Wuhan University Journal of Natural Sciences

2022, Vol.27 No.2, 169-176

Article ID 1007-1202(2022)02-0169-08

DOI https://doi.org/10.1051/wujns/2022272169

Energy Internet and Its Trusted Protection Architecture

□ WANG Haixiang[1], CAO Jingyi[1], LIU Zhe[2†]

1. China Electric Power Research Institute, Beijing 100192, China;

2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, Hubei, China

Abstract: Through the combination of new energy and Internet technology, the Energy Internet deeply integrates various complex network systems such as power, transportation and natural gas, aiming to change the energy utilization model and promote the sustainable development of economy and society. The Energy Internet takes the power grid as the "Backbone Network", integrating the autonomous units of distributed energy, and integrating information and energy through the open-peer information and energy integration architecture. Information interaction scenarios of the Energy Internet information interaction scenarios include "human-object", "human-human" and "object-object". In this new interconnection mechanism environment, the lack of any security defenses may leave the Energy Internet exposed to the risk of information leakage, theft and loss, resulting in immeasurable losses. From "human-object", "object-object" and "human-human" interaction scenarios, the paper puts forward fine-grained access control mechanism, trusted computing environment building in IoT devices and trusted communication channel construction, and designs a trusted protection architecture for the Energy Internet to ensure the data security throughout its life cycle. We verify that the proposed architecture can provide trusted environment for the Energy Internet.

Key words: Energy Internet; energy integration; access control; trusted computing

CLC number: TP 391

Received date: 2021-12-23

Foundation item: Supported by the State Grid Corporation of China Science and Technology Project Funding

Biography: WANG Haixiang, male, Master, research direction: electric power network and information security. E-mail: wanghx@epri.sgcc.com.cn

† To whom correspondence should be addressed. E-mail: 2016102110052@whu.edu.cn

0 Introduction

In 2011, American scholar Rifkin predicted in the The Third Industrial Revolution[1] that the Energy Internet, a new energy utilization system, characterized by the in-depth integration of new energy technology and information technology, is about to emerge. With the attention of the Chinese government, Rifkin and his Energy Internet concept have been widely spread in China. In 2014, China proposed a long-term strategy for energy production and consumption revolution, starting from the power system and trying to dominate the layout of the global Energy Internet. In 2016, the Global Energy Internet Development Cooperation Organization, exclusively initiated by State Grid, was announced. This organization is the first international organization initiated and established by China in the energy field, and it is also the first cooperation and coordination organization of the global Energy Internet.

The Energy Internet, comprehensively using advanced power electronic technology, information processing technology, Internet technology and other new technologies, consists of a large number of distributed energy harvesting devices, distributed energy storage devices and various new power networks, natural gas networks, oil networks and other energy sources. Autonomous units are interconnected to build a two-way energy exchange and information sharing network. The concept of the Energy Internet is proposed to realize the interconnection of the network under the energy production system. The focus is on modern communication technology to interconnect the energy and power systems and change the way of energy exchange and data exchange. According to Professor Junwei Cao in Tsinghua

University, the Energy Internet is a combination of Internet technology, renewable energy technology and modern power systems, and it is an inevitable trend for the integration and development of information technology and energy power technology[2]. Therefore, if the power system network is reconstructed based on the principles of openness, interconnection, reciprocity, and sharing, the security of the power grid and the efficiency of power production can be significantly improved, and the information sharing and data processing capabilities of the Energy Internet can be significantly improved.

As a key information infrastructure related to the national economy and people's livelihood, once the Energy Internet is damaged, data leakage or loss of function will seriously threaten national security and public interests, therefore, it is important to study the trusted protection architecture of the Energy Internet to ensure the smooth and reliable operation of the Energy Internet.

1 Related Work

In December 2008, the German Federal Ministry of Economics and Technology launched a technological innovation promotion plan to build a future energy system based on information and communication technology, and began to develop and test the core technology of the Energy Internet. In 2011, Europe launched the future smart Energy Internet project. The project aimed to build an information and communication technology platform for the future Energy Internet, support the intelligence of the power distribution system, and develop new innovative services[3]. The Energy Office of the Swiss Federal Government and the industry sector jointly initiated a research project "looking forward to the energy network of the future"[4], which aims to study the utilization of multi-energy transmission systems, the conversion and storage of distributed energy, and the development of corresponding systems' simulation analysis models and software tools. The future renewable power transmission and management system of the national science foundation of the United States proposed a high-efficiency power distribution system that adapts to high-penetration distributed renewable energy power generation and distributed energy storage grid connection, which is called the Energy Internet[5]. In 2014, Liu Zhenya, chairman of the state grid corporation of China, proposed to build a global Energy Internet at the IEEE conference in the United States. Beijing Electric Power Company takes the lead in undertaking research projects such as "Key Technologies for AC/DC Hybrid Distribution Networks", the 863 Project of the Ministry of Science and Technology, and is the first to carry out urban Energy Internet technology research and applications.

In the Energy Internet, the Internet of Things is the foundation, so the security and interaction of the Energy Internet are also guaranteed by the related technologies of the Internet of Things. The United States is the first country to implement hierarchical protection. It puts forward a security scheme between sensitive non-secret networks in its Multi-level Information System Security Plan (MISSI). MISSI aims at the secure transmission of multi-level interconnection. However, at present, the access control requirements and security requirements of multi-level interconnected systems are not specific. Xie *et al*[6] proposed a supported distributed authentication protocol to enhance the trust relationship between self-organizing hosts. In addition, an effective secure routing protocol is also discussed to protect the multi-hop routing of Internet and self-organizing communications. In order to reduce the design complexity and development cost of the application software of the Internet of Things, Xie *et al*[7] proposed a connection mechanism which can match and establish the connection between any two sensor/actuator elements according to the need. Taking the power grid as an example, the Energy Internet is composed of the power network as the backbone and the local area network of autonomous units, in which the communication of each local area network needs credible protection. He *et al*[8] proposed a new dynamic security interconnection mechanism, which isolates cloud computing systems into multiple dynamic virtual trust zones and implements different security policies for different customers to enhance the security of interaction. Suzuki *et al*[9] proposed a new software virtualization architecture for controlling hosts to connect devices distributed in Ethernet. It virtualizes remote devices that communicate through the host's standard network interface card into devices contained in the host's device tree. All kinds of computers, from handheld to rack, can control the equipment of remote local area network by installing relevant software. Hector *et al*[10] proposed a framework that integrates wireless sensor networks, Internet of Things platform and interactive applications, which makes the interaction between devices more reliable. Li[11] proposed to establish a directory protocol to solve the resource sharing and open system interconnection of the Internet of Things. Jia *et al*[12] put forward a SCOR (Supply Chain Operations Reference) model to promote the secure interconnection of the Energy Internet terminal entities by formulating countermeasures for energy production, transmission, consumption and other links. Ji *et al*[13] established a unified communication model of industrial Ethernet and Internet of Things from the network layer, and realized the integration of industrial network and Internet of Things. The access control requirements of multi-level interconnected systems clearly point out in the "Design Requirements": "maintain the consistency of security elements such as user identity, subject and object tags, access control policies, and secure the inter-operation and data exchange between interconnected systems". Lin *et al*[14] paid attention to the security of terminal devices entering the network, designed an access authentication protocol based on trusted computing, gave a specific authentication method for trusted devices to access the network, and used predicate logic to prove the security of the protocol to ensure the security and credibility of the access authentication process. Yang *et al*[15] proposed a secure access scheme for mobile terminals in cloud environment. The scheme fully considers the application background of mobile cloud computing, and uses ARM TrustZone hardware isolation technology to build a trusted mobile terminal to protect the cloud service client and the safe execution of security-sensitive operations on the mobile terminal. Zhao *et al*[16] put forward a research and implementation scheme of secure startup mechanism of embedded system based on trusted computing technology. Under the premise of the existing hardware architecture of mobile devices, an external trusted platform module is constructed by using secure TF card, which forms a complete trust chain from Bootloader to upper application programs and effectively ensures that the integrity of the terminal will not be destroyed. Zhang *et al*[17] proposed a trusted access authentication protocol for mobile terminals in the context of the Internet of Things. The authentication between the mobile sink node and the sensor node does not need the participation of the base station, and the key agreement and authentication are completed between the sensor node and the mobile node. During authentication, the anonymity of the mobile node is realized by using the pre-stored Kana and the corresponding public and private keys in the mobile node, and the security proof is given under the CK (Canetti-Krawczyk) model. The research of security early warning technology and visualization technology is also an important part of power grid security situation awareness research. Xu *et al*[18] proposed flexible DC interconnection for the Energy Internet, and constructed an AC/DC hybrid urban distribution network interconnection architecture with AC transformer as the core and DC bus as the framework. This scheme is guided by the goals and characteristics of the Energy Internet, that is, it meets the requirements of the Energy Internet and has the ability to analyze the security situation of the Energy Internet.

At present, a large number of technical applications such as intelligent measurement and control, protection devices and Internet of Things protocols are widely used in the Energy Internet, carrying a large number of core services of the energy interconnection system. Security protection adopts the inspection technology based on known "characteristics" represented by virus detection and intrusion detection, which cannot adapt to tens of thousands of virus Trojans and cannot resist the emerging unknown malicious code. And there are some problems, such as low efficiency, high consumption of system resources, great restriction on business functions and so on. Trusted computing aims at security and controllability and has the active defense capability against unknown malicious code attacks. The integration of this new technology into the energy interconnection system can scientifically and effectively improve the panoramic security defense capability of the Energy Internet.

2 Security Problem

The Energy Internet takes power as the core, but also emphasizes the integration and interconnection of multiple types of networks. It needs to break the isolation between different types of energy, so as to achieve the comprehensive coordination and optimization of multiple types of energy, and give users more options in energy terminals. In the process of promoting the Energy Internet, the development of information covers three information interaction scenarios: "human-thing", "thing-thing" and "human-human". Energy interconnection is a variety of energy physical interconnection network with power system as the core hub and the Internet of Things as its basis. With advanced sensors, control and software applications, we connect hundreds of millions of equipments, machines and systems of energy production end, energy transmission end and energy consumption end, forming its "foundation of Internet of Things". The lack of the defense in any link may bring huge information leakage, theft and loss, and cause immeasurable losses.

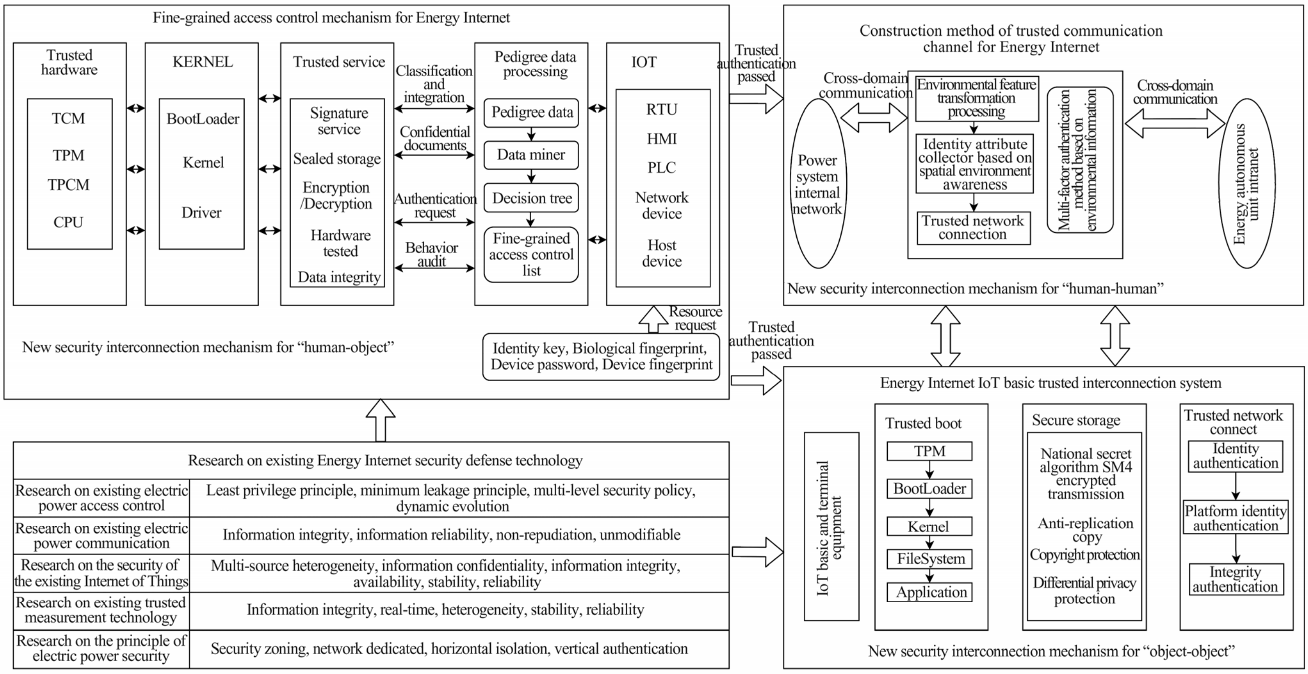
In the scenario of “human-object” connectivity, the main security threat comes from illegal users invading the energy interconnected systems through the network, and the safe and independent operating environment of the energy ecosystem depends on the access control mechanism. The elements of energy and Internet data subjects gradually tend to be multi-source, heterogeneous and dynamic. The traditional access control strategy fails to control the evolution process of data being empty at any time, which is easy to cause improper authorization and other problems. Common intrusion attacks include detection attacks, denial-of-service attacks, unauthorized access, network listening, resulting to major security events like theft, tampering and loss of data.

In the scene of the “object-object” interconnection, thousands of terminal devices are connected to the energy Internet of things. Mass Internet of Things sensing nodes collect data and transmit it to the data center through the network for data processing and storage, and a security flaw in either of them can cause damage to the entire security system. For example, in the perceptual layer, perceptual nodes are easy to be eavesdropped, controlled and disguised. In the network layer, networks also face the security problems of traditional networks, including illegal access to the networks, misconduct of confidentiality, integrity destruction, and denial of service attacks, middleman attacks, and virus intrusion.

In the scenario of “human-human” interconnection, multi-entity heterogeneous data collaboration can significantly improve the ability of data processing and operation. However, during the cloud environment data sharing process, data abuse problems may occur when sharing data with external business objects. A variety of energy sources need cross-domain interaction and collaborative scheduling. The traditional authentication mechanism such as key and password depends on the confidentiality of authentication information, and is vulnerable to imitation attack and middleman attack. In collaborative computing, data faces a serious threat of leakage and loss.

3 Trusted Protection Architecture

According to the different interaction objects, the Energy Internet trusted protection architecture takes three information interaction scenarios into consideration, including “human-thing”, “thing-thing” and “human-human”. This architecture proposes fine-grained access control mechanism, things basic trusted interconnection system and trusted communication channel construction to ensure the independent operation environment and its internal reliable interaction model. The Energy Internet trusted protection architecture is shown in Fig. 1.


Fine-grained access control mechanism for Energy Internet
Trusted hardware
TCM
TPM
TPCM
CPU
KERNEL
BootLoader
Kernel
Driver
Trusted service
Signature service
Sealed storage
Encryption /Decryption
Hardware tested
Data integrity
Classification and integration
Confidential documents
Authentication request
Behavior audit
Pedigree data processing
Pedigree data
Data miner
Decision tree
Fine-grained access control list
IOT
RTU
HMI
PLC
Network device
Host device
Resource request
Identity key, Biological fingerprint, Device password, Device fingerprint
New security interconnection mechanism for “human-object”
Trusted authentication passed
Construction method of trusted communication channel for Energy Internet
Cross-domain communication
Power system internal network
Environmental feature transformation processing
Identity attribute collector based on spatial environment awareness
Trusted network connection
Multi-factor authentication method based on environmental information
Cross-domain communication
Energy autonomous unit intranet
New security interconnection mechanism for “human-human”
Trusted authentication passed
Energy Internet IoT basic trusted interconnection system
IoT basic and terminal equipment
Trusted boot
TPM
BootLoader
Kernel
FileSystem
Application
Secure storage
National secret algorithm SM4 encrypted transmission
Anti-replication copy
Copyright protection
Differential privacy protection
Trusted network connect
Identity authentication
Platform identity authentication
Integrity authentication
New security interconnection mechanism for “object-object”

Research on existing Energy Internet security defense technology	
Research on existing electric power access control	Least privilege principle, minimum leakage principle, multi-level security policy, dynamic evolution
Research on existing electric power communication	Information integrity, information reliability, non-repudiation, unmodifiable
Research on the security of the existing Internet of Things	Multi-source heterogeneity, information confidentiality, information integrity, availability, stability, reliability
Research on existing trusted measurement technology	Information integrity, real-time, heterogeneity, stability, reliability
Research on the principle of electric power security	Security zoning, network dedicated, horizontal isolation, vertical authentication

Fig. 1 Energy Internet trusted protection architecture diagram

1) Fine-grained access control mechanism

In the scenario of "human-object" interconnection, the main threat to the Energy Internet security comes from unauthorized access into the Energy Internet through illegal means of attempted intrusion, camouflage attack, and infiltration of security control system. However, as the data subject gradually tend to be multi-source, isomerized and dynamic, the traditional access control strategy fails to control its evolution process, which is prone to illegal authorization.

The proposed method can get access control rules in the data, and store the access control rule in trusted hardware. The access control mechanism is built on trusted computing, which provides data signature, encryption operation, authentication request, behavior audit and other services for access control, to comprehensively guarantee the trust of access control, and to provide the fine-grained access control ability.

2) Internet of Things basic trusted interconnection system

In the scene of "object-object" interconnection, the deployed terminal equipment in the energy interconnection system has large volume, variety and complex structure. However, the external environment cannot effectively guarantee the reliable work of equipment. Perceptual nodes are prone to eavesdropping or control, and illegal network access causes data damage and integrity damage. The trusted interconnection system of the Energy Internet applies trusted computing to give the Internet of Things foundation trusted startup, trusted measure and safe storage capabilities, guaranteeing a reliable computing environment for the terminal equipment.

3) Trusted communication channel construction

In the scene of "human-human" interconnection, trusted communication channel is designed for data theft and privacy leakage in the Energy Internet, so as to realize trusted user identity authentication and efficient data collaborative use in the cloud environment. Big data analysis technology is an important method to depict user identity through rich identity characterization attributions and construct an attribution collection. The attribution collection can be employed to complete identity authentication in different application scenarios and realize "human-human" interconnection user authentication. In the Energy Internet data sharing process, trusted hardware platform can selectively limit user rights to special functions, effectively preventing cloud data leakage and misuse.

4 Experiment and Analysis

4.1 Test Environment

An access control system is designed for the "human-object" interconnection in the Energy Internet. The access control system is developed in Java language, the development tool is eclipse IDE for Java EE developers (64 bit) 4.5.1, the development environment is Java development kit 8, and the running environment is Java se runtime environment 64 bit. The experimental test of the prototype system of the trusted Energy Internet access control model contains four hosts, including three trusted terminals for the Energy Internet access, one as the security authentication center, one as trusted authorization center, and one as the trusted server and storage device. A local area network is formed by connecting a network cable and a switch.

For the "object-object" interconnection in the Energy Internet of Things, a trusted startup platform based on embedded devices is designed. The trusted startup test platform is an embedded device using Linux system. On the premise of satisfying the expansibility, we choose zynqax7020 development board (built-in security chip) as the main control module of mobile terminal entity. Zynq7020 development board is equipped with Linux operating system, and the security chip can support many cryptographic algorithms. By encapsulating the access interface of the security chip on the development board, we can get the interface package that can be directly called by the upper layer. Finally, it realizes the functions of simulated trusted root device management, cryptographic algorithm call, remote authentication and so on; In terms of chip secure storage, one is to protect the symmetric key with the user's private key, encrypt and store it in the secure area of the secure chip, and only legitimate users can access the symmetric key file and decrypt it; The other is to realize the corresponding interface and encrypt and decrypt the file data by using the compiled cryptographic algorithm.

4.2 System Function Test

Aiming at the problems existing in the original Energy Internet access scenario, the following three risk scenarios are designed for the trusted Energy Internet access prototype system, the security access control function is verified, and the control effect of the system is recorded. The contents and results of security access control function tests are shown in Table 1.

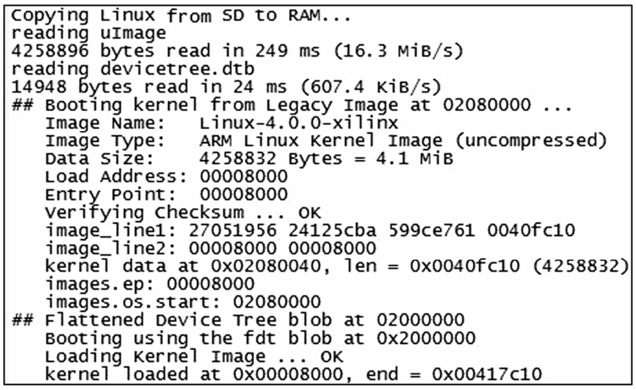
Table 1 Security access control function test

Test content	Test method	Times	Result
The user connection timeout	The user tried to access the Energy Internet system outside the login time	30	The user's trust level was reduced, the access security level was reduced, and the scope of authority was reduced
Abnormal terminal environment	Download the virus file, and the terminal protection software will check and record it	30	The system has been successfully detected, the access security level has been reduced, and the scope of authority has been reduced
Terminal integrity failure	Delete system authorization driver file	30	Platform integrity authentication failed, and user access failed

It can be seen from Table 1 that the system can sensitively detect the changes of user and terminal attributes in access control, and adjust the permissions according to different attribute changes, which has a good performance in the secure access control of the trusted Energy Internet.

The specific implementation of trusted launch of the Energy Internet of Things foundation includes the following four parts:

1) By setting the prompt code in the uboot source code, observe the execution of the code when the system is started from the serial port, and extract the information shown in Fig. 2.

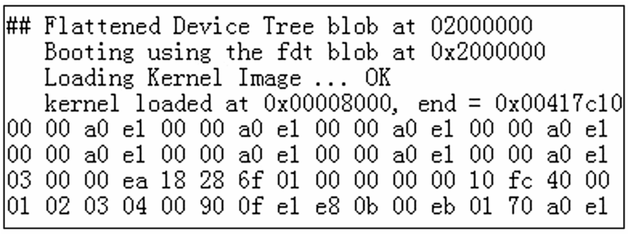


```
Copying Linux from SD to RAM...
reading uImage
4258896 bytes read in 249 ms (16.3 MiB/s)
reading devicetree.dtb
14948 bytes read in 24 ms (607.4 KiB/s)
## Booting kernel from Legacy Image at 02080000 ...
   Image Name:   Linux-4.0.0-xilinx
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    4258832 Bytes = 4.1 MiB
   Load Address: 00008000
   Entry Point:  00008000
   Verifying Checksum ... OK
   image_line1: 27051956 24125cba 599ce761 0040fc10
   image_line2: 00008000 00008000
   kernel data at 0x02080040, len = 0x0040fc10 (4258832)
   images.ep: 00008000
   images.os.start: 02080000
## Flattened Device Tree blob at 02000000
   Booting using the fdt blob at 0x2000000
   Loading Kernel Image ... OK
   kernel loaded at 0x00008000, end = 0x00417c10
```

Fig. 2 Uboot startup information

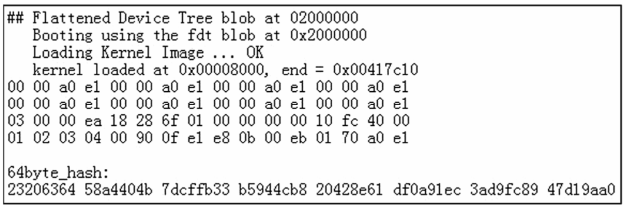
As is shown in Fig. 2, the total length of the kernel file uimage is 4 258 896 bit, including 64 bit header information for parsing. The actual length is 4 258 832 bit, and the loading address in the memory (DDR3) is 0x00 008000-0x00417c10.

2) Insert the test code into the uboot source code. After the kernel is loaded, directly read the data of the kernel loading address to obtain part of the kernel data (64 bit). Part of the data in the kernel is shown in the Fig. 3. Compared with the information in the uimage file, the results are consistent, and the result of comparison is shown in Fig. 4.



```
## Flattened Device Tree blob at 02000000
   Booting using the fdt blob at 0x2000000
   Loading Kernel Image ... OK
   kernel loaded at 0x00008000, end = 0x00417c10
00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1
00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1
03 00 00 ea 18 28 6f 01 00 00 00 00 10 fc 40 00
01 02 03 04 00 90 0f e1 e8 0b 00 eb 01 70 a0 e1
```

Fig. 3 Reading 64 bit data



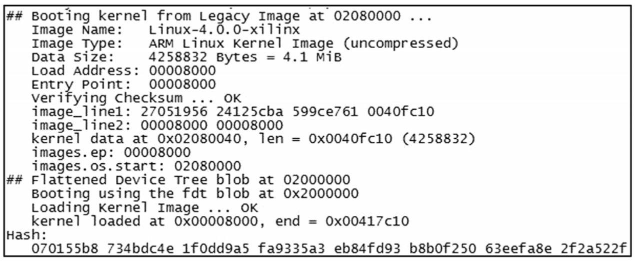
```
## Flattened Device Tree blob at 02000000
   Booting using the fdt blob at 0x2000000
   Loading Kernel Image ... OK
   kernel loaded at 0x00008000, end = 0x00417c10
00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1
00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1
03 00 00 ea 18 28 6f 01 00 00 00 00 10 fc 40 00
01 02 03 04 00 90 0f e1 e8 0b 00 eb 01 70 a0 e1

64byte_hash:
23206364 58a4404b 7dcffb33 b5944cb8 20428e61 df0a91ec 3ad9fc89 47d19aa0
```

Fig. 4 Uimage actual data

3) Add the calling interface of the SM3 algorithm IP core to the uboot source code to hash the obtained 64 bit data:figure hash results of some kernel data.

4) On this basis, the integrity measurement is verified. The general situation is as follows: expand the read address length to the length of kernel data, extract and hash the whole kernel data. The hash results are shown in Fig. 5. The results obtained from multiple starts are consistent.



```
## Booting kernel from Legacy Image at 02080000 ...
   Image Name:   Linux-4.0.0-xilinx
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    4258832 Bytes = 4.1 MiB
   Load Address: 00008000
   Entry Point:  00008000
   Verifying Checksum ... OK
   image_line1: 27051956 24125cba 599ce761 0040fc10
   image_line2: 00008000 00008000
   kernel data at 0x02080040, len = 0x0040fc10 (4258832)
   images.ep: 00008000
   images.os.start: 02080000
## Flattened Device Tree blob at 02000000
   Booting using the fdt blob at 0x2000000
   Loading Kernel Image ... OK
   kernel loaded at 0x00008000, end = 0x00417c10
Hash:
   070155b8 734bdc4e 1f0dd9a5 fa9335a3 eb84fd93 b8b0f250 63eefa8e 2f2a522f
```

Fig. 5 Hash results of complete kernel data

Based on the above experimental results, the integrity measurement of the kernel and device tree is realized. In order to ensure the security of the data and avoid disappearance after power failure, the hash value is encrypted with PUF (Physically Unclonable Function) key and stored in flash. Each time the system starts, the PUF key is reconstructed, and then the encrypted data is decrypted and compared with the newly obtained integrity measurement value. The system can be started successfully only when it is the same.

4.3 System Performance Test

In order to verify the function realization effect of the prototype system of the trusted Energy Internet access control model, the performance test is carried out on the main functions in the process of legal users accessing the Energy Internet to access resources. The test results are shown in Table 2.

By testing on the embedded development board, the trusted startup can be realized, and MLO (MyLifeOrganized) and uboot can be obtained by using the SHA-1 computing engine of TPM (Trusted Platform Module). According to the boot sequence, the component measures the boot loader before transferring the control right. Table 3 is the time test during the startup process. The code in the actual ROM (Read-Only Memory) is less than 32 Kb, but the specific size is unknown. The ROM code is taken as the trust root, so the ROM code is not measured. The results of trusted startup performance test of the Energy Internet are shown in Table 3.

Table 2 Energy Internet access control performance test

Test content	Test method	Times	Result
User authentication	After the user enters the user name and password, the security authentication center completes the Energy Internet identity authentication (ignoring the user input time)	60	There is no abnormality, the response time is between 0.15 s-0.29 s, and the average response time is 0.20 s
Device attribute and integrity information collection	Delete system authorization driver file	60	Collect terminal attribute and integrity information during user login authentication
Energy Internet resource access request	The user refreshes the resource request list and gets the response from the trusted server	60	There is no abnormality. The response time is between 0.22 s-0.61 s, and the average response time is 0.41 s
Energy Internet resource operation	Test the function of users using the terminal to upload and download Energy Internet data	60	No abnormality

Table 3 Energy Internet trusted boot performance test

Running program	Data size	Test time
Runtime of ROM code	≤32.0 Kb(+8.0 Kb)	10.8 ms
MLO measurement comparison time + MLO unsealing and running time	77 Kb(+7.9 Kb)	92.4 ms
For uboot Bin measurement comparison Hash value time + unpack and run uboot Bin time	361 Kb	304.5 ms
Comparison time of kernel measurement + unpacking and running time of Linux kernel	3.6 Mb	2 732.2 ms
Measure the comparison time of kernel parameters + unpacking and running time of kernel parameters	2 Mb	1 821.1 ms
Comparison time of root file system measurement + unpacking and running time of root file system	7.15 Mb	5 463.3 ms
Total	≤13 Mb	≤10.5 s

5 Conclusion

At present, the development prospect of the Energy Internet is huge, but it faces a quite grim security situation. The existing security protection methods lack the overall consideration of energy and Internet security, so it is difficult to resist new attacks. These methods have some limits, such as low efficiency, large resource consumption and great constraints on business functions. According to the different interaction objects, from three information interaction scenarios of “human-object”, “object-object” and “human-human”, we design the Energy Internet trusted protection architecture and propose the fine-grained access control mechanism, things basic trusted interconnection system and trusted communication channel construction, providing a new view to ensure the Energy Internet security. Through a wide test, we verify that the proposed architecture can provide a trusted environment for the Energy Internet from multiple interaction scenarios.

References

[1] Rifkin J. *The Third Industrial Revolution*: *How Lateral Power Is Transforming Energy*, *the Economy*, *and the World* [M]. London: Macmillan, 2011.

[2] Wang J Y, Meng K, Cao J W. A summary of the research on Energy Internet information technology [J]. *Computer Research and Development*, 2015, **52**(5): 1109-1126(Ch).

[3] Fluhr J, Williams F. FINSENY: Future internet for smart energy [J]. *Unternehmen der Zukunft*, 2011(2): 61-62.

[4] Shen Z, Liu Z M, Baran M. Power management strategies for the green hub [C]// *IEEE Power and Energy Society General Meeting*. Piscataway: IEEE, 2012: 1-4.

[5] Huang A Q. FREEDM system—A vision for the future grid [C]// *IEEE Power and Energy Society General Meeting*. Piscataway: IEEE, 2010: 1-4.

[6] Xie B, Anup K, Dharma A. Secure interconnection protocol for integrated Internet and ad hoc networks [J]. *Wireless Communications and Mobile Computing*, 2008, **8**: 1129-1148.

[7] Xie K, Chen H, Huang X, *et al*. Low cost IoT software development: Ingredient transformation and interconnection [C]// *IEEE International Conference on Parallel and Distributed Systems*. Piscataway: IEEE, 2015: 44-51.

[8] He L, Huang F, Zhang J, *et al*. Dynamic secure interconnection for security enhancement in cloud computing [J]. *International Journal of Computers Communications Control*, 2016, **11**(3): 348-357.

[9] Suzuki J, Tsuji A, Hayashi Y, *et al*. Device-Level IoT with virtual I/O device interconnection [C]// *IEEE International Conference on Cloud Computing Technology and Science* (*CloudCom*). Piscataway: IEEE, 2016: 67-74.

[10] Hector S, Carlos G C, Agudo J, *et al*. IoT and iTV for interconnection, monitoring, and automation of common areas of residents [J]. *Applied Sciences*, 2017, **7**(7): 696.

[11] Li X Q. *Design and Implementation of Lightweight Directory Protocol and Service of Internet of Things and Its Management System* [D]. Beijing: Beijing University of posts and Telecommunications, 2015(Ch).

[12] Jia J Z, Zeng M. Energy Internet construction based on SCOR model [J]. *Economic Research Guide*, 2019(5): 87-90(Ch).

[13] Ji S P. Research on the interconnection model of industrial Ethernet and Internet of things [J]. *Computer Measurement and Control*, 2011, **19**(8): 1998-2000(Ch).

[14] Lin Z P, Zou Q C. Design and security analysis of trusted equipment access network authentication protocol [J]. *Computer Simulation*, 2018, **35**(11): 254-258(Ch).

[15] Yang B, Feng D G, Qin N. Secure access scheme of trusted mobile terminal cloud service based on TrustZone [J]. *Journal of Software*, 2016, **27**(6): 1366-1383(Ch).

[16] Zhao B, Yu T, Zhang H G. Research and implementation of security enhancement of trusted embedded platform operating system [C]// *Proceedings of the* 18*th National Conference on Information Secrecy*. Beijing: Gold Wall Press, 2008: 104-110(Ch).

[17] Zhang X, Yang X Y, Zhu S S, *et al*. Trusted access authentication protocol for mobile nodes in the Internet of things [J]. *Computer Application*, 2016, **36**(11): 3108-3112(Ch).

[18] Xu C, Liang R, Cheng Z H, *et al*. Security situation awareness of intelligent distribution network for Energy Internet [J]. *Electric Power Automation Equipment*, 2016, **36**(6): 13-18 (Ch).

□