EAI Endorsed Transactions
on Energy Web
Research Article EAI.EU

Design and Implementation of an SGX Based Electricity Information Collection and Management System

Yao Song[1*,a], Kun Zhu[2,b]

[1*]Information Office, China Agricultural University, Beijing, 100083, China
[2]China Petroleum Engineering Construction Co., Ltd, Beijing, 100101, China

Abstract

With the rapid growth of the number and scale of smart grid users, traditional data encryption transmission methods can no longer meet the performance requirements of data aggregation. In response, a power consumption information collection and management system based on SGX software protection extension is proposed. The system mainly consists of three parts: user electricity data acquisition terminal, SGX data security processing and distributed storage module on the chain, and data monitoring management display platform. The user electricity data collection terminal collects electricity data from various buildings, residences, rooms, and other smart meters, analyzes and uploads it. After calling the trusted function of SGX technology, it enters the security zone provided by SGX for data processing. Finally, the data security processing results and data are uploaded to the blockchain for storage. In order to visually display user electricity usage data, an intelligent monitoring platform for user electricity collection and management has been established. This system can reduce the workload of user electricity data collection, ensure the accuracy of data collection, and provide an efficient and highly reliable system platform for user electricity data management.

Keywords: SGX, electricity information, information collection and management, block chain, web

Received on 15 November 2023, accepted on 5 April 2024, published on 12 April 2024

doi: 10.4108/ew.5756

1. Introduction

With the development of information technology and the improvement of living standards, people's demand for the security of electricity consumption data and information in the power grid continues to increase.[1,2] Traditional power grids have poor information security during the power transmission process, with a large amount of hidden losses. Attackers can easily steal users' electricity consumption data information, exposing personal privacy and disrupting system stability[3-6].

In recent years, the frequent major security incidents and privacy breaches around the world have elevated the security and privacy issues of smart grids to unprecedented heights.[7,8] In 2010, the "Zhenwang" virus exploited vulnerabilities in industrial control systems, causing at least one fifth of the uranium enrichment equipment at Iran's Bolsh nuclear power plant to be shut down due to the virus infection, successfully avoiding the fault detection system and causing misjudgment in management system decisions[9]. In 2015, the first large-scale power outage incident caused by malicious software in the Ivano Frankivsk region of Ukraine was attacked by hackers, resulting in a large-scale power outage that plunged about half of the region's households (approximately 1.4 million people) into darkness for several hours, once again sounding an alarm for power grid managers worldwide[10]. Faced with the increasing security threats, the current network defense security of the power system is very worrying, and the danger is imminent[11,12]. Once an attack launched by hackers breaks through the power system, it will lead to power grid paralysis. In addition, due to the real-time and high fidelity user electricity data transmitted in the smart grid information network, which contains a large amount of sensitive privacy information, malicious attackers can analyze and obtain user behavior habits based on user electricity data, leading to the constant risk of privacy leakage for grid users[13].

The frequent occurrence of security incidents and privacy breaches in smart grid systems has attracted high attention from governments and academia around the world, becoming

[*a] Corresponding author. Email: songyao@cau.edu.cn, [b]zhukun.se@cnpc.com.cn

a hot topic of concern for all parties. From the perspective of the smart grid system itself, the widespread application of information network technology has led to the increasing openness of the smart grid, which will inevitably lead to higher security risks; From the external environment, the attacker's ability to attack the system is also constantly improving[14-16].

Regarding the security of the power grid management system, at the centralized global control level, the management system of the power grid system analyzes the status of the power grid through user electricity consumption data collected by intelligent meter terminals, predicts future electricity consumption trends, and adopts timely and effective control and scheduling measures[17]. For distributed electricity consuming households, smart meters can also play the role of control centers, optimizing and scheduling the self-organizing network of smart homes[18]. They can adjust their electricity consumption plans and peak shaving and valley filling based on the global information feedback from the control center, thereby achieving energy conservation and emission reduction. However, once an attacker takes advantage of the lack of security authentication and access control mechanisms in smart home devices with embedded wireless communication modules, stealing communication data between smart meters and smart homes, and even controlling the operation of smart home devices, not only will it harm the economic interests of users, but once the attack range is large enough, it will also affect the overall operational efficiency of the power grid[19-21]. A large number of research results have emerged both domestically and internationally, proposing various methods from different perspectives, aiming to improve the security of smart grids and ensure that the privacy of users in the grid is not compromised[22].

This article utilizes smart electricity meters and collection terminals to collect user electricity usage information, and utilizes Intel Security Extension SGX to process the collected electricity usage data. All data is uploaded to the blockchain distributed platform to ensure the authenticity, security, and traceability of all electricity usage data. At the same time, establish a web-based data management platform to achieve real-time monitoring of user electricity consumption data information, historical data query, and statistical analysis, which helps electricity managers and users understand electricity consumption situation and improve electricity quality.

2. Technical Knowledge

2.1. Introduction to SGX

Intel's Software Guard Extension (SGX) is an extension of the Intel instruction set architecture. The purpose is to ensure hardware security as a mandatory guarantee, without relying on the security status of firmware and software, allowing applications to create a trusted executable area in memory, called an Enclave[23]. When the program executes to a trusted function, it will execute in the safe zone and can access the code and data in Enclave[24]. Other attempts to access Enclave outside the secure zone will be rejected by the CPU. After the data in Enclave is output to a non secure area through specialized encryption, other machines cannot decrypt the encrypted data even if they receive it, ensuring the accuracy and confidentiality of the data. Intel SGX provides two data sealing schemes. One is the Secure Zone Flag (MRENCLAVE) policy, where the key is exclusively owned by the secure zone[25]. Only the same secure zone of the same machine can unseal data; Another type is the sealing flag (MRSigner) strategy, which is based on a key generated by the authorized party of the security zone sealing, which can enable data sealed by one security zone to be unsealed by another security zone on the same machine. These two schemes can achieve data encryption and decryption on the same machine, ensuring the security of data storage and processing on the machine[26].

2.2. Introduction to Blockchain

Blockchain is a distributed ledger based on peer-to-peer networks[27-29]. Each block in the blockchain points to the previous block to ensure that the recorded data in the block is difficult to tamper with and traceable to its source. In addition, due to the blockchain system being a peer-to-peer distributed network, when a node experiences data loss due to downtime or other reasons, it can still recover data from the data stored by other nodes, solving the problem of node data loss and ensuring data integrity[30]. The general block structure is shown in Figure 1, where a block contains a header and a transaction list. The header mainly includes the hash value of the previous block, the difficulty value, and the Merkle root of the transaction.

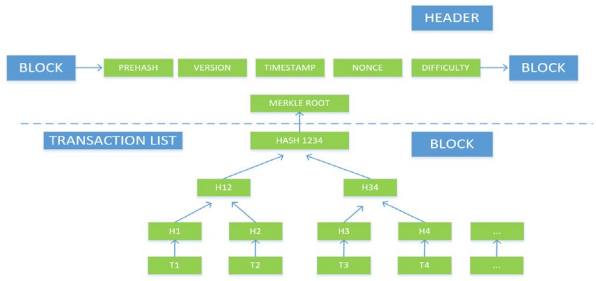

Figure 1. Block structure diagram

2.3. Web technology

Ajax (Asynchronous JavaScript and XML) actually integrates multiple technologies, each with its unique features, and together, it forms a powerful new technology. It combines Java technology, XML, JavaScript, CSS, DOM and other programming technologies, allowing developers to easily and freely build web applications based on Java technology. At the same time, it adopts advanced Web2.0 concepts, breaking the traditional convention of page

overloading and achieving local refresh and real-time display[31].

Node.js was released in May 2009 and developed by Ryan Dahl. It is a JavaScript runtime environment based on the Chrome V8 engine, using an event driven, non blocking I/O model to run JavaScript on a server-side development platform. It makes JavaScript a scripting language on par with server-side languages such as PHP and Python[32].

3. System Design

3.1. Overall System Framework

The system mainly consists of three modules: electricity data acquisition terminal, SGX data processing and on chain storage module, and electricity data monitoring display platform.

The overall system architecture is shown in Figure 2.

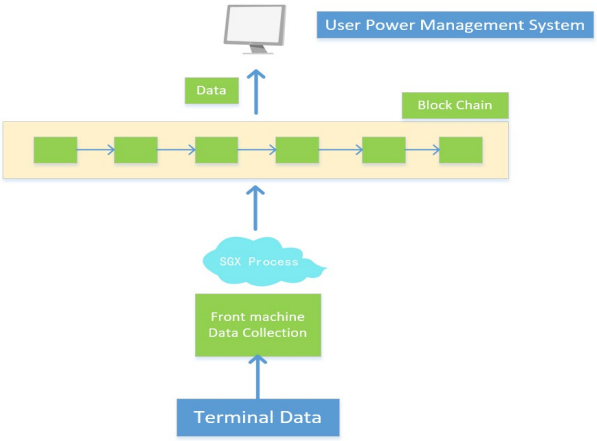

Figure 2. Overall System Architecture Diagram

The user electricity collection monitoring data collection terminal uses intelligent meters and other devices to monitor user electricity consumption. Real time collection of electricity data, transmission of data to SGX trusted environment through analysis, and processing and analysis of collected data; Then encrypt the data and upload it to the blockchain to ensure the authenticity and accuracy of the data source; Finally, the data monitoring platform can obtain real and effective real-time monitoring data from the chain and display it, achieving real-time monitoring of user electricity consumption and historical data query and statistics, as well as analyzing historical data.

3.2. System Hardware Design

The basic hardware equipment for electricity information measurement and collection equipment mainly includes intelligent energy meters and collection terminals.

1) Intelligent energy meter

Intelligent energy meters mainly include multi-functional single-phase intelligent energy meters for residential users and intelligent bidirectional metering energy meters for users with distributed power generation. Among them, intelligent bidirectional energy meters can achieve independent measurement and storage of bidirectional energy in distributed power and grid bidirectional power supply modes[33].

2) Acquisition terminal

The electricity information collection terminal is a device that collects electricity information from various information collection points. A device that can achieve the collection, management, bidirectional transmission, and forwarding or execution of control commands for electricity meter data. Electricity information collection terminals are divided into specialized transformer collection terminals, centralized meter reading terminals (including concentrators and collectors), distributed energy monitoring terminals, and other types according to their application locations.

At the same time, the hardware part of the acquisition terminal of the system also includes control units, data acquisition modules, power modules, communication modules, etc. The main function of the control unit is to analyze and process the communication data transmitted from the upper computer, and to transmit the data measured by various smart meters to the upper computer[34]. The main function of the data collection module is to collect data from various smart meters. The main function of the power module is to provide power to the control unit and communication module. The main function of the communication module is to transmit data between the upper computer and the control unit.

When receiving data from the upper computer, the control unit processes and judges the communication data, identifies the collection terminal for data collection based on the transmitted data, collects data from the corresponding smart meter, transfers the collected data to the control unit for corresponding processing, and then sends the collected data to the upper computer through 485 communication to complete the acquisition of monitoring data by the upper computer[35]. The software flowchart of the lower computer is shown in Figure 3.

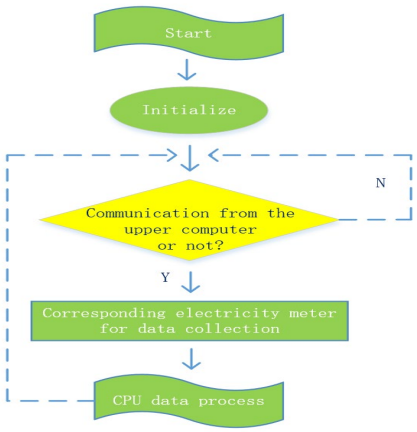

Figure 3. Flow chart

The communication module of the SGX based power consumption information collection and management system hardware design selects a combination of four communication methods for different application scenarios, as shown in Table 1.

Table 1. Communication Mode of Electricity Information Collection System

System Communication	Serial Number	Scope of use	Communication
Local communication	Communication method 1	Collector - Single phase energy meter	rs-485 bus
	Communication method 2	Collector - concentrator	Zigbee wireless communication
	Communication method 3	Intelligent bidirectional metering electricity meter - distributed generation measurement and control terminal	Can bus
Remote communication	Communication method 4	Various measurement and control terminals - main station	optical fiber

3.3. System Software Design

The software part of the system mainly includes a data trusted processing module, a data storage module, and a data management platform data display module. The software framework is shown in Figure 4.

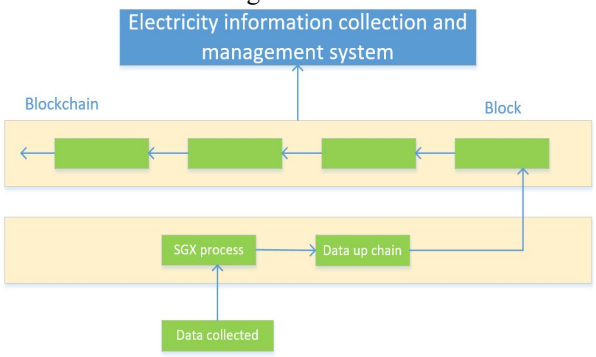

Figure 4. Software framework diagram

1) Data trusted processing module

After obtaining user electricity data from the data collection terminal, enter the SGX trusted environment through pre-programmed trusted functions to securely process the data. Trusted functions have their own code and data, which can provide confidentiality and integrity protection, and have controllable entry points. The processing process is shown in Figure 5. No external program can enter the trusted environment to read the data, ensuring the accuracy of the collected data and data processing results.

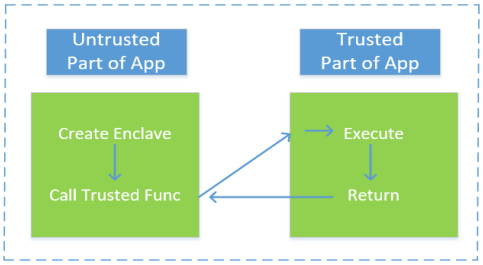

Figure 5. SGX process diagram

An example of pseudocode for processing functions in a trusted environment is as follows:

```
enclave{
import *;
trusted{
public string analyzeData(Power){
if Power.consumption Power.consumption_max
str = "Power high:"+ Power.consumption;
else if Power.consumption Power.consumption_min
str = "Power low:"+ Power.consumption;
else
```

```
str = Power.consumption;
…
}
}
untrusted{ … }
}
```

2) Data uplink module

After data processing is completed, there is still a risk of data being tampered with if it is directly output to an untrusted environment. In order to ensure the security and reliability of the data before being displayed on the system platform, a blockchain solution is introduced. Blockchain has the characteristics of decentralization and difficulty in tampering with data, providing secure storage. Pack the electricity consumption data collected by the collection terminal and the processed data through the blockchain light nodes in a trusted environment. The pseudocode for the uplink processing function is as follows:

```
trusted{
public string uploadBlock(data, result){
begin_b='0x . . . start address;
end_b='0x . . . end address';
Block_ch=collect(data, result); //Block_ch upchain data
tx={                          //create up chain
from: begin_b,
to: end_b,
power: 'user power',
nonce: 1, //random
value: 0, data: Block_ch
}
sendTx(tx); // Sending transactions containing data to blockchain networks
      }
}
```

Due to the collected user electricity consumption data being linked up in the transaction data domain, the electricity consumption data in the data domain is publicly searchable. However, in practical application scenarios, there may be multiple nodes corresponding to different management platforms, and the system platform can only obtain the electricity collection data of its corresponding users. Therefore, the solution is for the platform to negotiate secret keys with various collection nodes of the user to encrypt data and provide an additional layer of access control.

3) Data display module

The data display module is mainly the implementation of the user electricity collection and management platform. After the user's electricity consumption data is uploaded to the chain, the user electricity management platform can query the data from the chain and obtain the electricity consumption data of the users in the data domain. The web-based monitoring platform visualizes the electricity consumption status of users at various collection points, providing precise warnings for platform users or electricity managers on abnormal situations.

As shown in Figure 6, the main functions of the user electricity collection and management system platform are as follows:

1) Real time data monitoring of user electricity consumption.

2) Display the historical information curve of user electricity consumption data.

3) User electricity consumption data historical information report query.

4) Statistical analysis of user electricity consumption data.

5) User platform permission management.

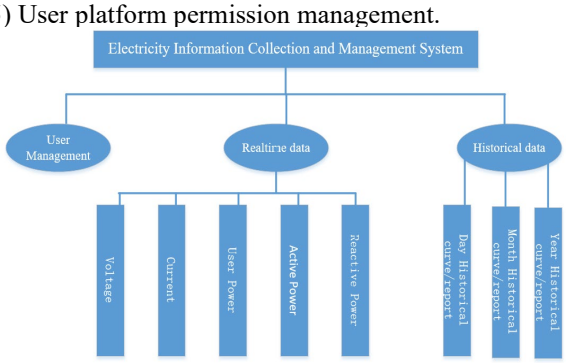

Figure 6. User electricity collection and management platform functions

4. System Implementation

The user electricity collection and management system platform based on SGX has achieved a combination of backend data read and write interfaces and web display pages. In the web display section, the front-end JS framework and Ajax asynchronous communication technology are used to exchange information at the data level with the on chain data server, without having to refresh the page every time, quickly building a user electricity data management display interface. In the interface development section, the application program interface based on JS libraries such as Node and web3 interacts with the data blockchain layer to obtain user electricity consumption data stored on the chain.

4.1. Realtime data

Using the electricity meter collection point as a unit, obtain the electricity consumption data collected at each collection point every 1 hour, and use the table component to display the electricity consumption data at the collection point. The display page is shown in Figure 7.

Click the call button in the interface, and the program will write a command to the system database. The front-end computer of the system will read and interpret the command, read the terminal data, and return it to the webpage for display. This includes information such as three-phase voltage, three-phase current, active power, reactive power, etc. corresponding to the collection terminal.

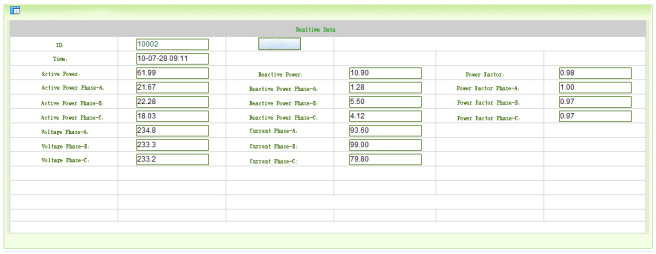

Figure 7. Realtime data show

4.2. Historical data

Considering the demand for statistical analysis of electricity consumption data, the average fluctuation of electricity consumption data in the information center is displayed based on daily units, monthly units, and annual units. A web-based visual graphics display plugin, FushionCharts, is introduced to achieve dynamic graph display of electricity consumption data.

User electricity history curve query, including voltage curve, current curve, zero sequence current curve, active power curve, reactive power curve, power factor curve, apparent power curve, load rate curve, transformer active loss, current imbalance curve, voltage imbalance curve, current distortion rate curve, voltage distortion rate curve, temperature curve, etc. Current curve is shown in Figure 8.

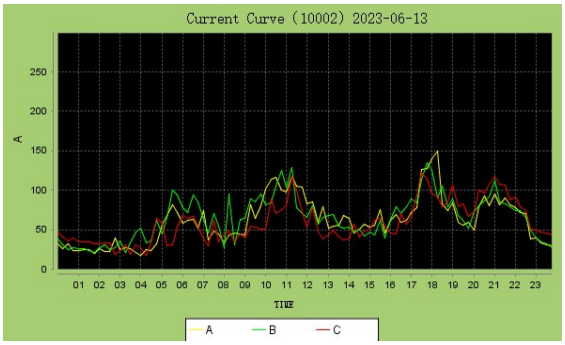

Figure 8. Historical data

4.3 Historical report

Historical report statistics, including collecting daily load reports, statistical reports, extreme value daily reports, event record daily reports, voltage qualification rate reports, etc., and providing monthly report statistics function. The following figure shows the daily statistical report of the collection terminal, including the total active energy of the distribution transformer, peak, flat, valley active and reactive energy, as well as the total reactive energy of the forward and reverse directions. Ordinary users can also query the historical data, electricity consumption, and other information of their corresponding electricity meter equipment. As shown in Figure 9.

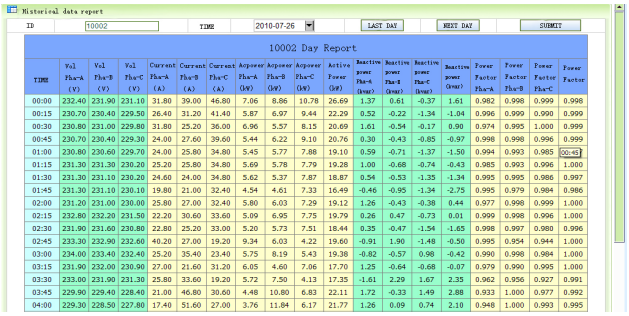

Figure 9. Historical data report

4.4. User management

In terms of user management, different access permissions are opened for different roles of user electricity managers to facilitate the management of user electricity usage. Users are mainly divided into system administrators, device administrators, and ordinary users. The system administrator has the highest access authority and can access all functions of the platform. The device administrator has secondary management authority and the ability to access data and statistical information collected by one or more collection terminals and electricity meter devices. However, ordinary users can only access the electricity consumption data information corresponding to their respective meter numbers. By dividing user permissions for easy system management, and by dividing users and system functional modules, we strive to achieve low coupling and high cohesion.

5. Conclusion

The SGX based electricity information collection and management system, as an important component of the power grid energy management system, is responsible for collecting various basic data of electricity consumption information for users within the network, providing necessary conditions for the bidirectional interaction between power companies and users. This electricity consumption information collection and management system can achieve functions such as automatic collection of electricity consumption information, safe management of electricity consumption data, intelligent electricity consumption statistics, and distributed electricity storage. This system utilizes intelligent collection terminals to analyze and process communication data transmitted from the upper computer. The user electricity data collected by each intelligent meter is transmitted to the upper computer, and SGX technology is used as the data security processing module and blockchain technology as the data security storage module. It realizes a web-based user electricity information management platform, displaying the user's voltage, current, and Relevant indicators such as electricity consumption and fluctuation information of environmental

conditions over different time spans provide management basis for electricity managers. The system greatly reduces the workload of electricity managers, and makes user electricity data transparent, electricity quality clear, electricity data secure. Establishing a bridge of integrity between electricity management units and users can help promote the healthy development of the electricity market.

References

[1] Feng Ruiqi, Wang Leilei, Lin Xiang, Xiong Jinbo SGX Based Safety Data Processing Framework for Vehicle Network Road Condition Monitoring [J/OL]. Computer Applications: 1-10 [2023-04-16] http://kns.cnki.net/kcms/detail/51.1307.TP.20220630.1539.008.html.

[2] Liu Mingda, Shi Yijuan, Rao Xiang, Fan Lei A Distributed Privacy Protection Data Search Scheme [J]. Computer Science, 2022,49 (10): 291-296

[3] Ru Sisong Research on Federated Learning Mechanism Based on Centralized Differential Privacy [D]. University of Science and Technology of China, 2022. DOI: 10.27517/dcnki. gzkju. 2022-001302

[4] Jin Cheng Research on Weak Password Monitoring and Publishing Technology for Privacy Protection [D]. University of Electronic Science and Technology, 2022. DOI: 10.27005/d. cnki. gdzku. 2022-003211

[5] Zhang Xiaoting, Li Xiaofeng, Fang Shiyu Design and Implementation of a Tea Garden Ecological Monitoring System Based on SGX [J]. Instrument Technology, 2021 (05): 1-4+34. DOI: 10.19432/j.cnki.issn1006-2394.2021.05.001

[6] Wei Wentao Privacy protected malware detection based on SGX [D]. Xi'an University of Electronic Science and Technology, 2021. DOI: 10.27389/d.cnki. gxadu.2021.003547

[7] Wang Jiamin Privacy Protection Scheme for Cloud Resource Auction Based on SGX [D]. Xi'an University of Electronic Science and Technology, 2020. DOI: 10.27389/dcnki. gxadu.2020.001887

[8] Sun Si Design and Implementation of a Privacy Protection Scheme for Face Recognition Based on SGX [D]. Guangzhou University, 2018

[9] Wang Jinwen, Jiang Yong, Li Qi, Yang Yuan Overview of SGX Technology Application Research [J]. Network New Media Technology, 2017,6 (05): 3-9

[10] Haonan Sun; Rongyu He; Yong Zhang; Ruiyun Wang; Wai Hung Ip; Kai Leung Yung; "ETPM: A Trusted Cloud Platform Enclave TPM Scheme Based On Intel SGX Technology", SENSORS (BASEL, SWITZERLAND), 2018. (IF: 3)

[11] Roland Kunkel; Do Le Quoc; Franz Gregor; Sergei Arnautov; Pramod Bhatotia; Christof Fetzer; "TensorSCONE: A Secure TensorFlow Framework Using Intel SGX", ARXIV-CS.CR, 2019. (IF: 3)

[12] Pengfei Wu; Qingni Shen; R. Deng; Ximeng Liu; Yinghui Zhang; Zhonghai Wu; "ObliDC: An SGX-based Oblivious Distributed Computing Framework with Formal Proof", PROCEEDINGS OF THE 2019 ACM ASIA CONFERENCE ON COMPUTER AND ..., 2019.

[13] Anter Faree; Yongzhi Wang; "Protecting Security-Sensitive Data Using Program Transformation and Intel SGX", 2019 INTERNATIONAL CONFERENCE ON NETWORKING AND NETWORK ..., 2019.

[14] Ishtiaq Ahmed; Saeid Mofrad; Shiyong Lu; Changxin Bai; Fengwei Zhang; Dunren Che; "SEED: Confidential Big Data Workflow Scheduling with Intel SGX Under Deadline Constraints", 2020 IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING ..., 2020.

[15] Zhongqiu Zhang; "Design and Implementation of High-performance Cloud Computing System", 2020 INTERNATIONAL CONFERENCE ON BIG DATA AND ..., 2020.

[16] Yarong Lv; "Analysis of Cloud Computing Security Based on SGX Enhanced National Secret Algorithm", 2021 IEEE ASIA-PACIFIC CONFERENCE ON IMAGE PROCESSING, ..., 2021.

[17] Anter Abdu Alhag Ali Faree; Yongzhi Wang; "Protecting Security-Sensitive Data Using Program Transformation and Trusted Execution Environment", 2021.

[18] Wenxiu Ding; Wei Sun; Zheng Yan; Robert H. Deng; "An Efficient and Secure Scheme of Verifiable Computation for Intel SGX", ARXIV-CS.CR, 2021.

[19] Tsu-Yang Wu; Liyang Wang; Xinglan Guo; Yeh-Cheng Chen; S. Chu; "SAKAP: SGX-Based Authentication Key Agreement Protocol in IoT-Enabled Cloud Computing", SUSTAINABILITY, 2022.

[20] Dalton Cézane Gomes Valadares; Matteus Sthefano Leite da Silva; Andrey Elísio Monteiro Brito; Ewerton Monteiro Salvador; "Achieving Data Dissemination With Security Using FIWARE And Intel Software Guard Extensions (SGX)", ARXIV-CS.CR, 2018. (IF: 3)

[21] Do Le Quoc; Franz Gregor; Jatinder Singh; Christof Fetzer; "SGX-PySpark: Secure Distributed Data Analytics", WWW, 2019. (IF: 3)

[22] Pengfei Wu; Qingni Shen; R. Deng; Ximeng Liu; Yinghui Zhang; Zhonghai Wu; "ObliDC: An SGX-based Oblivious Distributed Computing Framework with Formal Proof", PROCEEDINGS OF THE 2019 ACM ASIA CONFERENCE ON COMPUTER AND ..., 2019.

[23] Anter Faree; Yongzhi Wang; "Protecting Security-Sensitive Data Using Program Transformation and Intel SGX", 2019 INTERNATIONAL CONFERENCE ON NETWORKING AND NETWORK ..., 2019.

[24] Joao Guerreiro; Rui Moura; João Nuno Silva; "TEEnder: SGX Enclave Migration Using HSMs", COMPUT. SECUR., 2020.

[25] Qasmaoui Youssef; Maleh Yassine; Abdelkrim Haqiq; "Secure Software Defined Networks Controller Storage Using Intel Software Guard Extensions", INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND ..., 2020.

[26] Anter Abdu Alhag Ali Faree; Yongzhi Wang; "Protecting Security-Sensitive Data Using Program Transformation and Trusted Execution Environment", 2021.

[27] Munan Yuan; Xiaofeng Li; Xiru Li; Haibo Tan; Jinlin Xu; "Trust Hardware Based Secured Privacy Preserving Computation System for Three-Dimensional Data", ELECTRONICS, 2021.

[28] Tsu-Yang Wu; Liyang Wang; Xinglan Guo; Yeh-Cheng Chen; S. Chu; "SAKAP: SGX-Based Authentication Key Agreement Protocol in IoT-Enabled Cloud Computing", SUSTAINABILITY, 2022.

[29] Shaohua Li; Kaiping Xue; "SecGrid: A Secure And Efficient SGX-enabled Smart Grid System With Rich Functionalities", ARXIV-CS.CR, 2018. (IF: 3)

[30] Ferdinand Brasser; David Gens; Patrick Jauernig; Ahmad-Reza Sadeghi; Emmanuel Stapf; "SANCTUARY: ARMing TrustZone with User-space Enclaves", PROCEEDINGS 2019 NETWORK AND DISTRIBUTED SYSTEM SECURITY ..., 2019. (IF: 4)

[31] Roland Kunkel; Do Le Quoc; Franz Gregor; Sergei Arnautov; Pramod Bhatotia; Christof Fetzer; "TensorSCONE: A Secure

TensorFlow Framework Using Intel SGX", ARXIV-CS.CR, 2019. (IF: 3)
[32] Juan Wang; Shirong Hao; Yi Li; Zhi Hong; Fei Yan; Bo Zhao; Jing Ma; Huanguo Zhang; "TVIDS: Trusted Virtual IDS with SGX", CHINA COMMUNICATIONS, 2019.
[33] Franz Ferdinand Brasser; "Enclave Computing Paradigm: Hardware-assisted Security Architectures & Applications", 2020.
[34] Hongliang Liang; Mingyu Li; Yixiu Chen; Lin Jiang; Zhuosi Xie; Tianqi Yang; "Establishing Trusted I/O Paths for SGX Client Systems With Aurora", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2020. (IF: 3)
[35] Qasmaoui Youssef; Maleh Yassine; Abdelkrim Haqiq; "Secure Software Defined Networks Controller Storage Using Intel Software Guard Extensions", INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND ..., 2020.