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