Guest Editorial Preface

Special Issue on Recent Advances in Blockchain for Secure Software-Defined Networking in Smart Communities

Gunasekaran Manogaran, District University Francisco José de Caldas, Colombia
Ching-Hsien Hsu, Asia University, Taiwan
Qin Xin, University of the Faroe Islands, Denmark

Smart communities, in a broad sense, incorporate technology and data infrastructure to embrace digital innovations with the goal of maximizing the capabilities of existing services and amenities. Security deployments are recognized to be a comprehensive solution to facilitate foundational applications and technology in smart communities, similar to how the smart community itself runs and grows in an integrated environment. In this special issue, we investigated how often these two methods, blockchain and software-defined networking (SDN), could make a contribution to new potential for smart communities, thereby addressing the complicated obstacle of security in the emergence of futuristic societies. The widespread need for SDN might provide fresh opportunities for attackers to get into a system or a network of smart communities. The security breaches in the system are indeed possible in the instance of SDN. As a result, obtaining an adequate safety approach that enables enterprises to function without compromising speed and scalable features is already essential. Since this generates a forensically auditable and immutable log of events whilst creating a security gateway throughout SDN, blockchain-assisted SDN would be an appropriate choice. Although blockchain-enabled SDN might appear far-fetched for protecting smart communities today, it's essential to undertake further studies in this field since it can improve network architecture and boost adaptability for altering perspectives.

This special issue mainly focuses on blockchain-assisted secure software-defined real-time applications in smart communities. Based on the assessment criteria, fifteen papers were accepted for publication in this special issue after the peer-review procedures. The subsequent sections emphasise the significant technological discoveries of the accepted papers:

The first article is "Security in Data Sharing for Blockchain-Intersected IoT Using Novel Chaotic-RSA Encryption" by Priyadharshini K et al. Though IoT connects various equipment and is relatively uncontrolled, tracing the source of any fault is a significant challenge for the network, and the integrity of the blockchain intersected IoT devices is the fundamental threat. As a result, in this paper, the authors suggest a novel encryption technique known as the Chaotic-Rivest-Shamir-Adleman (C-RSA) algorithm. The chaotic systems are coupled with the RSA technique, and their sequences are highly reactive, exhibiting severe unpredictable behavior. This system achieved a maximum average of PSNR with a very low MSE as well as a very large key space.

The second article, by Kimmi Kumari et al., is titled "A Framework for Analysis of Incompleteness and Security Challenges in IoT Big Data." The goal of this research is to examine the effectiveness and incoherence of IoT big data. The MapReduce approach was introduced to address the concerns

and obstacles encountered on a frequent schedule when handling massive amounts of data, since security is a key problem in huge groups. The research in this article could well be classified into four categories: analysis, observation, model development, and evaluating their correctness and efficiency.

The next article, by Anjana S. Chandran, is titled "Review on Cryptography and Network Security Zero Knowledge Technique in Blockchain Technology." In a wireless network, cryptography and network security (NS) help to protect the network and the data transferred over it. As a result, this article demonstrates NS, cryptography, current advances in NS, and Linear Cryptanalysis (LC) in conjunction with Differential Cryptanalysis (DC). All the following: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Blowfish, and 3DES are all evaluated in this article with regard to encryption time (ET) vs file size. Furthermore, RSA, AES, Modified RSA (MRSA), and Nth Degree Truncated Polynomial Ring Units (NTRU) are evaluated with regard to decryption time (DT) vs file size.

The article by Dr. Ramesh S et al. is titled "K-Means Cluster-Based Interference Alignment With Adam Optimizer in Convolutional Neural Networks." This article describes clustering-based interference alignment, including a convolutional neural network, wherein the Adam's Optimizer and K-means clustering are employed for signal optimization and grouping the minuscule cells with the base station, correspondingly. The findings clearly take into consideration the characteristics such as degrees of freedom (DoF), spectral efficiency, energy efficiency, signal to interference noise ratio (SINR), and computational complexity, and demonstrate that the measured values of the proposed technique achieve greater effectiveness.

The fifth article, by Zhiyong Li et al., is titled "Intelligent Recommendation Method of Mobile Wireless Communication Information Based on Speech Recognition Technology Under Strong Multipath Interference." A novel approach to the problem of sparse data is presented here using speech recognition technology under strong multipath interference to develop an intelligent recommender of mobile wireless communication information. Ultimately, the extensive experiments reveal that the suggested technique has a high accuracy rate of prediction and resource diversity, as well as a strong excavation capability and good recommendation effects.

The upcoming article is titled "Content-Based Collaborative Filtering With Predictive Error Reduction-Based CNN Using IPU Model" and is written by Chakka S. V. V. S. N. Murty et al. In order to overcome the shortcomings of collaborative filtering-based techniques, this research proposes a unique deep learning-based error prediction system, as well as CF-based user-item interactions. The incentivized/penalized user-based content-based collaborative filtering (IPU-CBCF) approach was devised for acquiring low-dimensional vectors of individuals and objects independently. The experimental outcomes showed that IPU-CBCF utilizing PER-CNN outperformed the conventional methods with all performance indicators.

The seventh article, by Kusuma S M et al., is title "A Novel Chaotic Shark Smell Optimization With LSTM for Spatio-Temporal Analytics in Clustered WSN." This article discusses the CSSO-LSTM methodology for spatiotemporal analytics in clustered WSN, which integrates chaotic shark smell optimization (CSSO) and long short-term memory (LSTM). Initially, a CSSO-based clustering technique is inferred, and the CSSO algorithm generates an objective function representing multiple input variables to choose cluster heads (CHs) and build clusters.

The forthcoming article, by Abhijit Biswas et al., is titled "Interference Cancellation and Efficient Channel Allocation for Primary and Secondary Users Using Hybrid Cognitive (M2M) Mac Routing Protocol." The purpose of this study is to demonstrate the importance of the cognitive Medium Access Control (MAC) protocol, with an emphasis on the unique properties of M2M devices and the demands of smart grid communications. This study investigates MAC layer sensing methodologies in cognitive radio networks using both proactive and reactive sensing.

The ninth article, by Leelalakshmi S et al., is titled "Traffic Monitoring and Malicious Detection Multidimensional PCAP Data Using Optimized LSTM RNN." For recognising hazardous traffic, intrusion detection systems (IDSs) and network security assessments employ deep learning approaches

with certain advancements, including Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM). If hazardous traffic recognition at the packet level was performed initially, a substantial decrement in detection time arises, thereby assuring digital real-time malicious traffic identification relies on deep learning algorithms as a potential solution.

The tenth article, by Santhoshkumar K et al., is titled "An Energy-Aware Data Aggregation in Wireless Sensor Network Using Hybrid Multi-Verse-Optimized Connected Dominant Set." This research outlines the Multi-hop Low-Energy Adaptive Clustering Hierarchy (M-LEACH) protocol for Wireless Sensor Networks (WSNs). Due to the lack of centralised management or fixed infrastructure for the WSN, it's possible that there's a Connected Dominating Set (CDS) that operates as a virtual backbone to facilitate better connections and routing.

The eleventh article, by Bin Fang, is titled "Blockchain-Based Educational Management and Secure Software-Defined Networking in Smart Communities." In software-defined networking (SDN), this analysis offers a simple and energy-efficient blockchain clustering method for selecting the required cluster head. The Particle Swarm Algorithm-Educational Management Resources (PSA-EMR) approach enhances the teaching team's precision and effectiveness, and a cost-effective digital architecture for gathering and delivering high-quality instructional information has been established.

The next article, by Feilu Hang et al., is titled "Information Security Situation in Blockchain for Secure SDN-Based on Big Data in Smart Communities: Research on Information Security Situation Awareness Based on Big Data and Artificial Intelligence." This article describes an IoT-assisted Information Security Situation Awareness Framework (IoT-ISSAF) that can be used to optimise IoT security monitoring, emergency response, and forecasting prospects. The simulation demonstrated the software-defined network model's ability to appropriately evaluate the existing level of network security in blockchain.

The thirteenth article, by Jintao Chen et al., is titled "Prediction Method of Electric Energy Metering Device Based on Software-Defined Networking." This paper describes a unique Deep Learning-based Smart Energy Metering Prediction (DL-SEMP) approach towards narrowing the prediction accuracy discrepancy. In blockchain technology, a Blockchain-based Software-defined Network has been constructed as a potential architecture for generating a distributed network system.

The fourteenth article, by Xiang Ma et al., is titled "Balanced Scheduling Method of Network Information Resources for Cloud Storage: Cloud Storage." This report provides a strategy for allocating network information resources that is balanced for cloud storage. The test findings reveal that the network information resource balanced scheduling approach for cloud storage requires less time as well as less expense to accomplish, which completely fits the study objectives.

The final article, by Kalluri Rama Krishna et al., is titled "ETP-AKEP-Enhanced Three Party Authenticated Key Exchange Protocols for Data Integrity in Cloud Environments." This work describes an enhanced three-party authenticated key exchange protocol (ETP-AKE) which doesn't rely on symmetric key encryption but rather employs asymmetric key encryption. The devised ETP-AKE protocol utilizes elliptic curve encryption in combination with a one-way hash function to guard against multiple security risks.

We congratulate all researchers and supervisors for their timely and fruitful cooperation. We are grateful to the journal's Editor-in-Chief for allowing us to run a special issue of this renowned journal. We believe that this special issue will be immensely valuable to the academic community.

Gunasekaran Manogaran
District University Francisco José de Caldas, Colombia
Ching-Hsien Hsu
Asia University, Taiwan
Qin Xin
University of the Faroe Islands, Denmark