Design of Abnormal State Monitoring System for Multi-channel Transmission of Social Network Information

Jun Li[1,2(✉)], Hao-ding Murong[2], and Jun Xing[1]

[1] Shenzhen Academy of Inspection and Quarantine, Shenzhen 518045, China
zhengxiuli0831@aliyun.com
[2] Shenzhen Customs Information Center, Shenzhen 518045, China

Abstract. The security of social network communication is the most serious problem at present, because of the error of multiplex transmission, the risk of application security and the limited ability of most social network terminals. Based on this, the abnormal state monitoring system of social network information multiplex transmission process is optimized and designed. Through improving the system hardware and software functions, the accurate detection of multiplex transmission data is carried out. Finally, the experiment proves that the abnormal state monitoring system of social network information multiplex transmission process has higher monitoring accuracy and fully meets the research requirements.

Keywords: Social network · Information multiplexing · Abnormal state monitoring

1 Introduction

Social network is a kind of new technology energy, which is loved by people all over the world. With the improvement of information living standard, the challenge of information security is increasingly severe. Abnormal state monitoring technology of information multiplexing process has become the focus of attention. Communication security in social network environment is being studied by experts. The main problem is the security architecture of social network [1]. In the light of the information transmission process of social networks and the ability of the whole system to process information, the security framework is adjusted and constructed through three main ways: information collection, information processing and information transmission, the types of communication security threats under the social network environment are predicted, and an agreement on automatic reply by computers is signed [2]. In reference [3], aiming at the abnormal state monitoring of multi-sensors, the PCA model is established by using the principal component analysis adaptive reconstruction technology, and the multi-channel signals are detected by SPE statistics, thus realizing the fault detection and location. In reference [4], an abnormal state monitoring system is designed, which collects current and voltage information, and outputs it to the core chip operation module through the A/D

S. Liu and X. Ma (Eds.): ADHIP 2021, LNICST 416, pp. 403–415, 2022.
https://doi.org/10.1007/978-3-030-94551-0_32

conversion module for analysis, and constructs a system of multiplexing data collection and analysis.At present, there are few research methods on social network security monitoring, and the applied methods are all transmitted in one way, and the encryption intensity and authentication process are relatively small, so it has no security performance. Therefore, this paper puts forward the method of multiplex transmission, which has a great guarantee for communication security. By designing the overall hardware structure of the abnormal state monitoring system in the multiplex transmission process, the information acquisition module, data storage module and data transmission channel system are constructed. The hardware configuration and network port optimization were carried out to reduce the device drivers to achieve rapid response. Using the improved feature selection method to select abnormal traffic, the abnormal features of massive network traffic are extracted.

2 Multiplex Transmission Process Abnormal State Monitoring System

2.1 Hardware Structure of Multiplex Transmission Process Abnormal State Monitoring System

A monitoring and analyzing system for abnormal state of multiplex transmission process in social network is designed. This paper analyzes the main functions of the social network system and the possible abnormal conditions, designs the overall framework of the platform for monitoring the abnormal conditions of the multiplex transmission process, optimizes the hardware structure and interface of the system, and analyzes the overall technical scheme of the system, the system design specifications and the main functions of the system [5] The social network is a device module that integrates the collection of power consumption information, the monitoring of equipment operation status, intelligent control and communication, and is often installed at an important place where the collection of information and the monitoring data need to be collected from the distribution network, including places such as switches, ring network cabinets and

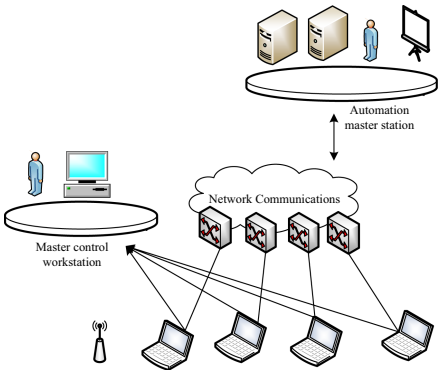

Fig. 1. Social network multiplex terminal architecture

feeder switches. According to the location of the distribution terminal, can be divided into terminal social network in the grid schematic diagram as shown in Fig. 1.

In order to meet the performance requirements of the network information security audit system, the device is developed based on CPU of X86 architecture, and the hardware platform NET-1711VD4N is adopted. The same hardware platform is used for the system device and the remote management device [6]. The NET-1711VD4N adopts the single board structure design of Intel 8456 V system chip, is a P4 gigabit network dedicated motherboard, and the motherboard integrates four Intel 825416 10M/100M/1000 Mbps gigabit network chip controllers, and directly leads out four RJ45 network interfaces and one serial interface on the board, which can be used to control the intranet, external network, ceasefire area, configuration network and control door, and there are also four network status indicator outputs on the trigger [7]. The Socket478 architecture supports 400/533 Delete Front-End Bus Pentium4/Celeron and Celeron D Series processors, storage aspects support DDR333/266, with VGA interfaces, PCI slots and CF card slots. The hardware parameters for this device are as follows (Table 1):

Table 1. List of hardware parameters

Processor	Intel pentium 4 2.8G
Memory	DDR 256M
CF card	256M
Hard disk	160G
Network interface	Four RJ45 network interfaces of Intel 82541
Serial port	1 COM interface
Supply voltage (V)	100–240 V AC, 6A, 50–60 Hz
Power supply (W)	520 W
Size	Standard 19 in. IU type, width × depth × height 430 mm × 355 mm × 44 mm
Weight	About 5 kg

Social network is the use of networking, information-based means to upgrade the traditional distribution terminal, its function is also more perfect. It is mainly capable of realizing the functions of monitoring the abnormal state of the multiplex transmission process, namely telemetry, telemetry, remote control and remote adjustment; realizing the short circuit fault detection function, realizing the fault recording and fault reporting, realizing the function of power quality monitoring, realizing the functions of intelligent charging, power management and remote communication, and realizing the distributed intelligent data exchange, etc. [8]. In the process of realizing the above functions, the key technologies include fault diagnosis and location technology, prejudgment and self-healing control technology, EMC adaptability under extreme conditions, compatibility and standardization of network communication protocol and feeder automation. In the hardware design, we can adopt two schemes: one is to use special embedded processor,

using X86 structure of Intel processor. However, different options have different impact on the project, and need to consider the development costs, development cycle and other aspects.

The overall framework of the monitoring platform for abnormal state of multiplex transmission process of social networks mainly includes three parts: one is the data acquisition module composed of sensors, the other is the data storage module composed of an integrated system with data storage and management functions, and the third is the data transmission channel system [9]. The principle of the system is as follows: Firstly, the data in remote and intelligent terminal are collected by sensors, then the data are classified by data storage module, and the analog signals are converted to digital signals. Finally, the data are transmitted through multi-channels. The Control Center is the integrated system responsible for the processing and management of all data [10]. The integrated system can achieve centralized control of the whole platform, and has high robustness and controllability. The overall hardware configuration of the system is shown below (Fig. 2):

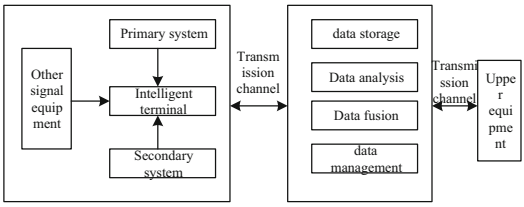

Fig. 2. System hardware configuration optimization

The hardware structure of automatic monitoring system for abnormal state of multiplex transmission process is composed of PC, switch, router and service. PC is the client of the system, also called the client. The main network monitors the data of the client through the access of the client. The monitoring system uses the C+ language, uses the ASP technology compilation dynamic monitoring code, monitors in the network each connection component the breakdown question.Switches exchange information between intranet and extranet, and exchange data between client and Internet database. To ensure the effectiveness of anomaly detection, the multiplex transmission network ports are optimized as follows (Fig. 3):

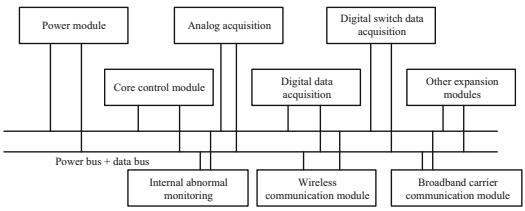

Fig. 3. Multiplex transport network port optimization

The system not only covers the normal functions, but also has the external interface to realize the docking with the external platform. The system needs login authentication, and can realize remote control. In the event of a state of emergency, an alarm signal will be issued and fault point information, images and data will be sent to the intelligent control terminal of the abnormal monitoring platform [11]. The platform can also provide historical data comparison and other functions to query and operate the corresponding control instructions. In addition, the system can also realize the analysis of the abnormal state inside the social network, that is, it is equipped with the monitoring module of internal abnormal.

System for network information monitoring applications, the key is to require the network function is perfect, compiling the kernel should be considered to meet this need. The key services provided by the standard kernel network subsystem are: data transmission, consistent device access interface, firewall and INET socket. These services are necessary for network applications, so they should be preserved when the kernel is clipped so that the system can provide complete network services. There are many network protocols and network hardware devices in the network subsystem. For the network security application, because it is used in the LAN environment to audit network information security, it needs the support of Ethernet communication protocol and Ethernet card device driver from the system kernel, and other network protocols and network hardware drivers can be simplified. Kernel configuration allows you to reduce kernel size by removing a large number of unused device drivers and modules from the kernel.

2.2 Optimization of Software Function of Multiplex Transmission Process Abnormal State Monitoring System

Aiming at the software function of abnormal state monitoring system in multiplex transmission process, the improved feature selection method is adopted. The aim of anomaly monitoring is to find the regular anomaly characteristics of network traffic based on the analysis of traffic data. Although the traditional analysis method is based on the general knowledge, it is only suitable for a small number of computing features. In the domain of network security, data mining will produce a large number of invalid data. Multiplex transmission process abnormal state monitoring system overall functions include packet capture, packet analysis and storage, query statistics and management 4 major modules [12]. The packet capture part includes initial filtering and capture. The data packet analysis section includes data packet analysis, keyword matching and storage; the query statistics section includes data query, data extraction analysis and data flow statistics; the management section includes the management of the keyword database and the management of account numbers of management personnel. The overall functional structure of the specific network information monitoring system is shown in the figure (Fig. 4).

Packet capture module can filter the original packet and catch the multiplex transmission model in the social network environment. The principle is that the information output path can be determined according to the stability of both sides of the communication network and the processing of the system terminal [13, 14]. Both the key of multiplexing and the process of multiplexing should follow this principle to select the

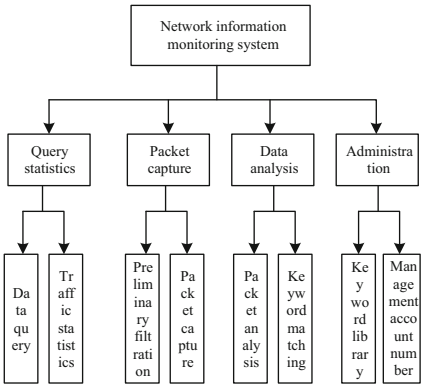

Fig. 4. System software module functional structure

path. The data packet capture module can filter and capture the original data packet. The module can get all the network adapters on the current monitoring system, set the preliminary filtering rules, and can capture the packets being transmitted in the current network. Data analysis module is the core module of the whole network information monitoring system [15]. Under this module, the administrator can analyze the content of the captured data, and use the keyword library to match the analyzed content, find out the information containing the keyword content, and store the captured and analyzed information for future reference. The management module can add, delete and modify the keywords in the keyword library, and encode the input keywords. Administrator account is divided into super administrator and ordinary administrator 2 permissions, super administrator can add, modify and delete the administrator account operation, account permissions can also be changed. Multiplex Traffic Monitoring Model in Social Network Environment is shown in Figure (Fig. 5).

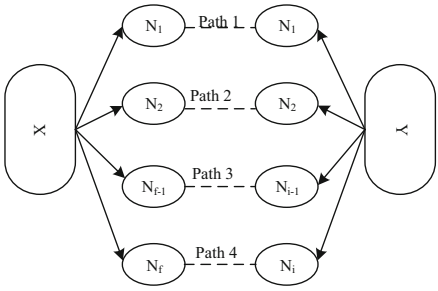

Fig. 5. Multiplex monitoring model in social network environment

As shown in the figure, x and y are the two terminals of communication. There are many paths of communication between these two terminals. N1,N2……Ni + 1 is the intermediate forwarding station on the path [16]. If x, y communicate by using one of the paths, the attacker can get all the information of x, y communication by attacking any

intermediate forwarding station on the path. If x, y communicate by using more than one path, the attacker must attack at least one site on each path to get part of the information of x, y communication. The system can be divided into three layers: application layer, data processing layer and data acquisition layer. The system hierarchy diagram is shown in the figure (Fig. 6).

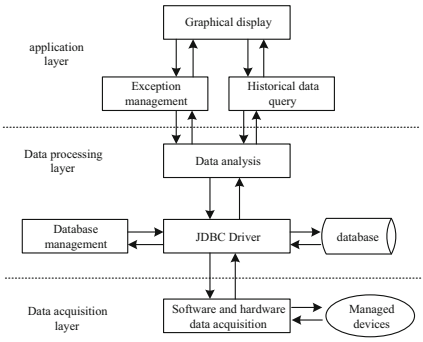

Fig. 6. Network state monitoring hierarchy

In the diagram, the data acquisition layer is responsible for the acquisition of the running state data of the equipment software and hardware (specific service running, CPU storage state, etc.). The client program deployed on the managed device acquires the running status of the host monitoring system and the status of the specific software through NETSNMP open source software and relevant Linux commands, and sends the collected device information to the monitoring server and stores the information in the database. In the data processing layer, the anomaly management module is responsible for analyzing the running state of the host computer monitoring system and the basic information of the equipment in the database. If any abnormality occurs, the abnormality information will be fed back to the application layer and alarm [17]. The application layer realizes the function of interacting with the user. This function will display the running state of the monitoring system and the running state of the managed devices to the user. If an exception occurs, the user is fed back the exception information. In addition, the user should set the operating state threshold of the managed device through the system management function of the application layer. Anomaly monitoring information collection is the necessary preparation for the distributed network, including information collection and processing. By analyzing the abnormal information, we can judge whether the client has accessed correctly and monitor the performance of the distributed network, so that the access information can be accurately monitored and the time consumed in network connection can be counted. During this period of time, the scope of network adaptation shall be predicted to obtain the information related to network security; the access mode of distributed network clients shall be selected to determine whether the information is abnormal. If the information is normal, it can be directly connected to the network client. Conversely, if the information is abnormal, it needs to be collected to provide data support for automatic monitoring database of subsequent access information.

2.3 Implementation of Abnormal State Monitoring in Multiplex Transmission Process

The general multiplex transmission process abnormal state monitoring system adopts the manager-agent model, and the manager-agent communicates with each other by standard protocol. The manager sends the order to the agent, the agent receives the order and collects the host status information from the controlled equipment and network equipment, and then feedback to the manager. The model diagram of network monitoring management is as follows (Fig. 7).

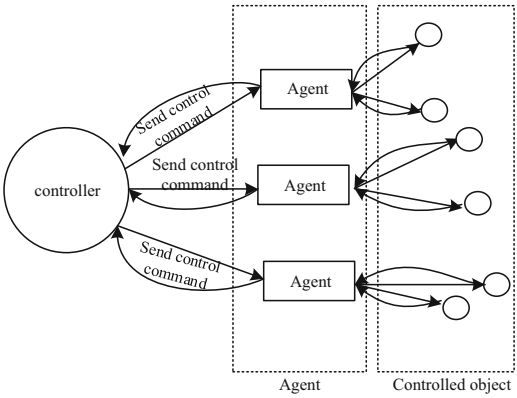

Fig. 7. Network monitoring management model

According to the definition of ISO, the management of abnormal state monitoring system for multiplex transmission process must include five major functions: anomaly management, configuration management, cost management, performance management, and security management. The collected information shall be pre-processed, and the relationship between information output and input components shall be analyzed according to the processing results. The specific calculation formula is as follows:

$$f(x_n, y_m) = \frac{\lambda(x_n, y_m)}{\sqrt{(x_n)(y_m)}} = \frac{\frac{1}{k}\sum_{m=1}^{k} x_{nm} y_m - \frac{1}{k^2}\left(\sum_{m=1}^{k} x_{nm}\right)\left(\sum_{m=1}^{k} y_m\right)}{\frac{1}{k}\sqrt{\sum_{m=1}^{k}(x_{nm} - x_n) \cdot \sum_{m=1}^{k}(y_m - \overline{y_m})^2}} \tag{1}$$

Where, $\lambda(x_n, y_m)$ represents the covariance between the input information x_n and the output information y_m; k represents the total amount of information. According to the formula, the input informationxn x_n and output information y_m can be normalized:

$$x' = \frac{x_n - x_{\min}}{x_{\max} - x_{\min}} \tag{2}$$

$$y' = \frac{y_n - y_{\min}}{y_{\max} - y_{\min}} \tag{3}$$

The formula is weighted to get the input data vector expression, as shown in the formula:

$$T = \left(f_1\left(x_1', y'\right)x', f_2\left(x_2', y'\right)x_{i-1}', \cdots f_1\left(x_j', y^+\right)x'\right)^{\mathrm{T}} \tag{4}$$

In the formula: T represents a period, from the formula can be obtained after weighting the input information vector. The monitoring system is divided into four modules: monitoring system state collection module, anomaly management module, database management module, data query module, the system module structure design as figure (Fig. 8).

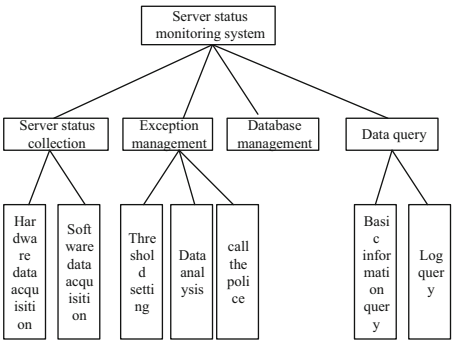

Fig. 8. System module structure optimization

The state acquisition module of abnormal state monitoring system in multiplex transmission process includes hardware data acquisition and software data acquisition. Anomaly management includes threshold setting, data analysis and alarm sub-functions. Data query includes basic information query and log query sub function. There are two kinds of data collected by monitoring system state acquisition module: fixed data and original data. Fixed data refers to data that does not need to be processed to determine whether it is abnormal, such as hardware data. Raw data refers to the data collected can not directly determine whether abnormal, need to be processed before judging, such as the number of secure access terminals online and site traffic data. Fixed data sent directly to the data analysis sub-function processing, if abnormal, then the alarm processing. The original data is stored in the temporary data table, after analysis and processing, the result data is obtained and sent to the data analysis sub-function. If there is an abnormality, alarm. Fixed data and original data are processed and the results are stored in the corresponding table in the database. The process of monitoring the abnormal state of the multiplexing process is shown in the figure (Fig. 9).

According to the schematic diagram of abnormal state monitoring system, the flow collection module, flow statistics module, anomaly monitoring module, alarm module and display module are designed. The flow collection module is mainly responsible for collecting all the flow data flowing through the collection point, and the flow statistics module is mainly responsible for splitting all captured network data packets and disassembling and storing them in the corresponding linked list structure. The abnormal

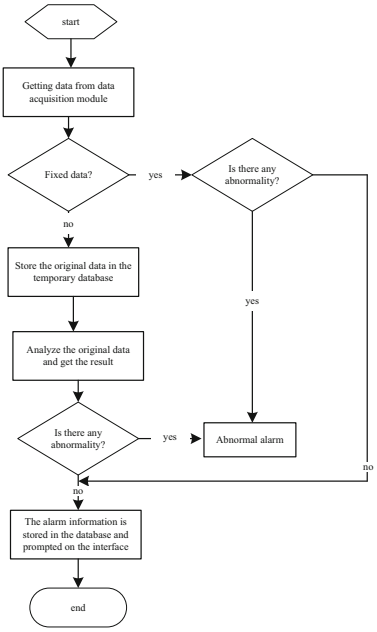

Fig. 9. Abnormal state monitoring process optimization

monitoring module is mainly responsible for monitoring the statistical results of abnormal data, the alarm module is mainly responsible for warning abnormal data, and the display module is mainly responsible for marking abnormal network information and displaying the monitoring results. By analyzing all the network traffic characteristics and selecting abnormal traffic by improved feature selection method, the abnormal traffic monitoring system of mobile communication network is designed.

3 Analysis of Experimental Results

In order to verify the operation effect of the abnormal state monitoring system in multiplex transmission process, the system equipment is connected to the internal LAN of the unit. The parameters of the tested equipment are shown in the table (Table 2).

The scale of the network on which the equipment under test is located is 20 hosts and the network segment is 192.168.18.0. The device is connected to the network via bypass mode, and the external Interact interface is connected to the hub, and the switch of the network shares the network data with the device under test through the hub. In this way, the device can monitor the Internet access information of all hosts in the network, and the Internet access information will be stored in the database of the system device. A host in the network, as the host of the management terminal, runs the management platform software under the Windows environment and connects to the database of the remote management terminal. In order to test the performance of monitoring technology, the traditional method is compared with this method, and 100 experiments are carried out to verify the information monitoring function of system equipment. Network packet

Table 2. Parameters of equipment under test

Processor	Intel Pentium 4 2.8G
Memory	DDR 256M
CF card	256M
Hard disk	160G
Network Interface	Gigabit network interface based on Intel 82541
Operating System	Embedded Linux based on 2.4.30 kernel

capture is the basis of the latter functions, and the results of protocol analysis and alarm are stored by database storage module to complete the data storage. The performance curve can be obtained as shown in the figure (Fig. 10).

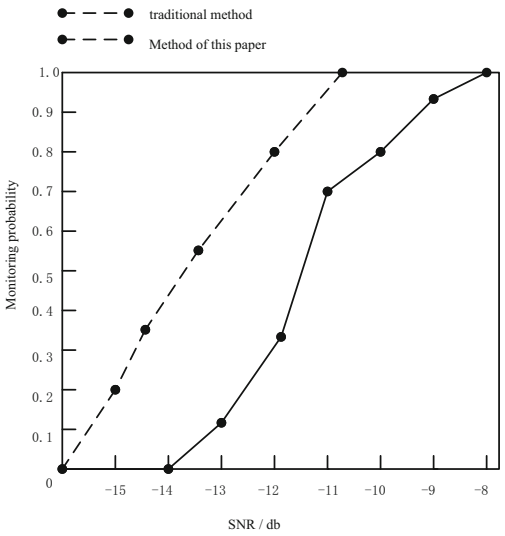

Fig. 10. Comparison of experimental results

It can be seen from the figure that, with the continuous improvement of the signal-to-noise ratio of the transmitted data, the monitoring probability of the traditional method is low and the response speed is slow, while the method in this paper can quickly reflect the abnormal data, and the monitoring accuracy of the abnormal data is high and the overall performance is good. Therefore, under the network delay, the monitoring system using the improved feature selection method is better than the traditional monitoring system to monitor the abnormal traffic of mobile communication network.

4 Conclusion and Outlook

At present, the level of social network technology is still in its infancy, the communication security design is not perfect, which brings great challenges to the communication security of social network. The security of communication system is the guarantee of every user's information, which has a direct impact on the effective operation of social network. Therefore, the design of communication security system should be strengthened. The design of secure communication system based on multiplex social network can make the system of computer terminal choose relatively simple decryption program and complex security performance, which greatly reduces the cost of network security prevention and control, and improves the processing capacity of terminal relatively. However, this paper has not been applied in the actual scene, and needs to analyze the needs of the actual environment in the future research, and further improve it to improve the perfection.

Fund Projects. National Key R&D Program of China (2018YFC0809105, 2018YFC0809100).

References

1. Olfat, M., Shokouhyar, S., Ahmadi, S., et al.: Organizational commitment and work-related implementation of enterprise social networks (ESNs): the mediating roles of employees organizational concern and prosocial values. Online Inf. Rev. **44**(6), 1223–1243 (2020)
2. Xu, S., Cao, J., Legg, P., et al.: Venue2Vec: an efficient embedding model for fine-grained user location prediction in geo-social networks. IEEE Syst. J. **14**(2), 1740–1751 (2020)
3. Chen, Y., Xu, P., Zhao, D., et al.: a fault detection and isolation algorithm for multi-sensor system. Comput. Sci. Appl. **9**(1), 8 (2019)
4. Jiang, S., Cheng, C., Wang, Q.: Design of voltage abnormal state detection system for power metering device. Comput. Meas. Control **28**(02), 44–47 (2020). No. 257
5. Shen, M., Zhang, J., Zhu, L., et al.: Secure SVM training over vertically-partitioned datasets using consortium blockchain for vehicular social networks. IEEE Trans. Veh. Technol. **69**(6), 5773–5783 (2019)
6. Salazar, J.J.R., Segovia-Vargas, M.J., Camacho-Miano, M.M.: Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Exp. Syst. Appl. **169**(10), 114470 (2020)
7. Jang, H., Hou, J.U.: Exposing digital image forgeries by detecting contextual abnormality using convolutional neural networks. Sensors **20**(8), 2262 (2020)
8. Yan, F., Huang, X., Yao, Y., et al.: Combining LSTM and DenseNet for automatic annotation and classification of chest x-ray images. IEEE Access **7**, 74181–74189 (2019)
9. Lu, S., Wei, X., Rao, B., et al.: LADRA: log-based abnormal task detection and root-cause analysis in big data processing with spark. Future Gener. Comput. Syst. **95**, 392–403 (2019)
10. Vijayan, A., Tahoori, M.B., Chakrabarty, K.: Runtime identification of hardware Trojans by feature analysis on gate-level unstructured data and anomaly detection. ACM Trans. Des. Autom. Electron. Syst. (TODAES) **25**(4), 1–23 (2020)
11. Thiyagarajan, K., Kodagoda, S., Ranasinghe, R., et al.: Robust sensor suite combined with predictive analytics enabled anomaly detection model for smart monitoring of concrete sewer pipe surface moisture conditions. IEEE Sens. J. **20**(15), 8232–8243 (2020)

12. Chen, T., Liu, X., Xia, B., et al.: Corrections to unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder. IEEE Access **8**(10), 117062 (2020)
13. Liu, S., Liu, D., Srivastava, G., Połap, D., Woźniak, M.: Overview and methods of correlation filter algorithms in object tracking. Complex Intell. Syst. **7**(4), 1895–1917 (2020). https://doi.org/10.1007/s40747-020-00161-4
14. Fu, W., Liu, S., Srivastava, G.: Optimization of big data scheduling in social networks. Entropy **21**(9), 902 (2019)
15. Liu, S., Bai, W., Zeng, N., et al.: A fast fractal based compression for MRI images. IEEE Access **7**, 62412–62420 (2019)