Effectivity Score of Simulation Tools towards Modelling Design in Internet-of-Things

Gauri Sameer Rapate
Assistant Professor
Dept. of Computer Science and Engineering
PES University, Bangalore, India

Dr. N C Naveen
Prof and Head
Dept. of Computer Science and Engineering
JSS Academy of Technical Education, Bangalore, India

***Abstract*—Simulation tools play an integral and significant role in studying the applicability and effectiveness of different algorithms for solving real-world problems cost-effectively. In the case of Internet-of-Things, the issues associated with real-world implementation are exponentially multi-fold. Although various simulators have facilitated the evolution of schemes to address the problems in IoT applications in the last few years, their applicability in the real world is highly questionable. Hence, this paper discusses the potential features of existing simulations (both commercial and research-based) and investigates features of different assessment environment tools to understand their current state. The paper further contributes toward a distinct research pattern. The core contribution of this manuscript is to review standard practices of using simulation tool along with different test environments. The paper also contributes towards exploring various prospects of unaddressed problems associated with a usage of existing simulation environment/tool for investigating the challenging and practical environment of an IoT ecosystem. The learning outcome of this study will assist the reader to make a decision towards adopting precise simulation tool for their work as well as it also highlights the need to perform more number of customization towards including the features that is found in research gap.**

***Keywords*—Internet-of-things; real-world; application; simulation model; environment**

I. INTRODUCTION

The process and various operation ranges involved in the real world are sometimes quite challenging to investigate and study, considering real-world entities. This problem can be solved by using simulation modeling to efficiently and safely perform the processes to offer solutions [1]. The implemented methods using different spectrums of the algorithm during the simulation study facilitate a simplified verification process over-controlled research environment [2]. This paper discusses the simulation perspective of studying various problems in Internet-of-Things (IoT), a network of different physical devices called things with distinct identifiers [3]. The dependable attributes for framing an IoT ecosystem are communication devices, sensors, processors, etc. [4]. An edge device or an IoT gateway node collects the sensory data shared via IoT devices and is forwarded to the cloud for storage or analysis [5]. However, implementing such a large ecosystem of an IoT is comprehensively a massive task as they are also associated with various implementation impediments, e.g., challenges of inappropriately aggregated data, processing of unstructured data, ensuring coverage and connectivity of a large number of IoT device, ensuring power management for resource constraint sensors, challenges associated with data storage, integrating with all points of an IoT with appropriate software, proper identification of an IoT device with legitimate authentication, and compatibility issues of a large number of heterogeneous system in an IoT [6]. However, it should be noted that IoT is not only about sensory data collection [7], routing [8], and storage [9], but it is strongly related to potential data analytical operations, too [10]. At present, there are various schemes to ensure an effective operation of IoT communication in the majority of the perspective [11]-[14]; however, it is seen that the majority of such studies are carried out using a simulation-based approach while only a few proportions of work is carried out over real-time models and data. Both such schemes (real world and simulation-based) have their benefits and limitation. However, simulation-based studies are still more favorable toward cost-effective analysis, leading to much successful deployment in the real world. However, such a simulation-based approach should be deeply investigated to find out if they are really at par with solving impending problems in an IoT.

There is no doubt about the availability of a list of different simulators in current times for deploying novel logic for implementing an IoT. However, questions still arise about the taxonomies of such simulators, the discrete beneficial features towards cost-effective deployment, judging the applicability of simulation outcomes in the practical world, and finding the most adopted simulation tool in recent years. Finding answers to these questions will eventually guide better decision-making, either towards adoption or the evolution of new simulators in IoT. The prime motivation of the proposed study is to showcase the discussion on simulators with a higher and lower adoption rate in the last few years. Therefore, the *novelty* of the proposed study is towards assessing the functionalities and features of existing simulators towards investigating problems in IoT. Finally, the study also elaborates on the first and second levels of the research gap, unlike any existing research update. The contribution of the paper is as follows:

1) The paper offers a brief and compact insight towards the existing 5 standard simulation tools of an IoT exercised in commercial sector as well as 16 frequently adopted simulation tools practiced in research-based area.

2) The paper highlights essential characteristics of 6 standard environments adopted for assessing the protocols and algorithms meant for an IoT environment.

3) Existing trends of research work that is found towards developing simulation-environment is discussed in this paper that assists in highlighting the highly adopted simulation tool for studying IoT ecosystem.

4) The paper exclusively discussed elaborately about the research gap associated with the existing developments towards IoT simulation tool that offers critical information about unaddressed research problems.

The manuscript's organization is as follows: Section II discusses the existing simulation tools into practice, while Section III discusses the assessment environment offered by such simulation tools. Discussion of existing research trends towards using simulation tools is carried out in Section IV. In contrast, a meeting of the research gap is carried out in Section V. Finally; Section VI provides conclusive remarks and future work direction.

II. Simulation Tools for IoT

The simulation tools for assessing the performance of a newly developed logic for an IoT environment must adhere to standard vital parameters. With an expected budget of communication link above 164 dB and modulation method of either BPSK or QPSK for uplink transmission and QPSK for downlink transmission, the simulation for an IoT should be set up in FDD half-duplex mode. The simulation key parameter includes 64 kbps and 25 kbps of uplink and downlink data transmission with a latency of around 10 seconds. The most simulation also considers SC-FDMA for uplink transmission while OFDM for downlink transmission. The above mentioned are the prevalent values of critical parameters to be considered while carrying out a simulation study. This section further highlights the frequently used standard simulation tool in an IoT as follows:

A. Commercial Simulation Tool

These are the commercially used tools to assess the conditional logic, novel logic for communication in an IoT, and during prototyping of certain sense of implementation in an IoT.

1) MIMIC simulation tool [15]: This simulator manages various essential entities in an IoT environment, e.g., all the connected devices, sensors, and gateway nodes. The idea is to form a standard test assessment scenario of IoT capable of deploying and evaluating Industry 4.0, architectures with event-driven approaches, agriculture, factories, and smart cities.

2) IoTNetSim tool [16]: This simulation tool can manage different variants of the IoT network environment and structural information of the heterogeneous IoT nodes. The core idea is to facilitate a better form of modeling toward network connectivity concerning target application logic. The complete simulation process is carried out over three layers, viz. i) cloud layer, ii) edge layer, and iii) IoT layer. The *cloud layer* is responsible for obtaining and managing the data processed by the edge layer, particularly in the data center of an IoT. The processed information is then forwarded to the sophisticated virtual machine via a specific set of the authenticated host. The *edge layer* is responsible for obtaining the data from the gateway node, followed by further processing the data to forward it to the devices that run under the supportability of the cloud layer. The *IoT layer* is responsible for deploying and generating the sensing devices to transmit the data to the link node. Further, this data is forwarded to the gateway node that can access and process this data to be forwarded to the edge layer in the form of aggregated information.

3) Cooja simulation tool [17]: This is a frequently used simulation tool mainly for sensory application. Due to this capability, it is also used for an IoT environment with the involvement of sensors. This simulation tool can evaluate sensors with intelligent capabilities, different communication technologies, and frequently used internet protocols in an IoT. This simulation tool uses Contiki mote to simulate the real-time assessment environment capabilities. Three forms of windows carry out the complete operation of this simulation tool, i.e., i) network window, ii) control window for simulation, and iii) note window. The *network window* can exhibit the environments of all mores and their respective radio traffic. It can also organize the physical elements associated with the sensor mote for a more in-depth and practical analysis of sensory devices in IoT. The *control window for simulation* is responsible for managing all the execution during simulation and simulation speed. Finally, the *note window* can store the execution logic and contains all the essential simulation points. It should be noted that the standard protocol of 6LoWPAN is adopted by this simulation tool. Apart from this, the standard protocol of IPv6 is also adopted by this tool concerning devices compliant with the family of IEEE 802.15.4 standards. This prime dependency of this simulation tool to develop an IoT environment are mainly two viz. i) Contiki operating system as a part of a software module and Tmote Sky as a part of the hardware module. Using both software and hardware module, this simulation tool can perform initialization of sync nodes and sensor nodes followed by establishing a reliable communication using standard protocols. Further, the sensor node is transmitted to the sink node from the transmitting node by this tool.

4) IBM bluemix [18]: This is one of the famous commercial simulation tools for assessing the prototypes without dependencies on the physical device associated with an IoT platform. It is an IoT platform made to be functional in the IBM open cloud system so that the developer can easily access the proprietary software of IBM. This can significantly evaluate certain essential vital functions and security features associated with mobile and web applications. The continuous availability of cloud services offers the practical application and service manageability.

5) SimpleIoTSimulator [19]: This is one of the simplified forms of commercial simulator used to assess the environment for many IoT devices. It also offers much supportability of conventional IoT protocols, e.g., HTTPS, CoAP, and MQTT. This simulation tool facilitates different vendors to enhance product quality by formulating a better test environment. It offers supportability of both IPv6 and IPv4 sensors with operational supportability towards the constraint environment of an IoT.

B. Research-based Simulation Tool

There is a big difference between the simulation tool adoption for commercial practices and research-based studies. The commercial rules call for simulation tools with specific evaluation features; however, this is not the case with research-based simulation studies. Research work towards an IoT environment calls for including many features, conditional logic, and a flexible deployment environment to testify the targeted logic. Hence, simulation tools adopted for research-based work offer a more discrete set of operations with comprehensive functionalities. This section highlights the existing research-based simulation tools (Table I) as follows:

1) ANSYS-IoT simulator [20]: This form of simulation tool analyzes various forms of challenges in an IoT. The core usage of this simulation tool is mainly to assess the cumulative integrity of sensing devices with innovative capabilities deployed in an IoT environment. It is also used to assess longevity and energy consumption and enhance reliability, followed by validation.

2) Bevywise simulation tool [21]: This tool is specifically used for the scenario when fog computing is used in collaboration with an IoT environment. The tool facilitates the virtual clients by deploying the MQTT protocol on-premise. It also offers different variants of functional assessment over the cloud environment by enabling the deployment of many commodity servers. Particularly helpful for the industrial IoT environment, this simulation tool offers an end-to-end solution considering the constraints of the practical world of IoT implementation.

3) IoTIFY [22]: This tool offers a software backbone for operations associated with hardware modules of an IoT. This tool provides a precise building of a digital lab by harnessing a simplified construction of an analytical model and virtualization of an IoT device. IT can be used for analytical scaling, solutions for load testing, and building prototypes of an embedded system. It also assists in generating records and can well manage IoT devices used in a fog computing environment.

4) EdgeCloudSim [23]: This simulation tool caters to the demands of IoT operation dependent on computational queries of edge devices. It can carry out sophisticated calculations and evaluate its capacity to process the query and allocate necessary resources. This simulation tool is mainly meant for developers to assess the impact of their machine parameters on the communication and processing needs of an IoT node.

5) MobIoTSim [24]: The majority of the existing simulators of IoT demand higher resources to be used and are meant to be run on computing devices, e.g., desktops or laptops. This simulation tool is intended to simulate mobile-device built on the Android operating system.

6) TOSSIM [25]: This is another frequently used simulator by researchers who adopts sensor mote running on TinyOS. Hence, this tool can assess the smart sensory application running over an action-based operating environment.

7) SWE Simulator [26]: This simulation tool is mainly meant to assess the large-scale deployment scenario of IoT, including sensors. The tool also assists in effective cost control during implementation scenarios. It can also evaluate the presence of any risk factor and its possible influence. The simulation tool also uses observation services of sensors to develop topology and assess the performance of the assessment in an IoT.

8) Atomiton [27]: This is another simulator capable of simulating all the innovative sensory applications and involving different forms of actuators. Hence, this simulation tool assesses a specific state of the operating environment used for the complex operation of smart sensors in an IoT.

9) QualNet [28]: When the simulation study demands high-end accuracy, this is a preferred simulation tool for IoT applications. However, it should be noted that not all sensor devices are used for this form of simulation. Only the sensors compliant with specific families of IEEE 802.15.4 consider smart sensors. Although this is a commercial simulation tool, they are used extensively for research-based study. It also offers enriching interactivity owing to the improvised form of the Glomosim simulator.

10)NS3 Simulator [29]: This frequently used network simulator considers networks of the practical world scenario in IoT. The prime usage of this simulator is to assess the robustness of security features to resist various threats in the communication environment of an IoT. The tool offers the developer to use python and C++ for scripting while making use of the standard protocol of LTE, ZigBee, and 6LOWPAN. While working in an IoT environment, this tool adds three discrete types of devices, e.g., IoT node, blockchain, and Gateway. This simulation toolbox also assists in routing the class of all these entities in an IoT. The prime set of operations in an NS3 is to deploy the sensing IoT nodes, followed by applying standard protocol implementation of MQTT, HTTP, and CoAP. Finally, the data is forwarded to the sink.

11)OMNet++ [30]: This simulation tool is popularly known for its discrete event simulation facilitation. A unique discrete simulation environment is constructed using enriched libraries from C++. Inspired by the Eclipse environment, this tool uses high-level language to develop more prominent components. It thereby forms an object-oriented model of simulation that could be used for different apps.

12)SimIoT [31]: This simulation tool can be used for any IoT system characterized by the static or dynamic attributes in a trial and error process. This mechanism is primarily meant

for managing the clouds environment system concerning its host of data centers. It assists in both method construction and the configuration of various entities.

13)CupCarbon [32]: This simulation tool is mainly used for assessing wireless sensor networks in their discrete form using multi-dimensional visualization features with multi-agents. Different forms of distributed algorithms can be validated using this simulation tool. It can also validate various iterative tasks over automation processes mainly meant for industrial applications. Further, it can also evaluate different forms of routing schemes, protocols, communication, and topologies in wireless networks involved in an IoT.

14)IoTSim [33]: This is another popular simulation tool used in IoT deployed alongside cloud environments. It can also be an extension of the popular cloud-based simulation CloudSim. One of the significant functions of this simulation tool is that it assists in processing big data that uses distributed software framework MapReduce. The process of identification, as well as outcome analysis, is carried out using this simulation tool. It can be used for both research-based studies and industrial evaluation.

15)iFogSim [34]: This simulation is meant to carry out multiple levels of evaluation-based operation associated with different environment variants. It can simulate network connection, edge devices, fog data centers, IoT, etc. It can also be used for assessing another performance metric to be carried out over an IoT cloud environment. This simulation tool can also perform extensive assessments of various QoS metrics.

16)DPWSim [35]: This simulation tool profiles the devices synced with the web services associated with information exchanges, classification of services, and effective identification. This simulation tool is mainly used for explicit devices and applications related to the IoT to assess the dual form of operation, i.e., a function that enables hosting and processes that are being hosted. It also offers a better form of secure exchange of data

TABLE I. SUMMARY OF RESEARCH-BASED SIMULATION TOOL

Tool	***Security Score***	***Service domain***	***API integration***	***Built-in IoT Standards***	***A layer of IoT Architecture***	***Programming***	***scope***	***Type***
Ansys-IoT	High	Industry	REST	Real-Time	Network	Java, Python	IoT industry	Autonomous
Bevywise-IoT	Medium	Smart City	REST	Real-Time	Network	Java, Python	IoT device	Broker
IoTIFY	High	Smart City	REST	Real-Time	Application, Network	Java, Python	Hardware connection	Mobile App
Edge CloudSim	High	Edge Orchestrator	SOAP	Mist Computing	Network	Matlab	Edge, WLAN	Realistic
MobIoTSim	Medium	Generic	REST	Device profile for web services	Application, network	C#, C++	IoT Network	Research-based
TOSSIM	High	Generic	REST	Injecting packets	Communication Network	Python, C	TinyOS	Sensor monitoring
SWE-IoT	High	Human Interface	SOAP	Collision Detection	Communication Network	C, C++	WSN	Sensor monitoring
Atominition IoT	High	MQIdentity	REST	Socialize	Communication Network	Java	IoT, IIoT	Edge
QualNet	Medium	Generic	REST	802.15.4	Perceptual Network	C++	Network	Discretization
NS3	High	Generic	REST	LoRaWAN	Perceptual Network	C++	Network	Discrete event
OMNeT++	Medium	Generic	SOAP	Manual extension	Perceptual Network	C++	Network	Discrete event
SimIoT	High	Generic	REST	No	Application	Java	Data Analysis	Discrete event
CupCarbon	High	Smart city	UDX	LoRaWAN, 802.15.4	Perceptual Network	Java	Network	Discrete event (agent)
IoTSim	Medium	Generic	REST	No	Application	Java	Data Analysis	MapReduce model
iFogSim	Medium	Generic	SOAP	No	Perceptual Network Application	Java	Fig	Discrete event
DPWSim	Medium	Generic	SOAP	Messaging Web services security	Application	Java	IoT	Open-source

III. Assessment Environment of IoT

The previous section has elaborated on various existing simulation tools for evaluating various problems and their respective solution. It should be noted that the simulation tool facilitates the user to deploy their logic of implementation by reducing the same problem space of the IoT environment. It also enables various libraries to develop novel solutions. However, the simulation tool itself cannot be assumed to be 100% fulfilling the outcomes of the simulation study. For this purpose, there is a need for a legal assessment environment to be considered while carrying out the simulation study in IoT. Hence, the assessment environment provides a spectrum of IoT environments to analyze the solution model of researchers and assess troubleshoots, debugging, developing, and creating new logic, which is universally accepted. The prime advantage of considering a legal assessment environment is that it offers practical world usage of devices, interactions with the operating system, remote administration, and the capability to execute real-world devices/services/applications. Some of the standard assessment environments for simulating an IoT are JOSE [36], Smart Santander [37], FIESTA-IoT [38], FIT IoT-LAB [39], WHYNET [40], and MBTAAS [41] that are briefed as follows:

1) JOSE [36]: This assessment environment is meant for evaluating the devices or services associated with outdoor communication. It also offers many subject trials to facilitate resource computation, sensor network deployment, storage management, etc.

2) Smart Santander [37]: This is another standard assessment environment in an IoT that facilitates the adoption of many IoT devices along with small radio-based services and identification code deployment over both the static and mobility aspects of the nodes. This tool can evaluate traffic intensity mainly for the mobile environment in an IoT.

3) FIESTA-IoT [38]: This is one of the giant assessment environments considered during IoT simulation to offer its semantic and interoperable assessment feature. It integrates multiple numbers of another assessment environment in an IoT to analyze the corpus of data. This large data further assists in facilitating webservices in live stream mode. The highly interconnected systems in this tool offer a significant ability to exchange information among various federated assessment environments in an IoT.

4) FIT IoT-LAB [39]: This form of assessment environment is made for performing experimentation on IoT on a huge scale. Various objects can be broadcasted and developed by this tool, considering many low-resource motes for assessment. It also uses mobile robots to testify various upcoming innovative applications in IoT.

5) WHYNET [40]: Essentially meant for hybrid networks, this assessment tool is for performing realization of applications, protocols of WSN, heterogeneous networks, etc. Different forms of emulation and physical entities are carried out by this assessment tool using its single end interface itself. This environment can assess adaptive networks and large/small/medium scale networks in an IoT.

6) MBTAAS [41]: This tool is meant to offer assessment in the form of a service model. It also provides first-hand experience working over an IoT and getting acquainted with its functionality. The tool also provides various test-case formulations and solutions to multiple services to carry out an on-premise assessment of cloud-based IoT applications and services.

Table II summarizes the characteristics of the existing assessment environment of an IoT. One of the potential beneficial factors of using a standard assessment environment is that it enables all the entities and devices to carry out interactivity during testing that device. Hence, without constructing an actual physical device, adopting a standard assessment environment assists in truly justifying the effectiveness of its operation when exposed to a real-time environment. Although it is strongly advisable to use such a traditional assessment environment while carrying out a simulation study for an IoT, there are still various challenges. The primary difficulties are higher dependencies on assessment area, mobility of hubs, scaling operation, and repeatability.

TABLE II. Summary of Existing Assessment Environment

Tool	***Virtualization Support***	***Service domain***	***API integration***	***Built-in IoT Standards***	***A layer of IoT Architecture***	***Programming***	***scope***	***Type***
JOSE [36]	Distributed cloud	Real-time	SOAP	Sensor network	Virtualized Network	Javascript, Java, C	SDN, WSN, IoT	Smart ICT platform
Smart Santader [37]	Management console	Smart city	REST	802.15.4 RFID	Application Network	JavaScript, Java	Mobile sensing	Map data
FIESTA-IoT [38]	Meta Cloud	Ambient Environment	REST	Energy consumption	Communication Network	Python, Java, C	Energy	Sensor Monitoring
FIT-IoT LAB [39]	FIT Cloud	Heterogeneous platform	REST	802.15.4 LoRaWAN	Perceptual Network	Java, nesC	IoT Network	IoT spectrum
WHYNET [40]	Web Portal	Energy	SOAP	Application	Network	Java	Wireless	Network Protocol
MBTAAS [41]	IoT dashboard	Smart city	REST	Model-based	All	OCL	IoT Platform	Service Oriented

IV. Existing Research Trends

To understand the existing research trends, manuscripts published in the last six years have referred to the explicit usage of two different variants of simulation tools.

A. Adoption of Commercial Simulation Tools

There is a total of 256 manuscripts in IEEE Xplore digital library which has reportedly used commercial simulation tools, with 243 conference papers and 13 journal publication (Fig. 1).

They are mainly used to investigate problems associated with traffic management, object monitoring, indoor agriculture, security analysis, the discovery of resources, etc. Out of all this, some of the significant literature has been witnessed on IoTNetSim [16], Cooja [42]-[52], and IBM Bluemix [53]-[54] only. No significant modeling is being carried out towards using the MIMIC simulation tool and SimpleIoTSimulator. The advantage explored towards such adoption of commercial tools found are i) it offers a point-to-point exploration process for the target problem, ii) various prototyping using hardware are feasible to be investigated, iii) specific product or service-based analysis can be easily carried out. While the limitation found toward such adoption are i) it requires explicit skill to work on such tools, ii) various add-ons and software patches are required to be acquired to experience the full-fledged operation, iii) it doesn't offer extensible, cross-platform libraries for heterogeneous products/applications/services in IoT.

B. Adoption of Research-based Simulation Tools

One hundred seventy manuscripts are being reported to adopt research-based simulation tools, consisting of 126 conference papers and 44 journal papers (Fig. 2).

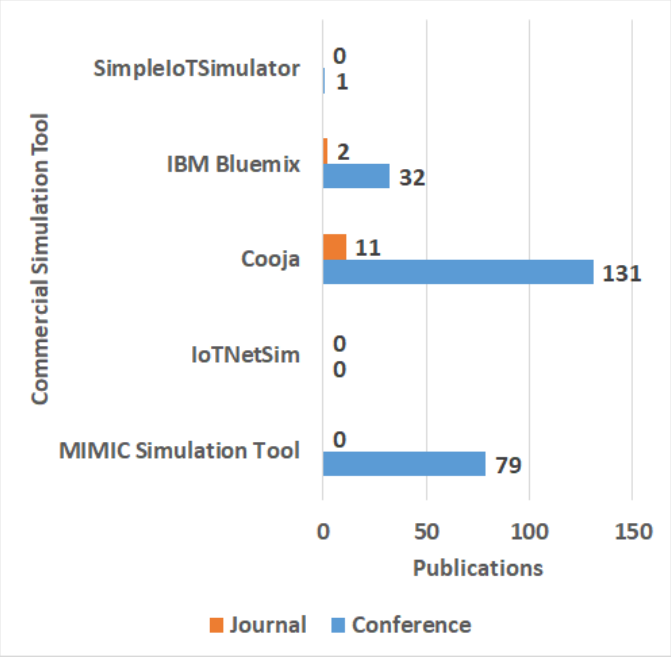

Fig. 1. Trends for Commercial on Simulation Tools.

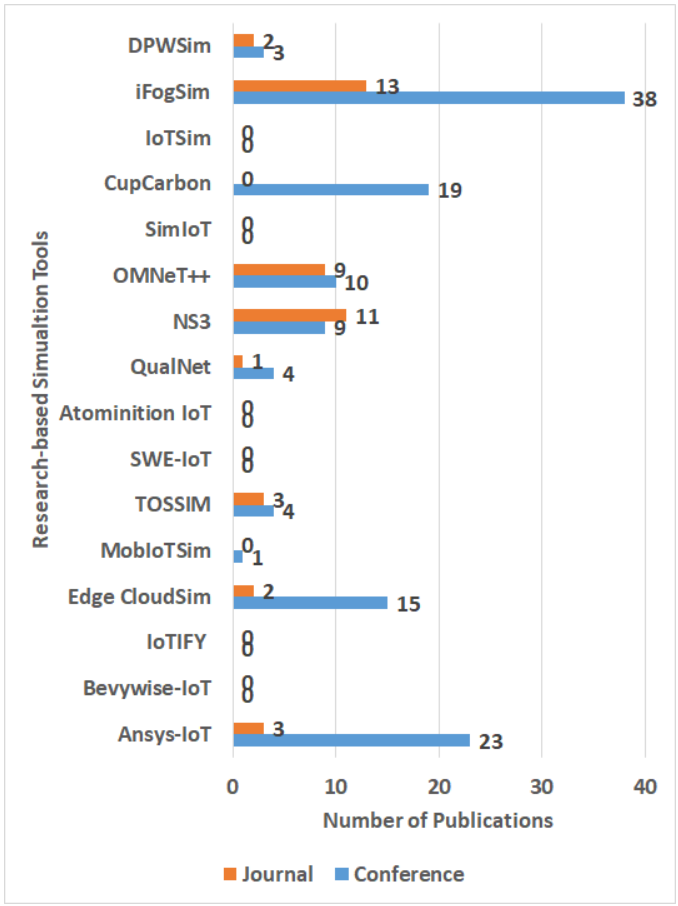

Fig. 2. Trends for Research-based Simulation Tools.

This will eventually mean that the adoption of research-based simulation tools is a bit lesser than commercial simulation tools. It is also noted that the adoption of each tool is used to solve some common problems and specific problems. The common problems will include traffic monitoring and security analysis, while the specific problems investigated by these tools will be scheduling, data transmission, application-specific evaluation, etc. Some of the significant literatures that has reported towards using Ansys-IoT [55]-[57], Edge CloudSim [58][59], TOSSIM [60]-[62], QualNet [63], NS3 [64]-[74], OMNeT++ [75]-[83], iFogSim [84]-[96], and DPWSim [97][98]. The beneficial points of this adoption are: i) the majority is open-sourced, ii) user-friendly, iii) extensible environment for analysis, and iv) it doesn't require complex configuration or setup. While the limiting factors are: i) inbuilt methods and libraries are sometimes challenging to match with the problem space of analysis, ii) each simulator has distinct features and functionalities while migration or integration is sometimes not possible, and iii) quite specific to environmental usage in IoT.

V. Literature Review

From the prior section, it is noted that not all the simulation tools are widely used either in case of commercial or research-based practices. Cooja is highest used in commercial simulation while iFogSim is majorly used for research-based study. It should be noted that all simulators, in either of the

categories, have some common functionalities as well as some exclusive functionalities. The prime contribution of the manuscript is actually to judge the constraints as well as limiting factors associated with existing simulation tools. This is the core reason that the biometric analysis of this paper mainly consists of only studies that adopted 103 sources which has adopted simulation tools. The analysis of some of the recent work towards investigation IoT has also developed a computational framework on the basis of customized simulation study [99]-[103]. However, it is to be noted that adoption of simulation is one of the critical decision to be made by the researcher on the basis of the problems to be addressed in their model. An effective simulation tool should offer higher flexibility to assess the algorithm or protocol without much skill and re-engineering process. Unfortunately, this is not the case with existing studies as researchers tends to adopts to frequently used standard simulation tools, which can cater up their investigation objectives. This is done by overlooking next sequence of investigation to be carried out in line of current research work. Apart from this, majority of existing simulation tool discussed in this paper doesn't offer much of customization privilege. Therefore, after reviewing the complete papers, this section discusses about the open-end issues in the form of contribution and thereby these findings are novel compared to any existing review work being carried out in current times.

A. Discussion of Research Gap

After reviewing the existing features of two variants of the simulation tool, standard assessment environment during simulation study, and research pattern, it is found that there are various contributory factors as well as open-end research issues. This section explicitly highlights the research gap in the first and second levels of research gap for better understanding.

1) First level of investigation: The first level of research gap will eventually mean all the open-end issues retrieved during the reviewing problem. IoT, which consists of highly interconnected devices in large numbers, consists of a multidisciplinary domain with multiple challenges that are quite difficult to assess. The existing simulation tools offer good privilege for investigating semantic queries, protocols, data transmission, routing, usability, privacy, and security considering various applications or services without considering scalability issues. At the moment of transition of problems associated with any factor from intra-net to inter-net, there is eventual evolution of scalability issues. Either commercial or research-based simulation tools cannot detect this. Although it is a well-known fact that repeatability of analysis is quite challenging in IoT, after knowing this fact, existing simulators don't offer much privilege toward addressing increasing heterogeneity of devices and information associated with it. Considering any use-cases of an IoT to be testified over current simulators, it is inevitable to assess multiple application domains (e.g., smart city, vehicular IoT, Industrial IoT, etc.). It will mean that such inclusion will extensively maximize the concurrency towards accessing the infrastructure. This is a computationally challenging task that is not facilitated by any existing simulators, and developers are required to write a snippet or script for this. However, this doesn't solve the problem as the script written for one problem investigation may reasonably not be applicable when the problem space alters. The lack of formal assessment environment adoption is another justified reason for this. Well, adoption of all existing reported assessment environments cannot be always encouraged as they may vary too with the demands of simulation and the type of data being used. So, a more benchmark simulation environment is needed for an IoT. This eventually gives rise to multiple arenas of research questions, e.g.

- What strategy can be adopted for modeling heterogeneous IoT devices to facilitate concurrent operation?
- What mechanism can be adopted towards achieving granularity in investigation towards the inclusion of a massive number of IoT devices over dynamic topology?
- How to develop a cost-effective simulator which has an inclusion of the majority of privilege to investigate one single platform? Unless all these local issues are not addressed, existing simulators cannot be deemed entirely reliable.

2) Second level of investigation: The second level of research gap is the global level extracted from the first level as a local form. This research gap is the direct consequence of the first level gap analysis. Therefore, the following are the finalized version of the research gap.

a) From all the existing features available in simulators, one potential problem is that one simulator cannot be used to carry out an extensive investigation of the issues that are not supported by it. With concurrency towards accessing infrastructure, there are inevitable complexities associated with identifying the uncertain problems that stay low and hidden while contributing to declined or unpredictable outcomes. Hence, the primary research gap is existing simulators doesn't facilitate granular investigation to identify the attributes affecting the operation of IoT device/services.

b) A closer look at the local level of open-end issues in existing simulators are i) scalability, ii) device heterogeneity, iii) concurrency towards accessibility, etc. If all these problems are looked at deeply, it can be seen that the root cause of all of the issues is the lack of adoption of resource parametric modeling in the existing simulation tool. Current simulators can perform initialization of resource parameters while the developers must script the constraints associated with its usage. Such scripts are consistently required to be upgraded with the change of services or network operations. Hence, the secondary research gap is that existing simulators are not designed to practically consider the resource modelling of IoT devices and other devices in the process of simulation. The consequences of such modeling will lead to unrealistic data transmission simulation outcomes.

c) It is closely observed that security is a much more standard set of the problem being addressed by existing simulators. However, they do it by an available set of libraries and developers' written security scripts. Almost all these security approaches are based on cryptographic based. The prime reason is its dependency on using cloud or fog as an environment on top of IoT applications, which has higher supportability towards the conventional encryption-based operation. The beneficial point in this factor is that they are 100% stopping a specific set of attackers that is coded. The limiting factor is that they are entirely not applicable if the attacker changes its plan of attack.

d) Moreover, all the cryptographic algorithms are not resistive against all attacks; they have strengths and weaknesses. Another practical rationale is that adopting cryptographic measures will also induce a higher load toward low-powered IoT devices. Hence, the ternary research gap is that existing simulators don't address the IoT nodes' sustainability factor by frequently using cryptographic measures towards security.

B. Critical Discussion for Existing Study

From the outcome of this study, it is also found that majority of the simulation tools are part of discrete event simulators (NS3, OMNeT++, SimIoT, CupCarbon, iFogSim) which offers finite set of functionalities and demands API integration. It will eventually mean that customizing them for heterogeneous research problem will be a computationally expensive process. Apart from this, existing assessment tools are mainly meant to executing standard protocol for networking and not for data analytics, which require a dependency with different set of tools. The constraints found in existing simulation tool are also associated with accessibility towards single user for one project. This will eventually pose an impediment towards distributed investigation process by different user on same project at same time. Hence, the investigation process is time consuming and platform specifics too restricted to one user at a time. Another closer observation towards existing simulation tools highlights the inferior security features embedded in it. The enhancement towards security system is very few to find, where almost all the simulation tools either uses user-deployed security patches or uses third party script to introduce security features. This process is quite challenging to be customized for projects with multiple and heterogenous target of addressing problems in IoT. Hence, there is an emergent need to develop a simulation tool that offers cost effective and proper utilization of its features.

VI. Conclusion

This paper has discussed the scale of effectiveness of existing simulators. There are multiple simulators in practice; the discussion has been carried out concerning commercially used and research-based usage. The novelty of this manuscript is that i) it offers an informative and compact description of frequently used simulation tools in practice for an IoT, ii) It exhibits a unique and updated research trend towards IoT simulators adoption in the last six years, which is not reported in any existing studies, and iii) it makes some interesting discoveries of limiting factors associated with the overall features of existing simulators. The above mentioned learning outcomes of proposed review work exactly matches with the core objectives of the paper associated with studying features as well as reviewing trends associated with simulation tools. The outcome of the paper also presents open-end research problem in the form of research gap discussion, thereby meeting the core study objective of this paper.

Hence, the future work will be carried out in the direction of addressing the finalized research gap as follows:

1) The primary research gap can be addressed by developing a novel computational model of a simulator to identify and construct a set of strategies that affect the accuracy of the simulation process. Discrete mathematical modeling can be carried out to address this gap.

2) The secondary research gap can be addressed by extending the first solution toward including various novel conditional logic. The development of such reasoning is accompanied by all the resource management attributes that affect IoT devices' sustainability factors during the simulation study. It will offer different reliable outcomes due to practical resource modeling during simulation.

3) The ternary research gap can be addressed by further developing another layer of security operation without using any form of encryption model or without using any existing techniques that are found to offer load towards low-powered IoT devices. Further novelty can testify to its resiliency towards maximum forms of reported threats in an IoT.

References

[1] P. Zeigler, L. Zhang, Y. laili, "Model Engineering for Simulation," Elsevier Science, ISBN: 9780128135440, 0128135441, 2019.

[2] D. Cvetković, G. Birajdar, Numerical Modeling and Computer Simulation, IntechOpen, ISBN: 9781838811969, 1838811966, 2020.

[3] P. Tomar, Integration, and Implementation of the Internet of Things through Cloud Computing, Engineering Science Reference, ISBN: 9781799869832, 1799869830, 2021.

[4] A. Khanna, D. Gupta, P. L. Mehta, V. H. C. de Albuquerque, Smart Sensors for Industrial Internet of Things Challenges, Solutions and Applications, Springer International Publishing, ISBN: 9783030526238, 3030526232, 2021.

[5] G. Sunitha, J. Avanija, K. R. Madhavi, S. B. Bhushan, S. Goundar, Innovations in the Industrial Internet of Things (IIoT) and Smart Factory, IGI Global, ISBN: 9781799833772, 1799833771, 2021.

[6] F. Al-Turjman, Real-Time Intelligence for Heterogeneous Networks Applications, Challenges, and Scenarios in IoT HetNets, Springer International Publishing, ISBN: 9783030756130, 3030756130, 2021.

[7] Velayutham, Sathiyamoorthi, Challenges, and Opportunities for the Convergence of IoT, Big Data, and Cloud Computing, IGI Global, 2021.

[8] F. Al-Turjman, Multimedia-enabled Sensors in IoT Data Delivery and Traffic Modelling, CRC Press, ISBN: 9781351166027, 1351166026, 2018.

[9] P. Y. Taser, Emerging Trends in IoT and Integration with Data Science, Cloud Computing, and Big Data Analytics, IGI Global, ISBN: 9781799841876, 1799841871, 2021.

[10] H. G. Perros, An Introduction to IoT Analytics, CRC Press, ISBN: 9781000337822, 1000337820, 2021.

[11] A. Kamilaris and A. Pitsillides, "Mobile Phone Computing and the Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 885-898, Dec. 2016, doi: 10.1109/JIOT.2016.2600569.

[12] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on quantum-resistant Cryptosystems for the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457-6480, July 2020, doi: 10.1109/JIOT.2019.2958788.

[13] K. Tange, M. De Donno, X. Fafoutis and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489-2520, Fourth quarter 2020, doi: 10.1109/COMST.2020.3011208.

[14] J. Zhang and D. Tao, "Empowering Things With Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 7789-7817, 15 May 15, 2021, doi: 10.1109/JIOT.2020.3039359.

[15] https://www.gambitcomm.com/site/mimic-simulator.php.

[16] M. Salama, Y. Elkhatib, G. Blair, "IoTNetSim: A Modelling and Simulation Platform for End-to-End IoT Services and Networking," ACM-Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, 2019, DOI:https://doi.org/10.1145/3344341.3368820.

[17] S. Badugu, "Role of COOJA Simulator in IoT," International Journal of Emerging Trends & Technology in Computer Science, vol.6, Iss.2, 2017.

[18] R. Stifani, "IBM Bluemix: The Cloud Platform for Creating and Delivering Applications," IBM Whitepaper, 2015.

[19] https://www.simplesoft.com/SimpleIoTSimulator.html.

[20] https://www.ansys.com/en-in/technology-trends/iiot.

[21] https://www.bevywise.com/iot-simulator/.

[22] https://iotify.io/.

[23] C. Sonmez, A. Ozgovde, and C. Ersoy, 'Edgecloudsim: An environment for performance evaluation of edge computing systems, Transactions on Emerging Telecommunications Technologies, e3493, 2018.

[24] T. Pflanzner, A. Kertesz, B. Spinnewyn and S. Latre, 'Mobiotsim: Towards a mobile iot device simulator, in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), IEEE, 2016, pp. 21–27.

[25] P. Levis and N. Lee, 'Tossim: A simulator for TinyOS networks,' UC Berkeley, September, vol. 24, 2003.

[26] P. Gimenez, B. Molına, C. E. Palau and M. Esteve, 'Swe-simulation and testing for the lot, in 2013 IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 2013, pp. 356–361.

[27] https://www.atomiton.com/#/home.

[28] https://www.scalable-networks.com/products/qualnet-network-simulation-software/#.

[29] https://www.nsnam.org/.

[30] https://omnetpp.org/.

[31] P. Akilandeswari, B. Vennila, and H. Srimathi, "Concurrent processing of cloudlets in CloudSim-SimIoT environment," AIP Conference Proceedings, 2019, DOI: https://doi.org/10.1063/1.5112277.

[32] K. Mehdi, M.Lounis, A. Bounceur, T. Kechadi, "CupCarbon: A Multi-Agent and Discrete Event Wireless Sensor Network Design and Simulation Tool".7th International ICST Conference on Simulation Tools and Techniques, Lisbon, Portugal,2014, DOI: 10.4108/icst.simutools.2014.254811.

[33] X. Zeng, S. K. Garg, P. Strazdins, P. P. Jayaraman, D. Georgakopoulos and R. Ranjan, 'Iotsim: A simulator for analyzing iot applications,' Journal of Systems Architecture, vol. 72, pp. 93–107, 2017.

[34] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh and R. Buyya, 'Ifogsim: A toolkit for modeling and simulation of resource management techniques in the Internet of things, edge and fog computing environments, Software: Practice and Experience, pp. 1275–1296, 2017.

[35] S. N. Han, G. M. Lee, N. Crespi, K. Heo, N. Van Luong, M. Brut, and P. Gatellier, 'Dpwsim: A simulation toolkit for iot applications using devices profile for web services, in 2014 IEEE World Forum on Internet of Things (WF-IoT), IEEE, 2014, pp. 544–547.

[36] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, 'Internet of things (iot): Research, simulators, and testbeds, IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1637–1647, 2018.

[37] L. Sanchez, L. Munoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis et al., 'Smartsantander: Iot experimentation over a smart city testbed', Computer Networks, vol. 61, pp. 217–238, 2014.

[38] A. Gyrard and M. Serrano, 'Fiesta-iot: Federated interoperable semantic internet of things (iot) testbeds and applications,' in ICT, 2015.

[39] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, et al., 'Fit iot-lab: A large scale open experimental IoT testbed–a valuable tool for iot deployment in smart factories,' IEEE ComSoc Multimedia Technical Committee E-Letter, 2015.

[40] J. Zhou, Z. Ji, M. Varshney, Z. Xu, Y. Yang, M. Marina, and R. Bagrodia, 'Whynet: A hybrid testbed for largescale, heterogeneous and adaptive wireless networks,' in Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization, ACM, 2006, pp. 111–112.

[41] A. Ahmad, F. Bouquet, E. Fourneret, F. Le Gall and B. Legeard, 'Model-based testing as a service for iot platforms,' in International Symposium on Leveraging Applications of Formal Methods, Springer, 2016, pp. 727–742.

[42] S. Chowdhury, A. Benslimane and C. Giri, "Noncooperative Gaming for Energy-Efficient Congestion Control in 6LoWPAN," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4777-4788, June 2020. doi: 10.1109/JIOT.2020.2969272.

[43] S. Taghizadeh, H. Elbiaze, and H. Bobarshad, "EM-RPL: Enhanced RPL for Multigateway Internet-of-Things Environments," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8474-8487, 15 May 15, 2021. doi: 10.1109/JIOT.2020.3047079.

[44] M. Mahyoub, A. S. Hasan Mahmoud, M. Abu-Amara, and T. R. Sheltami, "An Efficient RPL-Based Mechanism for Node-to-Node Communications in IoT," in *IEEE Internet Things Journal*, vol. 8, no. 9, pp. 7152-7169, 1 May 1, 2021. doi: 10.1109/JIOT.2020.3038696.

[45] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, Dec. 2017. doi: 10.1109/JIOT.2017.2749883.

[46] Y. Kim and J. Paek, "NG-RPL for Efficient P2P Routing in Low-Power Multihop Wireless Networks," in *IEEE Access*, vol. 8, pp. 182591-182599, 2020. doi: 10.1109/ACCESS.2020.3028771.

[47] M. Amoretti, O. Alphand, G. Ferrari, F. Rousseau, and A. Duda, "DINAS: A Lightweight and Efficient Distributed Naming Service for All-IP Wireless Sensor Networks," in *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 670-684, June 2017. doi: 10.1109/JIOT.2016.2640317.

[48] A. W. Abbas and S. N. K. Marwat, "Scalable Emulated Framework for IoT Devices in Smart Logistics Based Cyber-Physical Systems: Bonded Coverage and Connectivity Analysis," in *IEEE Access*, vol. 8, pp. 138350-138372, 2020. doi: 10.1109/ACCESS.2020.3012458.

[49] Kamaldeep, M. Malik, M. Dutta, and J. Granjal, "IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things," in *IEEE Sensors Journal*, vol. 21, no. 24, pp. 28066-28076, 15 Dec.15, 2021. doi: 10.1109/JSEN.2021.3124886.

[50] Y. Tahir, S. Yang, and J. McCann, "BRPL: Backpressure RPL for High-Throughput and Mobile IoTs," in *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 29-43, 1 January 2018. doi: 10.1109/TMC.2017.2705680.

[51] R. Monica, L. Davoli and G. Ferrari, "A Wave-Based Request-Response Protocol for Latency Minimization in WSNs," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7971-7979, Oct. 2019. doi: 10.1109/JIOT.2019.2914578.

[52] P. Sanmartin, D. Jabba, R. Sierra, and E. Martinez, "Objective Function BF-ETX for RPL Routing Protocol," in *IEEE Latin America Transactions*, vol. 16, no. 8, pp. 2275-2281, Aug. 201 doi: 10.1109/TLA.2018.8528246.

[53] M. Ma, W. Lin, J. Zhang, P. Wang, Y. Zhou, and X. Liang, "Toward Energy-Awareness Smart Building: Discover the Fingerprint of Your Electrical Appliances," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1458-1468, April 2018. doi: 10.1109/TII.2017.2776300.

[54] R. Bocu and C. Costache, "A homomorphic encryption-based system for securely managing personal health metrics data," in *IBM Journal of Research and Development*, vol. 62, no. 1, pp. 1:1-1:10, 1 Jan.-Feb. 2018. doi: 10.1147/JRD.2017.2755524.

[55] Y. Shafiq, J. Henricks, C. P. Ambulo, T. H. Ware, and S. V. Georgakopoulos, "A Passive RFID Temperature Sensing Antenna With Liquid Crystal Elastomer Switching," in *IEEE Access*, vol. 8, pp. 24443-24456, 2020. doi: 10.1109/ACCESS.2020.2969969.

[56] M. Shih, C. Huang, T. Chen, C. Wang, D. Tarng and C. P. Hung, "Electrical, Thermal, and Mechanical Characterization of eWLB, Fully Molded Fan-Out Package, and Fan-Out Chip Last Package," in *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 9, no. 9, pp. 1765-1775, Sept. 2019. doi: 10.1109/TCPMT.2019.2935477.

[57] L. Fan *et al*., "Stretchable Carbon Nanotube Thin-Film Transistor Arrays Realized by a Universal Transferable-Band-Aid Method," in *IEEE Transactions on Electron Devices*, vol. 68, no. 11, pp. 5879-5885, Nov. 2021. doi: 10.1109/TED.2021.3114140.

[58] I. -D. Filip, F. Pop, C. Serbanescu and C. Choi, "Microservices Scheduling Model Over Heterogeneous Cloud-Edge Environments As Support for IoT Applications," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2672-2681, Aug. 2018. doi: 10.1109/JIOT.2018.2792940.

[59] S. Pang, W. Li, H. He, Z. Shan and X. Wang, "An EDA-GA Hybrid Algorithm for Multi-Objective Task Scheduling in Cloud Computing," in *IEEE Access*, vol. 7, pp. 146379-146389, 2019. doi: 10.1109/ACCESS.2019.2946216.

[60] C. Esposito, A. Castiglione, F. Palmieri, and A. D. Santis, "Integrity for an Event Notification Within the Industrial Internet of Things by Using Group Signatures," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3669-3678, Aug. 2018. doi: 10.1109/TII.2018.2791956.

[61] A. A. Al-Roubaiey, T. R. Sheltami, A. S. H. Mahmoud and K. Salah, "Reliable Middleware for Wireless sensor-actuator Networks," in *IEEE Access*, vol. 7, pp. 14099-14111, 2019. doi: 10.1109/ACCESS.2019.2893623.

[62] C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed Group Key Management for Event Notification Confidentiality Among Sensors," in *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 566-580, 1 May-June 2020. doi: 10.1109/TDSC.2018.2799227.

[63] K. Husain and A. Awang, "Forwarding Angles and the Trade-Off Between Reliability, Latency and Unicast Efficiency in Content-Based Beaconless Forwarding," in *IEEE Access*, vol. 8, pp. 225522-225538, 2020. doi: 10.1109/ACCESS.2020.3044967.

[64] Z. Liu, C. Guo and B. Wang, "A Physically Secure, Lightweight Three-Factor and Anonymous User Authentication Protocol for IoT," in *IEEE Access*, vol. 8, pp. 195914-195928, 2020. doi: 10.1109/ACCESS.2020.3034219.

[65] G. Kaur, P. Chanak and M. Bhattacharya, "Energy-Efficient Intelligent Routing Scheme for IoT-Enabled WSNs," in *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11440-11449, 15 July 15, 2021. doi: 10.1109/JIOT.2021.3051768.

[66] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," in *IEEE Access*, vol. 7, pp. 85627-85644, 2019. doi: 10.1109/ACCESS.2019.2926578.

[67] S. Atiewi *et al*., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in *IEEE Access*, vol. 8, pp. 113498-113511, 2020. doi: 10.1109/ACCESS.2020.3002815.

[68] B. Bordel, R. Alcarria, D. M. De Andrés and I. You, "Securing Internet-of-Things Systems Through Implicit and Explicit Reputation Models," in *IEEE Access*, vol. 6, pp. 47472-47488, 2018. doi: 10.1109/ACCESS.2018.2866185.

[69] S. Dawaliby, A. Bradai, and Y. Pousset, "Distributed Network Slicing in Large Scale IoT Based on Coalitional Multi-Game Theory," in *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1567-1580, Dec. 2019. doi: 10.1109/TNSM.2019.2945254.

[70] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smart grid: A Survey of Trends Challenges and Prospect," in *IEEE Access*, vol. 10, pp. 4794-4831, 2022. doi: 10.1109/ACCESS.2022.3140595.

[71] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT," in *IEEE Access*, vol. 7, pp. 135632-135649, 2019. doi: 10.1109/ACCESS.2019.2941575.

[72] G. Choudhary, P. V. Astillo, I. You, K. Yim, I. -R. Chen and J. -H. Cho, "Lightweight Misbehavior Detection Management of Embedded IoT Devices in Medical Cyber-Physical Systems," in *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2496-2510, Dec. 2020. doi: 10.1109/TNSM.2020.3007535.

[73] S. Messaoud, A. Bradai, and E. Moulay, "Online GMM Clustering and Mini-Batch Gradient Descent Based Optimization for Industrial IoT 4.0," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1427-1435, Feb. 2020. doi: 10.1109/TII.2019.2945012.

[74] J. Yang, A. S. Akyurek, S. Tilak and T. S. Rosing, "Design of Transmission Manager in Heterogeneous WSNs," in *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 3, pp. 395-408, 1 July-Sept. 2018. doi: 10.1109/TETC.2017.2653064.

[75] C. Pu, "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937-4949, June 2020. doi: 10.1109/JIOT.2020.2971463.

[76] E. A. Khalil, S. Ozdemir and B. A. Attea, "A New Task Allocation Protocol for Extending Stability and Operational Periods in the Internet of Things," in *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7225-7231, Aug. 2019. doi: 10.1109/JIOT.2019.2915558.

[77] C. Pu and L. Carpenter, "Psched: A Priority-Based Service Scheduling Scheme for the Internet of Drones," in *IEEE Systems Journal*, vol. 15, no. 3, pp. 4230-4239, Sept. 2021. doi: 10.1109/JSYST.2020.2998010.

[78] A. Ali and M. M. Yousaf, "Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network," in *IEEE Access*, vol. 8, pp. 109662-109676, 2020. doi: 10.1109/ACCESS.2020.3002333.

[79] T. Qayyum, Z. Trabelsi, A. W. Malik and K. Hayawi, "Multi-Level Resource Sharing Framework Using Collaborative Fog Environment for Smart Cities," in *IEEE Access*, vol. 9, pp. 21859-21869, 2021. doi: 10.1109/ACCESS.2021.3054420.

[80] B. Pan, F. Yan, X. Xue, E. Magelhaes and N. Calabretta, "Performance assessment of a fast optical add-drop multiplexer-based metro access network with edge computing," in *Journal of Optical Communications and Networking*, vol. 11, no. 12, pp. 636-646, December 2019. doi: 10.1364/JOCN.11.000636.

[81] A. Arooj, M. S. Farooq, T. Umer, G. Rasool, and B. Wang, "Cyber-Physical and Social Networks in IoV (CPSN-IoV): A Multimodal Architecture in Edge-Based Networks for Optimal Route Selection Using 5G Technologies," in *IEEE Access*, vol. 8, pp. 33609-33630, 2020. doi: 10.1109/ACCESS.2020.2973461.

[82] A. Alharthi, Q. Ni and R. Jiang, "A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET," in *IEEE Access*, vol. 9, pp. 87299-87309, 2021. doi: 10.1109/ACCESS.2021.3086225.

[83] M. S. Akbar, H. Yu, and S. Cang, "Performance Optimization of the IEEE 802.15.4-Based Link Quality Protocols for WBASNs/IoTs in a Hospital Environment Using Fuzzy Logic," in *IEEE Sensors Journal*, vol. 19, no. 14, pp. 5865-5877, 15 July 15, 2019. doi: 10.1109/JSEN.2019.2900009.

[84] H. Huang, F. Liu, Z. Yang, and Z. Hao, "Automated Test Case Generation Based on Differential Evolution With Relationship Matrix for iFogSim Toolkit," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 5005-5016, Nov. 2018. doi: 10.1109/TII.2018.2856881.

[85] K. S. Awaisi *et al*., "Towards a Fog Enabled Efficient Car Parking Architecture," in *IEEE Access*, vol. 7, pp. 159100-159111, 2019. doi: 10.1109/ACCESS.2019.2950950.

[86] F. H. Rahman, S. H. S. Newaz, T. W. Au, W. S. Suhaili and G. M. Lee, "Off-Street Vehicular Fog for Catering Applications in 5G/B5G: A Trust-Based Task Mapping Solution and Open Research Issues," in

IEEE Access, vol. 8, pp. 117218-117235, 2020. doi: 10.1109/ACCESS.2020.3004738.

[87] H. Nashaat, E. Ahmed and R. Rizk, "IoT Application Placement Algorithm Based on Multi-Dimensional QoE Prioritization Model in Fog Computing Environment," in *IEEE Access*, vol. 8, pp. 111253-111264, 2020. doi: 10.1109/ACCESS.2020.3003249.

[88] B. K. Dar, M. A. Shah, S. U. Islam, C. Maple, S. Mussadiq and S. Khan, "Delay-Aware Accident Detection and Response System Using Fog Computing," in *IEEE Access*, vol. 7, pp. 70975-70985, 2019. doi: 10.1109/ACCESS.2019.2910862.

[89] H. Rafique, M. A. Shah, S. U. Islam, T. Maqsood, S. Khan and C. Maple, "A Novel Bio-Inspired Hybrid Algorithm (NBIHA) for Efficient Resource Management in Fog Computing," in *IEEE Access*, vol. 7, pp. 115760-115773, 2019. doi: 10.1109/ACCESS.2019.2924958.

[90] M. Ammad *et al*., "A Novel Fog-Based Multi-Level Energy-Efficient Framework for IoT-Enabled Smart Environments," in *IEEE Access*, vol. 8, pp. 150010-150026, 2020. doi: 10.1109/ACCESS.2020.3010157.

[91] I. Lera, C. Guerrero and C. Juiz, "YAFS: A Simulator for IoT Scenarios in Fog Computing," in *IEEE Access*, vol. 7, pp. 91745-91758, 2019. doi: 10.1109/ACCESS.2019.2927895.

[92] J. U. Arshed and M. Ahmed, "RACE: Resource Aware Cost-Efficient Scheduler for Cloud Fog Environment," in *IEEE Access*, vol. 9, pp. 65688-65701, 2021. doi: 10.1109/ACCESS.2021.3068817.

[93] R. Yadav *et al*., "Smart Healthcare: RL-Based Task Offloading Scheme for Edge-Enable Sensor Networks," in *IEEE Sensors Journal*, vol. 21, no. 22, pp. 24910-24918, 15 Nov.15, 2021. doi: 10.1109/JSEN.2021.3096245.

[94] B. Ali, M. Adeel Pasha, S. u. Islam, H. Song and R. Buyya, "A Volunteer-Supported Fog Computing Environment for Delay-Sensitive IoT Applications," in *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3822-3830, 1 March 1, 2021. doi: 10.1109/JIOT.2020.3024823.

[95] J. Fang and A. Ma, "IoT Application Modules Placement and Dynamic Task Processing in Edge-Cloud Computing," in *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12771-12781, 15 August 15, 2021. doi: 10.1109/JIOT.2020.3007751.

[96] A. Asghar, A. Abbas, H. A. Khattak, and S. U. Khan, "Fog Based Architecture and Load Balancing Methodology for Health Monitoring Systems," in *IEEE Access*, vol. 9, pp. 96189-96200, 2021. doi: 10.1109/ACCESS.2021.3094033.

[97] S. N. Han *et al*., "DPWSim: A Devices Profile for Web Services (DPWS) Simulator," in *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 221-229, June 2015. doi: 10.1109/JIOT.2014.2388131.

[98] S. N. Han, G. M. Lee and N. Crespi, "Semantic Context-Aware Service Composition for Building Automation System," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 752-761, Feb. 2014. doi: 10.1109/TII.2013.2252356.

[99] M. S. Al-Rakhami and M. Al-Mashari, "ProChain: Provenance-Aware Traceability Framework for IoT-Based Supply Chain Systems," in IEEE Access, vol. 10, pp. 3631-3642, 2022, doi: 10.1109/ACCESS.2021.3135371.

[100] A. S. M. S. Hosen, P. K. Sharma and G. H. Cho, "MSRM-IoT: A Reliable Resource Management for Cloud, Fog, and Mist-Assisted IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2527-2537, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3090779.

[101] T. Kamalakis, Z. Ghassemlooy, S. Zvanovec and L. Nero Alves, "Analysis and simulation of a hybrid visible-light/infrared optical wireless network for IoT applications," in Journal of Optical Communications and Networking, vol. 14, no. 3, pp. 69-78, March 2022, doi: 10.1364/JOCN.442787.

[102] X. Chen, J. Zhang, B. Lin, Z. Chen, K. Wolter and G. Min, "Energy-Efficient Offloading for DNN-Based Smart IoT Systems in Cloud-Edge Environments," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 3, pp. 683-697, 1 March 2022, doi: 10.1109/TPDS.2021.3100298.

[103] J. A. Barriga, P. J. Clemente, J. Hernández and M. A. Pérez-Toledano, "SimulateIoT-FIWARE: Domain Specific Language to Design, Code Generation and Execute IoT Simulation Environments on FIWARE," in IEEE Access, vol. 10, pp. 7800-7822, 2022, doi: 10.1109/ACCESS.2022.3142894.