Chapter 37

A Reliable Data Provenance and Privacy Preservation Architecture for Business-Driven Cyber-Physical Systems Using Blockchain

Xueping Liang
https://orcid.org/0000-0002-8764-9966
Institute of Information Engineering, Chinese Academy of Sciences, China & School of Cyber Security, University of Chinese Academy of Sciences, China & Old Dominion University, USA

Sachin Shetty
Old Dominion University, USA

Deepak K. Tosh
Department of Computer Science, University of Texas at El Paso, USA

Juan Zhao
Tennessee State University, USA

Danyi Li
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Jihong Liu
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

ABSTRACT

Cyber-physical systems (CPS) including power systems, transportation, industrial control systems, etc. support both advanced control and communications among system components. Frequent data operations could introduce random failures and malicious attacks or even bring down the whole system. The dependency on a central authority increases the risk of single point of failure. To establish an immutable data provenance scheme for CPS, the authors adopt blockchain and propose a decentralized architecture to assure data integrity. In business-driven CPS, end users are required to share their personal information with multiple third parties. To prevent data leakage and preserve user privacy, the authors isolate and feed different information retrieval requests using tokens specifically generated for each type of request. Providing both traceability of data operations, and unlinkability of end user activities, a robust blockchain-based CPS is prototyped. Evaluation indicates the architecture is capable of assured data provenance validation and user privacy preservation at a low overhead.

DOI: 10.4018/978-1-7998-2466-4.ch037

1. INTRODUCTION

Typical Cyber-Physical Systems (CPS) connect physical infrastructure to integrated computing devices and data storage facilities, with a combination of computation, communication and control. CPS are increasingly deployed in military, electrical and medical systems, as well as logistics or industrial production processes. However, due to system unstability and existing vulnerabilities in the heterogeneous subsystems, the control system may be faced with random system failures or even malicious cyber attacks. Meanwhile, end users of the CPS could be encountered with potential privacy concerns. Recent research (Han, Shah, Luk, & Perrig, 2007) indicates that the collected data of indoor humidity could reveal user activities, thus becoming a data leakage point, which could significantly raise privacy concerns for end users. It is also reported (Grid, 2010) that the smart meter can collect data from Home Area Network (HAN) to reveal home smart appliances, making end user privacy at high risks.

The distributed ledger which is being used by cryptocurrencies like Bitcoin (Nakamoto, 2008) and (Wood, 2014), is a decentralized architecture running among distributed and untrusted network nodes with cryptography algorithm and consensus mechanism, providing traceability and data protection for each transaction witnessed by participating nodes. Blockchain is one implementation of distributed ledger where a chain of blocks are generated from transactions between nodes. The adoption of blockchain in CPS is rarely studied but is quite promising. Due to the decentralized architecture of blockchain and the removal of trust among distributed nodes, the robustness of CPS can be improved with the redundancy capability achieved by the distributed copies maintained by every single node. Blockchain based data provenance is proposed (Liang et al., 2017) to preserve the integrity of data generated from communication and control procedures, with the capability to defend against deception attacks (Shirey, 2007).

According to the framework for CPS (Griffor, Greer, Wollman, & Burns, 2017) issued by the US National Institute of Standards and Technology (NIST), cybersecurity for CPS must address how a system can continue to function correctly when under attack, provide mechanisms that support fault-tolerance with mission- or business-driven priorities, and enable the system to fail-safe. Those requirements indicate the urgency of developing a survivable and reliable CPS. Modern power grid system, namely smart grid, is proposed in many countries to realize a reliable, scalable, manageable, extensible, secure, interoperable and cost-effective electric cyber-physical infrastructure (Khaitan & McCalley, 2013). A typical smart grid system consists of power generation, transmission, distribution and consumption domains and we aim to address the reliability and privacy preservation issues in these domains. Specifically, we focus on business-driven situations and adopt blockchain to design a reliable power delivery (in generation, transmission and distribution domain) provenance and privacy preserving user interface (in consumption domain especially in HAN), as a step towards a fully survivable architecture. However, to facilate CPS with blockchain architecture, several critical issues need be solved. We identify the concerns regarding the integration of blockchain with CPS and then propose a solution to fulfill the objectives of reliability and privacy protection. In this paper, we use power system as a sample CPS to illustrate how blockchain can be utilized in such environment. Most importantly, we implement a blockchain based power supply chain data provenance architecture for power delivery, and privacy protection scheme to prevent sensitive personal data leakage. Performance evaluation indicates that the proposed architecture achieves the above objectives at a low overhead with security guarantee.

Related Content

What We Know and What Else We Need to Do to Address the Problem of Violent Extremism Online: Concluding Chapter

Majeed Khader (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1618-1628).*

www.irma-international.org/chapter/what-we-know-and-what-else-we-need-to-do-to-address-the-problem-of-violent-extremism-online/251514

A White Hat Study of a Nation's Publicly Accessible Critical Digital Infrastructure and a Way Forward

Timo Kiravuo, Seppo Tiilikainen, Mikko Säreläand Jukka Manner (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1672-1685).*

www.irma-international.org/chapter/a-white-hat-study-of-a-nations-publicly-accessible-critical-digital-infrastructure-and-a-way-forward/251517

Using an Ontology for Network Attack Planning

Renier van Heerden, Peter Chan, Louise Leenenand Jacques Theron (2016). *International Journal of Cyber Warfare and Terrorism (pp. 65-78).*

www.irma-international.org/article/using-an-ontology-for-network-attack-planning/159885

A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications

Gaganjot Kaur Saini, Malka N. Halgamuge, Pallavi Sharmaand James Stephen Purkis (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 98-126).*

www.irma-international.org/chapter/a-review-on-cyberattacks/251420

The Role of Human Operators' Suspicion in the Detection of Cyber Attacks

Leanne Hirshfield, Philip Bobko, Alex J. Barelka, Mark R. Costa, Gregory J. Funke, Vincent F. Mancuso, Victor Finomoreand Benjamin A. Knott (2015). *International Journal of Cyber Warfare and Terrorism (pp. 28-44).*

www.irma-international.org/article/the-role-of-human-operators-suspicion-in-the-detection-of-cyber-attacks/141225