DOI: 10.1002/ett.????

Editorial: Security of Cloud Service for the Manufacturing Industry

With the rapid development of the industrial Internet, cloud service based manufacturing has emerged as a next generation manufacturing paradigm that has potential to revolutionize the manufacturing industry. It is foreseeable that cloud services will be popular in the next generation manufacturing industry. In recent years, more and more manufacturing companies have recognized the benefits of cloud service and have developed cloud based manufacturing models. However, the security problems need be researched and solved for the cloud services in the manufacturing industry, especially the data security issues are important, and restrict the cloud application in the manufacturing industry. Regarding the security of data, some people believe that when data is stored in the cloud, manufacturing companies lose control of the data. The manufacturing companies focus on how to secure the data from the top-level management and how to minimize the security risks, such as those caused by data security or service migration challenges. The manufacturing companies select the reliable cloud service while consider function and budget feasibility. How to ensure security in cloud service for the manufacturing industry has become a topic of increasing interest for both academic researchers and developers from the industry. This special issue addresses this emerging and fast developing research area on cloud security in manufacturing industry. The summary of these papers is as follows.

This paper "Probabilistic Analysis of Security Attacks in Cloud Environment using Hidden Markov Models" presents an effective threat modeling approach that has the ability to predict and detect the probability of occurrence of various security threats and attacks within the cloud environment using Hidden Markov Models. The model is trained to identify anomalous sequences or threats so that accurate and up-to-date information on risk exposure of cloud-hosted services are properly detected. Practically, it acts as an underlying framework and a guiding tool for cloud systems security experts and administrators to secure processes and services over the cloud.

The paper "Public key encryption with equality test for Industrial Internet of Things system in cloud computing" presents a Public Key Encryption with Equality Test based on DLP with double decomposition problems over near-ring. The proposed method solves the problem of quantum algorithm attacks in IIoT systems.

The paper "Secure Smart Contracts for Cloud Based Manufacturing using Ethereum Blockchain" demonstrates a use case exemplar of blockchain on securing the supply chain and logistics on international trade. The blockchain framework demonstrates that fraud scenarios in traditional supply chain operations could be avoided. Additionally, lack of coordination between entities involved in the logistics, centralized decision making, data unavailability, and lack of non-repudiation are other issues tackled using the proposed framework.

The paper "Integrating encryption techniques for secure data storage in the cloud" offers insights into the implementation of a novel architecture that can deliver an enhanced degree of security for outsourcing information from the cloud. This is vital when involving numerous independent cloud storage providers. The framework presented is made up of dual encryption and data fragmentation techniques that envision the secure distribution of information in a multi-cloud environment.

The paper "Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment" manages user access rights in a decentralized environment using smart contracts on the blockchain. Logs of access rights, the change process, and requests can be managed in the block network. Distributed environments can enhance integrity through distributed records and verification of records.

The paper "TamForen: A tamper-proof cloud forensic framework" introduces a new Cloud Forensics Tamper-Proof Framework for cloud forensics, which can be used in an untrusted and multi-tenancy cloud environment. This framework takes into account the untrustworthiness of participants in the forensics process and conducts tamper-proof protection of data in a decentralized way without violating users' privacy.

The paper "A permission-combination scalable access control model for Internet of Things" proposes a

https://doi.org/10.1002/ett.????

permission-combination scalable access control (PCS-AC) scheme, in which the methods of access permissions assignment, data encryption and data access are given. PCS-AC is proven secure under the hardness assumption of Discrete Logarithm (DLP) problem and Inverse Computational Diffe-Hellman (ICDH) problem.

The paper "MobiScan: An Enhanced Invisible Screen-camera Communication System for IoT applications" proposes a dynamic and invisible screen-to camera communication system that is able to ensure data security, real-time communication, and flexible capture angle.

The paper "Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry" analyses the benefits of implementing customized ML and Deep Learning (DL) techniques on the core of the operating system than application level services, which in effect increases the speed and correctness of attack detection. The kernel space security activities can be improved by proposed work where the process level attributes classified using ML and DL techniques. The cloud service helps in sharing of the kernel abilities of the system ensuring core level security. This technique finds application in manufacturing domain where the systems are protected from the various attacks to secure the data of the manufacturing company.

In summary, this special issue can be a useful reference to academia, researchers, and industrial practitioners who are interested in recent relevant advancement. The guest editors are very grateful to the contributing authors, to the dedicated reviewers and to the relevant supporting editorial staff members and especially to the guidance from the Editor-in-Chief to enable the success of this Special Issue.

Xiaochun Cheng
Middlesex University, London, United Kingdom

Zheli Liu
Nankai University, Tianjin, China

Yongsheng Ning
Guilin Power Capacitor Co., Ltd.

Correspondence
Xiaochun Cheng
https://orcid.org/0000-0003-0371-9646
Middlesex University, London, United Kingdom
Email: x.cheng@mdx.ac.uk