Journal of Ambient Intelligence and Smart Environments 13 (2021) 183–184
DOI 10.3233/AIS-210597
IOS Press

## Guest Editorial

# Trustworthy computing for secure smart cities

Wathiq Mansoor [a] and Vijayakumar Varadarajan [b]

[a] *University Of Dubai, United Arab Emirates*

[b] *University of New South Wales, Australia*

Supporting smart services are expected to become the characteristic of all cities in the world. This brings with it a number of security challenges as breaching security might have a devastating impact on citizen and city infrastructure. This thematic issue on trustworthy computing for secure smart cities attempts to shed light on the latest research trends on the improvement of smart city security using trustworthy computing methods and techniques. We hope that researchers will benefit from the papers in this issue and find more motivation to pay attention to this important need.

We gratefully thank all the reviewers for their work in providing evaluations and constructive comments. We would also like to thank all authors for their contributions to this thematic issue. Finally, we are grateful to JAISE editors for supporting this thematic issue.

The paper "**Multi-criteria decision making-based optimum virtual machine selection technique for smart cloud environment**" by Singh et al. analyses the performance efficiency of the data centre with and without job request consolidation. A technique for determining the order of preferences was proposed using similarity to the ideal solution-based virtual machine selection algorithm, which was able to select the best VM using parameters such as the provisioned or available capacity, and memory, as well as the state of the machine.

In the paper entitled "**DDoS prevention architecture using anomaly detection in Fog-empowered networks**" by Sharma et al., the authors propose a lightweight and robust framework for DDoS attack detection and prevention using mathematical models for detecting anomalies in the behaviour of Fog devices connected to the Fog node. The proposed approach is an efficient algorithm to identify and handle DDoS causing devices on a network by identifying the rogue node.

The paper "**M2FBalancer: A mist-assisted Fog computing-based load balancing strategy for smart cities**" by Tripathy et al. implements an optimization strategy applying a dynamic resource allocation method based on a genetic algorithm and reinforcement learning in combination with a load balancing procedure. The proposed model comprises four layers, namely the IoT layer, the Mist layer, the Fog layer, and the Cloud layer. The authors propose a load balancing technique called M2F balancer which regulates the traffic in the network incessantly, accumulates the information about each server load, transfers the incoming query, and disseminates them among accessible servers equally using a dynamic resource allocation method. To validate the efficacy of the proposed algorithm, resource utilization and the degree of imbalance (DOI) are considered as the scheduling parameters. The proposed method is compared with the least count, round robin, and weighted round-robin methods. The results demonstrate that the proposed solution enhances the QoS in the mist-assisted cloud environment concerning maximization resource utilization and minimizing the makespan, and hence serves as an effective method to utilize the resources efficiently while ensuring uninterrupted service.

In the paper "**A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities**" by Qureshi et al., the authors propose a trust evaluation model for smart grids (TEMSG) for secure data aggregation in smart grids and smart cities. This model tackles privacy and security issues such as data theft, denial of service, data privacy, inside and outside attacks, and malware attacks. Machine learning methods are used to gather

1876-1364/$35.00 © 2021 – IOS Press. All rights reserved.

trust values and then estimate the imprecise information to secure data aggregation in smart grids. Experiments are conducted to evaluate and analyse the proposed model in terms of detection rate, trustworthiness, and accuracy.

Finally, in the paper "**Smart contracts for automated control system in Blockchain-based smart cities**" by Pradhan and Singhre, a system design approach has been proposed for decentralized applications in smart cities which enables systems to share data without an intermediary between trusted and non-trusted stakeholders using self-executing contracts. Such contracts allow automated multi-step workflows for smart applications. Two use cases have been considered, namely smart healthcare and smart building monitoring. The performance of the proposed scheme for these use cases has been presented with the Keccack 256 transaction hash, the total number of transactions, and gas consumed by each contract. Such an attempt is a worthwhile addition to the state-of-the-art as evident from the results presented herein. The model's simulation and analysis of hashing power shows that for hashing power $>$ 55% the probability of double spending attack reaches a maximum of 42%. So it is concluded that the probability of double spending increases with an increase of transaction values.

## Acknowledgements

Wathiq Mansoor wishes to express his gratitude to the University of Dubai for supporting faculty to contribute to international research collaborations.