A Formal Model-Based Testing Framework for Validating an IoT Solution for Blockchain-based Vehicles Communication

Rateb Jabbar, Moez Krichen, Mohamed Kharbeche, Noora Fetais, Kamel Barkaoui

A Formal Model-Based Testing Framework for Validating an IoT Solution for Blockchain-based Vehicles Communication

Rateb Jabbar[1,2], Moez Krichen[3], Mohamed Kharbeche[4], Noora Fetais[1] and Kamel Barkaoui[2]
[1]*KINDI Center for Computing Research, College of Engineering, Qatar University, Doha, Qatar*
[2]*Cedric Laboratory, Computer Science Department, Conservatoire National des Arts et Metiers, France*
[3]*ReDCAD Laboratory, University of Sfax, Tunisia*
[4]*Qatar Transportation and Traffic Safety Center, Qatar University, Qatar*

Keywords: Blockchain, Automotive Communication, Internet of Vehicles, Model-Based Testing, Timed Automaton, Security, Attack Trees.

Abstract: The emergence of embedded and connected smart technologies, systems, and devices has enabled the concept of smart cities by connecting every "thing" to the Internet and in particular in transportation through the Internet of Vehicles (IoV). The main purpose of IoV is to prevent fatal crashes by resolving traffic and road safety problems. Nevertheless, it is paramount to ensure secure and accurate transmission and recording of data in "Vehicle-to-Vehicle" (V2V) and "Vehicle-to-Infrastructure" (V2I) communication. To improve "Vehicle-to-Everything" (V2X) communication, this work uses Blockchain technology for developing a Blockchain-based IoT system aimed at establishing secure communication and developing a fully decentralized cloud computing platform. Moreover, the authors propose a model-based framework to validate the proposed approach. This framework is mainly based on the use of the Attack Trees (AT) and timed automaton (TA) formalisms in order to test the functional, load and security aspects. An optimization phase for testers placement inspired by fog computing is proposed as well.

1 INTRODUCTION

The modern IoT technologies have profoundly transformed classical "vehicular ad-hoc networks" (VANETs) into the "Internet of Vehicles" (IoV) (F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, 2014). More precisely, the IoV is defined as the real-time data interaction between vehicles and between vehicles and infrastructures through information platforms, mobile communication technology, smart terminal devices and vehicle navigation systems. Vehicles are incorporated into the IoT by being connected to the Internet, to the other vehicles nearby as well as to traffic information systems. Yet, there are many challenges related to this concept due to high connectivity and exchange of sensitive data, compromising of security and privacy and leave the vehicles susceptible to malicious entities.

The proposed Decentralized IoT Solution for Vehicle communication (DISV) based on the concept of Blockchain aims at overcoming security and privacy challenges. By way of explanation, each member of the IoV networks receives messages and broadcasts them to the Blockchain server, whereas the server verifies the received block and decides if it should be added to the smart contract or not.

In order to validate the adopted solution, we propose, in addition, a "model-based testing" (MBT) (Krichen, 2018; Krichen, 2012; Krichen, 2007; Krichen and Tripakis, 2006) framework which allows to check the functional correctness, load and security aspects. This framework is mainly based on the model of Timed Automata (Bertrand et al., 2015; Bertrand et al., 2011). The latter corresponds to a rich modelling language which allows to describe the behaviors of a large class of distributed, dynamic and real-time systems.

Regarding security aspects testing, we model the behavior of the attacker using Attack Trees (AT) (Krichen and Alroobaea, 2019; Kordy et al., 2014). The root of the AT corresponds to the attacker's global goal. Internal nodes correspond to sub-goals and leaves correspond to "Basic Attack Steps" (BAS). Each AT is then transformed into a collection of Timed Automata from which test scenarios are extracted using test generation algorithms inspired

Jabbar, R., Krichen, M., Kharbeche, M., Fetais, N. and Barkaoui, K.
A Formal Model-Based Testing Framework for Validating an IoT Solution for Blockchain-based Vehicles Communication.
DOI: 10.5220/0009594305950602
In *Proceedings of the 15th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2020)*, pages 595-602
ISBN: 978-989-758-421-3

by the works of (Krichen, 2012; Tretmans, 1999).

Besides, we propose an approach for the optimization of the testers placement procedure inspired by fog computing approaches (Taneja and Davy, 2017; Gu et al., 2017; Mahmud et al., 2018; Barcelo et al., 2016) and by some of our previous contributions (Maâlej et al., 2018; Lahami et al., 2016; Lahami et al., 2012b). This placement procedure consists in allocating the set of testers on the different computational nodes of the system under test in an optimal way under different kind of constraints.

The remainder of this article is structured as follows. In section 2, an overview about Blockchain, Model Based Testing (MBT) and Timed Automata is presented. Section 3 is dedicated for reviewing several Blockchain techniques to IoT and practically for IoV. The design of the proposed solution is presented in Section 4. In Section 5, we present several details about the adopted testing framework. Section 6 is dedicated for the testers placement optimization problem. Finally, Section 7 summarizes the main finding and gives new directions for future research.

2 PRELIMINARIES

2.1 Blockchain

Blockchain has emerged through Bitcoin, introduced in 2008 by Satoshi Nakamoto. Bitcoin can be defined as a decentralized global currency cryptosystem. Blockchain employed in Bitcoin allows the use of secure and decentralized digital money in a payment system. This peer-to-peer network does not possess a central authority, and as such is powered entirely by the users. Its computing architecture is distributed and all the transactions are publicly announced. Thus, the users have a consensus about a single history of the transactions, referred to as a ledger. The transactions are separated into blocks; subsequently, each user receives a timestamp and then it will be published. It is challenging to modify published blocks as the hash of the previous blocks is inserted in the next successors in each block of the chain.

2.2 Model-Based Testing

Model-Based Testing (MBT) (Krichen, 2018; Krichen, 2010; Krichen, 2007; Krichen and Tripakis, 2006) is a methodology where the system of interest is described by a mathematical model which encodes the behavior of the considered system. This methodology consists in using this mathematical model to compute abstract test scenarios. These sequences of model are then transformed into concrete test sequences which are executed on the considered "System Under Test" (SUT). The verdict of this testing activity is provided by comparing the observed outputs from the system with the outputs generated by the model.

2.3 Timed Automata

"Timed Automata" (TA) (Bertrand et al., 2015; Bertrand et al., 2011) are an expressive and simple tool for describing the behavior of computer systems which combine continuous and discrete mechanisms. TA may be represented as finite graphs enriched with a finite set of clocks defined as real entities whose value progresses continuously over time.

3 RELATED WORKS

(X. Huang and Liu, 2018) developed an ecosystem model on the basis of Blockchain electric vehicle and charging pile management. This model employs Elliptic Curve Cryptography (ECC) for the computation of hash functions of charging piles of electric vehicles. Furthermore, (J. Kang and Hossain, 2017) developed PETCON, a P2P electricity-trading system, for illustrating localized and comprehensive operations of P2P electricity trading. The PETCON system employs a consortium Blockchain method to analyze, verify, and share transaction records publicly, while it is not necessary to have a reliable authority.

Besides, CreditCoin, a privacy-preserving scheme, was created by (L. Li and Zhang, 2018) in order to ensure that adequate announcements are forwarded without revealing users' identities. This scheme employs the Blockchain for sending anonymous announcements through an aggregation protocol between vehicles. Moreover, (Z. Yang and Leung, 2017) proposed a Blockchain-based reputation system to assess data credibility in the IoV. (Y. Yuan and FY. Wang., 2016) developed a Blockchain solution aimed at solving security problems and performance limitations in Intelligent Transportation Systems (ITS). (Leiding and Hogrefe., 2016) merged the Blockchain technology with vehicular ad-hoc network VANET.

(A. Lei and Sun, 2017) introduced dynamic key management using Blockchain for establishing communication systems to be used in vehicles that do not need the administration from the central manager. By relying on a decentralized Blockchain structure, it eliminates any other authorities. (A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak,

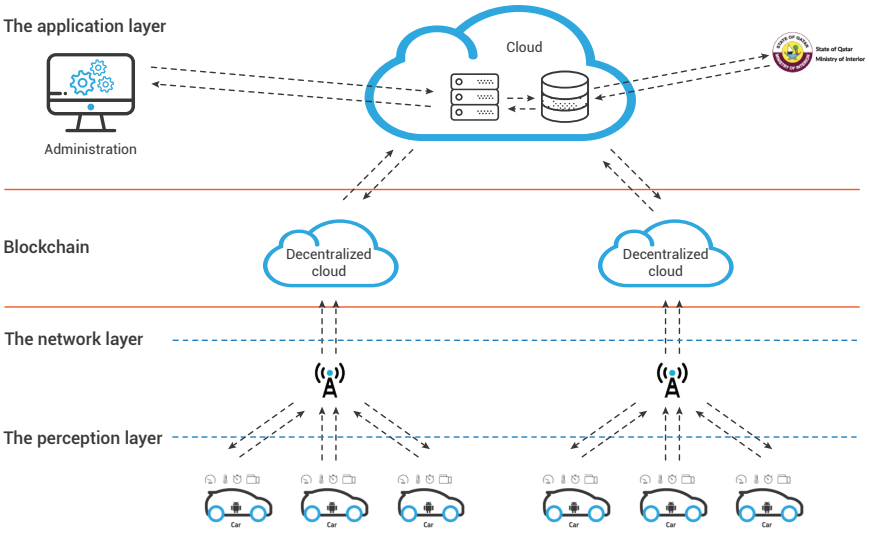

Figure 1: The architecture of the proposed Internet of Things solution.

2017) created a Blockchain technology mechanism that does not reveal any private data of vehicle users. (Sean Rowan and Goldrick, 2017) employed the visible light and acoustic side channels and applied the Blockchain technology for securing intelligent vehicle communication. (Madhusudan Singh, 2017) developed a framework for a secure trust-based environment with peer-to-peer communication between intelligent vehicles without disturbing/interfering other intelligent vehicles through the Blockchain mechanism for the intelligent vehicle communication environment. However, the use of this framework is limited only to smart cars.

4 PROPOSED SOLUTION

The adopted architecture is composed of three layers. Figure 1 depicts the architecture of the proposed solution.

4.1 The Perception Layer

In order to test possible scenarios involving various components, an Android application has been developed in the Internet of Vehicle system (AV) and for infrastructure (AP). On the first hand, AV is an Android application consisting of two sub-systems. The first subsystem is the Vehicle Data Collection System (VDCS) which collects data about the trip and the car. The second one is the Driver Drowsiness Detection system that collects data about the driver's behavior to identify if he or she is drowsy or not. More information about this system can be found in (Jabbar et al., 2018a; Jabbar et al., 2018b; Jabbar et al., 2019; Jabbar et al., 2020).

Mainly, the Android application has four pages as shown in Figure 2: The first page serves for logging in by using a username and password. Following the authentication, the user can start a new trip, or access the information about the last five trips on the second page. If the user chooses a new trip, the application will start recording and displaying all information as described in the previous section. Then, it will send the collected data via the web service to the cloud server. In the fourth page, the front camera will capture and display the driver's face.

4.2 The Network Layer

The network layer establishes the connection between the servers and transmits, and processes the sensor data. The application can use either Wi-Fi or mobile internet (3G/3G+/4G) to send the data to the server.

This collection process uses the hybrid system to gather and save data locally before transmitting it to the server. This technique has been proven to be highly effective for data collection when the internet connection is poor or unstable.

4.3 The Application Layer

Regarding the application layer, it contains two principal compounds: Central cloud server and the communication system using a Blockchain Network. First, the central cloud server delivers application-specific services to the end-user. It sends the collected data to the web services for processing and analy-

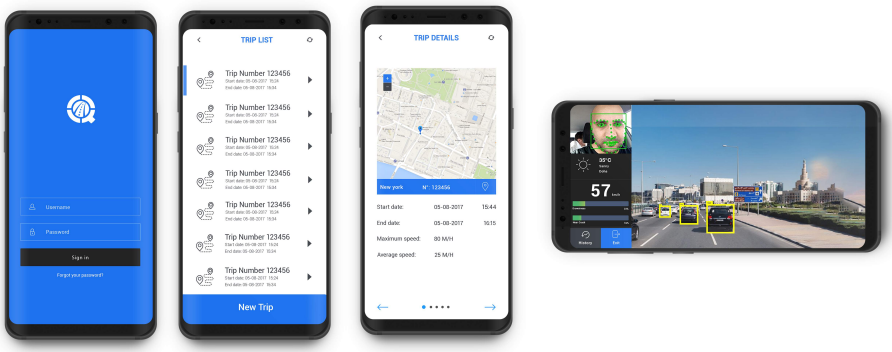

Figure 2: Screenshot of the four main pages of the Android application for Vehicles (AV).

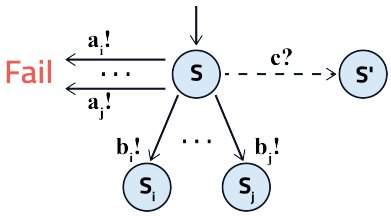

Figure 3: Test generation principle.

sis before showing them to the end-user. Second, the Blockchain network is responsible for managing communication between cars and traffic and transportation systems. Every time slot, the car sends the collected data to the central server via a web service, including the current location and the status of the connection to one of the existing Blockchain servers.

5 TESTING FRAMEWORK

5.1 Test Generation Principle

Our generation procedure is inspired by the work of (Tretmans, 1999). A test case may be considered as a tree. The nodes of the test tree may be seen as collections of states S of the model of the SUT. The adopted test generation procedure is in charge of extending the test tree by defining successors to an every leaf node, as shown in Figure 3. For every *non-acceptable* output a_i the test tree moves to $fail$ and for every acceptable output b_i, the test tree moves to a new node which corresponds to the set of states that the system can reach after producing b_i. The tester may also decide to emit a valid input c from the current node (dashed arrow).

5.2 Combining Functional and Load Aspects

At this level, our goal is to combine load and functional aspects in our modelling since our system is made of a number of interacting and concurrent components. For this purpose, we adopt an extended variant of Timed Automata equipped with integer shared variables.

As illustrated in Figure 4, the used integer variable of the proposed timed automaton corresponds to the number running instances of the considered system. In this example, we demonstrate how the answer time to generate an action b may vary according to the number of running instances.

5.3 Testing Security Aspects using Attack Trees

In the literature, “Attack Trees” (Krichen and Alroobaea, 2019; Kordy et al., 2014) are used to assess the security of critical systems. They allow to represent graphically the strategy of a given attacker. An example of an AT is proposed in Figure 5 (Krichen and Alroobaea, 2019). In this example, the considered attacker aims at cracking the password of some protected files.

In general, the root of an attack tree corresponds to the global goal of the attacker and the leaves of the tree correspond to basic attack steps the attacker needs to combine in order to achieve its global goal. Internal nodes correspond to intermediary sub-goals. The attack tree has two types of gates namely AND-Gates and OR-Gates. On the first hand, an AND-gate means that in order to fulfill the goal a parent-node all sub-goals of children-nodes of the considered node have to be achieved. On the other hand, an OR-Gate means that the goal of a parent-node can be achieved by fulfilling the sub-goal of only one of its children-

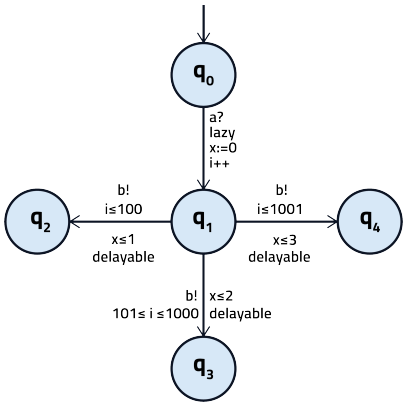

Figure 4: An example showing how the response time of the system under test varies regarding the current load level.

nodes.
After defining the attack tree modelling the behavior of the attacker, the second step consists in transforming the obtained tree into a network of Timed Automata which will serve as an input for our test generation procedure. The proposed transformation is inspired by the transformation proposed in (Kumar et al., 2015).

6 OPTIMIZATION OF TESTERS PLACEMENT

This problem is inspired by fog computing approaches (Taneja and Davy, 2017; Gu et al., 2017) and by some of our previous contributions (Maâlej et al., 2018; Lahami et al., 2016; Lahami et al., 2012b). It consists in allocating the set of testers on the different computational nodes of the SUT in an optimal manner under several types of constraints as mentioned below.

6.1 Different Types of Constraints

Node Constraints. For example in (Arkian et al., 2017), both CPU and storage were taken into account. In (Gu et al., 2017), the authors considered CPU, RAM and storage constraints.

Network Constraints. In (Mahmud et al., 2018) only latency constraint was taken into account. In addition in (Gupta et al., 2017; Ottenwälder et al., 2013), both bandwidth and latency were considered by the authors.

Energy Constraints. For instance in (Barcelo et al., 2016), the fog nodes were characterised with their energy capacities. Moreover, The writers of (Souza et al., 2016) defined the notion of "energy cells" to estimate the energy needed by the fog nodes.

6.2 Objective Functions

Energy. Energy optimization was taken into account from distinct levels. For example, the authors of (Barcelo et al., 2016) considered a linear objective measure of the energy consumption likewise in (Huang et al., 2014), the adopted goal consisted in diminishing the communication energy cost.

Execution Time and Network Delay. For example this objective function was adopted by the authors of (Skarlat et al., 2016). In addition in (Xia et al., 2018), the response time was optimised in order to augment the requests number to be served before a chosen deadline.

Migrations. In (Ottenwälder et al., 2013), the migrations number was optimised by reducing the network use without impacting its latency. Likewise in (Yang et al., 2016), the migrations number was optimised along with latency and resource consumption.

6.3 Algorithms

Search-based Algorithms. In (Gupta et al., 2017) an algorithm was proposed to find a placement scenario for internet of things applications. In addition in (Guerrero et al., 2019), a distributed search method was proposed for similar goals.

Dynamic Programming. In (Souza et al., 2016) the placement problem was modelled as a multidimensional knapsack problem (MKP). Likewise in (Rahbari and Nickray, 2017), the placement problem was modelled as a knapsack instance.

Mathematical Programming. This technique (Gu et al., 2017) is always adopted for solving optimization problems by investigating the space of the considered objective functions.

Game Theory. In (Zhang et al., 2017), the placement problem was encoded as a pair of games. The first one was introduced to calculate the cardinality of the set of necessary execution blocks and the second one was proposed to set prices in order to maximise the corresponding financial profits.

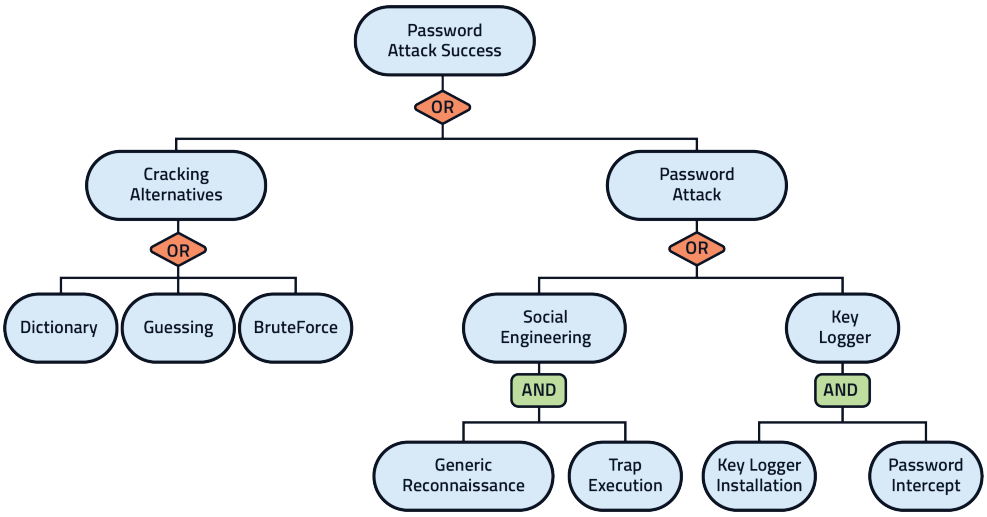

Figure 5: Example of an AT.

7 CONCLUSION

This study proposed an innovative Decentralized IoT solution for Vehicle communication (DISV) established with three primary layers based on Blockchain. Moreover, the article proposed an MBT approach in order to validate the proposed solution. The proposed testing approach is mainly based on the use of Attack Trees and Timed Automata in order to check functional, load and security aspects. An optimization phase for testers placement inspired by fog computing was also proposed.

Finally, DISV is an essential component of the Advanced Driver Assistance Systems (ADAS) that can potentially improve the transportation safety and mobility. In the future, we aim to establish a network for vehicles based on Blockchain to enable users to pay for tolls, parking spaces, and electrical charging by machine-to-machine transactions. Regarding test cases execution, standard-based platforms may be adopted like Testing and Test Control Notation version 3 (TTCN3) (Lahami et al., 2012a; Lahami et al., 2016). Moreover, it is necessary to use convenient test isolation techniques for avoiding interference between system functionalities and test scenarios as proposed and explained in (Lahami and Krichen, 2013).

ACKNOWLEDGEMENTS

This publication was made possible by QUCP-CENG-2019-1 grant from the Qatar University. The statements made herein are solely the responsibility of the authors.

REFERENCES

A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Commun. Mag.*, 55(12):119–125.

A. Lei, H. Cruickshank, Y. C. P. A. C. P. A. O. and Sun, Z. (2017). Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things*, 4(6):1832–1843.

Arkian, H. R., Diyanat, A., and Pourkhalili, A. (2017). Mist: Fog-based data analytics scheme with cost-efficient resource provisioning for iot crowdsensing applications. *Journal of Network and Computer Applications*, 82:152 – 165.

Barcelo, M., Correa, A., Llorca, J., Tulino, A. M., Vicario, J. L., and Morell, A. (2016). Iot-cloud service optimization in next generation smart environments. *IEEE Journal on Selected Areas in Communications*, 34(12):4077–4090.

Bertrand, N., Stainer, A., Jéron, T., and Krichen, M. (2011). A game approach to determinize timed automata. In *International Conference on Foundations of Software Science and Computational Structures*, pages 245–259. Springer, Berlin, Heidelberg.

Bertrand, N., Stainer, A., Jéron, T., and Krichen, M. (2015). A game approach to determinize timed automata. *Formal Methods in System Design*, 46(1):42–80.

F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun (2014). The internet of things: A survey. *China Communications*, 11(10):1–15.

Gu, L., Zeng, D., Guo, S., Barnawi, A., and Xiang, Y. (2017). Cost efficient resource management in fog computing supported medical cyber-physical system. *IEEE Transactions on Emerging Topics in Computing*, 5(1):108–119.

Guerrero, C., Lera, I., and Juiz, C. (2019). A lightweight decentralized service placement policy for performance optimization in fog computing. *Journal of Ambient*

Intelligence and Humanized Computing, 10(6):2435–2452.

Gupta, H., Dastjerdi, A. V., Ghosh, S. K., and Buyya, R. (2017). ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. *Softw., Pract. Exper.*, 47(9):1275–1296.

Huang, Z., Lin, K.-J., Yu, S.-Y., and jen Hsu, J. Y. (2014). Co-locating services in iot systems to minimize the communication energy cost. *Journal of Innovation in Digital Ecosystems*, 1(1):47 – 57.

J. Kang, R. Yu, X. H. S. M. Y. Z. and Hossain, E. (2017). Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Informatics*, 13(6):3154–3164.

Jabbar, R., Al-Khalifa, K., Kharbeche, M., Alhajyaseen, W., Jafari, M., and Jiang, S. (2018a). Applied internet of things iot: Car monitoring system for modeling of road safety and traffic system in the state of qatar. In *Qatar Foundation Annual Research Conference Proceedings Volume 2018 Issue 3*, volume 2018, page ICTPP1072. Hamad bin Khalifa University Press (HBKU Press).

Jabbar, R., Al-Khalifa, K., Kharbeche, M., Alhajyaseen, W., Jafari, M., and Jiang, S. (2018b). Real-time driver drowsiness detection for android application using deep neural networks techniques. *Procedia computer science*, 130:400–407.

Jabbar, R., Shinoy, M., Kharbeche, M., Al-Khalifa, K., Krichen, M., and Barkaoui, K. (2019). Urban Traffic Monitoring and Modeling System: An IoT Solution for Enhancing Road Safety. In *iintec 2019*, Hammamet, Tunisia.

Jabbar, R., Shinoy, M., Kharbeche, M., Al-Khalifa, K., Krichen, M., and Barkaoui, K. (2020). Driver drowsiness detection model using convolutional neural networks techniques for android application.

Kordy, B., Pièvre-Cambacédès, L., and Schweitzer, P. (2014). Dag-based attack and defense modeling: Don't miss the forest for the attack trees. *Computer Science Review*, 13-14:1 – 38.

Krichen, M. (2007). *Model-Based Testing for Real-Time Systems*. PhD thesis, PhD thesis, Universit Joseph Fourier (December 2007).

Krichen, M. (2010). A formal framework for conformance testing of distributed real-time systems. In *International Conference On Principles Of Distributed Systems*, pages 139–142. Springer.

Krichen, M. (2012). A formal framework for black-box conformance testing of distributed real-time systems. *IJCCBS*, 3(1/2):26–43.

Krichen, M. (2018). *Contributions to Model-Based Testing of Dynamic and Distributed Real-Time Systems*. Habilitation à diriger des recherches, École Nationale d'Ingénieurs de Sfax (Tunisie).

Krichen, M. and Alroobaea, R. (2019). A new model-based framework for testing security of iot systems in smart cities using attack trees and price timed automata. In *14th International Conference on Evaluation of Novel Approaches to Software Engineering - ENASE 2019*.

Krichen, M. and Tripakis, S. (2006). Interesting properties of the conformance relation tioco. In *ICTAC'06*.

Kumar, R., Ruijters, E., and Stoelinga, M. (2015). Quantitative attack tree analysis via priced timed automata. In Sankaranarayanan, S. and Vicario, E., editors, *Formal Modeling and Analysis of Timed Systems*, pages 156–171, Cham. Springer International Publishing.

L. Li, J. Liu, L. C. S. Q. W. W. X. Z. and Zhang, Z. (2018). CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Trans. Intell. Transp. Syst.*, page 1–17.

Lahami, M., Fakhfakh, F., Krichen, M., and Jmaïel, M. (2012a). Towards a TTCN-3 Test System for Runtime Testing of Adaptable and Distributed Systems. In *Proceedings of the 24th IFIP WG 6.1 International Conference Testing Software and Systems (ICTSS'12)*, pages 71–86.

Lahami, M. and Krichen, M. (2013). Test Isolation Policy for Safe Runtime Validation of Evolvable Software Systems. In *Proceedings of the 22nd IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'13)*, pages 377–382.

Lahami, M., Krichen, M., Bouchakwa, M., and Jmaïel, M. (2012b). Using Knapsack Problem Model to Design a Resource Aware Test Architecture for Adaptable and Distributed Systems. In *Proceedings of the 24th IFIP WG 6.1 International Conference Testing Software and Systems (ICTSS'12)*, pages 103–118.

Lahami, M., Krichen, M., and Jmaïel, M. (2016). Safe and Efficient Runtime Testing Framework Applied in Dynamic and Distributed Systems. *Science of Computer Programming (SCP)*, 122(C):1–28.

Leiding, Benjamin, P. M. and Hogrefe., D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. *the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct.*

Maâlej, A. J., Lahami, M., Krichen, M., and Jmaïel, M. (2018). Distributed and resource-aware load testing of WS-BPEL compositions. In *ICEIS (2)*, pages 29–38. SciTePress.

Madhusudan Singh, S. K. (2017). Blockchain based Intelligent Vehicle Data Sharing Framework. *arXiv preprint, arXiv: 1708.09721*.

Mahmud, R., Ramamohanarao, K., and Buyya, R. (2018). Latency-aware application module management for fog computing environments. *ACM Trans. Internet Technol.*, 19(1):9:1–9:21.

Ottenwälder, B., Koldehofe, B., Rothermel, K., and Ramachandran, U. (2013). Migcep: Operator migration for mobility driven distributed complex event processing. In *Proceedings of the 7th ACM International Conference on Distributed Event-based Systems*, DEBS '13, pages 183–194, New York, NY, USA. ACM.

Rahbari, D. and Nickray, M. (2017). Scheduling of fog networks with optimized knapsack by symbiotic organisms search. In *2017 21st Conference of Open Innovations Association (FRUCT)*, pages 278–283.

Sean Rowan, Michael Clear, M. H. and Goldrick, C. M. (2017). Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels. *eprint arXiv:1704.02553*.

Skarlat, O., Schulte, S., Borkowski, M., and Leitner, P. (2016). Resource provisioning for iot services in

the fog. In *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*, pages 32–39.

Souza, V. B., Masip-Bruin, X., Marin-Tordera, E., Ramirez, W., and Sanchez, S. (2016). Towards distributed service allocation in fog-to-cloud (f2c) scenarios. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.

Taneja, M. and Davy, A. (2017). Resource aware placement of iot application modules in fog-cloud computing paradigm. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 1222–1228.

Tretmans, J. (1999). Testing concurrent systems: A formal approach. In *Proceedings of the 10th International Conference on Concurrency Theory*, CONCUR '99, page 46–65, Berlin, Heidelberg. Springer-Verlag.

X. Huang, C. Xu, P. W. and Liu, H. (2018). LNSC: A security model for electric vehicle and charging pile management based on Blockchain ecosystem. *IEEE Access*, 6:13 565–13 574.

Xia, Y., Etchevers, X., Letondeur, L., Coupaye, T., and Desprez, F. (2018). Combining hardware nodes and software components ordering-based heuristics for optimizing the placement of distributed iot applications in the fog. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, SAC '18, pages 751–760, New York, NY, USA. ACM.

Y. Yuan and FY. Wang. (2016). Towards blockchain-based intelligent transportation systems. *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pages 2663–2668.

Yang, L., Cao, J., Liang, G., and Han, X. (2016). Cost aware service placement and load dispatching in mobile cloud systems. *IEEE Transactions on Computers*, 65(5):1440–1452.

Z. Yang, K. Zheng, K. Y. and Leung, V. C. M. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks. *IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.*, page 1–5.

Zhang, H., Xiao, Y., Bu, S., Niyato, D., Yu, F. R., and Han, Z. (2017). Computing resource allocation in three-tier iot fog networks: A joint optimization approach combining stackelberg game and matching. *IEEE Internet of Things Journal*, 4(5):1204–1215.