Guest Editorial

Krishna Kant Singh*, B. Balamurugan, Naveen Chilamkurti SMIEEE, and
Bharat S. Rawal Kshatriya

Machine Learning approaches for convergence of IoT and Blockchain

<https://doi.org/10.1515/comp-2020-0207>

Received Jul 26, 2020; accepted Jul 29, 2020

Abstract: Blockchain plays a significant role in providing security during data handling operations and defines how trusted transactions can be carried out addressing the solution for internet facing vulnerability problems. Blockchain solves the security fault line among AI and IoT, where most of the IoT devices are connected to each other through public networks. This special issue aims to publish a collection of high quality research articles in the area of blockchain, IoT and Machine Learning.

Keywords: Blockchain, IoT, Machine Learning, Artificial intelligence

1 Introduction

Digital revolution is characterized by the convergence of technologies, rapidly advancing the fourth industrial revolution thereby blurring the lines between physical, digital and biological objects. The speed of the fourth revolution which evolves at an exponential rate cannot by any means be compared with any previous technologies. AI and IoT employ the interactions and operations in various fields such as home appliances, autonomous vehicles, nanotechnology, robotics, cognitive systems, self-driving cars and wearable devices. The potential of blockchain technology is realized in many sectors nowadays as security plays a crucial role everywhere. There is a tremendous increase in the usage of AI and IoT technologies across industries. AI has a big potential to identify the patterns and anomalies in the data generated by IoT sensors. The

accuracy of operational predictions using AI technologies is greater when compared to threshold-based monitoring systems. IoT and connected systems drive AI as intelligent automation which makes sense of data generated from sensor devices in the decision-making process. Blockchain plays a significant role in providing security during data handling operations and defines how trusted transactions can be carried out addressing the vulnerability problems. Blockchain solves the security fault line among AI and IoT where most of the IoT devices are connected to each other through public networks. Linear and permanent indexed records are maintained in blockchain to face the vulnerability issues. Many applications and concepts, common to these technologies, are already in practice with promising results. Gaining control of a device and records in the blockchain system is hard and consequently blocks are maintained and safeguarded. IoT devices are sharing information via public networks which paves the way for vulnerability and the risks increase even more if AI is also involved. Furthermore, the blockchain system has robust security implementations able to afford scalable, secure and verifiable platforms. The peer-to-peer model is a competent solution for the effective communication in centralized client/server paradigm. Blockchain ensures security by using distributed ledger shared amongst the nodes in the network for transactions. Transactions are verified using cryptographic techniques to authenticate and identify the nodes and therefore there is no role for any central authority.

Nowadays, smart IoT medical devices are influenced by AI to make lifesaving decisions using biometric data. In smart vehicle insurance, IoT sensors are fixed in a car and fault may occur in any part of the car. In such a case, AI assists the sensor to detect the fault with the help of data generated by the IoT devices. Incorporating blockchain in these solutions can further increase their security and functionality. For instance, once a sensor detects a fault, the insurance claim can be automatically credited to the user's account. In fact, the convergence of blockchain, AI and IoT will revolutionize the insurance industry. Consider that self-driving trucks are designed with AI technologies to dispatch goods to distribution centres. Self-driving cars

*Corresponding Author: Krishna Kant Singh: Department of ECE, KIET Group of Institutions, Delhi-NCR, Ghaziabad, India; Email: krishnaiitr2011@gmail.com

B. Balamurugan: Galgotias University, India

Naveen Chilamkurti SMIEEE: La Trobe University, Melbourne, Australia

Bharat S. Rawal Kshatriya: Penn State Abington, USA

should be directed to a charging station for automatic charging. Smart contract framework allows the truck to be charged in the charging station after proper authentication and authorization. Ledger issued to record the transaction in the smart contract makes the system more secure which prevents tampering. The goods can be delivered to the customers with the IoT devices which is employed and monitored by retail companies. AI algorithms assess on-site safety management to examine the heat stress levels of workers using IoT sensor devices to measure data such as humidity, temperature etc. This scenario would be complete if workers were insured and the blockchain system implemented for assuring security. The AI algorithm detects heat stress of workers and ensures worker safety, whereas blockchain ensures prompt insurance. All these combined technologies can leverage the power of each other and suggest a way for a platform to be built where data can be generated, processed and secured by making use of the IoT system, AI algorithms and the blockchain technology.

This special issue contains a collection of high quality research articles in the area of blockchain, IoT and Machine Learning. The special issue comprises six high quality research papers. Article [1] presents a proposal for the development of a vehicle guard and alarm system using biometric authentication based on IoT technology. An assistive tool for children with Spectrum Disorder using IoT and emotion recognition techniques is presented in [2]. Another article presents a firefly swarm intelligence algorithm to perform link prediction in social network exploiting the topological and node attribute features [3]. A secure incidence and evidence management framework for Internet of Vehicles using Deep learning and blockchain is presented by the authors in [4]. The work addresses two challenges of predictive modelling for timely warning and secure evidence management for forensics analysis in case of accidents and traffic violations. The system proposes deep learning based predictive incident modelling with Blockchain and CP-ABE based access control on the incident data stored in blockchain. A Registration Authentication Storage Data Access (RASD) structure for giving security to authoritative information stored in cloud catalogues utilizing a novel security plot is presented. The system involves a stage-by-stage process: Enlistment of clients, Authentication of the client secret key, and Capacity of information just as information access on cloud registry. When the system is connected on cloud servers, all the sensitive information stored in the cloud will end up accessible just to the verified clients [5]. Metaheuristic algorithms namely Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) are utilized to tackle QoS based service composition

issues. QoS has turned into a critical issue in the management of web services because of the immense number of services that furnish similar functionality yet with various characteristics. Quality of service in service composition comprises different non-functional factors, for example, service cost, execution time, availability, throughput, and reliability. Choosing appropriate SC for IoT based applications in order to optimize the QoS parameters with the fulfilment of user's necessities has turned into a critical issue [6].

In conclusion, the editors of the special issue would like to extend their thanks to all those who have given significant support in this special issue. Specifically, we would like to thank the contributing authors for their original works in the field, the reviewers for their valuable comments. Also, we would like to thank the Editor-in-chief, the managing editor and other staff members of the Open Computer Science journal.

References

- [1] Elngar A., Kayed M., Vehicle Security Systems using Face Recognition based on Internet of Things, *Open Computer Science*, 2020, 10, 17–29
- [2] Singh A., Dewan S., AutisMitr: Emotion recognition assistive tool for Autistic Children, *Open Computer Science*, 2020, 10, 259–269
- [3] Srilatha P., Manjula R., Topological and Attribute Link Prediction using Firefly algorithm, *Open Computer Science*, 2020, 10, 33–41
- [4] Philip A. O., Saravanaguru R. A. K., Secure Incident & Evidence Management Framework (SIEMF) for Internet of Vehicles using Deep Learning and Blockchain, *Open Computer Science*, 2020, 10, 408–421
- [5] Jain R., Nayyar A., A novel homomorphic RASD framework for secured data access and storage in cloud computing, *Open Computer Science*, 2020, 10, 431–443
- [6] Kashyap N., Kumari A. C., Chhikara R., Service Composition in IoT using Genetic algorithm and Particle swarm optimization, *Open Computer Science*, 2020, 10, 56–64