Weiyong YANG, Wei LIU, Xingshen WEI, Zixin GUO, Kangle YANG, Hao HUANG, Longyun QI, 2021. EdgeKeeper: a trusted edge computing framework for ubiquitous power Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 22(3):374-399. https://doi.org/10.1631/FITEE.1900636

EdgeKeeper: a trusted edge computing framework for ubiquitous power Internet of Things

Key words: Internet of Things; Ubiquitous power Internet of Things; Edge computing; Trusted computing; Network security

Corresponding author: Kangle YANG
E-mail: yangkangle@sgepri.sgcc.com.cn
ORCID: https://orcid.org/0000-0001-7646-4336

Motivation

1. Ubiquitous power Internet of Things (IoT) is a smart service system oriented to all aspects of the power system, and has the characteristics of universal interconnection, human-computer interaction, comprehensive state perception, efficient information processing, and other convenient and flexible applications. It has become a hot topic in the field of IoT.

2. The general-purpose edge computing framework software is difficult to satisfy the ubiquitous power IoT requirements in terms of real-time, security, reliability, and business function adaptation.

Main idea

1. The edge computing framework, EdgeKeeper, is divided into the hardware layer, operating system (OS) layer, basic functional layer, and edge service layer in the functional architecture.

2. The hardware layer includes the unique identifier of the device, trusted computing module, trusted execution environment, and security cryptographic module.

3. The OS layer includes functions such as system monitoring, secure access, application isolation, and trust measurement.

Main idea (Cont’d)

4. The basic functional layer includes functions such as sub-device access, object model management, and message queues.

5. The edge service layer includes functions such as flow calculation, rule engine, and various microservices, which provide edge analysis and data processing.

Method

1. EdgeKeeper uses the four-level security OS named NARISecOS (the highest security level OS) to provide a secure execution environment at the operating system level for the business. NARISecOS builds a layer of “microkernel OS” to ensure that the maximum terminal response time is about 10 μs.

2. EdgeKeeper has the function of trusted verification, including four aspects: trusted startup, trusted measurement, trusted remote certification, and trusted security upgrade.

3. EdgeKeeper uses a microkernel architecture to provide partition isolation mechanism for different functional security-level services in user mode.

Major results

The overall test results of EdgeKeeper, OpenEdge, EdgeX, and KubeEdge are shown in the tables in the following pages, where “●” indicates full support, “○” indicates no support, and “◎” indicates partial support. EdgeKeeper has passed the tests of all functions, non-functions, performance, and application scenarios, and the performance is the most complete. EdgeX is not satisfactory in terms of the non-functional test. KubeEdge does not perform well in non-functional testing and application scenarios. OpenEdge does not perform well in some application scenarios, but in other tests, it performs relatively well.

Major results (Cont'd)

1. EdgeKeeper is compared with other IOT architectures in terms of functionality.

Verification test	Test item	Test point	OpenEdge	EdgeX	KubeEdge	EdgeKeeper
Functional test	Device access	Device registration and access	●	◎	●	●
		Access to the SDK	●	◎	○	●
		Data transfer protocol	●	◎	●	●
		Tenant and IoT agency relationship	●	◎	●	●
	Model definition and delivery	Object model definition	●	◎	●	●
		Object model launching	●	◎	●	●
		Data reporting	●	●	●	●
	Device shadow	Device shadow editing	●	●	◎	●
		Data reporting	●	◎	◎	●
		Status change	●	●	◎	●
	Equipment communication capability	MQTT protocol	●	●	●	●
		Offline storage capability	●	●	●	●
	Data collection	Device message import message queue	●	●	●	●
		Temporary storage of data	●	●	◎	●
		Data error retransmission	●	●	◎	●
	Data distribution	Status change	●	●	●	●
		Data subscription	●	●	●	●
		Send data command	●	●	●	●
Functional test	Firmware upgrade	Firmware upgrade	◎	●	◎	●
	APP management	Management of upper and lower shelves of the APP	●	●	◎	●
		Remote upgrade of the APP	●	●	◎	●
		APP remote configuration	●	●	◎	●
		APP version management	●	●	◎	●
	Rule engine	Rule configuration	●	●	◎	●
		Class SQL syntax and underlying semantic operations	●	●	◎	●
	Operation and maintenance management	Operation and maintenance management	◎	◎	●	●

Major results (Cont'd)

2. EdgeKeeper is compared with other IOT architectures in non-functional aspects.

Verification test	Test item	Test point	OpenEdge	EdgeX	KubeEdge	EdgeKeeper
Non-functional test	Remote configuration	Device remote configuration	●	○	○	●
		Operating system remote configuration	●	●	○	●
	Remote monitoring	Operating system remote monitoring	●	●	○	●
		Terminal operation status monitoring	●	●	○	●
		Application status monitoring	●	●	○	●
		Alarm information management	●	●	○	●
	Remote debugging	Edge proxy device remote debugging	●	●	○	●
		Remote debugging of terminal equipment	●	●	○	●
	Reliability	Batch device online success rate	●	●	○	●
		Cluster high availability deployment	●	●	○	●
	Safety	Edge proxy device access security	●	●	○	●
		Edge proxy device transmission security	●	●	●	●
		Message publishing subscription security	●	○	●	●
		API authentication	●	○	●	●
		Platform login security	●	○	●	●
		Platform safety	●	○	●	●
	Flexibility	Northbound interface	●	○	●	●
		Southbound interface	●	○	●	●
	Openness	Northward openness	●	○	●	●
		Southward openness	●	○	●	●
	Loose coupling	Support of mainstream databases	◎	○	○	●
		Grayscale update capability	●	○	○	●
		Support of component automatic expansion and contraction	●	○	○	●

Major results (Cont'd)

3. EdgeKeeper is compared with other IoT architectures in terms of performance and application scenarios.

Verification test	Test item	Test point	OpenEdge	EdgeX	KubeEdge	EdgeKeeper
Performance test	Performance test	The maximum number of simultaneous connections	◎	○	○	●
		The number of messages a single node that can process per second	●	○	○	●
		Performance of issuing instructions	●	○	○	●
		The maximum number of online users	●	○	○	●
		Average response time of the core function	◎	○	○	●
		Support of 8-h continuous reporting information	◎	○	○	●
		Support of 8-h continuous delivery instructions	◎	○	○	●
Application scenario	Zone area scene	Meter data reporting	◎	●	●	●
		Meter data calling	○	○	○	●
		Remote meter status	○	○	○	●
		Distribution monitoring data reporting	●	●	●	●
		Remote debugging of the circuit breaker	●	●	●	●

"●" indicates full support, "○" indicates no support, and "◎" indicates partial support

Conclusions

An edge-trusted computing framework named EdgeKeeper is designed and implemented, which completes the design of the object model, edge computing, cloud-edge interaction, and breakthrough key technologies, yielding features such as good performance, good security, good reliability, high reliability, and intelligent ecology. Through functional, non-functional, performance, and application scenario tests, and comparison with OpenEdge, EdgeX, and KubeEdge, EdgeKeeper illustrates its advantages in business satisfaction and adaptability.

Weiyong YANG received his PhD degree from Nanjing University. He is a deputy general manager of Nanjing NARI Information and Communication Technology Co., Ltd., and a professor-level senior engineer. He has long been engaged in research on safety protection of electric power monitoring system, and has won the first prize of China Electric Power Science and Technology Progress Award, the first prize of Technology Invention of China Institute of Electronics, the first prize of Science and Technology Progress of State Grid Corporation, etc.

Kangle YANG graduated from Nanjing Institute of Technology in 2018. His main research direction is power system information security. Now, he works at NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing, China.