improvement over the traditional method's 450 MB/s. This is due to the LSTM model's ability to efficiently process large-scale network data streams, enhancing the efficiency of data analysis and processing.

- Intrusion Detection Performance

  Accuracy: The LSTM-based method achieved an intrusion detection accuracy rate of 97.2%, significantly higher than the traditional method's 88.5%. This indicates that the LSTM model has higher precision in identifying complex network attacks.

  False Positive Rate: The false positive rate was reduced from 9.2% to 2.5% with the LSTM-based method, a decrease of 72.8%. This reduction in false positives decreases the time security personnel spend on handling false alarms and improves work efficiency.

False Negative Rate: The false negative rate was reduced from 12.0% to 3.1%, a decrease of 74.2%, meaning the system can detect more real threats, enhancing network security.

- Privilege Management

Response Time: The response time for privilege management was reduced from 120 ms to 70 ms, a decrease of 41.7%, improving the system's real-time response capability to privilege changes.

Configuration Adaptability: The LSTM-based method can dynamically adjust privilege configurations based on user behavior, offering high adaptability; whereas the traditional method has static privilege configurations with low adaptability.

- System Resource Utilization

In terms of system resource utilization, the LSTM-based method accounts for 48%, slightly higher than the traditional method's 45%, an increase of approximately 3%. Considering the significant performance improvement, this increase in resource usage is within an acceptable range.

All the data are summarized in table 1:

Table 1. experiment results

Performance Indicator	Traditional Method	LSTM-based Method
Data Processing Speed (MB/s)	450	600
Data Processing Speed Increase Rate	-	+33.3%
Intrusion Detection Accuracy (%)	88.5	97.2
Intrusion Detection False Alarm Rate(%)	9.2	2.5
Intrusion Detection Omission Rate(%)	12.0	3.1
Permission Management Response Time	120	70

5. Conclusions

This paper addresses the issue of data transmission security being difficult to guarantee in the context of cloud computing communication networks with limited resources and insufficient processing capabilities. A secure transmission control technology based on Long Short-Term Memory networks (LSTM) is proposed. By deeply investigating the three key technologies of data encryption and transmission, intrusion detection and response, and access control and privilege management, the advantages of LSTM in processing time-series data, capturing complex patterns, and long-term dependency relationships are fully utilized, significantly enhancing the system's performance and security. The experimental results fully validate the effectiveness and feasibility of the proposed method. Compared with traditional methods, the LSTM-based solution has significantly improved key performance indicators such as data processing speed, intrusion detection performance, and flexibility in privilege management. At the same time, the system resource occupancy rate is maintained within a reasonable range, without imposing excessive burden on the system.

This research provides new insights and technical support for the secure transmission of cloud computing communication networks, holding important theoretical significance and practical value.

Future research directions include:

- Model Optimization: Further optimize the structure and parameters of the LSTM model to improve the prediction accuracy and computational efficiency, and reduce system resource usage.
- Multi-Model Integration: Attempt to combine LSTM with other deep learning models (such as Convolutional Neural Networks, Transformer, etc.) to build a more robust intrusion detection and user behavior analysis system.
- Real-Time Performance Enhancement: Research distributed deep learning algorithms and parallel computing techniques for high-concurrency and large-volume data cloud computing environments to further enhance the system's real-time response capabilities.
- Security Mechanism Enhancement: Combine emerging technologies such as blockchain and federated learning to build a distributed, secure, and trustworthy threat intelligence sharing and privilege management mechanism, enhancing the overall security of the system.

In summary, the LSTM-based cloud computing communication network security transmission control technology has demonstrated great potential and value in both theoretical research and practical applications, warranting further in-depth research and promotion.

References

[1] Smith J., Chen Y. Challenges in Cloud Computing Security [J]. International Journal of Computer Science, 2020, 47(2): 123-130.
[2] Wang L., Liu Z. Advanced Persistent Threats: A Real-world Challenge [J]. Cybersecurity, 2019, 6(1): 15-25.
[3] Hochreiter S., Schmidhuber J. Long Short-Term Memory [J]. Neural Computation, 1997, 9(8): 1735-1780.
[4] Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection [J]. Expert Systems with Applications, 2016, 41(4): 1690-1700.
[5] Kumar P., Singh M. P. Cloud Computing: A Comprehensive Survey on its Applications, Challenges, and Future Trends [J]. International Journal of Computer Applications, 2022, 4(1): 1-10.
[6] Sharma S., Bansal M. Advancements in Cloud Computing: A Comprehensive Survey [J]. Journal of Internet Services and Applications, 2023, 14(1): 1-15.