



HAL
open science

Un Cadre de Test Formel pour la Validation d'un Système de Communication Inter-Véhiculaire Basé sur les IOTs et la Blockchain

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

► **To cite this version:**

Rateb Jabbar, Moez Krichen, Mohamed Kharbeche, Noora Fetais, Kamel Barkaoui. Un Cadre de Test Formel pour la Validation d'un Système de Communication Inter-Véhiculaire Basé sur les IOTs et la Blockchain. 2020. hal-02513235

HAL Id: hal-02513235

<https://hal.science/hal-02513235v1>

Preprint submitted on 20 Mar 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Un Cadre de Test Formel pour la Validation d'un Système de Communication Inter-Véhiculaire Basé sur les IOTs et la Blockchain

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

* KINDI Center for Computing Research,
College of Engineering, Qatar University, Doha, Qatar
** Cedric Laboratory, Computer Science Department,
Conservatoire National des Arts et Metiers, France
*** ReDCAD Laboratory, University of Sfax, Tunisia
**** Qatar Transportation and Traffic Safety Center,
Qatar University, Qatar
rateb.jabbar@qu.edu.qa, moez.krichen@redcad.org,
mkharbec@qu.edu.qa, n.almarri@qu.edu.qa,
kamel.barkaoui@cnam.fr

Résumé. L'émergence de technologies, systèmes et dispositifs intelligents intégrés et connectés a permis le concept de villes intelligentes en connectant chaque "chose" à Internet et en particulier dans le transport via l'Internet des véhicules (IoV). Le but principal de l'IoV est de prévenir les accidents mortels en résolvant les problèmes de circulation et de sécurité routière. Néanmoins, il est primordial d'assurer une transmission et un enregistrement sûrs et précis des données dans les communications "Vehicle-to-Vehicle" (V2V) et "Vehicle-to-Infrastructure" (V2I). Pour améliorer la communication "Vehicle-to-Everything" (V2X), ce travail utilise la technologie Blockchain pour développer un système IoT visant à établir une communication sécurisée et à développer une plateforme de cloud computing entièrement décentralisée. De plus, les auteurs proposent un cadre basé sur un modèle pour valider l'approche proposée. Ce cadre est principalement basé sur l'utilisation des formalismes des arbres d'attaque et des automates temporisés afin de tester les aspects fonctionnels, de charge et de sécurité. Une phase d'optimisation du placement des testeurs inspirée du calcul dans de brouillard (fog computing) est également proposée.

1 Introduction

Les technologies IoT modernes (23) ont profondément transformé les "réseaux ad-hoc véhiculaires" classiques (vehicular ad-hoc networks - VANET) en "Internet des véhicules" (Internet of Vehicles - IoV) (7). Plus précisément, l'IoV est défini comme l'interaction de données en temps réel entre les véhicules et entre les véhicules et les

infrastructures via les plateformes d'information, la technologie de communication mobile, les terminaux intelligents et les systèmes de navigation des véhicules. Les véhicules sont intégrés à l'IoT en étant connectés à Internet, aux autres véhicules à proximité ainsi qu'aux systèmes d'information de trafic. Pourtant, il existe de nombreux défis liés à ce concept en raison de la connectivité élevée et de l'échange de données sensibles, compromettant la sécurité et la confidentialité et laissant les véhicules sensibles aux entités malveillantes.

La solution IoT décentralisée proposée pour la communication avec les véhicules (Decentralized IoT Solution for Vehicle communication - DISV) basée sur le concept de Blockchain vise à surmonter les défis de sécurité et de confidentialité. À titre d'explication, chaque membre des réseaux IoV reçoit des messages et les diffuse sur le serveur Blockchain, tandis que le serveur vérifie le bloc reçu et décide s'il doit être ajouté au contrat intelligent ou non.

Afin de valider la solution adoptée, nous proposons, en plus, un cadre de "test basé sur modèle" (Model Based Testing - MBT) (22; 18; 20; 19) qui permet de vérifier l'exactitude fonctionnelle, la charge et les aspects de sécurité. Ce cadre est principalement basé sur le modèle des automates temporisés (6; 5). Ce dernier correspond à un langage de modélisation riche qui permet de décrire les comportements d'une large classe de systèmes distribués, dynamiques et temps-réels.

Concernant les tests des aspects de sécurité, nous modélisons le comportement de l'attaquant à l'aide des arbres d'attaque (Attack Trees - AT) (24; 17). La racine de l'AT correspond à l'objectif global de l'attaquant. Les nœuds internes correspondent aux sous-objectifs et les feuilles correspondent aux "étapes d'attaque de base" (Basic Attack Steps - BAS). Chaque AT est ensuite transformé en une collection d'automates temporisés à partir desquels des scénarios de test sont extraits à l'aide d'algorithmes de génération de test inspirés des travaux de (18; 41).

En outre, nous proposons une approche pour l'optimisation de la procédure de placement des testeurs inspirée des approches de "Calcul de Brouillard" (Fog Computing) (40; 8; 34; 4) et de certaines de nos contributions précédentes (32; 27; 30). Cette procédure de placement consiste à allouer l'ensemble des testeurs sur les différents nœuds de calcul du système testé de manière optimale sous différents types de contraintes.

Le reste de cet article est structuré comme suit. Dans la section 2, un aperçu concernant la blockchain, les tests basés sur modèle (Model Based Testing - MBT) et les automates temporisés est présenté. La section 3 est dédiée à l'examen de plusieurs techniques Blockchain pour l'IoT et pratiquement pour l'IoV. La conception de la solution proposée est présentée dans la section 4. Dans la section 5, nous présentons plusieurs détails sur le cadre de test adopté. La section 6 est dédiée au problème d'optimisation du placement des testeurs. Enfin, la section 7 résume le résultat principal et donne de nouvelles directions pour les recherches futures.

2 Préliminaires

2.1 Blockchain

La blockchain a émergé grâce au Bitcoin, introduit en 2008 par Satoshi Nakamoto. Le Bitcoin peut être défini comme un cryptosystème de monnaie mondial décentralisé. La blockchain utilisée dans Bitcoin permet d'utiliser de l'argent numérique sécurisé et décentralisé dans un système de paiement. Ce réseau peer-to-peer ne possède pas d'autorité centrale et, à ce titre, est entièrement alimenté par les utilisateurs. Son architecture informatique est distribuée et toutes les transactions sont annoncées publiquement. Ainsi, les utilisateurs ont un consensus sur un seul historique des transactions, appelé grand livre. Les transactions sont séparées en blocs; par la suite, chaque utilisateur reçoit un horodatage qui sera ensuite publié. Il est difficile de modifier les blocs publiés car le hachage des blocs précédents est inséré dans les successeurs suivants de chaque bloc de la chaîne.

2.2 Test basé sur modèle

Test basé sur modèle (Model Based Testing - MBT) (22; 21; 20; 19) est une méthodologie dans laquelle le système d'intérêt est décrit par un modèle mathématique qui code le comportement du système considéré. Cette méthodologie consiste à utiliser ce modèle mathématique pour calculer des scénarios de test abstraits. Ces séquences de modèle sont ensuite transformées en séquences de test concrètes qui sont exécutées sur le "système sous test" (System Under Test - SUT) considéré. Le verdict de cette activité de test est fourni en comparant les sorties observées du système avec les sorties générées par le modèle.

2.3 automates temporisés

Les "automates temporisés" (Timed Automata - TA) (6; 5) sont un outil expressif et simple pour décrire le comportement des systèmes informatiques qui combinent des mécanismes continus et discrets. TA peut être représenté comme des graphes finis enrichis d'un ensemble fini d'horloges définies comme des entités réelles dont la valeur progresse continuellement dans le temps.

3 Travaux connexes

(42) a développé un modèle d'écosystème sur la base de la gestion des véhicules électriques Blockchain et de la pile de charge. Ce modèle utilise la cryptographie à courbe elliptique pour le calcul des fonctions de hachage de la charge des piles de véhicules électriques. En outre, (12) a développé PETCON, un système d'échange d'électricité P2P, pour illustrer les opérations localisées et complètes du commerce d'électricité P2P. Le système PETCON utilise une méthode Blockchain du consortium pour analyser, vérifier et partager publiquement les enregistrements de transaction, alors qu'il n'est pas nécessaire d'avoir une autorité fiable.

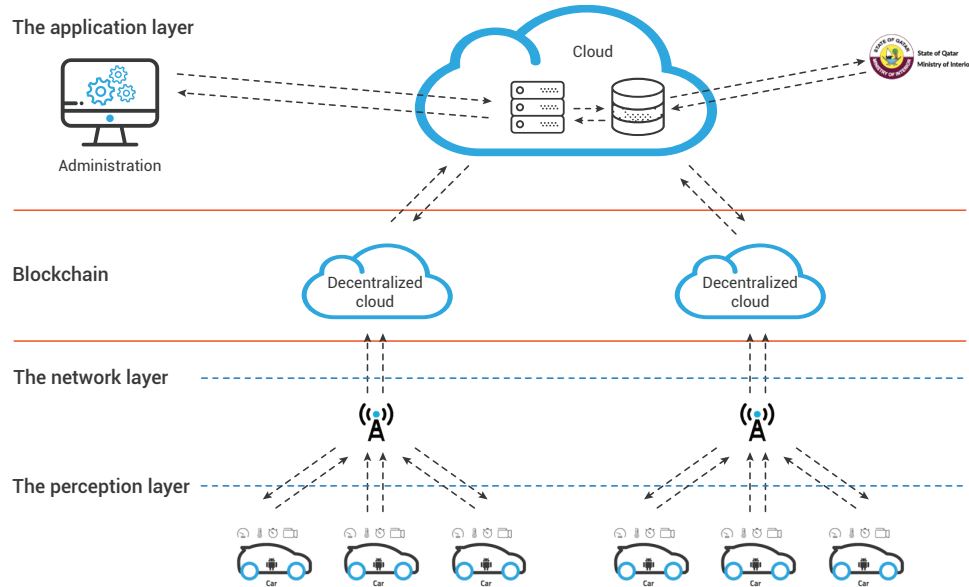


FIG. 1 – L'architecture de la solution proposée.

En outre, CreditCoin, un système de protection de la vie privée, a été créé par (26) afin de garantir que les annonces adéquates sont transmises sans révéler l'identité des utilisateurs. Ce schéma utilise la Blockchain pour envoyer des annonces anonymes via un protocole d'agrégation entre véhicules. De plus, (46) a proposé un système de réputation basé sur Blockchain pour évaluer la crédibilité des données dans l'IoV. (44) a développé une solution Blockchain visant à résoudre les problèmes de sécurité et les limitations de performances dans les systèmes de transport intelligents (ITS). (31) a fusionné la technologie Blockchain avec le réseau véhiculaire ad hoc VANET.

(2) a introduit la gestion dynamique des clés en utilisant Blockchain pour établir des systèmes de communication à utiliser dans les véhicules qui n'ont pas besoin de l'administration du gestionnaire central. En s'appuyant sur une structure Blockchain décentralisée, il élimine toute autre autorité. (1) a créé un mécanisme technologique Blockchain qui ne révèle aucune donnée privée des utilisateurs de véhicules. (37) a utilisé la lumière visible et les canaux latéraux acoustiques et a appliqué la technologie Blockchain pour sécuriser la communication intelligente du véhicule. (33) a développé un cadre pour un environnement sécurisé basé sur la confiance avec une communication d'égal à égal entre des véhicules intelligents sans perturber/interférer avec d'autres véhicules intelligents via le mécanisme Blockchain pour l'environnement de communication des véhicules intelligents. Cependant, l'utilisation de ce cadre est limitée uniquement aux voitures intelligentes.

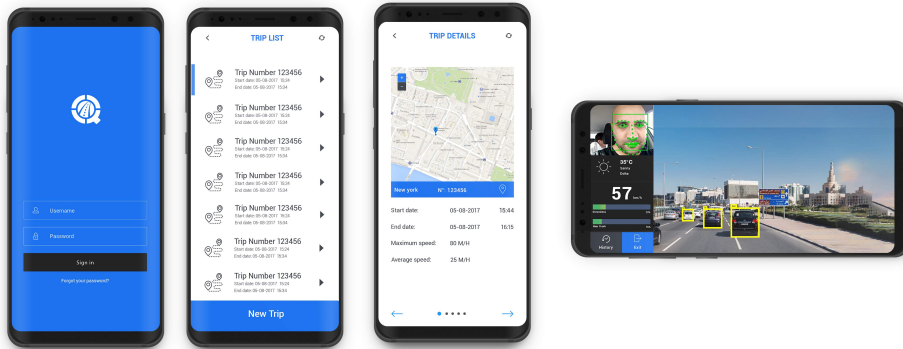


FIG. 2 – Capture d'écran des quatre pages principales de l'application Android.

4 Solution Proposée

L'architecture adoptée est composée de trois couches. La figure 1 illustre l'architecture de la solution proposée.

4.1 La couche de perception

Afin de tester des scénarios possibles impliquant divers composants, une application Android a été développée dans le système Internet of Vehicle (AV) et pour l'infrastructure (AP). D'une part, AV est une application Android composée de deux sous-systèmes. Le premier sous-système est le système de collecte de données sur les véhicules (VDCS) qui collecte des données sur le trajet et la voiture. Le deuxième est le système de détection de somnolence du conducteur qui recueille des données sur le comportement du conducteur pour déterminer s'il est somnolent ou non. Vous trouverez plus d'informations sur ce système dans (13; 14; 15; 16).

Principalement, l'application Android comporte quatre pages, comme indiqué dans Figure 2 : La première page sert à la connexion en utilisant un nom d'utilisateur et un mot de passe. Après l'authentification, l'utilisateur peut commencer un nouveau voyage ou accéder aux informations sur les cinq derniers voyages sur la deuxième page. Si l'utilisateur choisit un nouveau voyage, l'application commencera à enregistrer et afficher toutes les informations comme décrit dans la section précédente. Ensuite, il enverra les données collectées via le service Web au serveur cloud. Sur la quatrième page, la caméra avant capture et affiche le visage du conducteur.

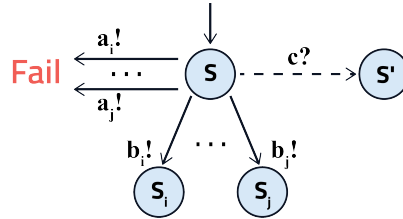


FIG. 3 – Principe de génération de test.

4.2 La couche réseau

La couche réseau établit la connexion entre les serveurs et transmet, et traite les données des capteurs. L'application peut utiliser le Wi-Fi ou l'Internet mobile (3G/3G+/4G) pour envoyer les données au serveur.

Ce processus de collecte utilise le système hybride pour collecter et enregistrer les données localement avant de les transmettre au serveur. Cette technique s'est avérée très efficace pour la collecte de données lorsque la connexion Internet est mauvaise ou instable.

4.3 La couche d'application

En ce qui concerne la couche application, elle contient deux composants principaux : le serveur cloud central et le système de communication utilisant un réseau Blockchain. Tout d'abord, le serveur cloud central fournit des services spécifiques à l'application à l'utilisateur final. Il envoie les données collectées aux services Web pour traitement et analyse avant de les montrer à l'utilisateur final. Deuxièmement, le réseau Blockchain est responsable de la gestion de la communication entre les voitures et les systèmes de circulation et de transport. À chaque créneau horaire, la voiture envoie les données collectées au serveur central via un service Web, y compris l'emplacement actuel et l'état de la connexion à l'un des serveurs Blockchain existants.

5 Framework de test

5.1 Principe de génération de test

Notre procédure de génération est inspirée du travail de (41). Un cas de test peut être considéré comme un arbre. Les nœuds de l'arbre de test peuvent être vus comme des ensembles d'états S du modèle du SUT. La procédure de génération de test adoptée est en charge de l'extension de l'arbre de test en définissant successeurs à chaque nœud feuille, comme illustré dans Figure 3. Pour chaque sortie *non acceptable* a_i , l'arbre de test se déplace vers *fail* et pour chaque sortie acceptable b_i , l'arbre de test se déplace vers un nouveau nœud qui correspond à l'ensemble des états que le système peut atteindre après avoir produit b_i . Le testeur peut également décider d'émettre une entrée valide c à partir du nœud actuel (flèche en pointillés).

5.2 Combinaison des aspects fonctionnels et de charge

À ce niveau, notre objectif est de combiner la charge et les aspects fonctionnels dans notre modélisation, car notre système est composé d'un certain nombre de composants interactifs et simultanés. À cette fin, nous adoptons une variante étendue des automates temporisés équipés de variables partagées entières.

Comme illustré dans la figure 4, la variable entière utilisée de l'automate temporisé proposé correspond au nombre d'instances en cours d'exécution du système considéré. Dans cet exemple, nous montrons comment le temps de réponse pour générer une action b peut varier en fonction du nombre d'instances en cours d'exécution.

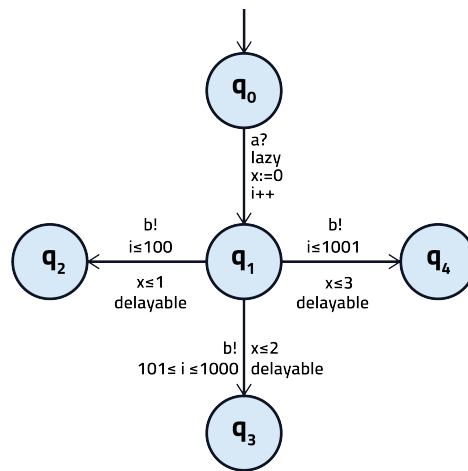


FIG. 4 – Un exemple montrant comment le temps de réponse du système testé varie en fonction du niveau de charge actuel.

5.3 Test des aspects de sécurité à l'aide d'arbres d'attaque

Dans la littérature, les "arbres d'attaque" (Attack Trees - AT) (24; 17) sont utilisés pour évaluer la sécurité des systèmes critiques. Ils permettent de représenter graphiquement la stratégie d'un attaquant donné. Un exemple d'AT est proposé dans la figure 5 (24). Dans cet exemple, l'attaquant considéré vise à casser le mot de passe de certains fichiers protégés.

En général, la racine d'un arbre d'attaque correspond à l'objectif global de l'attaquant et les feuilles de l'arbre correspondent aux étapes d'attaque de base que l'attaquant doit combiner pour atteindre son objectif global. Les nœuds internes correspondent à des sous-objectifs intermédiaires. L'arbre d'attaque a deux types de portes, à savoir les portes ET et les portes OU. D'une part, une porte ET signifie que pour atteindre l'objectif d'un nœud parent, tous les sous-objectifs des nœuds enfants du nœud considéré doivent être atteints. D'un autre côté, une porte OU signifie que l'objectif d'un nœud parent peut être atteint en remplissant le sous-objectif d'un seul de

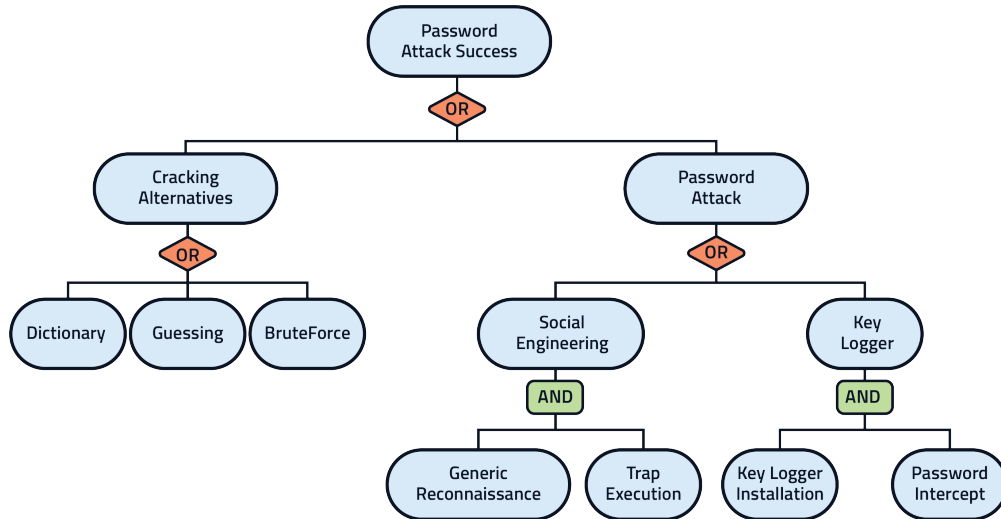


FIG. 5 – Un exemple d'arbre d'attaque.

ses nœuds enfants. Après avoir défini l'arbre d'attaque modélisant le comportement de l'attaquant, la deuxième étape consiste à transformer l'arbre obtenu en un réseau d'Automates Temporisés qui servira d'entrée à notre procédure de génération de test. La transformation proposée est inspirée de la transformation proposée dans (25).

6 Optimisation du placement des testeurs

Ce problème est inspiré des approches de calcul du brouillard (40; 8) et de certaines de nos contributions précédentes (32; 27; 30). Elle consiste à allouer l'ensemble des testeurs sur les différents nœuds de calcul du SUT de manière optimale sous plusieurs types de contraintes comme mentionné ci-dessous.

6.1 Différents types de contraintes

Contraintes de nœud Par exemple, dans (3), le CPU et le stockage ont été pris en compte. Dans (8), les auteurs ont considéré les contraintes de CPU, de RAM et de stockage.

Contraintes réseau Dans (34) seule la contrainte de latence a été prise en compte. En plus dans (10; 35), la bande passante et la latence ont été prises en compte par les auteurs.

Contraintes énergétiques Par exemple dans (4), les nœuds de brouillard ont été caractérisés par leurs capacités énergétiques. De plus, les auteurs de (39) ont défini la notion de "cellules d'énergie" pour estimer l'énergie nécessaire aux nœuds de brouillard.

6.2 Fonctions objectives

Énergie L'optimisation énergétique a été prise en compte à différents niveaux. Par exemple, les auteurs de (4) ont considéré une mesure objective linéaire de la consommation d'énergie également dans (11), l'objectif adopté a consisté à diminuer le coût de l'énergie de communication.

Temps d'exécution et délai réseau Par exemple, cette fonction objective a été adoptée par les auteurs de (38). De plus, dans (43), le temps de réponse a été optimisé afin d'augmenter le nombre de demandes à traiter avant une échéance choisie.

Migrations Dans (35), le nombre de migrations a été optimisé en réduisant l'utilisation du réseau sans impact sur sa latence. De même dans (45), le nombre de migrations a été optimisé avec la latence et la consommation de ressources.

6.3 Algorithmes

Algorithmes basés sur la recherche Dans (10), un algorithme a été proposé pour trouver un scénario de placement pour les applications Internet des objets. De plus, dans (9), une méthode de recherche distribuée a été proposée pour des objectifs similaires.

Programmation dynamique Dans (39), le problème de placement a été modélisé comme un problème de sac à dos multidimensionnel. De même dans (36), le problème de placement a été modélisé comme une instance de sac à dos.

Programmation mathématique Cette technique (8) est toujours adoptée pour résoudre les problèmes d'optimisation en étudiant l'espace des fonctions objectives considérées.

Théorie des jeux Dans (47), le problème de placement a été codé comme une paire de jeux. Le premier a été introduit pour calculer la cardinalité de l'ensemble des blocs d'exécution nécessaires et le second a été proposé de fixer les prix afin de maximiser les bénéfices financiers correspondants.

7 Conclusion

Cette étude a proposé une solution IoT décentralisée innovante pour la communication avec les véhicules (DISV) établie avec trois couches principales basées sur la Blockchain. De plus, l'article proposait une approche MBT afin de valider la solution proposée. L'approche de test proposée est principalement basée sur l'utilisation d'arbres d'attaque et d'automates temporisés afin de vérifier les aspects fonctionnels, de charge et de sécurité. Une phase d'optimisation du placement des testeurs inspirée du calcul du brouillard a également été proposée. Enfin, le DISV est une composante essentielle des systèmes avancés d'aide à la conduite (ADAS) qui peuvent potentiellement améliorer la sécurité et la mobilité des transports.

À l'avenir, nous visons à établir un réseau de véhicules basé sur Blockchain pour permettre aux utilisateurs de payer les péages, les places de stationnement et la recharge électrique par des transactions de machine à machine. En ce qui concerne l'exécution des cas de test, des plates-formes basées sur des normes peuvent être adoptées comme Testing and Test Control Notation version 3 (TTCN3) (28; 27). De plus, il est nécessaire d'utiliser des techniques d'isolation de test pratiques pour éviter les interférences entre les fonctionnalités du système et les scénarios de test, comme proposé et expliqué dans (29).

Références

- [1] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak. BlockChain : A Distributed Solution to Automotive Security and Privacy. *IEEE Commun. Mag.*, 55(12) :119–125, Dec. 2017.
- [2] Y. Cao P. Asuquo C. P. A. Ogah A. Lei, H. Cruickshank and Z. Sun. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things*, 4(6) :1832–1843, Dec. 2017.
- [3] Hamid Reza Arkian, Abolfazl Diyanat, and Atefe Pourkhalili. Mist : Fog-based data analytics scheme with cost-efficient resource provisioning for iot crowdsensing applications. *Journal of Network and Computer Applications*, 82 :152 – 165, 2017.
- [4] M. Barcelo, A. Correa, J. Llorca, A. M. Tulino, J. L. Vicario, and A. Morell. Iot-cloud service optimization in next generation smart environments. *IEEE Journal on Selected Areas in Communications*, 34(12) :4077–4090, Dec 2016.
- [5] Nathalie Bertrand, Amélie Stainer, Thierry Jéron, and Moez Krichen. A game approach to determinize timed automata. In *International Conference on Foundations of Software Science and Computational Structures*, pages 245–259. Springer, Berlin, Heidelberg, 2011.
- [6] Nathalie Bertrand, Amélie Stainer, Thierry Jéron, and Moez Krichen. A game approach to determinize timed automata. *Formal Methods in System Design*, 46(1) :42–80, 2015.
- [7] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun. The internet of things : A survey. *China Communications*, 11(10) :1–15, 2014.
- [8] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang. Cost efficient resource management in fog computing supported medical cyber-physical system. *IEEE Transactions on Emerging Topics in Computing*, 5(1) :108–119, Jan 2017.
- [9] Carlos Guerrero, Isaac Lera, and Carlos Juiz. A lightweight decentralized service placement policy for performance optimization in fog computing. *Journal of Ambient Intelligence and Humanized Computing*, 10(6) :2435–2452, Jun 2019.
- [10] Harshit Gupta, Amir Vahid Dastjerdi, Soumya K. Ghosh, and Rajkumar Buyya. 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, 2017.

- [11] Zhenqiu Huang, Kwei-Jay Lin, Shih-Yuan Yu, and Jane Yung jen Hsu. Co-locating services in iot systems to minimize the communication energy cost. *Journal of Innovation in Digital Ecosystems*, 1(1) :47 – 57, 2014.
- [12] X. Huang S. Maharjan Y. Zhang J. Kang, R. Yu and E. Hossain. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Informatics*, 13(6) :3154–3164, Dec. 2017.
- [13] Rateb Jabbar, Khalifa Al-Khalifa, Mohamed Kharbeche, Wael Alhajyaseen, Mohsen Jafari, and Shan Jiang. 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), 2018.
- [14] Rateb Jabbar, Khalifa Al-Khalifa, Mohamed Kharbeche, Wael Alhajyaseen, Mohsen Jafari, and Shan Jiang. Real-time driver drowsiness detection for android application using deep neural networks techniques. *Procedia computer science*, 130 :400–407, 2018.
- [15] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Urban Traffic Monitoring and Modeling System : An IoT Solution for Enhancing Road Safety. In *iintec 2019*, Hammamet, Tunisia, December 2019.
- [16] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Driver drowsiness detection model using convolutional neural networks techniques for android application, 2020.
- [17] Barbara Kordy, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. Dag-based attack and defense modeling : Don't miss the forest for the attack trees. *Computer Science Review*, 13-14 :1 – 38, 2014.
- [18] M. Krichen. A formal framework for black-box conformance testing of distributed real-time systems. *IJCCBS*, 3(1/2) :26–43, 2012.
- [19] M. Krichen and S. Tripakis. Interesting properties of the conformance relation tioco. In *ICTAC'06*, 2006.
- [20] Moez Krichen. *Model-Based Testing for Real-Time Systems*. PhD thesis, PhD thesis, Universit Joseph Fourier (December 2007), 2007.
- [21] Moez Krichen. A formal framework for conformance testing of distributed real-time systems. In *International Conference On Principles Of Distributed Systems*, pages 139–142. Springer, 2010.
- [22] Moez Krichen. *Contributions to Model-Based Testing of Dynamic and Distributed Real-Time Systems*. Habilitation à diriger des recherches, École Nationale d'Ingénieurs de Sfax (Tunisie), August 2018.
- [23] Moez Krichen. Improving formal verification and testing techniques for internet of things and smart cities. *Mobile Networks and Applications*, Sep 2019.
- [24] Moez Krichen and Roobaea Alroobaea. 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*, 2019.
- [25] Rajesh Kumar, Enno Ruijters, and Mariëlle Stoelinga. Quantitative attack tree analysis via priced timed automata. In Sriram Sankaranarayanan and Enrico Vicario, editors, *Formal Modeling and Analysis of Timed Systems*, pages 156–171, Cham, 2015. Springer International Publishing.
- [26] L. Cheng S. Qiu W. Wang X. Zhang L. Li, J. Liu and Z. Zhang. CreditCoin : A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Trans. Intell. Transp. Syst.*, page 1–17, 2018.
- [27] M. Lahami, M. Krichen, and M. Jmaïel. Safe and Efficient Runtime Testing Framework Applied in Dynamic and Distributed Systems. *Science of Computer Programming (SCP)*, 122(C) :1–28, 2016.
- [28] Mariam Lahami, Fairouz Fakhfakh, Moez Krichen, and Mohamed Jmaïel. 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, 2012.
- [29] Mariam Lahami and Moez Krichen. 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, 2013.
- [30] Mariam Lahami, Moez Krichen, Mariam Bouchakwa, and Mohamed Jmaïel. 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, 2012.
- [31] Parisa Memarmoshrefi Leiding, Benjamin and Dieter Hogrefe. Self-managed and blockchain-based vehicular ad-hoc networks. *the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing : Adjunct.*, 2016.
- [32] Afef Jmal Maâlej, Mariam Lahami, Moez Krichen, and Mohamed Jmaïel. Distributed and resource-aware load testing of WS-BPEL compositions. In *ICEIS (2)*, pages 29–38. SciTePress, 2018.
- [33] Shiho Kim Madhusudan Singh. Blockchain based Intelligent Vehicle Data Sharing Framework. *arXiv preprint, arXiv : 1708.09721*, Sept. 2017.
- [34] Redowan Mahmud, Kotagiri Ramamohanarao, and Rajkumar Buyya. Latency-aware application module management for fog computing environments. *ACM Trans. Internet Technol.*, 19(1) :9 :1–9 :21, November 2018.
- [35] Beate Ottenwälder, Boris Koldehofe, Kurt Rothermel, and Umakishore Ramachandran. 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, 2013. ACM.

- [36] D. Rahbari and M. Nickray. Scheduling of fog networks with optimized knapsack by symbiotic organisms search. In *2017 21st Conference of Open Innovations Association (FRUCT)*, pages 278–283, Nov 2017.
- [37] Meriel Huggard Sean Rowan, Michael Clear and Ciaran Mc Goldrick. Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels. *eprint arXiv :1704.02553*, April 2017.
- [38] O. Skarlat, S. Schulte, M. Borkowski, and P. Leitner. Resource provisioning for iot services in the fog. In *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*, pages 32–39, Nov 2016.
- [39] V. B. Souza, X. Masip-Bruin, E. Marin-Tordera, W. Ramirez, and S. Sanchez. Towards distributed service allocation in fog-to-cloud (f2c) scenarios. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, Dec 2016.
- [40] M. Taneja and A. Davy. 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, May 2017.
- [41] Jan Tretmans. Testing concurrent systems : A formal approach. In *Proceedings of the 10th International Conference on Concurrency Theory, CONCUR '99*, page 46–65, Berlin, Heidelberg, 1999. Springer-Verlag.
- [42] P. Wang X. Huang, C. Xu and H. Liu. LNSC : A security model for electric vehicle and charging pile management based on Blockchain ecosystem. *IEEE Access*, 6 :13 565–13 574, 2018.
- [43] Ye Xia, Xavier Etchevers, Loïc Letondeur, Thierry Coupaye, and Frédéric Desprez. 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, 2018. ACM.
- [44] Y. Yuan and FY. Wang. Towards blockchain-based intelligent transportation systems. *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pages 2663–2668, 2016.
- [45] L. Yang, J. Cao, G. Liang, and X. Han. Cost aware service placement and load dispatching in mobile cloud systems. *IEEE Transactions on Computers*, 65(5) :1440–1452, May 2016.
- [46] K. Yang Z. Yang, K. Zheng and V. C. M. Leung. 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, Oct. 2017.
- [47] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu, and Z. Han. 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, Oct 2017.