Testing Techniques in IoT-based Systems

Noha Medhat
Department of Information Systems, Faculty of Computer and Information Sciences, Ain Shams University,
Cairo, Egypt, 15566
noha_medhat@cis.asu.edu.eg

Sherin Moussa
Department of Information Systems, Faculty of Computer and Information Sciences, Ain Shams University,
Cairo, Egypt, 15566
sherinmoussa@cis.asu.edu.eg
ORCID: 0000-0001-9593-6909

Nagwa Badr
Department of Information Systems, Faculty of Computer and Information Sciences, Ain Shams University,
Cairo, Egypt, 15566
nagwabadr@cis.asu.edu.eg
ORCID: 0000-0002-5382-1385

Mohamed F. Tolba
Department of Scientific Computing, Faculty of Computer and Information Sciences, Ain Shams University,
Cairo, Egypt, 15566
fahmytolba@cis.asu.edu.eg

***Abstract*— Internet of Things (IoT) systems are fast evolving nowadays, in which huge amounts of data are produced rapidly from heterogeneous sources. The nature of IoT-based systems implies many challenges, in terms of operation, security, quality control and data management. Thus, testing such systems is a key element to their success. In this paper, we present a comprehensive study for the main testing techniques and tools that have been considered for the IoT-based systems. Detailed comparison and analytical criticism are conducted, identifying the different testing types that have been applied for the main application domains. The research gaps are addressed, which highlight the future directions that can be adopted.**

Keywords—Testing, Internet of things (IoT), IoT-based systems, Testing Framework, Testing Tools, IoT Applications.

I. INTRODUCTION

Internet of Things (IoT) has now become the fastest-evolving computational paradigm, where physical devices and virtual objects are integrated together through network technologies, such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Bluetooth, Wi-Fi or cloud related. Any used real life devices are connected to sensors or actuators to sense and receive data for specific tasks [1]. The produced data are dramatically huge, supporting the Big data characteristics [2]. IoT systems like transportation, weather-related, smart homes, wearables and medical health applications are the main propagated examples [3][4].

One of the most significant challenges over these IoT-based systems is testing. What makes testing different on such systems is the divergent used technologies that need to be tested, in terms of the enormous storage requirements, speedy real time processing for the received heterogeneous data and the context-aware technologies such as MQTT, COAP, and LWM2M protocols [5][6]. Testing IoT systems examines the main four layers constructing them [7][8][9]. As shown in Fig. 1, the first layer produces data, such as by sensors and actuators, whereas the second layer is the middleware gateway where these data are received through the Internet and connected to the IoT services and technologies, representing the third layer, and then reach the user's applications as the fourth layer. The cloud storage is used as a third party. The services offered through this layered architecture should comply with some Quality of Service (QOS) metrics to ensure the achievement of features on the edge or fog level, where the sensors are connected to the gateway network, such as: functional stability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability [10]. Testing over IoT systems faces several challenges. The limitations in the memory and processing power lead to a serious need for Performance Testing [11]. Malware attacks that are caused by the connectivity between large numbers of users and devices lead to continuously innovative Security Testing [12]. The connection between hardware and software, in which the devices are simulated using virtualization tools necessitates a customized Reliability Testing [13][14]. Moreover, the different used platforms require persistent Compatibility Testing consequently with the perpetual emerging platforms [15], while the integration between all used variant components imposes continual Integration Testing [16] [17]. Functionality Testing is regarded all times to detect any problems related to the main functionalities of any component [18]. The determination of the exact needed testing types depends on the system domain, the nature of users and the severity of its tasks [16].

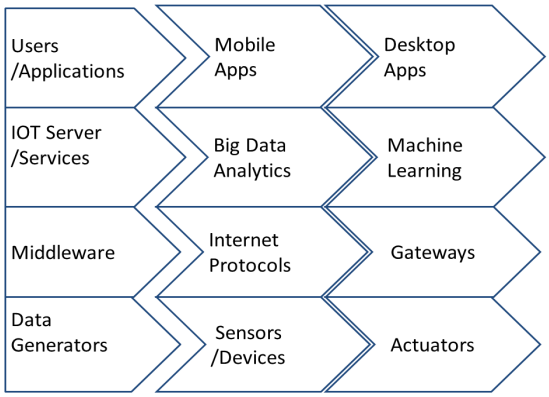

Fig. 1. Generic IoT-based System Architecture

The diverse complex components of IoT systems enforce customized testing paradigms [19][20]. A sample list of items that should be addressed in IoT-related testing strategies is: hardware devices, embedded software, sensors and actuators, the integration between devices, network interruptions, network protocols, data encryption /decryption, cloud storage as a third party, and data transmit frequency [21]. In this paper, a comprehensive study is provided for the main testing techniques, levels, types and tools that have been considered for the IoT-based systems in the three dominant IoT application domains; health and medical, smart cities, and precision agriculture. Detailed comparison and analytical evaluation are conducted, discussing the different testing types that have been applied for the main application

978-1-7281-3995-119$31.00 ©2019 IEEE

domains, and the limitations that have been deduced. The rest of the paper is organized as follows. Section 2 explores the different testing levels and types of IoT systems. Section 3 discusses testing IoT systems in the medical and health sector. Section 4 addresses IoT testing in the smart cities, whereas section 5 investigates testing IoT solutions in the precision agriculture domain. Section 6 provides a detailed discussion and analytical evaluation for the presented researches and the main current research gaps deduced in this field, and finally, section 7 concludes our research study, highlighting the future directions that can be adopted.

II. IoT SYSTEMS TESTING LEVELS AND TYPES

With the rapid technological advancements in the IoT-based systems, main testing methods and types have been reconsidered to propose a testing framework of five main testing levels for the IoT systems, as in Fig. 2 [18]. The System Under Test (SUT) should pass all these testing levels using Sandbox environment for testing, where all parts must be tested, including hardware, software, network and the interaction with users [22][23]. The first level is the unit testing, where testing is done individually on each component in the system, including the hardware devices, sensors, actuators and the software applications. The second level is the integration testing between each component and the other, where a huge bulk of issues arise due to the diversity of hardware devices, software modules, user interfaces and protocols integrating with each other [24]. The integration between IoT-based systems and the cloud introduces a new theme into integration testing. This integration overcomes most of the IoT systems' limitations, in which the cloud monitors and connects the distributed devices, where it can handle, process and compute the big data generated from the IoT systems [25]. Moreover, the different protocols between devices would lead to the need for a middleware, adding extra burden on integration testing [26]. The third level is the performance testing, in which load and stress testing are conducted by applying different mechanisms and approaches to investigate huge workloads received over the network and the enormous requests that should be managed and prioritized to reduce delays and cost for optimum Quality of Service (QoS).

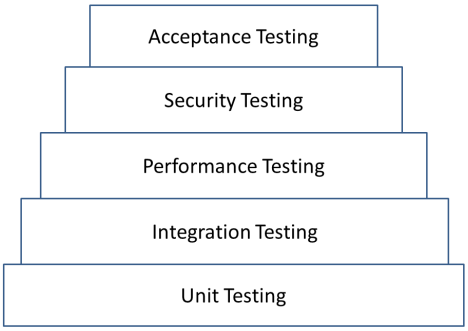

Fig. 2. IoT-based System Testing Levels

Reliability and scalability testing are considered as well to measure if the virtualized components, either simulated or emulated devices, are fitting with the changes and still working as required [18]. The fourth level is the most important and problematic area, representing the security to detect threats, malwares, hackers and penetrators that try to steal/manipulate with users' data. Many researches have discussed the types of attacks, providing possible solutions [27]. The fifth level is the acceptance testing, putting into consideration the system users. This includes the usability testing of the application's user interface and compatibility testing, in which the same software can run on different platforms. System testing would also be deliberated when examining all components of the IoT system together, by understanding the functionality of each sensor whether it sends alerts or gets periodic readings. So emulating for the application sensors and devices helps in control the testing of the whole system, which can be done by specific tools such as COOJA, NETSIM, Azure or Matlab [6].

III. MEDICAL AND HEALTH IoT SYSTEMS

A. The Application Scenarios

Tracking patients' condition is the main goal behind the IoT medical and healthcare applications, where data are collected and transformed through the Internet into a cloud storage, applying different analytics and processes to provide patients with the needed services [28]. Critical diseases may cause sudden death if not monitored, i.e. heart diseases' patients are not discovered easily, as the symptoms start to appear only on the latest stages of the disease, so the blood pressure and heart rate should be read frequently [29]. Patients with diabetes need to know the needed amount of insulin. This is triggered by measuring the glucose in blood that can be determined by a sensor, with no need to visit a doctor [30]. Elders need to track their movement and alert when a fall is detected to avoid bone troubles [31]. In addition, tracking users' lifestyle to offer exercises or healthy food routines for their fitness became well desired [32] [33].

B. The Used Technologies

Such applications have common features. Different sensors and actuators are used as data collectors, i.e. heart rate (ECG), blood pressure, pulse rate, glucose rate, temperature, fats and muscle mass [21]. The type of sensors depends on the application that is being developed; it could be attached to wearable things or embedded into the patient's surrounding devices, where frequent real time sensing is considered [34]. These sensors are the indicators to provide the IoT services [35]. RFID, Bluetooth, 3G/4G network, Wi-Fi and other network technologies that do not require Internet connection are the most used technologies for transferring the collected data. Several researches have compared between these used technologies [28][35].

C. Testing Types and Methods

Most of the studies focused on the security testing and performance testing. The integration of different hardware, software and backend components were involved, assessing various formats of cyber-attacks to protect patients' data from being penetrated or hacked and analyzing performance to offer urgent response at the right time to rescue humans lives [36]. [37] provided a full definition of all possible IoT threats, either on the wearable devices, network level/ middleware or the application layer, describing different types of attackers and categorizing the levels of harms and their consequences to help testers define the methods and types of testing to apply. In [38], an encryption algorithm was proposed based on the Wireless Sensor Network (WSN) and Data Encryption Standard (DES) to enhance the security of data transfer between the different layers. However, its scalability is a major concern, as it does not provide secured

keys when huge amounts of sensor nodes are utilized. Another encryption algorithm was developed in [39] based on Advanced Encryption Standard (AES) encryption algorithm to verify the authentication between users transferring medical images by creating randomly encrypted images by the One Time Password (OTP) generator. However, a crypto stego encryption model should be utilized to ensure highly secured images transfer. Authors in [40] considered securing biometrics data collected for medical treatments by applying Weber Local Descriptor (WLD) or Local Binary Pattern (LBP) decryption methods. It was proved to be efficient for face recognition only, but was not tested for other biometric data, such as fingerprints and speech recognition. Cryptography encryption was considered in [41] to generate images with color or gray scale to hide messages by applying both AES and Rivest-Shamir-Adleman (RES) algorithms, integrated with the 2D-Discrete Wavelet transform levels 1 and 2. This proposed hybrid model was tested against another proposed model only, without clarifying how worked to prove performance.

The optimization of cryptography was investigated in [42] by generating a hybrid encryption methodology using Elliptic Curve Cryptography (ECC) with Particle Swarm Optimization (PSO) and Grasshopper Optimization (GO) encryption methods for better use of memory, tested against Peak Signal To Noise Ratio (PSNR) metrics, but it was not tested against the tamper localization in medical images. In [43], a testing database tool was defined for medical IoT applications to detect vulnerabilities and cyber-attacks over the network by testing IP addresses to detect denial of the service (DOS) attacks. However, not all involved devices were included in the security testing, besides, there was no alert for devices that the vulnerability was detected from. The data transmission between cloud services and user devices was monitored in [44] to determine the main parameters to secure, in which different protocols were used to test memory processing, virtual machines performance, gateway usage, and the amount of delay to produce and store results, but there was no real application as a case study to assure the security of the medical applications.

IV. SMART CITIES IOT SYSTEMS

A. The Application Scenarios

The need for smart solutions are continuously increasing due to the dramatic worldwide population increase, causing more problems in pollution, traffic congestions, educational facilities and energy consumption [45]. Information and communication technology (ICT) was applied in smart cities for education [46], in which teaching was through the Internet and students are receiving and sharing materials using sky drive or "Mindomo" tool [47]. Handling emergencies and incidents especially for critical applications that require electricity, leads to the need for smart grid applications and energy management ways to quick recover any sudden failures that use various network technologies to support electricity from different stations to different network areas, i.e. WAN, BAN, NAN, or other smart meter reading applications for electricity, gas and water usage [48]. To manage parking times and reduce traffic jams, a smart parking management system was developed, in which sensors were attached to sense whether a car was parked in place, processing data over cloud computing systems to alert people who want to park with empty places using Wi-Fi through their smart phones [49]. To make sure that all garbage around the city was collected with efficient time and effort, a waste management system was introduced that dynamically calculated the best route to follow where sensors are attached with each garbage[50].

Energy conservation, cost reduction, and providing ease to life allow fast growth of smart homes, in which facilities such as an AC receives that inhabitants coming near home to turn on before arriving with a certain time, or wind power generators, solar generators, lightening options when sensors detect entrance to a room to turn on or exit a room to turn off [51]. However, the main challenges include improving reliability, usability, interpretability, scalability, security, which need customized testing techniques and methodologies at all testing levels [52].

B. The Used Technologies

Different technologies are combined to fulfill any of the facilities in smart cities. Communication technologies such Wi-Fi, fiber optical, ZigBee, Z-Wave, DSL, Ethernet, WiMax, Bluetooth and LTE, with various protocols, are required to provide services for indoor/outdoor applications [48]. Several platforms can be used by developers to keep on generating smart ideas and applications, but they are not open source, such as smartSantander, City SDK and Sentilo [53]. RFID technology is used instead of digital cameras for the detection process, as when detecting cars plates to register cars and facilitate parking payments [54].

Testing over simulated environment would be more applicable to assure all functional and non-functional requirements and to generate reports. Selecting the correct simulation tool is based on the system characteristics. A variety of simulating tools has been used, but MATLAB is the most common used tool [55].

C. Testing Types and Methods

Testing smart cities applications is a major phase for their sustainability, where some key performance indicators should be verified [56]. For instance, energy consumption reduction, scalability (number of coverage meters and bandwidth range), and the number of devices of enhanced machine type communication (eMTC) could be some of the metrics considered in performance testing [57]. Long Term Evolution (LTE) standard has been tested in smart city applications, in which its performance needed enhancement [58]. Thus, LTE Random Access (RA) was developed and tested using Network Simulator (ns-3) under large number of connections. However, the proposed approach lacked quick responses when overloaded with huge number of requests. Smart parking requires smart sensors, in which testing the performance and accuracy of the used sensors is important. a comparison between Light Dependable Resistor (LDR) and Infra-Red (IR) sensors was conducted connected to a WSN to detect the free parking slots and the vehicles or the objects better [59]. In [60], a Building Energy Management Open Source Software (BEMOSS) was developed, where performance testing was applied in smart buildings to evaluate saving energy in different embedded systems. However, the integration with these embedded systems was not declared to clarify how performance testing was investigated [60]. The huge number of connected devices to a network requires that the network should be scalable. Accordingly, Low Power Wide Area Networks (LPWANs)

and Long Range WAN (LORAWAN) were presented [61]. Performance testing was conducted using Long Range (LORA) over network simulator (ns-3) to evaluate the bandwidth coverage scalability according to some metrics, like the used number of gateways, Spreading Factor (SF) and the Adaptive Data Rate (ADR). However, the coverage of the used gateways is limited with a fixed number of devices only. In addition, it lacked scalability, as it did not work when the number of devices increased.

Another level of testing is the security testing to keep the users' data secured, many researches have addressed the security requirements of IoT applications. In [62], Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) approach was introduced to discover threats for both cyber and physical security, where confidentiality testing was applied on all involved devices, to test the data transfer between devices, and servers Integrity testing was then investigated to detect how devices would respond to the wrong and fake servers inserted between the devices and real server. Also access control testing was configured by applying password guessing attacks to check if the used protocols were strong enough to protect. This paper did not propose a case study on a real smart environment due to the difficulty of the used services. In [63], an Intelligent Transportation System (ITS) was proposed to provide some features, like: cyber security, traffic management and emergency responses, in which vehicles should be monitored and the users' information should be kept secured using triple bloom filter security (TBFS) protocol for encryption and decryption on the edge level. The performance was tested to investigate the computational time and delay, but it was not mentioned whether this was on a real or simulated environment.

Fast Identity Online (FIDO) protocol was presented in [64] to tackle weak security authentication passwords over IoT clouds, where cryptographic keys were generated and users could access them through biometric ways or a pin password with minimum delay time. However, this proposed security solution still needs to be tested on hardware devices not only simulated platforms. To add security to smart city applications, authors in [65] proposed a framework to evaluate the integration of block-chain technology with the communication technologies at the communication level of a system for security purposes. However, there was no implementation of this proposed solution to test the integration correctness, nor the performance enhancement that could have been achieved. Attacks detection in smart city applications using deep learning models was investigated to test their accuracy and fault detection rate against the shallow models [66] in the fog level where network protocols are used, but it is still needed to be tested against other machine learning algorithms as decision trees and neural network algorithms. For the acceptance testing level in smart environment applications, a full study was conducted in [67], indicating that the acceptance of any new technology in smart environments applications such in education relies on the Unified Theory of Acceptance and Use of Technology (UTAUT), which defined seven metrics to be measured. The major concern is that these metrics were considered over native students with high education level, which may vary when applied on other level of students. Hence, no research has addressed other level of testing on smart environments domain, where most of the work was solely on the security and performance levels of testing.

V. Precision Agriculture IoT Systems

A. The Application Scenarios

It is important to have precision agriculture to manage farms and corps for better quality, productivity and save energy with respect to temperature, humidity, rain and other weather changes that influence farms' corps and soil fertility [68]. IoT-based software applications were developed to help farmers track pests by leaf monitoring and maintain their farms by receiving alerts about the farm's condition SMSs to take actions like turning sprinklers, fans, lights, pumps or boosters on/off or using chemical treatments.

B. The Used Technologies

Precision agriculture is achieved using smart devices, sensors, and image capturing sensors with screens, connected to the Internet to provide solutions to collect, analyze, monitor and make decisions over cloud computing platforms. Different wireless technologies were used, such as Li-Fi, Wi-Fi, LORA, LR-WPAN, Bluetooth [69]. Gateway communications such as ZigBee, NFC and RFID were mostly used for tracking and detecting animals in farms. Huge number of sensors were used to detect sun light, temperature, humidity, water level and soil moisture [70]. Precision seeding was also considered using the Global Positioning System (GPS) technology [71].

C. Testing Types and Methods

Most of the testing studies in the agriculture domain were unit testing and performance testing, where new devices and modules were developed and tested for their efficiency and performance. Protecting farms against any rodents was discussed in [72], in which CCTV cameras were not useful in agriculture applications. Thus, an algorithm was implemented based on Passive Infra-Red (PIR) sensors and Ultrasonic Ranging devices to detect different readings according to the distance and time. Performance testing was applied to prove the accuracy of the proposed solution, but it still needs to differentiate between the moving objects, whether it is a human, rodent, or any other animal in order to send correct alerts. Seed testing was studied in [73], where an application was developed using Rasberry PI model, temperature sensors and network gateways to test the quality of seeds from the very first phase of planting till harvesting and storing, and to define the needs of these seeds, as the light and watering needs. Acceptance testing was applied using the Technology Acceptance Model (TAM), measuring the ease of use and usefulness, but it is still needed to test the proposed architecture when using sensors or actuators.

An automatic soil testing module was presented in [74] in order to save time and efforts, where a module based on moisture sensor (YL69), temperature sensor (LM35) and humidity sensor (DHT11) were used, and the readings are viewed on the screen to control the use of water pumps. Performance testing was conducted to check its efficiency and accuracy to define the amounts of nutrients and chemical's needs. However, the proposed module was not evaluated against other modules nor with other sensor types. A pesticide device with a solar energy generator was developed and tested in [75] with a PIR sensor. The performance was tested under the used technologies and network to check its functionality till 60 meters distance, but it still needs to trigger the soil and moisture condition using

sensors. A smart irrigation system was developed and tested in [76] that used ZigBee network, moister and soil sensors. To decide when watering pumps should work and stop, its performance was tested in a real farm to prove conversing power and cost using a machine learning algorithm. However, the scalability was not tested against different areas, as the case study was applied in a specific area.

VI. DISCUSION AND RESEARCH GAPS

Most of the studies that addressed testing of IoT systems lack significant issues, as they do not consider many critical testing types and approaches. Tables A1, A2, and A3 provides a summary for the analyzed research, including the considered testing types, proposed approaches, used technologies and devices, the environment applied in testing. While the focus was on the load performance testing and security testing techniques, integration and acceptance testing were less fortunate, in which this level of testing requires a lot of testing efforts as the rate of errors increases. As for performance testing, the most commonly used equations were:

$$Accuracy = (TP+TN)/(TP+TN+FP+FN) \quad (1)$$

$$Precision = (TP)/(TP+FP) \quad (2)$$

$$Recall = (TP)/(TP+FN) \quad (3)$$

where TP is true positive, TN is true negative, FP is false positive, and FN is false negative Other testing techniques have never been investigated, such as the stress, limit, soak, and spike performance testing techniques, in addition to use case testing for systems acceptance, compatibility testing, configuration testing, scalability testing, recovery testing, and regression testing techniques. To the best of our knowledge, there is no comprehensive framework that covers all these testing levels for any IoT-based system, testing levels has been evaluated. Few studies mentioned the use of an automated tool to apply their performance or security testing, while most of the research works did not present how they performed their testing. Thus, the need to produce dynamic customized tools and automated approaches for IoT-based systems testing is rapidly increasing, due to the enormous number of connected devices over the internet. On the other hand, IoT-based systems should be tested in a simulated environment closer to the real environment to ensure the testing accuracy results, which is considered as a serious testing challenge to mimic diverse uncontrolled contexts. An efficient alternative could be proposing customized static formal specification approaches for those IoT-based systems where dynamic testing is inapplicable.

VII. CONCLUSION

Nowadays, a vital need is rapidly increasing for efficient testing approaches that fit IoT-based systems in different domains. In this paper, a comprehensive study has been conducted to evaluate the current state-of-art in testing techniques that were considered for IoT-based systems in three different domains; medical and health, smart cities, and precision agriculture. The main levels of testing that should be addressed in IoT-based systems were evaluated to be five levels, where not all of them were investigated in the literature. Through this exhaustive analytical study, it can be concluded that there is no generic framework that handles all testing levels for IoT-based systems, while considering both devices and platforms heterogeneity, limited resources utilization, the operating contexts, and the quality of service. In addition, the simulation of real diverse uncontrolled contexts in IoT-based systems is another testing challenge, in which new customized static formal specification approaches would be required to ensure that such simulated environments are closer to the real environment to achieve accurate testing results.

APPENDIX

TABLE A1: TESTING APPROACHES IN PRECISION AGRICULTURE IOT SYSTEMS

R#	Approach	Test Type	Gaps	Used Technologies	Metrics	Used Devices	Testing Environment	Evaluation Results
73	Testing quality detection of seeds for light and watering	Acceptance testing	Testing is needed with sensors or actuators	TCP/IP protocols, Wi-Fi, MVC framework	Ease of use and use fullness	Personal Computer and Temperature sensors	Real environment	Acceptance degree 70%
72	Testing readings detection at different ranges	Performance testing	No differentiation between moving objects	WSN, RFID and HTTP	Time and distance	CCTV camera , Raspberry Pi 2, PIR Sensor, URD	Real environment	Test cases succeeded with 84.8%
74	Automatic soil testing to control water pumps use		Tested at ordinary ways and no related modules mentioned	Bluetooth, Wi-Fi technologies	Covering area, productivity, user feedback	water pump devices and sensors	Real environment	High sensors productivity for 10 meters
75	Testing a solar energy generator for covering range		Needs to trigger the soil and moisture condition	6LoWPAN, Wi-Fi, Zigbee technologies	Batteries and power usage, coverage range	PIR sensor and pesticide devices	Real environment	Pesticide Delivery till 60m
76	Testing a smart irrigation system to control water pumps use		Scalability	ZigBee and Crossbow Technologies	Areas coverage, water loss and irrigation facilitate	accelerometer sensors	Real environment	Decreased water loss about 14 %

TABLE A2: TESTING APPROACHES IN MEDICAL IOT SYSTEMS

R#	Approach	Test Type	Gaps	Used Technologies	Metrics	Used Devices	Testing Environment	Evaluation Results
38	Testing proposed encryption algorithm based on DES	Security testing	Scalability	ZigBee, TCP/IP protocols and WSN	Attacks rate, encryption speed rate	Wearable devices, sensors	Simulated environment	Transmit rate > 0.986, error rate < 0.05
39	Testing with proposed encryption algorithm based on AES		crypto-stego encryption model	OPT embedding system and DICOM	MSE and PSNR error metrics	3 servers	NIST test suite	entropy 7.33
40	Testing biometrics data applying WLD and LBP methods		Not tested for other biometric data	Wi-Fi 4G, WBAN, Ethernet, RFID, Bluetooth, ZigBee	chi-square distance metric	Smart phones and Biometric sensors	Real time environment	Accuracy 98.1% at WLD 97.3% at LBP
43	Test database to detect vulnerabilities and cyber-attacks		Not all devices in, no alert for vulnerable devices	Internet enabled insulin pumps	Nessus Network scan	Devices with virtualized machines	Simulation using "Shodan" tool	9.97% of devices with vulnerabilities
41	Testing with proposed encryption applying AES and RES		Lacked to clarify how worked to prove enhancement	WMSN	PSNR, MSE, and BER	Personal computer	Simulation environment	PSNR 57.02, MSE 0.1288 and BER=0
42	Generating a hybrid encryption using ECC with PSO and GO	Performance Testing	Not tested against tamper localization	The used technologies were not mentioned	PSNR, MSE, BER, and SSI metrics	Personal computer	Real environment	1.5 min to finish encryption
44	Testing between cloud services and user devices	Both	No real application	TCP, SSL protocol, Cloud computing	storage, processing, delays	Smart devices, biometric readers, cloud	No case study	No studied Experiment with results

TABLE A3: TESTING APPROACHES IN SMART CITY IOT SYSTEMS

R#	Approach	Test Type	Gaps	Used Technologies	Metrics	Used Devices	Testing Environment	Evaluation Results
58	Testing LTE standard in smart city applications	Performance testing	Lacked quick responses when a huge overload of requests is triggered	LTE protocol stack and EPC network	Delay time of access	No mentioned devices	Simulation environment using ns-3 tool	Delay range (0.1s-1m)
59	Testing parking sensors using LDR and IR		Consumed a lot of energy	WSN, GPS and RFID	Accuracy of vehicle detection	LDR and IR sensors	Real environment	Detection rate range 0.45-2.5
60	Test saving energy in smart embedded systems		The integration with embedded systems was not declared	Wi-Fi, TCP/IP communication networks	Electricity utility, power consumption	PC, smart phones, Temperature sensors	Emulated environment	No numeric results
61	Testing LORA for bandwidth coverage scalability		Limited coverage of gateways with fixed number of devices	LPWANs	SF gateway coverage	Smart devices	Simulation environment using ns-3 tool	Coverage reliability is >90%
62	OCTAVE approach to discover threats for both cyber and physical security	Security testing	No case study on a real smart environment due to the difficulty of the used services	WSN, RFID, Bluetooth, NFC, IP, EPC and Wi-Fi	Identify threats rate	Embedded computers, wearable devices, lightening system and cameras	No case study	No studied Experiment with results
63	Cyber security in traffic management using TBFS protocol		No mention how the approach detected any cyber-attacks.	Cellular networks, short-range (DSRC) and 5G	Delays, precision in encryption and decryption	Computers, aerial vehicles and embedded sensors	Simulated environment	Delay time (0-70ms)
64	FIDO to tackle weak authentication passwords over IoT clouds.		Not tested on hardware devices, only simulated platforms were used	Cloud computing, MQTT, HTTP, COAP protocols	Delay rate, authentication response	Embedded devices, smart phones, home devices	Simulation environment	Delay time (0-150ms)
65	Testing integration of block-chain with communication for security purposes		No implementation to detect faults	Bluetooth, 6LoWPAN, Wi-Fi, Ethernet, 3G, and 4G	Reliability, fault tolerance and scalability	Motion, light and humidity sensors	No case study	No studied Experiment with results
66	Attacks detection using deep learning against shallow models		Not tested against other machine learning algorithms	IP/TCP protocols	False alarm rate, accuracy, precision and recall	Computer devices	Simulated Environment	Accuracy 99.20%, Prec. 99.36% and Recall 99.15
67	Acceptance testing relying on UTAUT technology	Acceptance testing	Metrics tested over native students with high education	3G and 4G technologies and UTAUT	PE, and Effort Expectancy	Computer devices	Real environment	Sustain. 92%, Sec. 85%, PE 83%, EE 90%

REFERENCES

[1] Y. Li, Y. Guo, and S. Chen, "A survey on the Development and Challenges of the Internet of Things (IoT) in China," 2018 Int. Symp. Sens. Instrum. IoT Era, ISSI 2018, pp. 1–5, 2018.

[2] H. Kaur and A. S. Kushwaha, "A Review on Integration of Big Data and IoT," Proc.-4th Int. Conf. Comput. Sci. ICCS 2018, pp. 200–203, 2019.

[3] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Bus. Horiz., vol. 58, no. 4, pp. 431–440, 2015.

[4] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," 2016 4th IEEE Int. Conf. Smart Energy Grid Eng. SEGE 2016, vol. i, pp. 381–385, 2016.

[5] E. J. Marinissen et al., "IoT: Source of test challenges," Proc. Eur. Test Work., vol. 2016-July, 2016.

[6] P. Martins Pontes, B. Lima, and J. Pascoal Faria, "Izinto: A Pattern-Based IoT Testing Framework," Companion Proc. ISSTA/ECOOP 2018 Work. - ISSTA '18, pp. 125–131, 2018.

[7] T. Kanstr, "Architectures and Experiences in Testing IoT Communications," 2018.

[8] K. Kaur, "A Survey on Internet of Things – Architecture , Applications , and Future Trends," 2018 First Int. Conf. Secur. Cyber Comput. Commun., pp. 581–583, 2018.

[9] A. Vakaloudis and C. O. Leary, "A framework for rapid integration of IoT Systems with industrial environments," 2019 IEEE 5th World Forum Internet Things, pp. 601–605, 2019.

[10] M. Singh and G. Baranwal, "Quality of Service (QoS) in Internet of Things," Proc. - 2018 3rd Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2018, pp. 1–6, 2018.

[11] H. C. Kuo and F. J. Lin, "Performance Management of IoT / M2M Platforms," pp. 119–124, 2016.

[12] J. Choi, Y. Shin, and S. Cho, "Study on information security sharing system among the industrial IoT service and product provider," Int. Conf. Inf. Netw., vol. 2018-Janua, pp. 551–555, 2018.

[13] L. J. Perez and J. S. Rodriguez, "Simulation of scalability in IoT applications," Int. Conf. Inf. Netw., vol. 2018-Janua, pp. 577–582, 2018.

[14] M. O. Thomas and B. B. Rad, "Reliability Evaluation Metrics for Internet of Things, Car Tracking System: A Review," Int. J. Inf. Technol. Comput. Sci., vol. 9, no. 2, pp. 1–10, 2017.

[15] E. Park, Y. Cho, J. Han, and S. J. Kwon, "Comprehensive Approaches to User Acceptance of Internet of Things in a Smart Home Environment," IEEE Internet Things J., vol. 4, no. 6, pp. 2342–2350, 2017.

[16] M. Bures, "Framework for Integration Testing of IoT Solutions," 2017 Int. Conf. Comput. Sci. Comput. Intell., pp. 1838–1839, 2017.

[17] G. Murad, A. Badarneh, A. Quscf, and F. Almasalha, "Software Testing Techniques in IoT," 2018 8th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2018, pp. 17–21, 2018.

[18] S. Popereshnyak, O. Suprun, O. Suprun, and T. Wieckowski, "IoT application testing features based on the modelling network," 2018 14th Int. Conf. Perspect. Technol. Methods MEMS Des. MEMSTECH 2018 - Proc., pp. 127–131, 2018.

[19] H. Kim et al., "IoT-TaaS: Towards a Prospective IoT Testing Framework," IEEE Access, vol. 6, no. c, pp. 15480–15493, 2018.

[20] J. D. Hagar, "Software Test Architectures and Advanced Support Environments for IoT," 2018 IEEE Int. Conf. Softw. Testing, Verif. Valid. Work., pp. 252–256, 2018.

[21] C. Perera, S. Member, A. Zaslavsky, and P. Christen, "Context Aware Computing for The Internet of Things : A Survey," pp. 1–41, 2013.

[22] E. S. Reetz, K. Daniel, T. Ralf, and A. Lehmann, "Test Driven Life Cycle Management for Internet of Things based Services : a Semantic Approach," no. c, pp. 21–27, 2012.

[23] J. Esquiagola, L. Costa, P. Calcina, G. Fedrecheski, and M. Zuffo, "Performance Testing of an Internet of Things Platform," no. IoTBDS, pp. 309–314, 2017.

[24] H. El-Sayed et al., "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," IEEE Access, vol. 6, pp. 1706–1717, 2017.

[25] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with internet of things: Challenges and open issues," Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017, vol. 2018-Janua, pp. 670–675, 2018.

[26] R. K. Lomotey, J. Pry, S. Sriramoju, E. Kaku, and R. Deters, "Middleware Framework for IoT Services Integration," 2017.

[27] S. Cristian, O. Grigorescu, R. Deaconescu, and C. Mihnea, "Why IoT security is failing . The Need of a Test Driven Security Approach," 2018.

[28] K. Ullah, "Effective Ways to Use Internet of Things in the Field of Medical and Smart Health Care," 2016.

[29] C. Li, X. Hu, and L. Zhang, "ScienceDirect ScienceDirect The IoT-based heart disease monitoring system for pervasive The IoT-based heart disease monitoring system for pervasive healthcare service healthcare service," Procedia Comput. Sci., vol. 112, pp. 2328–2334, 2017.

[30] M. Leotta et al., "Towards an Acceptance Testing Approach for Internet of Things Systems," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10544 LNCS, pp. 125–138, 2018.

[31] S. Pinto, J. Cabral, and T. Gomes, "We-Care : An IoT-based Health Care System for Elderly People."

[32] J. J. P. C. Rodrigues et al., "Enabling Technologies for the Internet of Health Things," vol. XX, no. 1, 2020.

[33] S. M. R. Islam, D. Kwak, and H. Kabir, "The Internet of Things for Health Care : A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015.

[34] H. N. Saha et al., "Health Monitoring using Internet of Things (IoT)," pp. 69–73, 2017.

[35] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "Journal of Industrial Information Integration The internet of things in healthcare : An overview," J. Ind. Inf. Integr., vol. 1, pp. 3–13, 2016.

[36] D. Stephen and D. Wolthusen, "ScienceDirect Towards Towards Composable Composable Threat Threat Assessment Assessment for for Medical Medical IoT IoT (MIoT) (MIoT)," Procedia Comput. Sci., vol. 113, pp. 627–632, 2017.

[37] F. Alsubaei and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," no. 6, pp. 112–120, 2017.

[38] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," Proc. - Int. Symp. Parallel Archit. Algorithms Program. PAAP, vol. 2016-Janua, pp. 217–222, 2016.

[39] S. Rajagopalan, S. Janakiraman, A. Rengarajan, S. Rethinam, S. Arumugham, and G. Saravanan, "IoT Framework for Secure Medical Image Transmission," 2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2018, pp. 1–5, 2018.

[40] T. Iot and T. Internet, "T oward E nd - to -E nd B iometrics -B ased S ecurity for I o T I nfrastructure," no. October 2016, pp. 44–51, 2020.

[41] M. Elhoseny, G. Ramírez-González, O. M. Abu-elnasr, S. A. Shawkat, and N. Arunkumar, "Secure Medical Data Transmission Model for IoT-based Healthcare Systems," vol. 3536, no. c, 2018.

[42] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," Neural Comput. Appl., vol. 3456789, 2018.

[43] E. Mcmahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing Medical Device Vulnerabilities on the Internet of Things," pp. 176–178, 2017.

[44] E. Guillén, J. Sánchez, and L. R. López, "IoT Protocol Model on Healthcare Monitoring," pp. 193–196, 2017.

[45] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities," J. Internet Serv. Appl., vol. 6, no. 1, pp. 1–15, 2015.

[46] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," J. Urban Technol., vol. 22, no. 1, pp. 1–19, 2015.

[47] A. Delić-Zimić and N. Gadžo, "Implementation of ICT in Education," Lect. Notes Networks Syst., vol. 28, pp. 215–222, 2018.

[48] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," Comput. Networks, vol. 67, pp. 74–88, 2014.

[49] A. R. Masoud, H. Al Mamari, S. I. Ali Kazmi, J. Pandey, and S. Al Hinai, "IoT based smart parking and traffic management system for middle east college," 2019 4th MEC Int. Conf. Big Data Smart City, ICBDSC 2019, pp. 1–6, 2019.

[50] P. Amirian et al., "Challenges and Opportunities of Waste Management in IoT-Enabled Smart Cities: A Survey," IEEE Trans. Sustain. Comput., vol. 2, no. 3, pp. 275–289, 2017.

[51] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," J. Clean. Prod., vol. 140, pp. 1454–1464, 2017.

[52] I. Yaqoob et al., "Enabling Communication Technologies for Smart Cities," IEEE Commun. Mag., vol. 55, no. 21, pp. 112–120, 2017.

[53] P. Chamoso, A. González-Briones, S. Rodríguez, and J. M. Corchado, "Tendencies of Technologies and Platforms in Smart Cities: A State-of-the-Art Review," Wirel. Commun. Mob. Comput., vol. 2018, 2018.

[54] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, K. Jambi, and M. Alrasheedi, "A novel and secure smart parking management system (SPMS) based on integration of WSN, RFID, and IoT," 2018 15th Learn. Technol. Conf. L T 2018, pp. 102–106, 2018.

[55] A. A. Baloch, P. H. Shaikh, F. Shaikh, Z. H. Leghari, N. H. Mirjat, and M. A. Uqaili, "Simulation tools application for artificial lighting in buildings," Renew. Sustain. Energy Rev., vol. 82, no. March, pp. 3007–3026, 2018.

[56] M. D. Lytras and A. Visvizi, "Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research," Sustain., vol. 10, no. 6, pp. 1–16, 2018.

[57] M. El Soussi, P. Zand, F. Pasveer, and G. Dolmans, "Evaluating the Performance of eMTC and NB-IoT for Smart City Applications," IEEE Int. Conf. Commun., vol. 2018-May, pp. 1–7, 2018.

[58] M. Polese, M. Centenaro, A. Zanella, and M. Zorzi, "M2M massive access in LTE: RACH performance evaluation in a Smart City scenario," 2016 IEEE Int. Conf. Commun. ICC 2016, pp. 0–5, 2016.

[59] M. Bachani, U. M. Qureshi, and F. K. Shaikh, "Performance Analysis of Proximity and Light Sensors for Smart Parking," Procedia Comput. Sci., vol. 83, no. Ant, pp. 385–392, 2016.

[60] X. Zhang, R. Adhikari, M. Pipattanasomporn, M. Kuzlu, and S. R. Bradley, "Deploying IoT devices to make buildings smart: Performance evaluation and deployment experience," 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 530–535, 2017.

[61] D. Magrin, M. Centenaro, and L. Vangelista, "Performance evaluation of LoRa networks in a smart city scenario," IEEE Int. Conf. Commun., 2017.

[62] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," Sensors (Switzerland), vol. 18, no. 3, pp. 1–17, 2018.

[63] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "SECURITY AND PRIVACY OF CONNECTED VEHICULAR CLOUD UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles," no. June, pp. 42–51, 2018.

[64] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, "A security A [64"A [64]a security authorization scheme for smart home Internet of Things devices," Futur. Gener. Comput. Syst., vol. 86, pp. 740–749, 2018.

[65] K. Biswas and A. B. Technology, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst., pp. 1392–1393, 2016.

[66] A. A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things," Futur. Gener. Comput. Syst., 2017.

[67] P. Baudier, C. Ammi, and M. Deboeuf-rouchon, "Technological Forecasting & Social Change Smart home : Highly-educated students ' acceptance," Technol. Forecast. Soc. Chang., no. June, pp. 1–19, 2018.

[68] P. K. A. Patil, "A Model for Smart Agriculture Using IoT," pp. 543–545, 2016.

[69] M. S. Mekala, "A Survey : Smart Agriculture IoT with Cloud Computing," 2017.

[70] P. P. Ray, "Internet of things for smart agriculture : Technologies , practices and future direction," vol. 9, pp. 395–420, 2017.

[71] K. Lakhwani, H. Gianey, and N. Agarwal, Development of IoT for Smart Agriculture a Review. Springer Singapore.

[72] T. Baranwal, "Development of IoT based Smart Security and Monitoring Devices for Agriculture," pp. 597–602, 2016.

[73] R. S. De Souza et al., "Continuous monitoring seed testing equipaments using internet of things," Comput. Electron. Agric., vol. 158, no. January, pp. 122–132, 2019.

[74] S. Saha, S. Paul, S. Halder, and K. Majumder, "Smart Agricultural System : Better Accuracy and Productivity," pp. 23–24, 2017.

[75] S. Giordano, I. Seitanidis, M. Ojo, D. Adami, and F. Vignoli, "IoT Solutions for Crop Protection against Wild Animal Attacks," 2018 IEEE Int. Conf. Environ. Eng., pp. 1–5.

[76] R. C. Andrew, "IoT solutions for precision agriculture," 2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron., pp. 345–349, 2018.