Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 4, pp. 2671–2678, DOI 10.12694/scpe.v25i4.2980

SECURE ENCRYPTED TRANSMISSION OF NETWORK DATA IN CLOUD COMPUTING TECHNOLOGY ENVIRONMENT

ZHIFENG MIAO *AND CHUNPING ZHAO†

Abstract. In order to solve the problem of communication data theft in conventional network communication data transmission methods and ensure the security of network communication data transmission, it is necessary to design new network communication data security transmission methods based on cloud computing technology, formulate network communication data security transmission agreements, construct a network communication data security transmission model based on cloud computing technology, and design a network communication data security transmission scheme, implement secure transmission of network communication data. The experimental results show that after using the designed network communication data secure transmission method, the amount of stolen communication data is less than that of conventional methods. This proves that the designed network communication data secure transmission method has high transmission security, good transmission effect, and reliability, and can be used as a reference for subsequent network communication data encryption transmission.

Key words: Cloud computing technology, Network data security, Encrypted transmission, Resource scheduling

1. Introduction. With the popularization of cloud computing applications, the massive amount of enterprise and user data in the cloud has enormous asset value, attracting a large number of hackers to attack and steal. Various security vulnerabilities bring potential security threats, and new network attack methods are constantly being introduced [1]. The security forms faced by cloud computing environments are becoming increasingly complex. Intelligent protection measures need to be utilized, using industrial intelligence as the engine, based on expert knowledge bases, deep learning, and big data analysis, to deeply analyze internal and external threat intelligence data, providing intelligent perception, intelligent warning, intelligent decision-making, and intelligent response for the computing environment, as shown in Figure 1. Enhance the intelligence level of cloud computing system security protection to more quickly respond to complex and changing cloud computing security threats [2,3]. Cloud technology categorizes and solves database information on Internet technology to ensure the data transmission efficiency of various multimedia communication connection functions, and can provide real-time feedback in all data information running system software. A partition planning method is proposed based on the application characteristics of cloud computing technology. It is necessary to obtain authorization from the customer to ensure the construction of a data information connection security exit from the physical server to the network server. In addition, the entire process of data transmission is logically operated according to the original operating procedures, and each step of the data analysis method has corresponding operability. During data transmission, customers can manually operate and issue instructions. So as to achieve real-time changes in data information transmission. Secondly, enhance the characteristics. In terms of data transmission methods, the security performance of software systems is an important guarantee for all data transmission processes. Finally, detailed features [4]. For traditional computer devices, frame loss and other situations often occur when transmitting data, resulting in incomplete transmission of data information. And by applying cloud computing technology, further authorization can be granted based on the instructions of data information, ensuring accurate communication between customer commands and the workflow processing system generated by data information, making the data management process more logical

*Department of information engineering, Guangxi Vocational College of Water Resources and Electric Power, Nanning, Guangxi, 730050, China
†Department of information engineering, Guangxi Vocational College of Water Resources and Electric Power, Nanning, Guangxi, 730050, China (Corresponding author, zcp79685615@163.com)

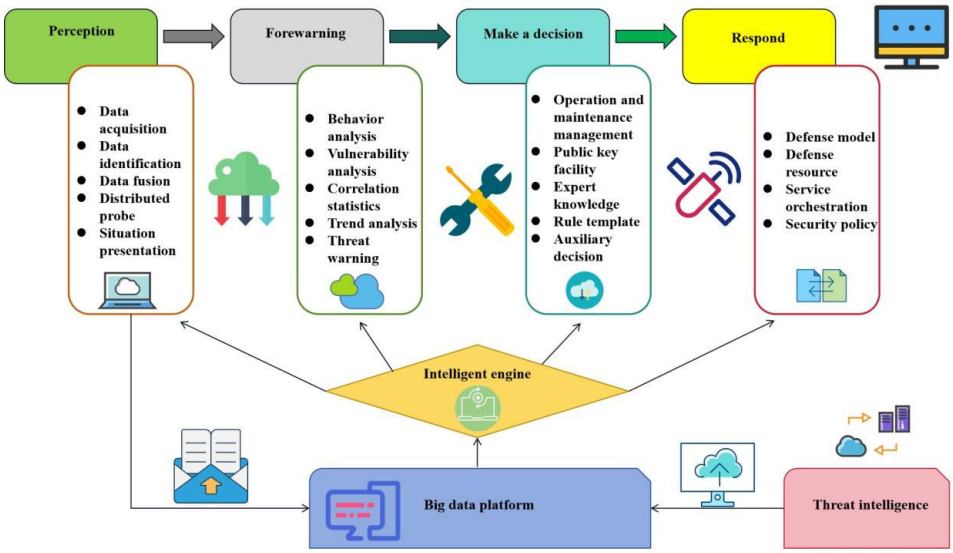

Fig. 1.1: Intelligent Cloud Security Defense

and less susceptible to external influences. Regarding cloud technology, the establishment of virtual environments involves synchronously projecting data and information onto physical servers to ensure precise connection between communication workflows and intelligent terminal workflows [5]. However, in the first stage, expanding the technological nature of open internet data transmission will have a corresponding impact on network information security. Therefore, it is necessary to strengthen the stability and basic construction of Internet technology, effectively avoiding security risks caused by data information loss or theft.

2. Methods.

2.1. Develop secure transmission protocols for network communication data. The conventional network communication data transmission methods are susceptible to internal and external transmission attacks. Therefore, the network communication data security transmission method designed by the author has formulated an effective network communication data security transmission protocol based on the transmission information of each node in the network communication [6,7]. The protocol designed by the author uses the principle of information bundling to resist unknown information transmission theft attacks. In the process of network communication data transmission, there are often multiple transmission nodes, and the distribution of these transmission nodes is also very irregular, so they are easily captured during the data transmission process. Therefore, the author used the deployment resource method to pre determine the location of node aggregation in the communication transmission network, and determined the attack model that poses a threat to data security transmission at this time. The designed transmission protocol was divided into two different parts. TESLA was used to set a node shared clock, and a protocol verification system was constructed. The sender can verify the legitimacy of the initial data packet based on the transmission delay of the signal. At this time, it can be assumed that the identity of the initial data packet m is id, and its transmission format is shown in Equation 2.1 [8].

$$m = id, T_{int}, K_0, T_0, N, I_0, d \geqslant Sign(m), cert \tag{2.1}$$

In Equation 2.1, d represents the transmission delay of the secret key, Sign (m) represents the signature, cert represents the certificate distributed by the center, and $T_{int}, K_0, T_0, N, I_0$ represents the transmission authentication parameters. After the transmission starts, adjacent nodes will immediately send verification IDs to generate the location information of each data secure transmission node. At this time, nodes can be re

planned and beacon grouping can be carried out, as shown in Equation 2.2 [9].

$$B_j = \{id, id_x, id_y, I_i, e_j, P(B_{j+1})\} \tag{2.2}$$

In Equation 2.2, id_x, id_y represents the location information of data transmission, I_t represents the transmission time interval, e_j represents the sleep group variable, $P(B_j + 1)$ represents the expected beacon group, and B_j represents the beacon group packet. The authentication delay within the network communication data secure transmission protocol developed by the author needs to be strictly calculated according to the hash function. Therefore, this delay is always in a changing state, consistent with the periodic relationship of network communication nodes. Therefore, based on the energy relationship of beacon changes, the attack location for the next communication data transmission can be predicted to achieve secure transmission. Research has shown that as time intervals increase, the secret keys within the established transmission protocol remain confidential and there are different beacon groups. In order to further improve the security of the protocol, the author conducted beacon location verification, first sending beacon packets by a neighboring node and then receiving them by the receiver. At this time, the security conditions of the protocol are shown in Eqaution 2.3.

$$[\frac{t_r - T_0}{T_{int}}] \leqslant I_t + d \tag{2.3}$$

In Equation 2.3, t_r represents the local receiving time, and T_{int} represents the actual receiving time. If the network communication data security transmission conditions at this time meet the above security conditions, it proves that the network communication data can be safely received, on the contrary, it proves that network communication data cannot be securely received and needs to be re grouped to verify the authenticity of the transmission in sequence until the transmission conditions meet the transmission conditions specified in the protocol [10]. This can improve the security of network communication data transmission and effectively reduce the number of information theft.

2.2. Building a secure transmission model for network communication data based on cloud computing technology . In the process of transmitting network communication data, it is necessary to continuously schedule communication data transmission resources and improve the reliability of network data transmission channels in real time. However, conventional network communication data security transmission methods do not have an effective resource scheduling security transmission model, which does not meet the reliability requirements of current network communication data transmission, therefore, the author has constructed an effective network communication data security transmission model based on cloud computing technology, further improving the effectiveness of network communication data transmission. The author combines the principles of virtual resource scheduling in cloud computing technology and designs a network communication data virtualization sampling model p, as shown in Equation 2.4.

$$p = x(t + q\delta t) - h(t + q\delta t) + \omega \tag{2.4}$$

In Equation 2.4, x represents the center reconstruction transmission data, t represents the reconstruction time, q represents the minimum dimension, δt represents the initial reconstruction time, h represents the cloud computing security function, and ω represents the weighting coefficient, this model can fully extract the transmission characteristics of network communication data, randomly allocate the features, and then input them into the cloud computing data resource analysis center for resource scheduling processing, at this point, the model can be used to complete network communication data sampling, and the sampled data can be stored in the cloud computing center resource library, which is then processed by the host system to complete the initial resource configuration. At this time, the cloud computing center resource library contains multiple limited datasets X, as shown in Equation 2.5 [11].

$$X = \{x_1, x_2, ..., x_n\} \tag{2.5}$$

In Equation 2.5, $x_1, x_2, ..., x_n$ represents the secure transmission data node, at this point, spatial action capture can be performed to obtain the initial features of the cloud computing center resource library and perform feature evolution. At this point, the evolution peak parameter needs to be calculated, and the calculation

formula Y is shown in Equation 2.6.

$$Y = X(T + K) \sum_{t=1}^{n} h_i (N - 1)^r \tag{2.6}$$

In Equation 2.6, T represents the action capture time, K represents the cloud computing feature vector, hi represents the security matching parameter, N represents the sampling time delay, and r represents the number of sampling times, at this point, using this peak can determine the fitting relationship between network communication data and resources, and design a secure transmission model C for cloud computing data centers, as shown in Equation 2.7 [12].

$$C = XYf^{-j2\pi fk} \tag{2.7}$$

In Equation 2.7, f represents the normalized frequency, j represents the real-time traffic of the cloud computing center, and k represents the secure transmission constant. This model can recombine and decompose resources based on the nonlinear characteristics of network communication data transmission, identify data center resource information in real time, and improve the stability of the internal environment of network communication transmission, due to the transferability of network communication data, the transmission method designed by the author assigns relevant correlation rules within it, and combines the frequency of data output for feature description. The descriptive formula Q is shown in Equation 2.8 [13].

$$Ra_n e^{-j2\pi f} \tag{2.8}$$

In Equation 2.8, R represents the transmission matching function, an represents the center resource scheduling information $e^{-j2\pi f}$, and represents the cloud computing transmission coefficient. Based on the feature description, data transmission security optimization can be advanced, that is, three-dimensional reconstruction of the cloud computing center can be performed to obtain the network data security transmission iteration formula as shown in Equation 2.9.

$$W = \theta_1(k) - R[\phi(k)] \tag{2.9}$$

In Equation 2.9, $\theta_1(k)$ represents the resource information after iteration, $\phi(k)$ representing secure filtering resources, this iterative formula can be used to complete the secure iteration of network communication data, conduct comprehensive spectrum analysis, and obtain the resource transmission optimization scheduling set as shown in Equation 2.10.

$$A(t) = E + W\sqrt{a}B \tag{2.10}$$

In Equation 2.10, E represents the output spectrum vector, W represents the data transmission initialization parameter, a represents the oscillation amplitude, and B represents the correlation coefficient [14]. Using the resource transmission optimization scheduling set obtained above can ensure the network communication data transmission environment and improve the security of network communication data transmission.

2.3. Design a secure transmission plan for network communication data . The final step in achieving secure transmission of network communication data is to design a secure transmission scheme for network communication data[15]. Combining the secure transmission requirements of network communication data and existing data security transmission frameworks, the communication cost of the secure transmission scheme can be formulated, which aims to achieve autonomous and secure transmission of data, perform data flow authentication and encryption, design relevant WIA-PA node packets, and improve the security of the network communication scheme. The scheme designed by the author includes the HMAC-SM3 authentication part, which can be combined with the SM4 encryption algorithm for transmission initialization processing, and then send node authentication and key design identification to relevant communication data transmission nodes. Each node can use this identification to complete message authentication, send request messages to the gateway, and then the gateway performs reasonable verification to complete bidirectional transmission

Table 3.1: Key length and transmission weight

Key length	Transmission weight	Key length	Transmission weight
RSA 16	0.17	ECC 16	0.18
RSA 32	0.46	ECC 32	0.54
RSA 64	0.14	ECC 64	0.43
RSA 128	0.1	ECC 128	0.02
RSA 256	0.09	ECC 256	0.02
RSA 512	0.06	ECC 512	0.04
RSA 1024	0.15	ECC 1024	0.06
RSA 2048	0.24	ECC 2048	0.15

and response. In order to increase the controllability of the design scheme and avoid irregular attacks during data transmission, the CCM algorithm was set up in the early stage of data transmission, and a random number factor was introduced to effectively avoid random attacks and achieve secure transmission of network communication data.

The secure transmission scheme for network communication data designed by the author can ensure the authenticity of transmitted messages, that is, during the data exchange process, it can effectively authenticate the identities of the transmitting party and the sending party, improve the reliability of data exchange, timely use relevant processing parameters for verification, and minimize the impact of external attacks on the secure transmission of network communication data [16]. Ensuring data security and integrity, attackers cannot maliciously tamper with verification information, steal transmission information, update transmission keys in a timely manner, avoid information interception, improve the anti forgery of network communication data transmission, and enhance transmission reliability.

3. Results and Analysis . In order to verify the transmission security of the cloud computing technology-based network communication data secure transmission method designed by the author, the author compared it with conventional network communication data secure transmission methods and conducted experiments as follows.

3.1. Experimental preparation. In order to ensure the effectiveness of the experiment, the WIA-PA principle was adopted to ensure the reliability of the experiment. In addition, the ONS network security experimental platform was selected as the communication data secure transmission experimental platform. The experimental platform selected Pentium Dual 1.86G CPU with 56G memory and used Windows XP SP3 as the operating system, due to the large amount of network communication data involved, the experimental platform also added a 120G experimental hard drive and used JavaJDK 1.6.0_ 24 virtual machines completed the experiment, and the experimental platform mainly uses TA-ONS and AM OSCM as security mechanisms, uses MAC functions to reduce computational difficulty and reduce the number of operations, in addition, the number of communication mechanism interactions in the experiment is not fixed and has a certain correlation with actual secure transmission operations and queries. At this time, the RSA network communication data secure transmission experiment docking key can be formulated in combination with the above security mechanism parameters. The length and transmission weight of the key selected by the author are shown in Table 3.1, Figure 3.1, 3.2 [17].

As shown in Table 3.1, the security level of keys with different lengths varies, and there are certain differences in the length and transmission weight of the above keys. This proves that the selected transmission key meets the experimental requirements and can effectively reduce network data communication transmission security detection errors, the author selected a total of 126465 network communication transmission data for experiments, all of which met the requirements of SM3 communication transmission password grouping. In order to better fit the actual data transmission situation, the experimental platform selected by the author combined with the CCM experimental mode to design a virtual attack module, it contains a rich attack library that can simulate actual data theft situations and complete network communication data security transmission experiments. At present, there is a high cost in conducting network communication data security transmission experiments,

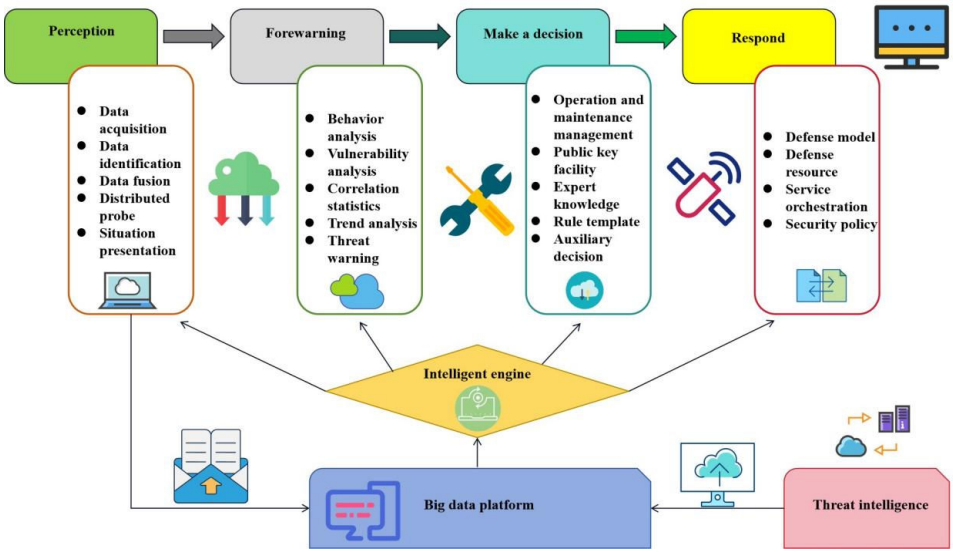

Fig. 3.1: Transmission Weight 1

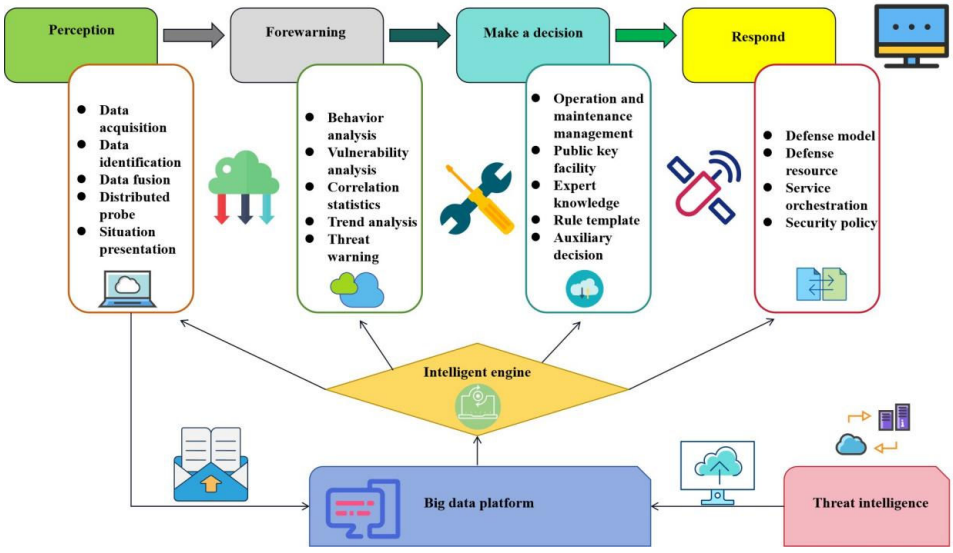

Fig. 3.2: Transmission Weight 2

which can easily generate high testing delays and is very detrimental to ensuring the accuracy of the experiments, therefore, before starting the experiment, it is necessary to first calculate the experimental delay to minimize its interference on the experiment. The average delay T calculation formula at this time is shown in Equation 3.1 [18].

$$T = \frac{\sum_{i=1}^{n} (t_0 - t_1)}{n} \tag{3.1}$$

In Equation 3.1, represents the number of cost calculations and represents the authentication time of each

Table 3.2: Experimental Results

Number of data transmitted	The number of stolen data in the network communication data security transmission method based on cloud computing technology designed by the author	The number of data stolen from conventional network communication data transmission methods
59	0	2
136	0	5
248	0	13
365	1	15
496	1	18
598	1	26
638	1	43
781	2	69
1052	3	86

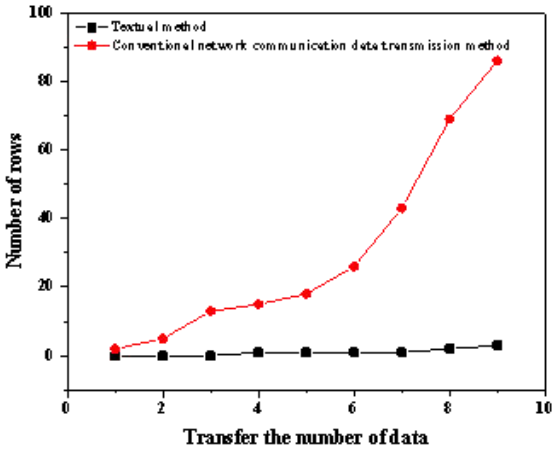

Fig. 3.3: Comparison of experimental results

communication transmission node. At this point, the calculated average delay can be excluded, providing reference for subsequent network communication data security transmission experiments.

3.2. Experimental Results . In the selected experimental platform, 126465 selected network communication transmission data were transmitted using the cloud computing technology based secure transmission method designed by the author and the conventional network communication data transmission method, in order to reduce experimental time, the author randomly selected several data points from 126465 for transmission experiments and detected the total number of data points stolen after transmission using two methods. The experimental results are shown in Tables 3.2 and figure 3.3 [19].

From Table 3.2 and Figure 3.3, it can be seen that the network communication data secure transmission method designed by the author based on cloud computing technology has fewer data stolen after transmission, while the conventional network communication data transmission method has more data stolen. This proves that the transmission effect of the designed network communication data secure transmission method is good and reliable [20].

4. Conclusion. The development of network technology has changed the transmission environment of wireless communication networks, and has also generated many security issues related to network communication data transmission. Research has shown that conventional network communication data transmission methods are affected by network environment fluctuations, and their transmitted data is easily stolen, which does not meet the current reliability requirements of network communication data transmission, therefore, the author designed a new network communication data secure transmission method based on cloud computing technology and conducted experiments. The results showed that the designed network communication data secure transmission method had fewer data stolen after transmission, proving its high transmission security and certain application value. It can be used as a reference for subsequent communication network security maintenance.

REFERENCES

[1] Kumar, N., & Samriya, J. (2022). Secure data validation and transmission in cloud and iot through ban logic and kp-abe. International Journal of Sensors, Wireless Communication and Control555(1), 12.
[2] Mandal, M.,& Dutta, R. (2021). Identity-based outsider anonymous cloud data outsourcing with simultaneous individual transmission for iot environment. Journal of information security and applications(Aug.), 456(76),60.
[3] Sarper, O., Ware, J. L., Yue, T., & Yangmin, D. (2023). Long-term monitoring and analysis of brood x cicada activity by distributed fiber optic sensing technology. Journal of Insect Science456(6), 6.
[4] Zhong, J., & Xiong, X. (2021). Data security storage method for power distribution internet of things in cyber-physical energy systems. Wireless Communications and Mobile Computing.23(68),80
[5] Whaiduzzaman, M., Farjana, N., Barros, A., Mahi, M. J. N., Satu, M. S., & Roy, S., et al. (2021). Hibaf: a data security scheme for fog computing. J. High Speed Networks, 27(21), 381-402.
[6] Xie, H., Zhang, Z., Zhang, Q., Wei, S., & Hu, C. (2021). Hbrss: providing high-secure data communication and manipulation in insecure cloud environments. Computer Communications, 174(5),890.
[7] Wu, X., Ren, F., Li, Y., Chen, Z., & Tao, X. (2021). Efficient authentication for internet of things devices in information management systems. Wireless Communications and Mobile Computing, 2021(57), 1-14.
[8] Wang, J. Z. B. (2021). Intelligent system for interactive online education based on cloud big data analytics. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 40(2),3211.
[9] Li, C., Liang, S. Y., Zhang, J., Wang, Q. E., & Luo, Y. (2022). Blockchain-based data trading in edge-cloud computing environment. Information Processing & Management: Libraries and Information Retrieval Systems and Communication Networks: An International Journal245(1), 59.
[10] Shanmuganathan, H., & Mahendran, A. (2021). Encryption based on cellular automata for wireless devices in iot environment. The international arab journal of information technology46(3), 18.
[11] Liazid, H., Lehsaini, M., & Liazid, A. (2023). Data transmission reduction using prediction and aggregation techniques in iot-based wireless sensor networks. Journal of Network and Computer Applications, 211(666), 103556-.
[12] Kaushik, S., & Gandhi, C. (2021). Fine grained decentralized access control with provable data transmission and user revocation in cloud. International Journal of Information Security and Privacy, 15(2), 29-52.
[13] Waqas, M., Tu, S., Wan, J., Mir, T., Alasmary, H., & Abbas, G. (2023). Defense scheme against advanced persistent threats in mobile fog computing security. Computer Networks, 221(35), 109519-.
[14] Sharma, M., & Sharma, M. K. (2021). Implementing hybrid security mechanism for cloud considering intrusion, sql injection and performance degradation. International Journal of Recent Technology and Engineering, 9(6), 142-150.
[15] Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. Computers & Electrical Engineering, 96(456), 107527-.
[16] Liu, Y. (2021). International logistics taxation data monitoring based on 5g network and cloud computing platform. Microprocessors and Microsystems, 82(54), 103826.
[17] Huang, W., Qi, Y., Zhang, W., Pang, L., & Fan, P. (2021). Remote data transmission of intelligent cloud robot based on google protobuf. Journal of Physics Conference Series, 1721(57), 012034.
[18] Gao, X. (2021). Role of 5g network technology and artificial intelligence for research and reform of english situational teaching in higher vocational colleges. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 40(2),56.
[19] Wang, Z., Qin, J., Xiang, X., Tan, Y., & Peng, J. (2023). A privacy-preserving cross-media retrieval on encrypted data in cloud computing. J. Inf. Secur. Appl., 73(24), 103440.
[20] Singh, R., & Pateriya, R. K. (2021). An efficient data security mechanism based on data groups in cloud computing environment. Solid State Technology, 64(2), 131-141.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Dec 6, 2023
Accepted: Dec 25, 2023