Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6691348, 13 pages
https://doi.org/10.1155/2021/6691348

Research Article

Nonintrusive Load Management Based on Distributed Edge and Secure Key Agreement

Jing Zhang[1], **Qi Liu**[1], **Lu Chen**[2], **Ye Tian**[3] and **Jun Wang**[1]

[1]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2]*Department of Information Security, Naval University of Engineering, Wuhan 430033, China*
[3]*China Information Communication Technologies Group Corporation (CICT), Wuhan 430205, China*

Correspondence should be addressed to Lu Chen; ieucl@163.com

Received 13 November 2020; Revised 30 December 2020; Accepted 9 January 2021; Published 29 January 2021

Academic Editor: Sotirios K. Goudos

With the advancement of national policies and the rise of Internet of things (IoT) technology, smart meters, smart home appliances, and other energy monitoring systems continue to appear, but due to the fixed application scenarios, it is difficult to apply to different equipment monitoring. At the same time, the limited computing resources of sensing devices make it difficult to guarantee the security in the transmission process. In order to help users better understand the energy consumption of different devices in different scenarios, we designed a nonintrusive load management based on distributed edge and secure key agreement, which uses narrowband Internet of things (NB-IoT) for transmission and uses edge devices to forward node data to provide real-time power monitoring for users. At the same time, we measured the changes of server power under different behaviors to prepare for further analysis of the relationship between server operating state and energy consumption.

1. Introduction

In the new era, the Internet has fundamentally changed social life, and people's demand for the Internet is also increasing. A new generation of network communication reform is emerging. The IoT can be regarded as the extension of the Internet, that is, the Internet extends its tentacles to the field of embedded computer systems and their supporting sensors, connecting all objects to the network through information sensing devices such as QR codes, radio frequency identification, and sensors, so as to transmit information, so as to form a worldwide interconnected mode to realize automatic identification, precise positioning, real-time tracking, and timely management [1]. At present, IoT technology has been widely used in agriculture, retail, logistics, storage, medical, energy, and other fields. Figure 1 shows the ecological map of the IoT [2]. Due to the impact of global warming, as well as the trend of diversified social energy use, global energy consumption continues to increase; energy conservation and emission reduction have become an important topic in the world [3]. NB-IoT technology as a high security, high-quality, low-power, and low-cost IoT technology has been applied to energy management field more and more [4]. The existing energy management pays more attention to providing users with equipment status monitoring, household energy consumption statistical analysis, differential electricity price information, and other services through the monitoring of electric energy information [5]. Energy management not only provides users with visual information statistics but also allows users to get more information and sense of participation, so as to encourage users to actively save energy and improve household energy utilization rate [6]. In addition, the statistics of relevant electric energy information can also provide the basis for the smart allocation and pricing of the State Grid and improve the security and reliability of power grid operation [7].

The energy management and control system based on IoT mainly uses wireless transmission mode. Different application scenarios involve different communication modes, including Bluetooth, ZigBee, WiFi, GSM/3G/4G cell, and HTTP. Due to the use scenarios, different sensing means must be used. However, due to the limited memory and computing power of a large number of sensing devices in the basic layer, it is difficult to achieve security defence, and the

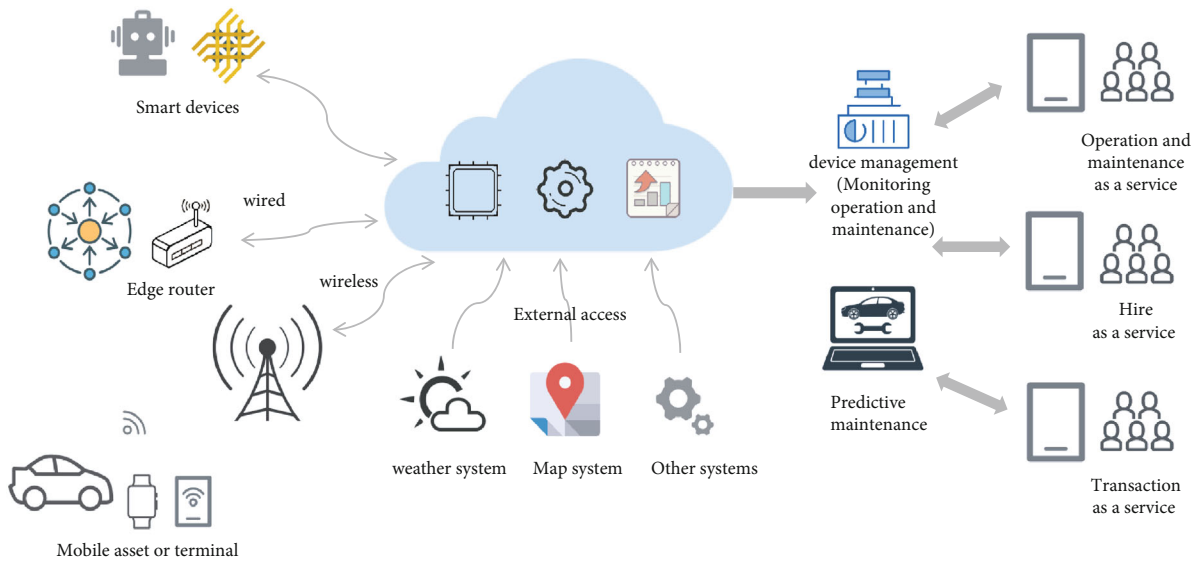


Figure 1: The ecosystem of IoT. The ecosystem includes equipment, platform, application, and business. After the platform is connected to the equipment, it can be used to build and manage IoT solutions for different industries.

data exposed in the public environment is very easy to steal and is easy to be interfered with [8]. Therefore, how to maintain the system data security and reliability is a problem we need to consider [9]. The IoT can be divided into sensing layer composed of sensors and other sensing devices, network layer responsible for data transmission, and application layer for visual display. Due to the variety of sensors in the sensing layer and the complexity of data format, it is difficult to completely unify, so the security control of network layer transmission is more complex [10]. Due to the limited resources of the sensing layer devices, only a small amount of computation can be performed. The deployment of classical encryption and authentication algorithms will not only consume equipment energy but also occupy resources and reduce the computing efficiency of devices. The existing security algorithms are mainly aimed at remote user authentication to prevent illegal users from gaining access to privacy data and controlling intelligent devices [11]. We designed a nonintrusive load management based on distributed edge and secure key agreement to provide real-time power monitoring for users. At the same time, we designed a lightweight encryption authentication algorithm between cloud edge devices to maintain the cloud server's receiving of sensor data and ensure the operation security of the energy management system.

After the second part introduces the related technology of the energy management system, we introduce the design of the secure energy management system in the third part. Then, the system performance is discussed in the fourth part. In the fifth part, we summarize our nonintrusive load management based on distributed edge and secure key agreement.

2. Related Work

The characteristics of IoT connecting a variety of sensors and sensing devices bring indispensable convenience to users' life and industrial production. In order to realize intelligent irrigation and save the cost of water resources, Rao et al. designed the adaptive control algorithm of a home irrigation system based on IoT. The water demand of plants was calculated by using the data of temperature and humidity sensor, and the water pump was controlled to irrigate plants in time to promote plant growth [12]. In the logistics and transportation industry, in order to ensure food safety, Gialelis and others designed a food traceability platform using low-cost IoT nodes to monitor the logistics chain from the "loading point" and continuously monitor the product storage environment [13]. In the health care industry, the IoT technology also has a variety of applications. Onasanya and Elshakankiri proposed a cancer medical system based on the IoT, which monitors the status of patients and environmental data through implanted and nonimplanted sensors, so as to provide timely and detailed information feedback for follow-up treatment, so as to help patients get better treatment and nursing [14]. In power, the IoT is mainly used in large-scale power grid and household small switch control. At present, the existing power Internet of things products mainly include smart meters and household appliances with wireless control module [15], while the equipment transmission mode mainly includes Bluetooth, WiFi, ZigBee, and NB-IoT. Adiono et al. proposed a Bluetooth-based smart home Android Software to help users control the power switch, lighting, curtain, door lock, and other devices in the home and monitor the temperature and humidity status in real time [16]. Madhu and Vyjayanthi designed a smart home controller using WiFi networking and controlled the corresponding equipment through the running software on the smart phone [17]. Jhang et al. designed a smart home control device based on ZigBee, and the sensor realized remote monitoring of door opening and closing and water leakage [18]. Due to its short communication distance and less connection number, Bluetooth technology is more suitable for the transmission of short

distance and less devices, such as wearable devices and small audio [19]. Because most of the intelligent products on the market, such as mobile phones, laptops, and TV boxes, have the function of accessing the Internet through WiFi, many products in the field of energy monitoring use WiFi as wireless communication mode. However, its configuration is complex, its security is low, and its power consumption is high, so it needs to be charged frequently. It is not applicable to sensor networks that need to transmit a small amount of data and contain a large number of nodes [20]. However, NB-IoT has the characteristics of low power consumption, large number of connections, wide transmission range, and low cost, so it has a great application prospect [21].

With the extensive use of NB-IoT technology, the user experience and product security need to be improved. For example, once the data of intelligent meter reading is stolen, it can be inferred whether the household is at home according to the data, which leads to the risk of property loss. At present, the existing IoT solutions not only face the problem of bandwidth delay but also face challenges in resource constraints and security. Because the extra security increases the cost of most manufacturers rather than the profit of equipment sales, many manufacturers give up providing security patches and firmware update services. Based on this, there are many high-risk vulnerabilities in the current Internet of things devices, especially in the default password, plaintext transmission key, and so on [22]. As shown in Figure 2, the IoT system is mainly composed of three layers, and each layer has different security vulnerabilities due to different technologies used [23]. Generally, the front-end devices of the sensing layer are limited by resources and cannot carry out complex computing tasks, so it is difficult to protect data security. Therefore, Batalla and Gonciarz designed a security algorithm deployed on edge devices [24]. Unde and Deepthi analyzed the rate distortion of compressive sensing (CS) using structural random matrix (SRM), injected artificial noise into the quantization CS measurement to resist CPA, and proposed a lightweight cryptography system based on compressed sensing for IoT, which reduced the computational burden and effectively reduced the complexity of CS encoder [25]. The energy management and control system based on the IoT may face active attacks and passive attacks, among which active attacks mainly include tampering and forgery, while passive attacks mainly include eavesdropping and deception, which are easy to cause a large amount of perceived information and user privacy information leakage [26]. Rehman and Gruhn developed a security algorithm to establish a sicher firewall between the software system and the smart home network as a filter to protect the system from virus attacks and unauthorized access [27]. Lyu et al. designed an antitracking mutual authentication scheme deployed on the ifttt server to achieve the anonymity of data transmission and ensure system security [28]. Naoui et al. proposed a user authentication scheme with additional security functions, which can resist multiple attacks such as internal attacks and simulation attacks and improve the security of user authentication [29].

We design a load management system with cloud edge architecture, which places the computing requirements of the sensing layer on the edge devices, which can effectively save the computing cost of the sensing layer and reduce the system delay. Meanwhile, we adopt a lightweight access control algorithm to ensure the communication security between the edge device and the cloud server and reduce the risk of perceived data and user information leakage. In addition, we use the load management system to test the power consumption of the server under different actions, so as to further analyze the relationship among the server power consumption with its running state.

3. The Proposed Secured Nonintrusive Load Management System

The nonintrusive secure load management system is designed to monitor, store, and process the power consumption of the detected equipment in real time. Compared with intrusive monitoring, the nonintrusive system is easy to install, so the system adopts nonintrusive design. Considering the limited storage and computing resources of monitoring nodes, the system adopts the cloud edge architecture design and uses edge devices to package and forward, which can reduce the computing cost of monitoring nodes. Meanwhile, compared with protecting the data being processed, it is usually much easier to protect the data transmitted through the network, and the system reliability is higher. At the same time, we use a lightweight access control algorithm to ensure the reliability of process transmission without affecting the transmission efficiency.

The system is mainly composed of monitoring nodes, edge devices, cloud servers, and clients. The overall design structure is shown in Figure 3. The system consists of three parts, including the perceptual layer composed of monitoring nodes, the transport layer consists of edge devices and cloud servers, and the application layer. Wireless sensor network adopts tree topology structure, with cloud server as the core, supplemented by multiple edge devices and monitoring nodes. Take the power management of the server room as an example. When the system works, the monitoring node regularly reads the power consumption data of the server and then sends messages to the edge device. The power data is packaged and encrypted by the edge device and transmitted to the cloud server through the wireless communication network. Users can view and manage network nodes through visual web pages and application programs in the application layer and access the power consumption data of corresponding servers to prepare for subsequent data analysis.

3.1. Nonintrusive Metering Module. The nonintrusive metering module is devoted to monitor the power consumption value of the monitored equipment at the current moment and forward the messages to the edge devices. The overall structure is shown in Figure 4. The core of the module is the STC15W404S chip, with power monitoring module, external memory, NB-IoT transmission module, and some peripheral circuits.

The main control unit adopts STC15W404AS single-chip microcomputer with an enhanced 8051 core produced by Hongjing Technology company to control data storage and

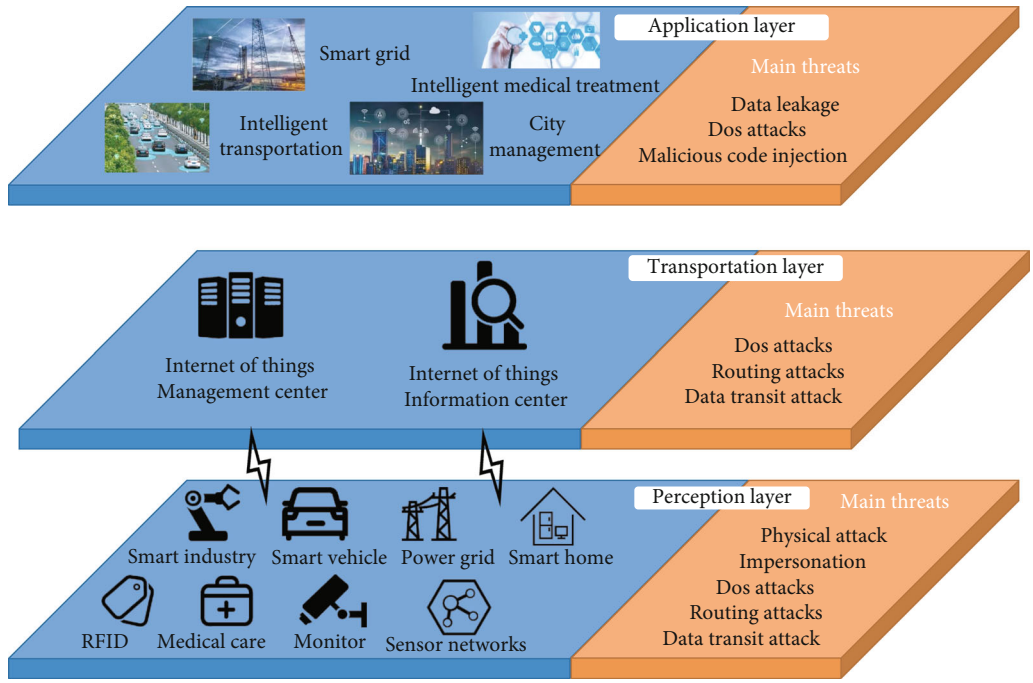


Figure 2: Threats in the IoT system model. Threats of perception layer: physical attack, impersonation, dos attacks, routing attacks, and data transit attack. Threats in the transport layer: dos attacks, routing attacks, and data transit attack. Threats of application layer: data leakage, dos attacks, and malicious code injection.

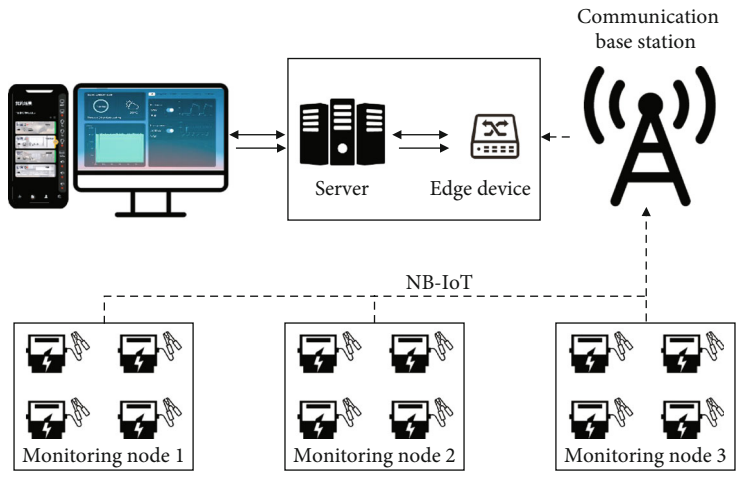
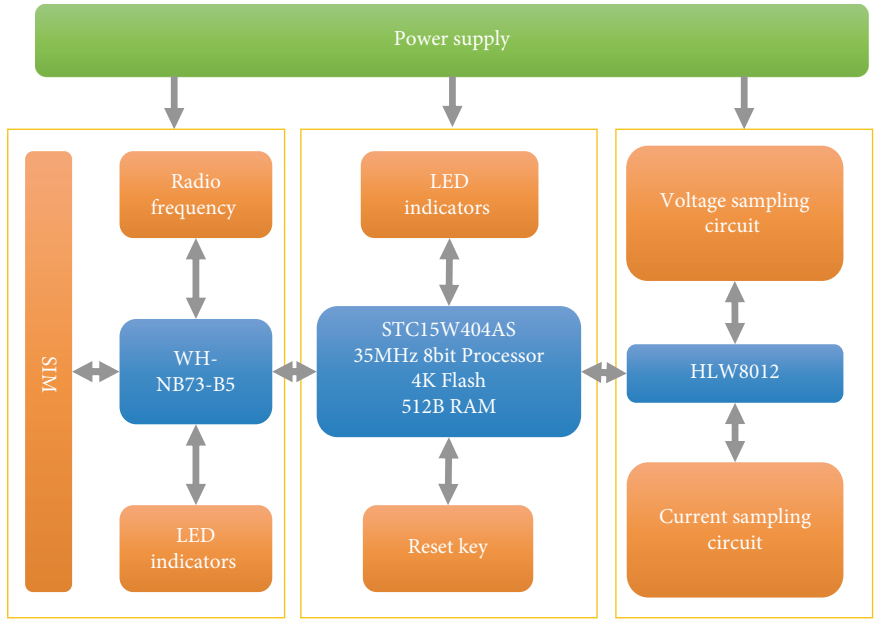
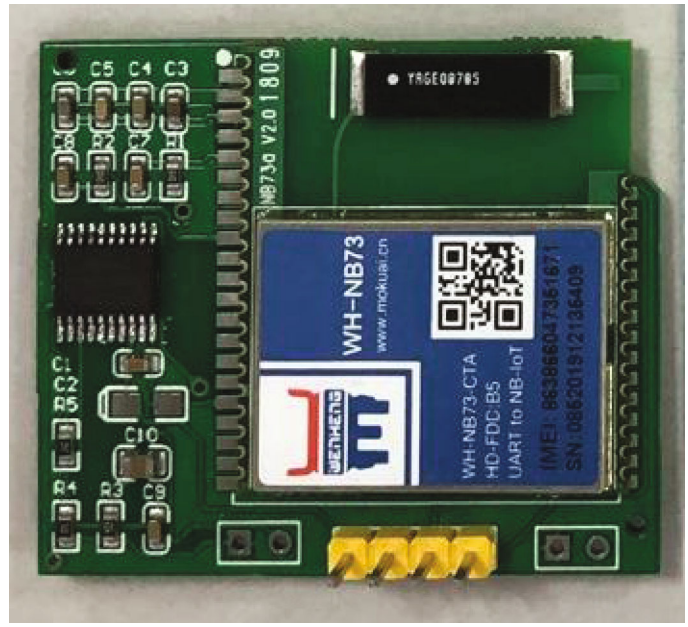


Figure 3: System architecture. The system includes monitoring node, edge device, cloud server, and client. The data is collected and transmitted to the edge device by the monitoring node and then packaged and sent to the cloud server for display at the client.

transmission. The chip not only has low power consumption and low price but also has an ultra-high-speed CPU core with the highest frequency of 35 MHz. The chip is driven by an internal crystal oscillator without an external crystal oscillator and reset. It contains a high-speed asynchronous serial interface (UART) and has rich pin functions. It can also be connected with 74HC595 to expand the general I/O port. The current and voltage sampling methods of the electric energy metering module are divided into transformer sampling and resistance sampling. The monitoring node adopts the isolation method to monitor the power consumption value. The 2 mA/2 mA current type voltage transformer cooperates with the resistance to convert the voltage signal into the current signal meeting the input conditions in the voltage acquisition circuit. In the current sampling circuit, the current transformer with the transformation ratio of 1000 : 1 combined with the sampling resistance converts the measured current into a low-voltage signal, which is also input into the power monitoring chip through the filter circuit. NB-IoT has the benefit of low power consumption, high security, large number of devices allowed to be connected, and communication distance of more than 10 km, which



(a)



(b)

Figure 4: Design of monitoring node circuit: (a) PCB and block diagram of monitoring node; (b) prototype of control module and sensor.

can be well applied to most IoT application scenarios. Therefore, the WH-NB73 module produced by Shanghai Wenheng Technology Co., Ltd. is adopted as the communication module. The power metering module and MCU are powered by 5 V DC voltage, and the NB-IoT communication module WH-NB73-B5 is powered by 3.3 V. The monitoring node adopts the AC-DC power module WA3-220S05A3 to convert 220 V AC to 5 V DC. At the same time, the node uses the AMS 117-3.3 DC voltage regulator chip of AMS company to realize the DC voltage stabilizing function from 5 V to 3.3 V.

3.2. Cloud-Edge-Node Architecture System. The most important work of the cloud server is to accept the electricity messages from users and store them into the persistent database after aggregation. The data analysis and mining process will analyze the data from users in the cloud, push the analysis results to the client application, and respond to the client data request. The data is measured and transmitted to the edge devices by the sensing layer monitoring nodes. The edge devices are packaged and encrypted and sent to the cloud server. Before the message is stored, the cloud server processes and analyses the data, and then, users can access the data of each node in real time.

3.2.1. Node and Edge Communication. TCP communication mode is used in the system sensing layer and network layer

communication. After the monitoring node is powered on, MCU and energy metering module are initialized. At the same time, the network is searched and added. The power consumption data and node address of the monitored equipment are read regularly and packaged into data packets and sent to edge devices. After receiving the message, the edge device judges whether it is the target node according to the address and Sn in the message. If so, it will process the message; otherwise, the message will be ignored. Considering reducing the energy consumption of the node, if there is no event to be handled, the monitoring node will automatically enter into the sleep state. The sleep includes the NB-IoT communication module sleep and the power monitoring module sleep. When the system finishes regularly and needs to read and send monitoring data, it wakes up the two sleep modules and only wakes up the communication module when processing other events. The main process of monitoring node program is shown in Algorithm 1.

```
Begin
Initialize the resource
Search for network, Read SSID and Password
While Successfully joined the network
    Start timing
    If have an event
        End timing
        Read power
        Send data
    Else if system sleep
Endwhile
End
```

Algorithm 1: Monitoring node algorithm.

The monitoring node communicates with the edge device in TCP mode, and the data packet is transmitted in JSON format, as shown in Table 1. For the data package uploaded by the monitoring node, the edge device first judges the packet type, then analyzes whether the node address matches with Sn, processes the monitoring data, and caches it. In a certain time interval, the received message is packaged and encrypted and transmitted to the cloud server to protect the security in the transmission process.

Table 1: Monitoring node upload data protocol.

Name	Data type	Mean
Type	char	The data type of this data
ID	int	Equipment number
SN	char	Serial number of the device
Power	float	Instantaneous electric power
Time	int	Current time

3.2.2. Cloud and Edge Communication. The program of the edge device is written in Java, and the NIO nonblocking communication is realized by using the Java Mina communication framework, which improves the communication performance of the edge device under the condition of high concurrency. After receiving the monitoring node, the edge device packs and encrypts the node and forwards it to the cloud server. After adding the corresponding node with the configuration function on the WeChat applet and application program, the user can access the corresponding node data, such as node number, real-time energy consumption, and historical statistics. The energy management system provides users with visual information statistics, which makes users more convenient and efficient to obtain equipment energy consumption and equipment operation status, timely handle abnormal operation equipment, save energy, and ensure safe operation of equipment. The logical architecture of device cloud and edge communication is shown in Figure 5.

The communication between cloud edges mainly includes three operations: connection, transmission, and disconnection. The specific process is as follows:

The connection function process is divided into four steps: (1) the edge device initiates the connection, and the API gateway establishes the connection and records the ID; (2) the API gateway notifies the edge device that the connection is established; (3) triggers the connection function to run and transfers the connection ID; (4) records the connection ID to the database and changes the device online status.

The transfer function process is divided into three steps: (1) the edge device initiates the message; (2) the API gateway transmits the message and triggers the transfer function; (3) the information in the message is extracted and stored in the database.

The process of disconnection function is divided into three parts: (1) the edge device initiates the disconnection request; (2) the API gateway triggers the disconnection function and transfers the connection ID; (3) queries the corresponding ID in the database and changes the online status.

3.2.3. Secure Communication Protocol. In the energy management system of IoT, data delay and reliability are the important judgment basis of the system. Pei et al. compared and analyzed the memory consumption and avalanche effect of six high-performance lightweight block ciphers and found that speck has the best comprehensive performance [30]. Therefore, based on the nonintrusion load management system, we use a speck algorithm to ensure the safety of message transmission. Here, we briefly introduce the speck algorithm.

The speck series algorithm is a kind of lightweight block cipher algorithm proposed by the national security agency of the United States. The algorithm adopts the deformed Feistel structure, and the round function is the ARX component. It is composed of mixed operations of modular integer addition, cyclic shift, and XOR operation. The main nonlinear operation is modular integer addition. Speck algorithm is more flexible than other algorithms. It supports 32, 24, 64, 96, and 128 bit blocks. The round function of the speck series algorithm is shown in Table 2.

Speck 2n/mn is used to represent speck algorithm with a packet length of 2n bit and key length of mn bit, where $n \in \{16, 24, 32, 48, 64\}$, $m \in \{2, 3, 4\}$. Remember the algorithm master key $K = (L_{m-2}, L_{m-3}, \cdots, L_0, K_1)$, where $K_0, L_0 \in$

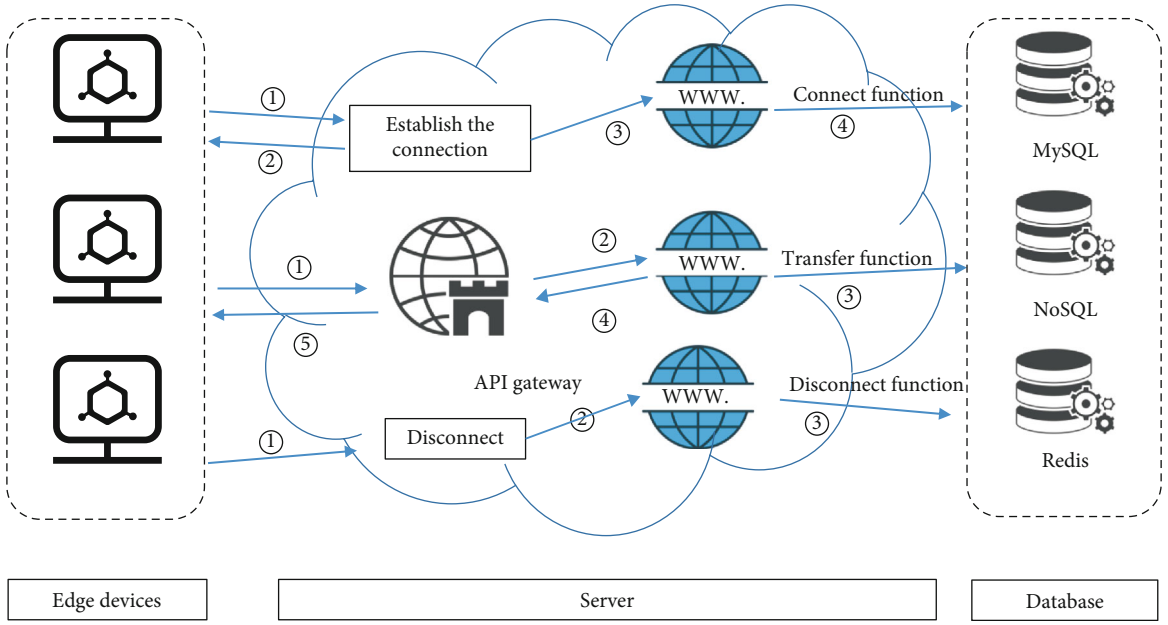


Figure 5: Logical process of cloud edge. Data is transferred and processed between edge devices, servers, and databases. The communication between cloud edges mainly includes three operations: connection, transmission, and disconnection.

Table 2: Speck series algorithm version.

Block size	Key size	Speck rounds	n	m
32	64	22	16	4
48	72	22	24	3
48	96	23	24	4
64	96	26	32	3
64	128	27	32	4
96	96	28	48	2
96	144	29	48	3
128	128	32	64	2
128	192	33	64	3
128	256	34	64	4

$\{0, 1\}^n$, and m is the number of key blocks of each algorithm. The key expansion algorithm is

$$\begin{cases} l_{i+m-1} = (K_i + l_i >>> \alpha) \oplus i, \\ K_{i+1} = (K_i <<< \beta) \oplus l_{i+m-1}. \end{cases} \quad (1)$$

Output N subkey $K_0, K_1, \cdots, K_{N-1}$.

4. Experiments and Performance Evaluation

4.1. Experiments. After the system design is completed, the actual deployment is tested. The system server is deployed on the Tencent cloud platform, and the API gateway is used for data interaction. Tencent cloud server with CPU of 2.3 GHz, 1 GB memory, and Ubuntu 16.04.1 LTS operating system is used to forward messages instead of edge devices. The monitoring nodes are deployed on the power lines of 5 different electrical equipment, connected to the power supply, waiting for the equipment networking, and 10 simulators are turned on at the same time. When the system works, bind the device name, device ID, and device location on the applet configuration interface, as shown in Figure 6. The main interface displays the current device name, current power, and total load power consumption in a list mode, and the historical data of the corresponding device can be viewed in the scene interface; also, we can configure it in the metainterface.

4.2. Feasibility Analysis. We use the monitoring equipment to measure the energy consumption changes of the server under different behaviors. The results show that the energy consumption waveform of the server is similar under the consent action, and the waveform diagram is shown in Figure 7. We divide the behavior into three categories: U-disk operation, network communication, and office software operation. Among them, U-disk operation includes U-disk plug-in and file transmission, network communication includes communication software start-up and shutdown, network transmission file, and office software operation includes office start-up and shutdown. When measuring the changes of server energy consumption, we record the performance changes of server CPU, memory, and network, which provide the basis for us to further finding the relationship among server power consumption with performance changes.

In (i) U-disk insertion operation and (ii) U-disk pull-out operation in Figure 7(a), the plug-in edge event characteristics are very obvious, and the peak energy consumption increases between 30 and 45 W, and the peak value of pulling out the U-disk is generally lower than that of inserting the U-disk. In the operation of transferring files to a USB flash disk, as shown in Figure 7(b), power consumption increases during transmission, but the fluctuation law is not obvious. As shown in Figure 7(c), QQ software operation (i) on and (ii)

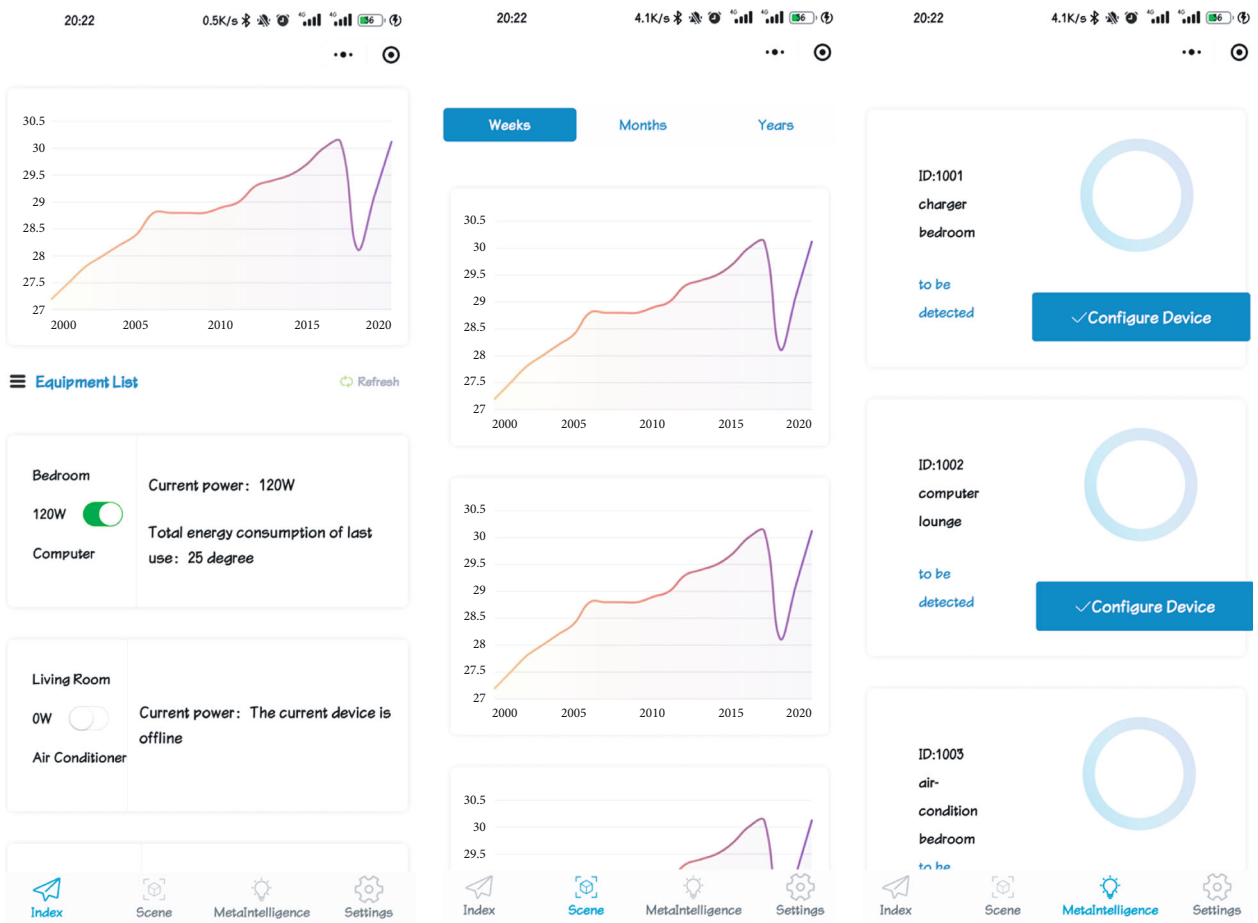
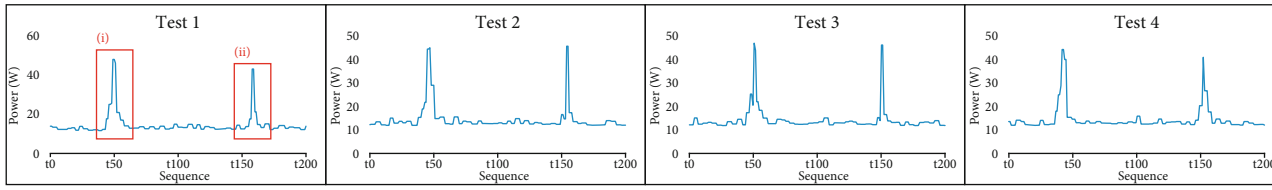


Figure 6: Main interface of the applet: (a) main interface; (b) scene interface; (c) metaintelligence interface.

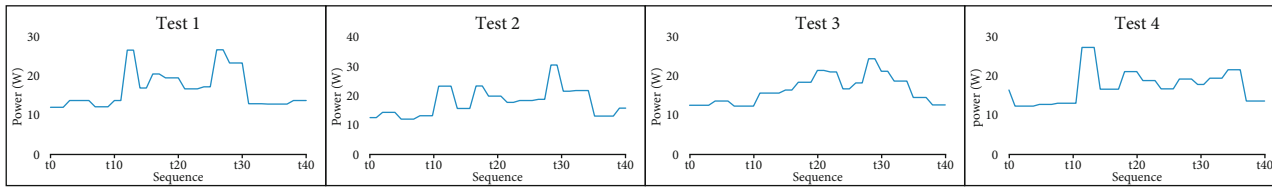
off edge event characteristics are obvious, and the waveform changes are regular. The opening event generally lasts 50~60 ms and tends to be flat after three main peak fluctuations, and the first peak fluctuates the most and then shows a decreasing trend. The closure events generally last for 25~40 ms and tend to be flat after 2~3 main peak fluctuations, and the first peak fluctuation is the smallest and then presents an increasing trend. In the process of QQ transmission, as shown in Figure 7(d), there is no obvious energy consumption fluctuation. As shown in Figure 7(e), WeChat software operation (i) on and (ii) off edge event characteristics are obvious, and the waveform changes are regular. The opening event generally lasts 15~20 ms and tends to be flat after 1~2 main peak fluctuations, and the former fluctuation is small. The closing event usually lasts 15~20 ms, and the peak fluctuation is less than the maximum fluctuation of the opening operation. In order to use WeChat software to transfer files, as shown in Figure 7(f), the energy consumption increases significantly and fluctuates regularly. At the beginning, there will be a small fluctuation, and then, the energy consumption will last for a period of 40~60 W. As shown in Figure 7(g), for PDF file (i) open and (ii) close operation, edge event characteristics are obvious and regular. In conclusion, it is feasible to infer the current event based on the change of server energy consumption. Then, we further measure the relationship between the server energy consumption change and the performance changes of CPU, memory, and network under specific events.

As shown in Figure 8, there is a correlation between the change of server energy consumption and the change of CPU, memory, network, and other performance under specific events. The correlation between CPU utilization and energy consumption is the most significant, which is the main factor affecting the change of energy consumption. In the first column, the mutation of the energy consumption curve is very similar to the mutation of CPU utilization, and the change of memory is similar. In the second column, the curve of CPU is closely related to the curve of energy consumption. The third column of QQ open and close operation and the fourth column of WeChat transfer files have the same rules. At the same time, we found that the change of the network operating with chat software is also full of rules, and different software has its own characteristics. Therefore, it is feasible to infer the current server performance change or even the current running software according to the server energy consumption change. In the next work, we will further explore the relationship between them and energy consumption.

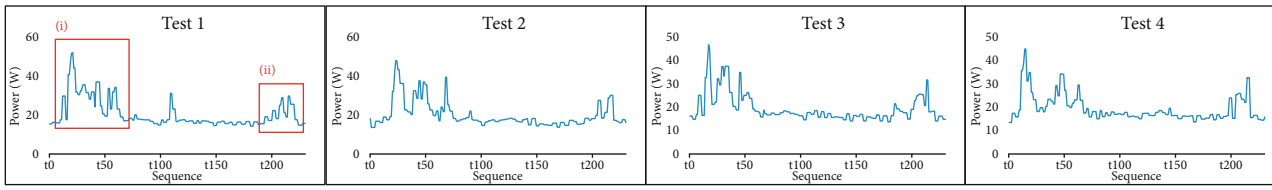
4.3. Performance Analysis. In this paper, a nonintrusive load management based on distributed edge and secure key



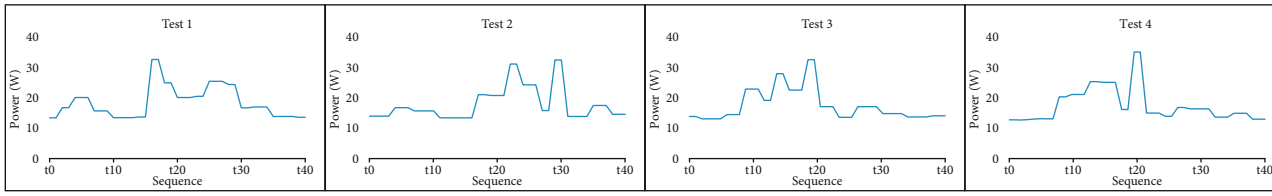
(a)



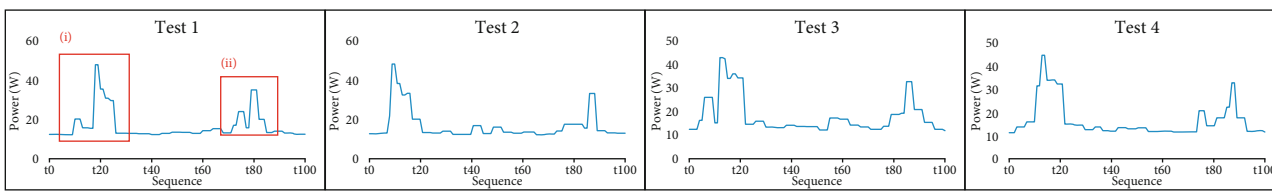
(b)



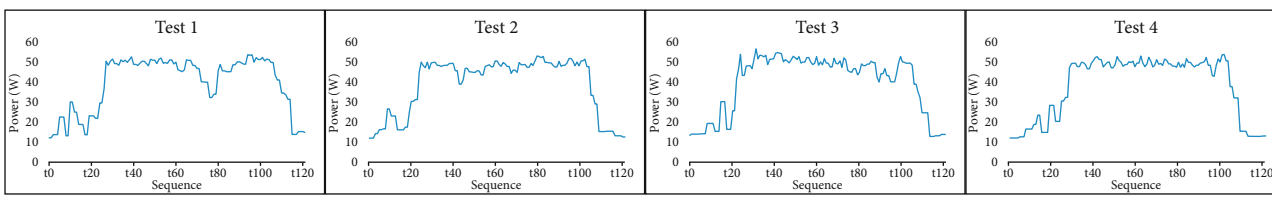
(c)



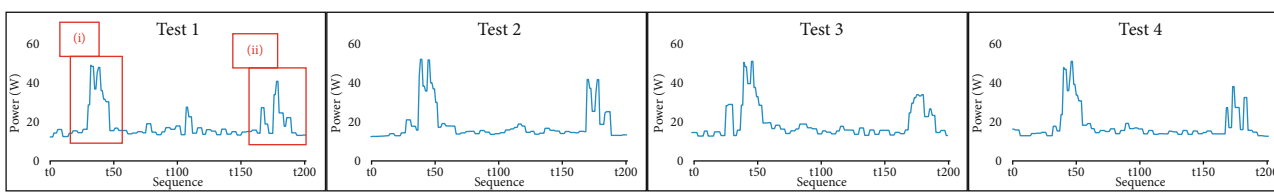
(d)



(e)



(f)



(g)

Figure 7: Energy consumption waveform: (a) U-disk plug and pull; (b) disk transfer files; (c) open and close QQ software; (d) use QQ to transfer files; (e) open and close WeChat software; (f) use WeChat to transfer files; (g) open and close PDF files.

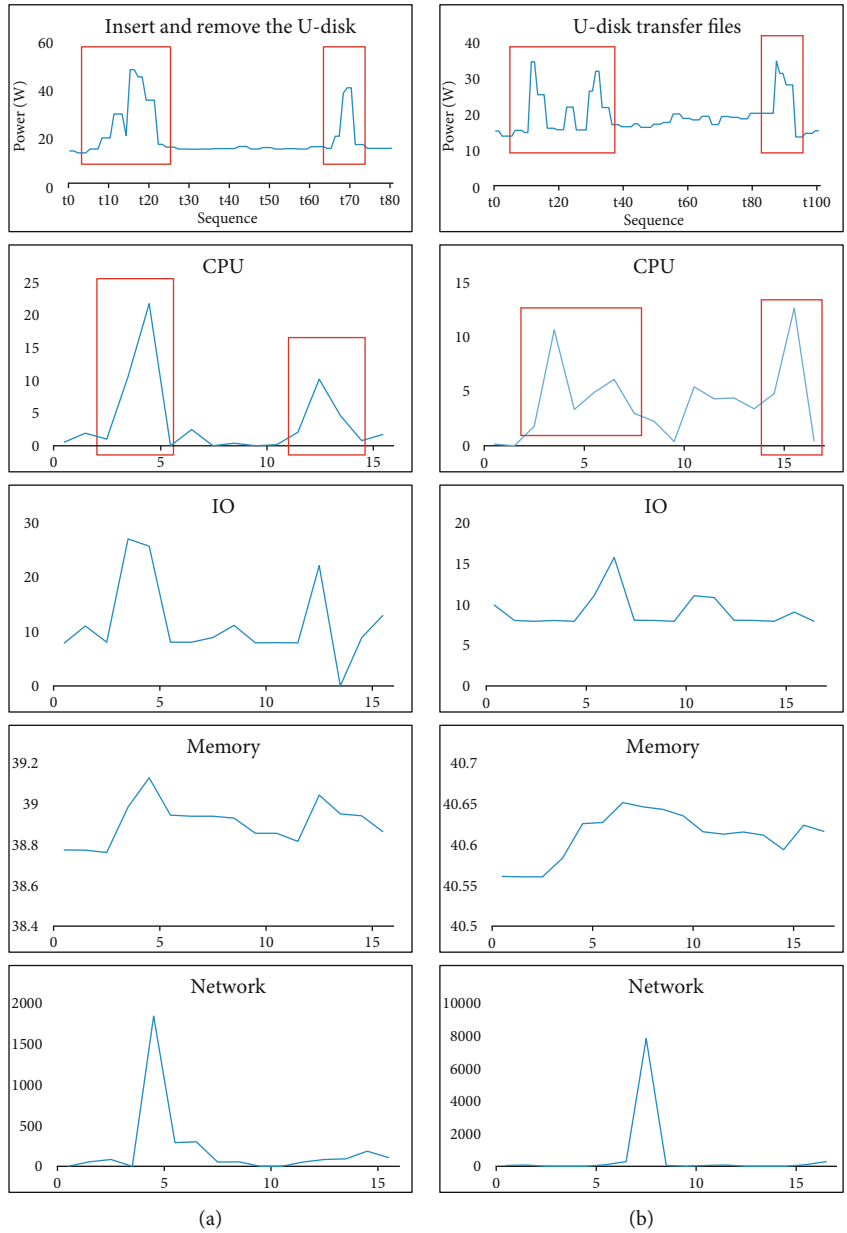


Figure 8: Continued.

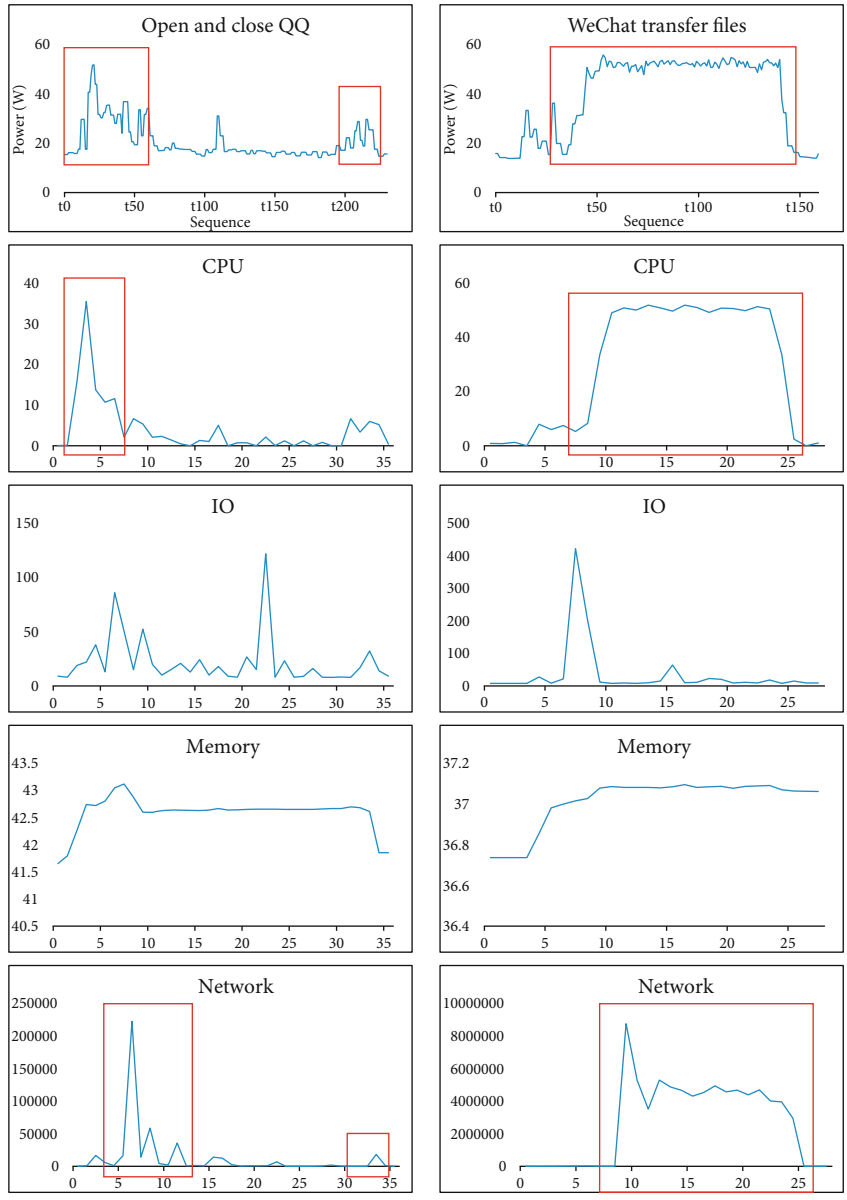


Figure 8: Energy consumption and the relationship among CPU, IO, memory, and network. The first column is insert and remove the U-disk, the second column is U-disk transfer file, the third column is open and close QQ, and the fourth column is WeChat transmission file.

agreement is designed. Compared with other energy consumption monitoring systems, the system uses NB-IoT as communication module, which has longer communication distance, better signal strength, and higher security. The non-intrusive calliper monitoring design can well meet the application requirements of various occasions and is easy to install. Meanwhile, the architecture design of cloud edge reduces the computing resources of monitoring nodes, which is convenient for deploying higher security encryption algorithm to ensure system security. Speck lightweight encryption algorithm used in the system takes less computing resources, can resist various types of attacks, and has a good security margin.

In our experiment, we run the monitor node simulator on a personal computer (HP with an inter (R) core (TM) i7-7700hq @ 2.80 GHz 2.81 GHz processor, 16 GB main memory, and window 10 operating system) and an app on a personal mobile device (Huawei nova5 pro with quad-core 2.6 g processor, 8 GB memory, and Android 10 operating system) as a user. We have done this 4000 times to get the average run time.

Table 3: Data transfer time (MS).

Operations	T_1	T_2	T_3	T_4	T_5	T_{Avg}
User times	29.32	30.15	34.31	32.80	34.27	34.97

We test the time delay between the edge device and the cloud platform when the system is running. As shown in Table 3, we calculate the transmission delay and the

total average delay of five groups of devices. The minimum delay is 10 ms, the maximum delay is 193 ms, and the delay is concentrated between 25 and 35 ms to meet the transmission requirements, which is affected by the network changes.

5. Conclusions

Power data acquisition technology based on NB-IoT technology will be the main technical direction of 5 g technology applied in smart grid in the future, based on the characteristics of low power consumption and wide transmission range of NB-IoT; this paper designs a nonintrusive load management based on distributed edge and secure key agreement, which uses edge devices to encrypt and forward node data and accesses control algorithm to ensure system data security. In addition, this paper measured the server power change under different behaviors, and the results show that the waveform of server power change is similar under fixed behavior. Next, we plan to further analyze the relationship between energy consumption and server performance change by measuring the server CPU, memory, GPU, network, and energy consumption change data at the same time, so as to infer the abnormal state of the server by using the energy consumption change to provide managers with more detailed early warning.

Data Availability

Our processed data involve two parts. One is from 3rd party, i.e., REDD, which can be downloaded via this link: http://redd.csail.mit.edu/. The other data were generated in our own lab for testing and evaluating purposes by using smart sockets.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

Jing Zhang and Qi Liu contributed equally to this work.

Acknowledgments

This work has received funding from the National Natural Science Foundation of China (Nos. 41911530242 and 41975142), 5150 Spring Specialists (05492018012 and 05762018039), Major Program of the National Social Science Fund of China (Grant No. 17ZDA092), 333 High-Level Talent Cultivation Project of Jiangsu Province (BRA2018332), Royal Society of Edinburgh, UK, and China Natural Science Foundation Council (RSE Reference: 62967_Liu_2018_2) under their Joint International Projects funding scheme, National Natural Science Foundation of China (Grant No. 41875184), Innovation Team of "Six Talent Peaks" in Jiangsu Province (Grant No. TD-XYDXX-004), and Basic Research Programs (Natural Science Foundation) of Jiangsu Province (BK20191398 and BK20180794).

References

[1] K. Chopra, K. Gupta, and A. Lambora, "Future internet: the internet of things-a literature review," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 135–139, Faridabad, 2019.

[2] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta, and A. Bhatnagar, "CRAIoT: concept, review and application(s) of IoT," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–4, Ghaziabad, India, 2019.

[3] S. S. Hosseini, K. Agbossou, S. Kelouwani, and A. Cardenas, "Non-intrusive load monitoring through home energy management systems: a comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 79, pp. 1266–1274, 2017.

[4] Z. Qin, F. Y. Li, G. Y. Li, J. A. Mccann, and Q. Ni, "Low-power wide-area networks for sustainable IoT," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 140–145, 2019.

[5] O. Elma and U. S. Selamoğullar, "A survey of a residential load profile for demand side management systems," in *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 85–89, Oshawa, ON, Canada, 2017.

[6] L. Liu, Y. Liu, L. Wang, A. Zomaya, and S. Hu, "Economical and balanced energy usage in the smart home infrastructure: a tutorial and new results," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 4, pp. 556–570, 2015.

[7] G. Gaur, N. Mehta, R. Khanna, and S. Kaur, "Demand side management in a smart grid environment," in *2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, pp. 227–231, Singapore, Singapore, 2017.

[8] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 887–890, Palladam, India, 2017.

[9] Y. Chen, X. Wang, Y. Yang, and H. Li, "Location-aware Wi-Fi authentication scheme using smart contract," *Sensors*, vol. 20, no. 4, pp. 1062–1083, 2020.

[10] L. Li, F. Zhu, H. Sun, Y. Hu, Y. Yang, and D. Jin, "Multi-source information fusion and deep-learning-based characteristics measurement for exploring the effects of peer engagement on stock price synchronicity," *Information Fusion*, vol. 69, pp. 1–21, 2021.

[11] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.

[12] R. Y. Rao, J. J. Koola, N. D. Mehta, and A. M. Haque, "Design and implementation of adaptive control algorithm for IoT based domestic irrigation system," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Kanpur, India, 2019.

[13] J. Gialelis, G. Theodorou, and C. Paparizos, "A low-cost internet of things (IoT) node to support traceability: logistics use case," in *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good*, pp. 72–77, Valencia, 2019.

[14] A. Onasanya and M. Elshakankiri, "Smart integrated IoT healthcare system for cancer care," *Wireless Networks*, vol. 2019, pp. 1–16, 2019.

[15] H. Ikezawa and M. Imafuku, "Convenience survey of IoT house equipment for a smart life," in *2020 IEEE 2nd Global*

Conference on Life Sciences and Technologies (LifeTech), pp. 290–294, Kyoto, Japan, 2020.

[16] T. Adiono, S. F. Anindya, S. Fuada, K. Afifah, and I. G. Purwanda, "Efficient android software development using MIT app inventor 2 for Bluetooth-based smart home," *Wireless Personal Communications*, vol. 105, no. 1, pp. 233–256, 2019.

[17] G. M. Madhu and C. Vyjayanthi, "Implementation of cost effective smart home controller with Android application using node MCU and internet of things (IOT)," in *2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE)*, pp. 1–5, Shillong, India, 2018.

[18] W. H. Jhang, L. Chen, W. Chang, C. Yang, and C. Yu, "Design of a low-cost level-triggered Zigbee network multi-application sensor in smart homes," in *2017 6th International Symposium on Next Generation Electronics (ISNE*, pp. 1–3, Keelung, Taiwan, 2017.

[19] H. Joh, I. Yang, and I. Ryoo, "The internet of everything based on energy efficient P2P transmission technology with Bluetooth low energy," *Peer-to-Peer Networking and Applications*, vol. 9, no. 3, pp. 520–528, 2016.

[20] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan et al., "A survey on communication components for iot-based technologies in smart homes," *Telecommunication Systems*, vol. 69, no. 1, pp. 1–25, 2018.

[21] L. Wan, Z. Zhang, and J. Wang, "Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 2–12, 2019.

[22] L. Touati, H. Hellaoui, and Y. Challal, "Threshold yoking/-grouping proofs based on CP-ABE for IoT applications," in *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 568–575, Tianjin, 2016.

[23] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[24] J. M. Batalla and F. Gonciarz, "Deployment of smart home management system at the edge: mechanisms and protocols," *Neural Computing and Applications*, vol. 31, no. 5, pp. 1301–1315, 2019.

[25] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 167–171, 2020.

[26] U. Saxena, J. S. Sodhi, and Y. Singh, "Analysis of security attacks in a smart home networks," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 431–436, Noida, 2017.

[27] S. Rehman and V. Gruhn, "An approach to secure smart homes in cyber-physical systems/internet-of-things," in *2018 Fifth International Conference on Software Defined Systems (SDS)*, pp. 126–129, Barcelona, Spain, 2018.

[28] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely access "my" smart home in private: an anti-tracking authentication and key agreement scheme," *IEEE Access*, vol. 7, pp. 41835–41851, 2019.

[29] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Lightweight and secure password based smart home authentication protocol: LSP-SHAP," *Journal of Network and Systems Management*, vol. 27, no. 4, pp. 1020–1042, 2019.

[30] C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in industrial wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, 134 pages, 2018.