Journal of Service Science Research (2019) 11:47-67
DOI 10.1007/s12927-019-0003-8

A State-of-the-Art Survey on Formal Verification of the Internet of Things Applications

Alireza Souri, Monire Norouzi

Received: 21 February 2018 / Accepted: 31 May 2019 / Published: 30 June 2019

ABSTRACT

In recent years, Internet of Things (IoT) has been one of the most popular technologies that facilitate new interactions among things and humans to enhance the quality of life. With the rapid development of the IoT, Industrial and enterprise IoT are emerging as an attractive solution for processing the IoT applications. On the other hand, due to the guarantee of safety-critical conditions without system failures in smart devices, formal verification approaches are essential to manage and evaluate critical failures and reachable status in these problems. In this paper, a review of the formal verification approaches in the IoT applications is presented to recognize the state-of-the-art mechanisms on this important topic. The formal verification approaches of the IoT environments are compared with each other according to the advantages and limitations.

KEYWORDS

Internet of Things, Service Application, Formal Verification, Safety Critical System

Alireza Souri (✉), corresponding author
Young Researchers and Elite Club, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran
e-mail: alirezasouri.research@gmail.com
Monire Norouzi
Young Researchers and Elite Club, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran
e-mail: Monire_norouzi@yahoo.com

1. INTRODUCTION

By increasing actuators, sensor, smart devices and intelligent systems an innovative evolution of well-organized and connected factories and applications, some key challenges including guaranteeing low energy consumption, managing data access (Souri et al. 2018b), safety critical deployments and latency have emerged (Ahmad et al. 2019). The centralized traditional networks which deal with simple data sharing operations possibly will be unable to satisfy severe requests (Asghari et al. 2019; Souri et al. 2017). With respect to the growing use of the Internet of Things (IoT) technologies in the health-care, transportations, agriculture, smart city and industrial domains, emphasizing on appropriate frameworks and architectures have already been noticed (Asghari et al. 2018). Therefore, in IoT, due to the limitation of the network of IoT objects, the smart devices as more capable distributed local storage proxies for IoT nodes have been employed. It is obvious that the energy consumption of the IoT nodes, specifying the locations of proxies in the network and the high level of access latency and system failures that consumer nodes can bear the distribution of the data on each smart devices, should be specified to improve the lifetime of the resource-constrained network. Therefore, it is important to have a complete examination of the safety-critical systems for supporting expected requirements. Further, there is an essential effort to prove the correctness of the collaboration between smart devices and IoT applications using formal verification approaches (Ghobaei-Arani et al. 2018; Souri et al. 2018a). In addition, recognizing and proving the correctness of the smart workflows are more significant when system failures directly lead to safety problems in IoT applications (Souri et al. 2019).

To the best of our knowledge, despite the importance of formal verification approaches in the IoT environments, there is no systematic survey and review about this issue that realizes the need for researchers to do more work on IoT fields. Therefore, the aim of this paper is to review and analyze the existing verification approaches in the IoT. This study provides a survey for the formal modeling and verification approaches in the IoT applications. This survey categorizes the formal verification approaches in three main categories: model checking IoT, process algebraic IoT, and automated theorem proving IoT.

Briefly, the main contributions of this paper are as follow:

- Presenting a summary of the significant issues and the current challenges related to the

formal analysis of the IoT applications.

- Providing a survey of the existing formal verification approaches in IoT environment.
- Discussing the important aspects of formal verification approaches in the IoT environment for improving their mechanisms in future research.
- Exploring the future research directions the role that the formal verification approaches can play in the IoT.

The rest of this paper is organized as follows: In Section 2, some important aspects and motivations are illustrated. Section 3 provides the classification and analysis of formal verification approaches in IoT environments. The comparison and a discussion about the reviewed techniques are presented in Section 4. Finally, Section 5 concludes the paper.

2. IOT APPLICATIONS

One of the important issues in the IoT is recognizing critical defects to avoid system failures (Deng et al. 2018). Analyzing the correctness of the behavioral workflows of IoT deployments with system failures involves companies using real-time information from smart sensors and devices in critical manufacturing systems. Prediction of system failures in IoT deployments can effect on the high-risk conditions such as refining safety of industries gas and oil, smart grids and manufacturing, against the consumer-centric products of IoT applications (Ali et al. 2019). In other hand, IoT applications have some business benefits to comfort commercial interactions between manufacturing employers and end customers. These benefits include enhanced consumer satisfaction, consumer-centric product roadmaps, provided customer equipment and improved ability management. Figure 1 illustrates a conceptual variety of IoT applications. Some major activities include manufacturing, smart grid, industry, robotics and enterprise environment. The enterprise environment contains some main activities such as health-care, agriculture, smart and home cities, smart communication and smart buildings. All of the major activities are connected and interacted with many sensors, actuators, and RFID nodes.

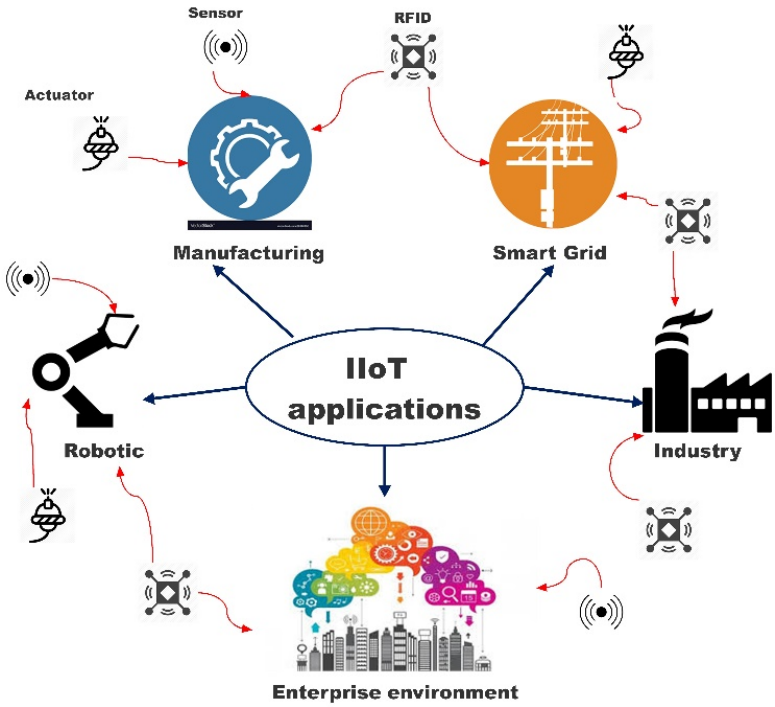

Figure 1. Variety of IoT Applications in the IoT and Enterprise Activities

Many challenges of IoT can be solved through a comprehensive collection of solutions by formal verification techniques. This technique leads to provide formal verification tools that are capable to check and verify the whole behavior of a system and prove in a mathematical manner that no error or bug remains in it. It is obvious that simulation and emulation of systems cannot afford to ensure verifying and detecting all bugs. It means that formal verification technologies contribute to emerging fully safe hardware or software systems (Ahmad et al. 2019).

Specific formal applications can investigate needing to be fail-safe for safety purposes in developments and designs in order to evaluate the casual faults, besides specifying those faults which don't have an impact on the ordinary functional procedure of the hardware. Furthermore, formal applications are capable to verify the correctness of hardware safety operations and also provide comprehensive fault analysis. Formal verification outcomes can be merged with fault analysis from simulator performs intelligently. Combining the results of formal assessing with simulation can be one of the most important fragments of evaluating entire verification evolution and determining the time of beginning the next phase of the development (Souri et al. 2016). It is essential to specify when and how formal methods

should be applied in the first steps of the verification process. Verification techniques support to choose and combine verified engines during the design according to the design desires. It has been may be considered that verification of IoT semiconductor devices seems to be an easy process, however, this is hardly the case (Perković et al. 2019).

3. CLASSIFICATION ON FORMAL VERIFICATION OF IOT

In this section, a state-of-the-art review of the formal verification approaches in the IoT applications is provided. Figure 2 presents a brief taxonomy for formal verification of IoT applications in this survey. Three main verification methods including model checking, process algebra and theorem proving are considered to evaluate the existing IoT applications including security, health-care, communication protocols, and environmental monitoring.

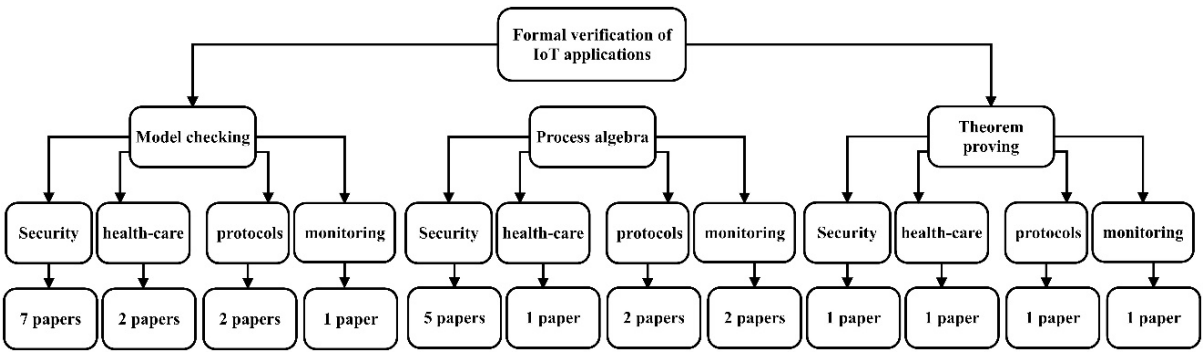

Figure 2. Technical Taxonomy of the Formal Verification Approaches in the IoT Applications

Aziz (2016) modeled and analyzed the MQ Telemetry Transport (MQTT) version 3.1 protocol, which is used in communications with small devices that exhibit limited computational and storage power. The first two QoS modes of operation in the protocol are specified and their message delivery semantics to subscribers are verified to hold. The model of MQTT is verified using process algebra called TPi, which is a synchronous message-passing calculus capable of expressing timed inputs. This model should be verified using any of automated verification tools.

Dhillon and Kalra (2017a) proposed a lightweight multi-factor remote user authentication protocol which employs gateway node based architecture for IoT environment that requires the user to first register itself through gateway node. The security analysis proved that it is

robust against multiple security attacks. The AVISPA is performed as a formal verification tool to prove the protocol security in the vicinity of a possible intruder. A testbed is needed to examine the memory requirements of the proposed protocol and confirm using the proposed protocol for real IoT devices.

Moreover, Hameed et al. (2017) proposed a zero watermarking method to ensure the integrity of data to be processed by base stations (BS) in the context of wireless sensor network (WSN) applications. A watermark built with the data sent by source nodes. For testing this mechanism, two different environments and comparison with Asymmetric Cryptography (ACT) and Reversible Watermarking (RW) frameworks have been considered. ACT and RW frameworks use a hash function to generate the watermark. The experimental results proved that zero watermarking framework gets better computational efficiency and consume lower energy. Using the proposed zero watermarking frameworks should be tested for secure provenance in IoT.

La (2016) have proposed a conceptual framework for disease diagnosis schemes with medical IoT contexts. A formal model presented for essential terms, concepts and proposed disease diagnosis. Moreover, five representative frameworks proposed for diagnosing diseases with the repository of medical measurements. Smart Toilet System implemented based on this prototype and implementation results show that the proposed diagnosis frameworks are practically implementable and yield quite precise diagnosis results. Moreover, the patterns, frequencies and persistency of trajectory-related measurements were useful in identifying the medical abnormality. This proposed framework should be tested for building various digital healthcare services within IoT contexts.

In addition, Lanotte and Merro (2018) proposed a process calculus called CaIT to investigate the semantic theory of networked systems in the IoT paradigm. The authors formalized dynamics of CaIT using an intuitive reduction semantics and a more operational labeled intentional semantics. The authors reported that the main differences between CaIT and the IoT-calculus. In CaIT, timed behaviors supported with desirable time, consistency and fairness properties. This semantic proof-methods used to confirm run-time properties of a non-trivial case study.

Drozdov et al. (2017) have presented an approach of using time-aware computations in

order to permit the controller to evaluate the quality of the input data. Formal verification method is used to check the Cyber-physical agnosticism (CPA) property of the IoT in industrial automation applications. In order to reduce the SMV model complexity, an abstract model of the plant was created which consists of four state machine instances included one elevator car and three doors. The abstract plant model is converted to SMV language and NuSMV model checker. Implementation results showed that if the communication delay was ignored, the elevator would stop in-between the floors and open the doors that are considered unsafe. Time-aware computation is used to make sure that the elevator always follows safe behavior which is the advantage of this study. This approach should be done in a more real-life industrial example.

Kim et al. (2017) presented a Secure Swarm Toolkit (SST) for constructing an authorization service infrastructure for the IoT. We expect heterogeneous IoT devices, ranging from sensor nodes to electric power grid control systems, can be integrated into the authorization infrastructure by virtue of SST's diverse security alternatives. A formal security analysis using an automated verification tool Alloy Analyzer performed in this study. The Alloy Analyzer is a tool to execute a model or automatically verify it against the desired property. Simulation results showed that SST can prepare necessary security guarantees. Defense and mitigation against denial-of-service attacks breaching availability are some of the challenges in the security of the IoT.

Moreover, Mohsin et al. (2017) presented a novel IoT Risk Analyzer framework for automated verification and probabilistic quantification of attack likelihoods against generic IoT system configurations. A formal model-driven verification approach used to verify all possible behaviors of the reference model using a finite state space and precisely assess the cause and degree of security risks. The (Markov Decision Process) MDP models generated by the proposed framework are used in the PRISM model checker to automatically analyze the system-level risk profiles. Evaluation results indicated that IoT Risk Analyzer is efficient and automatically prioritizes the input configurations on the basis of risk exposure.

Nishiwaki (2016) introduced a new programming language for application construction of self-stabilizing field computation named F-calculus. The proof of the equivalence between the class of the self-stabilizing field calculus and the class of unconditionally terminating F-

calculus is the main advantage of this study. The implementation results showed that static prediction of self-stabilization reduced to standard terminating verification. But, F-calculus does not provide a way to control dynamic behavior during stabilization.

Saxena and Raychoudhury (2017) presented NHealthIoT which is a human and data-centric smart system that uses named data networking (NDN) for naming, service discovery, device registration, securely publish data, and etc. The authors extended the workflows intuitive formal approach (WIFA) model to analyze and verify the correctness of NHealthIoT workflow during the emergency which is the main contribution of this study. The experimental results proved the validity of NHealthIoT. The performance of NHealthIoT should be optimized on a wider scale, under different scenarios and applications.

In addition, Xu et al. (2016) presented a novel framework to evaluate the QoS of IoT applications against specified performance queries based on the generated the Network of Priced Timed Automata (NPTA) models as the model of computation of the extended ThingML modeling language that implemented in Java. Using the proposed mapping rules in this study, extended ThingML designs automatically transformed into NPTA models for the quantitative analysis. Experimental results using two case studies demonstrated that the proposed approach effectively conduct the QoS evaluation and comparison for variation-based ThingML designs, which significantly facilitate the decision making of IoT designers.

Zahra et al. (2017) focused on deploying the Shibboleth protocol in a Cloud-IoT network for secure data access and outsourcing. The Shibboleth protocol provides an architecture which manages both security and access. This study proposed the Shibboleth-based Fog-IoT network which includes Shibboleth for ensuring security between Fog Client and Fog Node. To prove its correctness of Shibboleth against selected security properties the authors formally verified it using High Level Petri nets (HLPN) which is a tool for the mathematical and graphical modeling. Moreover, the Z3 SMT solver used for analyzing the rules of information flow, which proved the correctness of system against the three security properties and its results exposed that the asserted security properties approved Shibboleth the best fit for ensuring strong security in Fog-IoT network. In addition, the verification results showed that all the selected security properties executed in finite time which means these properties truly exist in Shibboleth.

Moreover, Bae (2017) proposed a security protocol to address the security vulnerabilities in medical IoT communication. The proposed software-based communication protocol used inter-device cross-authentication and encryption to deter diverse attacks and was verified with Casper/FDR (Compile for the Analysis of Security Protocols/Failure Divergence Refinements), which is used for the formal verification of processes. Verification results showed that the proposed protocol proved itself to ensure the security and safety of wireless communication between medical devices. Moreover, this study proved that the formal verification tool can reduce mistakes and errors in designing the security protocol and ensures effective verification.

Desnitsky and Kotenko (2016) proposed a new technique and a software tool for combining security components of IoT device, considering non-functional characteristics. Checking information flow security policy, taking into account specific kinds of anomalies between the rules, testing anomalous data from sensors, and revealed a few kinds of security component conflicts examined using a technique and a software tool. A security policy verified by checking network information flows using SPIN tool and PROMELA language and the correctness of this approach was successfully confirmed. Provisioning of specific expert knowledge for design, verification, and testing of systems with embedded devices and construction of tools to improve the security within the concept of the IoT are the main advantages of this study.

Diwan and D'Souza (2017) proposed a framework using refinement and decomposition techniques of Event-B to model three communication IoT protocols MQTT, MQTT-SN, and CoAP. Through simulation in Rodin, QoS formally verified. Simulation results showed that the protocols work as intended in an uninterrupted network as well as with an intruder which consumes messages in the network. Moreover, this framework provided reliable message transfer over a lossy network and reduced overhead by providing features like persistent connections, and retain messages. Other aspects of protocols like security, user authentication, and encryption should be analyzed.

Elleuch et al. (2017) presented a new approach for the formal examination of the coverage performance of wireless sensor networks utilizing the k-set randomized planning to save energy. This approach applied to perform the formal probabilistic investigation of a hybrid

monitoring structure for environmental IoT applications. Describing the primary formalizations of the k-set randomized planning and its coverage properties utilizing new probability theory within the HOL4 theorem prover is the main advantage of this research.

In addition, Han and Bae (2016) proposed a communication protocol based on an improved protocol. The proposed protocol made it virtually impossible for intruders to intervene in communication for hacking attacks because agents use session keys to authenticate each other and to verify hash functions before transmission. To prove the stepwise security of the proposed authentication protocol, it was specified in Casper language and verified with the FDR tool in terms of livelock, deadlock, and safety. The verification results showed that the proposed protocol met all security attributes in the trial.

Kammüller (2018) and Kammüller (2017) presented a new formal modeling by integrating former formal methods to model actors, devices and also policies of human-centric infrastructures for IoT Health Care Systems with the aim of investigating privacy and security risks. The authors used the interactive theorem prover named Isabelle which provisions modeling and examination of human-centric infrastructures by attack paths analysis. The strong point of suggested formal modeling is providing a direct foundation instead of an on-paper mathematical formalization to make it applicable to real scenarios without demanding to any further mathematical tools. The weakness of the offered attack tree framework is its restriction in contrast with the current foundation.

Mangano et al. (2017) presented an effective case study on reasonable verification of a memory allocation module in Contiki to ensure security and safety of software for the IoT with FRAMA-C which is an influential tool for examination of C code. In this paper, two aspects were considered: 1) the common implementation of the module for all types of blocks (especially in pointer arithmetic and casts) and the requirement to identify the number of available blocks (demanding accepted definitions for counting elements in the block status array) which were two main challenges for formal verification of C software before, However, they can be effectively applied by recent verification tools such as FRAMA-C/WP. This report paper confirms that automatic theorem provers can be used on properties that are difficult to be proven automatically and have made a major improvement.

Tata et al. (2017) proposed a formal approach for decomposing process-aware applications

to be used in a set of communication fragments in IoT ecosystems. The authors implemented a formal method in Petri nets, to verify the correctness of the decomposition regarding language preservation. They extended the Node-RED tool for modeling distribution and running of IoT applications.

Moreover, Aktas and Astekin proposed a run-time proof method of things for self-managing ability in the IoT environment. In this paper, an architecture was presented in real-time big data framework to apply offered verification method of IoT objects. Also, they proposed a new depiction for verifying events and relations of IoT components. Furthermore, verification rules for each IoT element were defined according to their technical specifications to activate self-healing activities in the IoT domain. In this work, two samples of the suggested architecture were implemented to show the performance and scalability of the proposed solution.

Dhillon and Kalra (2017b) proposed a protected multi-factor distant user verification protocol for IoT environments. The scheme applies three elements for protecting user identity including password, smart device, and biometrics. Then, to evaluate the security of the protocol, the authors presented a formal and informal security examination. Finally, comparative analysis regarding the computational and communication overhead of other protocols was carried out.

Ouaddah et al. (2016) proposed a novel framework based on blockchain concept for access control in IoT. In this paper, a model was provided for the proposed framework which contains architecture, mechanism specification and models in IoT. The authors introduced a privacy-preserving permission controlling framework to allow users to have and manage their own data and adapted blockchain technology to the proposed framework. The advantage of the offered solution is introducing new categories of transactions that are used to give, get, grant, and cancel access, contrasting the financial bitcoin transactions. The authors implemented their proposed model with a Raspberry PI device and local blockchain.

In addition, Venckauskas et al. (2016) offered a modeling framework that contains feature-based modeling to specify abstract models for illustration of relations and restrictions between QoS properties of an IoT application such as performance, security and environmental factors. The authors proposed a lower level modeling by providing physical quantities to find the measurable attributes to approximate QoS between the modeled features. They used

feature-based models to make effective configurations of modeled features to provision the validity needs of the IoT application. Also, they used measurement-based models to create the three-dimensional attribute space to find measurable associations between performance, security levels, and energy.

Finally, Zhang and Chen (2015) proposed an approach for constructing scalable IoT services regarding their event-driven models that their data model, computation logic, and communication behavior are identified with respect to the environmental restrictions. In this paper, an event session technique is applied to define the management between IoT services and their unlike activities. By the event-driven IoT service model, the service's decoupling possibilities which are discovered from three sides and acts as its scalable structure. The first side is to solve concurrent performing services. The services behavior decoupling is recognized by the behavior of the decomposition algorithm. The second side is to solve the problem of distributed execution of a business process, and the business process behavior decoupling is specified with respect to decomposing it into parts of local computation logic and event composition logic. The third side is to answer the problem of state explosion of proving the composite service attributes. Finally, the authors proposed a platform to provision generating scalable IoT services with the behavior decoupling properties and adapt the application to concept-prove the work.

4. DISCUSSION, CHALLENGES AND FUTURE DIRECTIONS

In this section, the analytical analysis is presented. Figure 3 illustrates a comparison side of formal verification techniques on the IoT applications. Model checking has most usage with 46% for evaluating the correctness of IoT applications in research studies (Desnitsky & Kotenko 2016; Dhillon & Kalra 2017a; Diwan & D'Souza 2017; Drozdov et al. 2017; Hameed et al. 2017; Han & Bae 2016; Kim et al. 2017; Mohsin et al. 2017; Saxena & Raychoudhury 2017; Tata et al. 2017; Xu et al. 2016; Zahra et al. 2017). Also, the process algebra approach has 39% to assess the correctness of the IoT applications in research studies (Aktas & Astekin 2019; Aziz 2016; Bae 2017; Dhillon & Kalra 2017b; La 2016; Lanotte & Merro 2018; Nishiwaki 2016; Ouaddah et al. 2016; Venckauskas et al. 2016; Zhang & Chen 2015). Finally, some research studies (Elleuch et al. 2017; Kammüller 2017, 2018; Mangano

et al. 2017) have used theorem proving to prove and evaluate the correctness of the proposed case studies on the IoT applications.

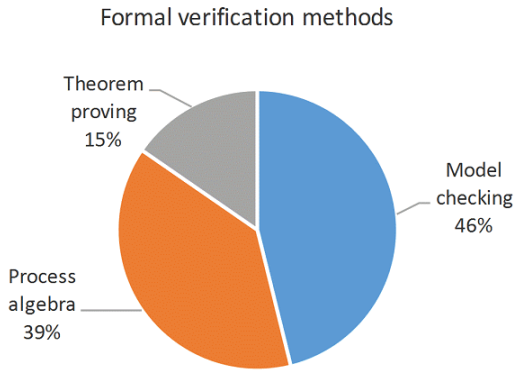

Figure 3. Formal Verification Techniques on the IoT Applications

Figure 4 presents the number of IoT applications in the formal verification methods. The security issue is the most important topic to consider formal verification of IoT applications using model checking and process algebra methods. The environmental monitoring such as smart home, smart city, vehicular transportations, industrial systems has new open issues for verifying the existing case studies. Table 1 shows the comparison of quality factors for existing studies according to a related topic, measurement method and evaluation factors.

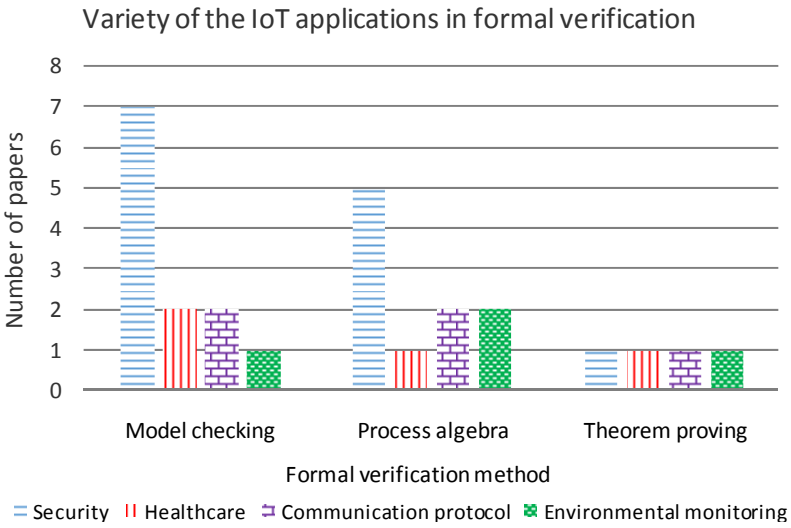

Figure 4. Formal Verification Techniques on the IoT Applications

Figure 5 presents the variety of published research studies on the formal verification of the IoT applications. Most popular conference papers have been published in the Springer. Also, most journal papers have been published in the Elsevier and Wiley journals.

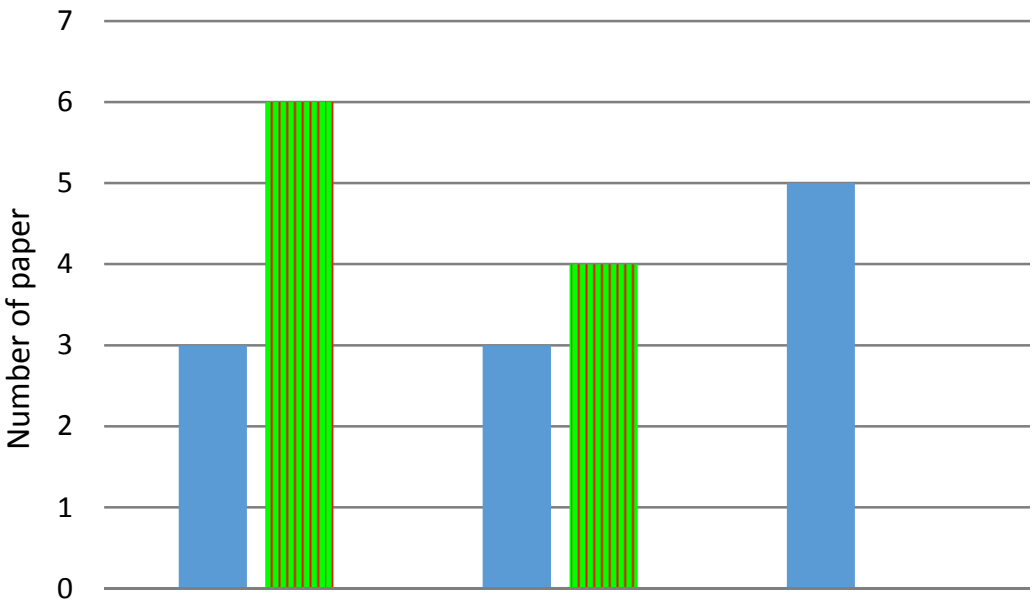

Figure 5. Distribution of the Research Studies in the Formal Verification

There are many future works in IoT application fields. Scalability and mobility have several weak points in studied works that have not addressed the time. To improve scalability criterion in a fog environment, it is required to cover scaling the resources from the few included spaces in the fog layer and the utilized smart devices in the IoT/end-clients layer. Hybrid cloud environments can joint to smart devices of IoT end users as a potential key solution to provide upstream resource management through a worldwide perspective of the fog environment. The mobility research direction is the most important challenge in application placement approach to cover mobile entities such as health-care and transportation applications. Using a vehicular ad hoc network (VANET) architecture can effect on covering application mobility with IoT smart devices and fog computing. Some new challenges to this open issue include using hybrid clouds, applying device mobility, and providing dynamic migration.

Table 1. The Comparison of Quality Factors for Existing Research Studies

References	IoT topic	IoT domain	Main weaknesses	Evaluation method/tool
Bae (2017), Desnitsky & Kotenko (2016), Kammüller (2018), Aktas & Astekin (2019), Dhillon & Kalra (2017b), Ouaddah et al. (2016), Venckauskas et al. (2016), Drozdov et al. (2017), Kim et al. (2017), Mohsin et al. (2017), Zahra et al. (2017), Dhillon & Kalra (2017a), Hameed et al. (2017)	Security	Authentication, Cyber physical system, Cyber-attack, Block-chain, Cryptography	• Simple abstraction model to verify all conceptual characteristics • High verification time and memory consumption	AVISPA, MATLAB, Petri Net, Alloy, UPPAAL
Aziz (2016), Xu et al. (2016), Nishiwaki (2016), Mangano et al. (2017), Diwan & D'Souza (2017)	Communicat ion protocols	MQ, memory allocation	• State space exclusion • High verification time	Contiki, UPPAAL
Han & Bae (2016), Kammüller (2017), Saxena & Raychoudhury (2017), La (2016)	Healthcare	Disease Diagnosis, Hospital, Health attacks	• Presenting a simple state space of the model • Not analyzing verification time	HOL, MATLAB
Lanotte & Merro (2018), Zhang & Chen (2015), Elleuch et al. (2017), Tata et al. (2017)	Environment al monitoring	Train monitoring, Industrial, Smart home	• Omitting some critical properties such as deadlock and reachability • Static construction for formal analysis	Petri Net, HOL, MATLAB

In addition, according to the generating a large volume of data by diverse sources in IoT, the challenges in some other key problems such as data processing, efficient data retrieval, protected data storing and dynamic data gathering in IoT, have been arisen. Therefore, working on cost-effective and practical frameworks are essential to address the mentioned challenges through using the fog computing and cloud computing. With respect to the wide range of using wireless communication technologies in IoT applications, supporting real-time communication in open environments and over license-free bands is an inspiring issue. Conversely, the traffic made by uncontrolled stations in open communication environments, cannot be protected by current Medium Access Control (MAC) protocols. Hence, developing new MAC methods that are able to support low power communication is an inspiring issue.

5. CONCLUSION

In this paper, a state of the art survey is presented in the formal verification of the IoT applications. We considered just formal verification approaches that directly evaluated the IoT applications based on correctness proof mechanisms. The formal verification approaches of the IoT applications were compared with each other according to the advantages and limitations based on three categorizations including model checking, process algebra and theorem proving. Model checking has the most usage for evaluating the correctness of IoT applications. The security issue is the most important topic to consider formal verification of IoT using model checking and process algebra methods. The environmental monitoring such as smart home, smart city, vehicular transportations, and industrial systems has new open issues for verifying the existing case studies. In the future work, we will try to consider a systematic mapping study on the entire formal verification mechanisms on the sensor, actuators, smart devices and applications of IoT environments.

REFERENCES

Ahmad S, Malik S, Ullah I, Park DH, Kim K, & Kim D (2019). Towards the Design of a Formal Verification and Evaluation Tool of Real-Time Tasks Scheduling of IoT Applications. Sustainability 11(1): 204.

Aktas MS, & Astekin M (2019) Provenance aware run-time verification of things for self-healing Internet of Things applications. Concurrency and Computation: Practice and Experience, e4263-n/a. doi: 10.1002/cpe.4263.

Ali MS, Jewel MKH, Li Y, & Lin F (2019) Frequency-domain channel equalisation for LTE-based uplink narrowband Internet of Things systems. IET Communications 13(3): 281-288. https://digital-library.theiet.org/content/journals/10.1049/iet-com.2018.5119

Asghari P, Rahmani AM, & Javadi HHS (2018) Service composition approaches in IoT: A systematic review. Journal of Network and Computer Applications 120: 61-77. doi: https://doi.org/10.1016/j.jnca.2018.07.013.

Asghari P, Rahmani AM, & Javadi HHS (2019). Internet of Things applications: A systematic review. Computer Networks 148: 241-261.

Aziz B (2016) A formal model and analysis of an IoT protocol. Ad Hoc Networks 36: 49-57.

Bae WS (2017) Verifying a secure authentication protocol for IoT medical devices. Cluster Computing. doi: 10.1007/s10586-017-1107-x.

Deng Y, Chen Z, Zhang D, & Zhao M (2018) Workload scheduling toward worst-case delay and optimal utility for single-hop Fog-IoT architecture. IET Communications 12(17): 2164-2173.

Desnitsky V & Kotenko I (2016) Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge. Journal of Ambient Intelligence and Humanized Computing 7(5): 705-719.

Dhillon PK & Kalra S (2017a) A lightweight biometrics based remote user authentication scheme for IoT services. Journal of Information Security and Applications 34: 255-270.

Dhillon PK & Kalra S (2017b) Secure multi-factor remote user authentication scheme for Internet of Things environments. International Journal of Communication Systems 30(16): e3323-n/a.

Diwan M & D'Souza M (2017) A Framework for Modeling and Verifying IoT Communication Protocols. In K. G. Larsen, O. Sokolsky & J. Wang (Eds.), Dependable Software Engineering. Theories, Tools, and Applications: Third International Symposium, SETTA 2017, Changsha, China, Proceedings (pp. 266-280). Cham: Springer International Publishing.

Drozdov D, Patil S, Dubinin V, & Vyatkin V (2017) Towards formal verification for cyber-physically agnostic software: A case study. Paper presented at the IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society.

Elleuch M, Hasan O, Tahar S, & Abid M. (2017) Formal Probabilistic Analysis of a WSN-Based Monitoring Framework for IoT Applications. In C. Artho & P. C. Ölveczky (Eds.), Formal Techniques for Safety-Critical Systems: 5th International Workshop, FTSCS 2016, Tokyo, Japan, November 14, 2016, Revised Selected Papers (pp. 93-108). Cham: Springer International Publishing.

Ghobaei-Arani M, Rahmanian AA, Souri A, & Rahmani AM (2018) A moth-flame optimization algorithm for web service composition in cloud computing: Simulation and verification. Software: Practice and Experience, 48(10): 1865-1892.

Hameed K, Khan A, Ahmed M, Goutham Reddy A, & Rathore MM (2017) Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things

based-wireless sensor networks. Future Generation Computer Systems. doi: https://doi.org/10.1016/j.future.2017.12.009.

Han KH, & Bae WS (2016) Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices. Cluster Computing 19(4): 2335-2341.

Kammüller F (2017) Formal Modeling and Analysis with Humans in Infrastructures for IoT Health Care Systems. In T. Tryfonas (Ed.), Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings (pp. 339-352). Cham: Springer International Publishing.

Kammüller F (2018) Human Centric Security and Privacy for the IoT Using Formal Techniques. In D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17−21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA (pp. 106-116). Cham: Springer International Publishing.

Kim H, Kang E, Lee EA, & Broman D (2017) A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things. Paper presented at the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI).

La HJ (2016) A conceptual framework for trajectory-based medical analytics with IoT contexts. Journal of Computer and System Sciences 82(4): 610-626.

Lanotte R & Merro M (2018) A semantic theory of the Internet of Things. Information and Computation 259: 72-101.

Mangano F, Duquennoy S, & Kosmatov N. (2017) Formal Verification of a Memory Allocation Module of Contiki with Frama-C: A Case Study. In F. Cuppens, N. Cuppens, J.-L. Lanet & A. Legay (Eds.), Risks and Security of Internet and Systems: 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers (pp. 114-120). Cham: Springer International Publishing.

Mohsin M, Sardar MU, Hasan O, & Anwar Z (2017) IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. IEEE Access 5: 5494-5505.

Nishiwaki Y (2016) F-Calculus: A Universal Programming Language of Self-Stabilizing Computational Fields. Paper presented at the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W).

Ouaddah A, Abou Elkalam A, & Ait Ouahman A (2016) FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks 9(18): 5943-5964.

Perković T, Čagalj M, & Kovačević T (2019) LISA: Visible light based initialization and SMS based authentication of constrained IoT devices. Future Generation Computer Systems.

Saxena D & Raychoudhury V (2017) Design and Verification of an NDN-Based Safety-Critical Application: A Case Study With Smart Healthcare. IEEE Transactions on Systems, Man, and Cybernetics: Systems 99: 1-15.

Souri A, Asghari P, & Rezaei R (2017) Software as a service based CRM providers in the cloud computing: Challenges and technical issues. Journal of Service Science Research 9(2): 219-237.

Souri A, Norouzi M, Safarkhanlou A, & Sardroud SHEH (2016) A dynamic data replication with consistency approach in data grids: modeling and verification. Baltic Journal of Modern Computing 4(3): 546.

Souri A, Nourozi M, Rahmani AM, & Jafari Navimipour N (2018a) A model checking approach for user relationship management in the social network. Kybernetes 48(3): 407-423.

Souri A, Rahmani, AM, & Jafari Navimipour N (2018b), Formal verification approaches in the web service composition: A comprehensive analysis of the current challenges for future research. International Journal of Communication Systems 31(17): e3808.

Souri A, Rahmani AM, Navimipour NJ, & Rezaei, R. (2019) Formal modeling and verification of a service composition approach in the social customer relationship management system. Information Technology & People, (Earlycite) https://doi.org/10.1108/ITP-02-2018-0109.

Souri A, Rahmani AM, Navimipour NJ, & Rezaei R (2019) A symbolic model checking approach in formal verification of distributed systems. Human-centric Computing and

Information Sciences 9(1): 4. doi: 10.1186/s13673-019-0165-x.

Tata S, Klai K, & Jain R (2017) Formal Model and Method to Decompose Process-Aware IoT Applications. In H. Panetto, C. Debruyne, W. Gaaloul, M. Papazoglou, A. Paschke, C. A. Ardagna & R. Meersman (Eds.), On the Move to Meaningful Internet Systems. OTM 2017 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, October 23-27, 2017, Proceedings, Part I (pp. 663-680). Cham: Springer International Publishing.

Venckauskas A, Stuikys V, Damasevicius R, & Jusas N (2016) Modelling of Internet of Things units for estimating security-energy-performance relationships for quality of service and environment awareness. Security and Communication Networks 9(16): 3324-3339.

Xu S, Miao W, Kunz T, Wei T, & Chen M (2016) Quantitative Analysis of Variation-Aware Internet of Things Designs Using Statistical Model Checking. Paper presented at the +2016 IEEE International Conference on Software Quality, Reliability and Security (QRS).

Zahra S, Alam M, Javaid Q, Wahid A, Javaid N, Malik SUR, & Khan MK (2017) Fog Computing Over IoT: A Secure Deployment and Formal Verification. IEEE Access 5: 27132-27144.

Zhang Y & Chen JL (2015) Constructing scalable Internet of Things services based on their event-driven models. Concurrency and Computation: Practice and Experience 27(17): 4819-4851.

AUTHOR BIOGRAPHIES

Alireza Souri received his B.S. degree in Software Engineering from University College of Nabi Akram, Iran, in 2011 and his M.Sc. and PhD degrees in Software Engineering from Science and Research Branch, Islamic Azad University, Iran in 2013 and 2018. He is a researcher and lecturer at Islamic Azad University. Up to now, he has authored/co-authored 40 academic articles. He served on the program committees and the technical reviewer of several ISI-index journals and international conferences. He currently is an Associate Editor member of Human-Centric Computing and Information Sciences (Springer), Cluster Computing (Springer) and IET Communications (IEEE) journals. His research interests include Formal Specification & Verification, Model checking, Grid & Cloud computing, IoT and Social networks. Now, He is a member of The Society of Digital Information and Wireless Communications.

Monire Norouzi received her B.Sc. in Computer Engineering at University College of Nabi Akram, Iran in 2011. She received M.Sc. in Software Engineering from Shabestar Branch, Islamic Azad University in Iran. Her main research interests are Software Analysis, Wireless Network and Sensor Network, verification and validation of Software Systems.