SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 4, Issue 1, 2019
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Progress of Research Papers in Internet of Things (IoT): A Systematic Literature Review

Jayson E. Tamayo
College of Computing Sciences
Pangasinan State University
jayson.tamayo2@gmail.com

Abstract - *In 2014, J. Stankovic identified the research questions and directions to achieve the vision of Internet of Things (IoT). In this paper, we explore the spectrum of research conducted in connection to these research directions: (1) massive scaling, (2) architecture and dependencies, (3) creating knowledge and big data, (4) robustness, (5) openness, (6) security, and (7) privacy. The methodology used in this paper is a systematic literature review. Security and privacy were the common research direction related to IoT. This showed that the common issues and challenges faced by IoT is on security and privacy. It is worth noting that while there is an increased concern on IoT devices' dependencies, there are fewer studies conducted on that domain.*

Keywords: internet of things, IoT research directions

1 INTRODUCTION

It has been nearly impossible to come across with the term "Internet of Things (IoT)" in the computing world. Especially in the previous years where a tremendous surge of interest in the Internet of Things has been seen. Consortia have been formed to define frameworks and standards for the IoT. Numerous companies have started introducing IoT-based products and services. Number of IoT-related acquisitions also have been making the headlines. For example, on January 14, 2014, Google Inc. acquired Nest Labs – a company pioneer in home IoT-based devices [1]. In the same year, Samsung acquired SmartThings – a company headquartered in California, specializing in building an open platform for smart homes and the consumer of Internet of Things. Politicians as well as practitioners increasingly acknowledge the Internet of Things as a real business opportunity, and according to Gartner Insights, the IoT market will have a tremendous growth by 2028.

The realization of the idea of the Internet of Things (IoT) is made possible through the growing number of physical objects that are being connected to the Internet. A basic example of this includes thermostats and HVAC (Heating, Ventilation, and Air Conditioning)[2][3][4][5][6][7] monitoring and control systems [8][9] that enable smart homes. There are other domains and environments where IoT can play a remarkable and beneficial role. These applications include smart homes [10][11][12][13][14][15], smart cities [16][17][18][19][20], transportation [21][22][23][24], healthcare [25][26][27][28][29][30], industrial automation [31][32][33][34], agriculture [35][36][37][38][39][40], emergency response [41][42][43] to natural and man-made disasters where human-decision making is difficult.

In 2014, J. Stankovic identified the research questions and directions to achieve the vision of IoT. The spectrum of research required to achieve IoT at the scale envisioned requires significant research along many directions. Stankovic's paper outlined those research directions. This paper aims to explore the spectrum of researches conducted in connection to these research directions: (1) massive scaling, (2) architecture and dependencies, (3) creating knowledge and big data, (4) robustness, (5) openness, (6) security, and (7) privacy.

The rest of the paper is organized as follows: section 2 discusses the methodology to be used. In addition, section 2 also discusses the seven (7) specific issues and challenges, and research directions in Internet of Things (IoT). This will be the basis of categorization of explored IoT-specific researches. Then in section 3, results will be discussed. Different IoT researches are discussed according to the seven (7) research directions. Finally, section 4 concludes the paper.

2 METHODOLOGY

This paper uses the SLR method in undertaking a systematic literature review. By complying to the systematic procedure defined by the said research method, this paper can provide a more objective process in selecting relevant and note-worthy studies. The major steps in SLR include the following: (1) defining a research question, (2) search strategy for selecting studies and (3) management of studies.

Using the SLR methodology, the author should be able to define a research question that is anchored to the purpose of the literature review. The author should also be able to plan for the search strategy and specify the steps needed. Lastly, the author should be able to manage the studies, filtering the irrelevant studies and selecting the pilot studies to be evaluated. In order to properly manage the solutions introduced in the studies.

2.1 Defining a research question

This paper aims to identify the progress of and defining a research question is the initial step. The research question will be the basis for the search strategy and the selection of the pilot studies to be evaluated.

2.2 Planning a search strategy

The initial step in planning a search strategy is selecting the input data source. In this paper, ACM Digital will be used as a source for the relevant studies. ACM Digital Library has been chosen as the main source because this is the most comprehensive database of full-text articles covering computing and information technology. The second step in our search strategy is to construct a query based on the research question. Keywords should be chosen carefully to maintain the proper balance between specificity and generality.

2.3 Managing the studies

After running the query in the ACM Digital Library, studies will be obtained. But there is a need for each of the study to be assessed for its actual relevance through inclusion criteria. Table 1 shows the inclusion criteria.

Table 1: Inclusion Criteria

No.	Criterion	Description
1	It should be written in English.	There are some studies that are written in other language. They have provided English title and abstract so these papers will show up in the search results. Only studies written in English will be included.

2	It should be peer-reviewed.	To ensure the quality of this systematic literature review, only peer-reviewed studies will be included.
3	The publication date must not be earlier than 2013.	To ensure that only up-to-date energy-efficiency solutions are included, only studies that were published in the year 2013 onwards are selected.

To furtherly filter the researches and articles, abstract and conclusion of each study are carefully examined. After selecting the pilot studies to be evaluated, the studies will be ordered and arranged according to the following type of issues being solved, presented by [63]: (1) massive scaling, (2) architecture and dependencies, (3) creating knowledge and big data, (4) robustness, (5) openness, (6) security, and (7) privacy. Each of the research directions are discussed.

2.4 Massive Scaling

This research direction emanated from the current trajectory of the number of smart devices being deployed in realization of IoT. If there will be trillions of devices or things that will be on the Internet, several problems, issues and challenges will occur like how to name each device, authenticate access, maintain, protect, use, and support such a large scale of things. Other questions such as: will IPv6 suffice? Will protocols such a 6LowPAN emerge? Will there be new development of standards and protocols? Since devices in the Internet of Things (IoT) will require their own energy source, will there be new ways to scavenge energy and implement low power circuits to finally eliminate the need for batteries? How will be the massive data be collected, used and stored? How will the real-time and reliability aspects be supported? How will devices be discovered? Will there a utility model to be developed? It is unlikely that any solution immediately becomes a norm. There will be many protocols and standards that will be developed, and they will co-exist. Will there be an architectural model that supports heterogeneity of devices and applications?

2.5 Architecture and Dependencies

The fact that trillions of devices will be connected to the Internet, it is important to have an adequate architecture to easily allow devices to connect, control, communicate and use applications. How will these devices interact in and across applications? Will things or set of things be disconnected on certain intervals to protect them from other devices? Of course, it makes sense for devices to share devices and information. Will the architecture of IoT borrow some approach from the smartphone world? Will the architecture include an app store? This has many advantages including an unbounded development of applications that can execute on heterogeneous devices. This similar architectural approach can also be used for IoT. However, the underlying platform for IoT is much more complicated than smartphones.

2.6 Creating Knowledge and Big Data

There will be vast amount of raw data that will be continuously collected in IoT. It is then necessary to develop techniques and tools to convert these raw data into usable knowledge. For example, in the medical field, various sensor values are collected from a person’s activities such as eating, respiration and others. In this situation, main challenges are in data interpretation and formation of knowledge. Limitations also include the cost of computations. Also, the amount of collected data will be enormous because of very large number of real-time sensor data streams. In this situation, main challenges are data provenance, the way data is processed, and the privacy and security applied to it. Consequently, uncertainty in interpreted data can easily cause users not to trust the system.

2.7 Robustness

The vision of IoT applications is based on a deployed sensing, actuation, and communication platform. In these kinds of deployments, it is necessary for the devices to know their locations, synchronized clocks, know their neighbor devices when cooperating, and have a coherent set of parameter settings such as consistent sleep/wake schedules, appropriate power levels for communication, and security keys. However, this is not always maintained over time because conditions can deteriorate. The most common problem in deterioration is with clock synchronization. Over time, clock drifts cause nodes to different time to result in application and computational failures. While clock re-synchronization is part of IoT maintenance, this activity poses challenges because more and more nodes may become out of place over time.

2.8 Openness

Majority of sensor-based systems have been closed or proprietary systems. For example, cars, airplanes and ships have networked systems that operate within that type of vehicle only. These systems require openness to achieve IoT greater benefits. However, supporting openness creates many research problems. All of our current composition techniques, analysis techniques and tools need to be re-thought and developed to account for this openness. New unified communication should be developed to enable efficient information exchange across diverse systems. However, this new communication should be balanced between functionality and security and privacy.

2.9 Security

A pervasive and fundamental problem in the Internet today is on how to solve and deal with security attacks. Security attacks are also a problem for the IoT because of the minimal capacity of devices being used, the physical accessibility to sensors, actuators and objects, and the openness of the systems, including the fact that IoT devices communicate wirelessly. The security problem is further exacerbated because transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. IoT applications must be able to continue to operate satisfactorily in the presence of security attacks and to be able to recover effectively after these attacks. In connection to this, a system should be able to detect the attack, diagnose the attack, and deploy countermeasures and repairs, but this should be performed in a lightweight manner due to the types of low capacity devices involved.

2.10 Privacy

While the interactions involved in IoT will provide many conveniences and useful services for individuals, it can also create many opportunities to violate privacy. To solve this, privacy policies for each system must be specified. An IoT infrastructure must enforce privacy. There should also be a mechanism to evaluate each data request if it violates privacy policies.

3 RESULTS AND DISCUSSION

This section will discuss the results of each step in the SLR methodology and later part will discuss the selected pilot studies according to type of issues.

3.1 Research question defined

This paper aims to answer the following question: What is progress of IoT-based researches with regards to the research directions identified by J. Stankovic?

3.2 Results of the search strategy

Keywords were constructed from the research question. These keywords will be used in the search query in ACM Digital Library. The following search query will be used: "*IoT researches*". Table 2 shows the number of search results per source:

Table 2: Number of search results

Search query	Number of results (ACM Digital Library)
IoT researches	158,779

3.3 Managing the studies

The search result for the first query has been furtherly refined by publication year (>= 2014). Table 3 shows the number of search results for the given query.

Table 3: Search result for the refined query

Search query	Number of results (ACM Digital Library)
IoT researches	56,879

To furtherly filter the results, advanced search feature has been used. The first where clause will be on the Title field that matches all (compared to matches any) of the following words or phrases: "internet of things". The next where clause will on the field of Publication Year, this is set to on or after (>=) 2014. The full query syntax is as follows:

```
"query": { acmdlTitle:(+internet+of+things) }

"filter": {"publicationYear":{ "gte":2014 }}, {owners.owner=HOSTED}
```

The above query resulted to fewer matches. From a total of 56,879 ACM Full-text Collection records, there were only 24 results found.

To furtherly filter the results and finally select the pilot studies, abstract and conclusion were read to verify and assess the paper's relevance to the research question. Table 4 shows the 14 final pilot studies to be evaluated.

Table 4: Final list of research with publication year

No.	Research Title	Publication Year
1	Efficient and dynamic scaling of fog nodes for IoT devices. [44]	2014
2	Introducing the QEST broker: Scaling the IoT by bridging MQTT and REST [45]	2014
3	Semantic gateway as a service architecture for iot interoperability [46]	2015
4	DIAT: A scalable distributed architecture for IoT [47]	2015
5	Survey of real-time processing technologies of iot data streams [48]	2016
6	Processing distributed internet of things data in clouds [49]	2015
7	Robust waste collection exploiting cost efficiency of IoT potentiality in smart cities [50]	2015
8	Robust relay selection for large-scale energy-harvesting IoT networks [51]	2017

9	Towards designing open and secure IoT systems: insights for practitioners [52]	2018
10	OCCI-IOT: an API to deploy and operate an IoT infrastructure [53]	2017
11	Blockchain for IoT security and privacy: The case study of a smart home [54]	2017
12	Network-level security and privacy control for smart-home IoT devices [55]	2015
13	Professional issues in consulting clients and educating users on IoT privacy and security [56]	2017
14	Privacy preference modeling and prediction in a simulated campuswide IoT environment [57]	2017

Additionally, the studies were categorized according to the type of issues and challenges. Table 5 shows the categorized studies:

Table 5: Categorized research

Research Direction	Studies
Massive Scaling	[44][45]
Architecture and Dependencies	[46][47]
Creating Knowledge and Big Data	[48][49]
Robustness	[50][51]
Openness	[52][53]
Security	[54][55][47]
Privacy	[56][57][47][54]

The study of Kafhali and Salah [44] focused on efficient scalability. They presented a queuing mathematical and analytical model to study and analyze the performance of IoT computing systems. Their mathematical model determines under any offered IoT workload the number of nodes needed so that the QoS parameters are satisfied. From the model, they derived formulas for key performance metrics which include system response time, system loss rate, system throughput, CPU utilization, and the mean number of messages request. Their analytical model is cross validated using DES (Discrete Event Simulator) simulations. While the study of Kim, et. Al. [45] proposed an IoT Home Gateway that supports abstracted device data to remove heterogeneity, device discovery by DPWS, Auto-configuration for constrained devices such as Arduino. Also, the IoT Home Gateway provides lightweight information delivery using MQTT protocol. In addition, they showed implementation results that access and control the device according to the home energy saving scenario.

With regards to IoT architecture research direction, Desai, et. Al. [46] proposed a gateway and Semantic Web enabled IoT architecture to provide interoperability between systems, which utilizes established communication and data standards. The Semantic Gateway as Service (SGS) allows translation between messaging protocols such as XMPP, CoAP and MQTT via a multi-protocol proxy architecture. Utilization of broadly accepted specifications such as W3C's Semantic Sensor Network (SSN) ontology for semantic annotations of sensor data provide semantic interoperability between messages and support semantic reasoning to obtain higher-level actionable knowledge from low-level sensor data. While the study of Sarkar, et. Al. [47] proposed a Distributed Internet-like Architecture for Things (DIAT), which will overcome most of the obstacles in the process of large scale expansion of IoT. It specifically addresses heterogeneity of IoT devices, and enables seamless addition of new devices across applications. In addition, they proposed a usage control policy model to support security and privacy in a distributed environment. They proposed a layered architecture that provides various levels of abstraction to tackle the issues such as, scalability, heterogeneity, security and interoperability. The proposed architecture is coupled with cognitive capabilities that helps in intelligent decision making and enables automated service creation.

In terms of IoT big data processing, Yasumoto, et. Al. [48] surveyed the emerging technologies toward the real-time utilization of IoT data streams in terms of networking, processing, and content curation and clarified the open issues. Then they proposed a new framework for IoT data streams called the Information Flow of Things (IFoT) that processes, analyzes, and curates massive IoT streams in real-time based on distributed processing among IoT devices.

In terms of IoT robustness, the paper of Anagnostopoulos, et. Al. proposed a dynamic routing algorithm for IoT smart cities which is robust and copes when a truck is overloaded or damaged and need replacement. They also incorporated a system model which assumes two kinds of trucks for waste collection, the Low Capacity Trucks (LCTs) and the High Capacity Trucks (HCTs). By incorporating HCTs they achieved reduction of the waste collection operational costs because route trips to the dumps are reduced due to high waste storage capacity of these trucks. Finally, the proposed models are evaluated on synthetic and real data from the city municipality of St. Petersburg, Russia. While in the paper of Kabawata, et. Al., proposed a new energy-harvesting EH relay selection scheme which is based on the residual energy at each relay's battery, and on information on the distribution of the channels between relays and the destination. The method thus minimizes both the outage probability and the feedback cost.

In terms of IoT security-related research directions, Dorri, et. Al. [54] presented a lightweight instantiation of a blockchain (BC) particularly geared for use in IoT by eliminating the Proof of Work (POW) and the concept of coins. Their approach was exemplified in a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home. Their proposed BC-based smart home framework is secure by thoroughly analyzing its security with respect to the fundamental security goals of confidentiality, integrity, and availability. While the paper of Sivaraman, et. Al. [55] proposed a software defined networking technology to be used to dynamically block/quarantine devices, based on their network activity and on the context within the house such as time-of-day or occupancy-level. They believe that their network-centric approach can augment device-centric security for the emerging smart-home.

In terms of IoT privacy-related research direction, Lee and Kobsa [57] proposed an intelligent software helping users make better privacy decisions as the researchers believe that this is an important component of privacy-preserving IoT environments.

4 CONCLUSION

In this paper, different IoT research papers were discussed. These research papers were collated based on the IoT research directions that were discussed by Stankovic in 2014. The papers were categorized according to the following: (1) massive scaling, (2) architecture and dependencies, (3) creating knowledge and big data, (4) robustness, (5) openness, (6) security, and (7) privacy.

Research directions related to security and privacy were the most common directions among the papers reviewed. This showed that the common issues and challenges faced by IoT is on security and privacy. It is worth noting that while there is an increased concern on IoT devices' dependencies, there are fewer studies conducted on that domain.

REFERENCES

[1] Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.

[2] Serra, J., Pubill, D., Antonopoulos, A., & Verikoukis, C. (2014). Smart HVAC control in IoT: Energy consumption minimization with user comfort constraints. The Scientific World Journal, 2014.

[3] Ruano, A., Silva, S., Duarte, H., & Ferreira, P. M. (2018). Wireless Sensors and IoT Platform for Intelligent HVAC Control. Applied Sciences, 8(3), 370.

[4] Silva, S., & Ruano, A. (2018). The IMBPC HVAC system: Wireless Sensors and IoT Platform. IFAC-PapersOnLine, 51(10), 1-8.

[5] Lee, T., Jeon, S., Kang, D., Park, L. W., & Park, S. (2017, January). Design and implementation of intelligent HVAC system based on IoT and Bigdata platform. In Consumer Electronics (ICCE), 2017 IEEE International Conference on (pp. 398-399). IEEE.

[6] Choi, M. I., Cho, K., Hwang, J. Y., Park, L. W., Jang, K. H., Park, S., & Park, S. (2017, March). Design and implementation of IoT-based HVAC system for future zero energy building. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 605-610). IEEE.

[7] Irudaya Raj, V. D., Logesh, K., Vasudevan, A., Bhavesh Nishant, B., Deepak, A., & Arvind, T. (2017). Experimental investigation on energy saving potential of smart HVAC unit. International Journal of Ambient Energy, 1-4.

[8] Pavithra, D., & Balakrishnan, R. (2015, April). IoT based monitoring and control system for home automation. In Communication Technologies (GCCT), 2015 Global Conference on (pp. 169-173). IEEE.

[9] Liu, Q., Ma, Y., Alhussein, M., Zhang, Y., & Peng, L. (2016). Green data center with IoT sensing and cloud-assisted smart temperature control system. Computer Networks, 101, 104-112.

[10] Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN-and IOT-based smart homes and their extension to smart buildings. Sensors, 15(5), 10350-10379.

[11] Mano, L. Y., Faiçal, B. S., Nakamura, L. H., Gomes, P. H., Libralon, G. L., Meneguete, R. I., ... & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. Computer Communications, 89, 178-190.

[12] Kang, B., Park, S., Lee, T., & Park, S. (2015, January). IoT-based monitoring system using tri-level context making model for smart home services. In 2015 IEEE International Conference on Consumer Electronics (ICCE) (pp. 198-199).

[13] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[14] Mandula, K., Parupalli, R., Murty, C. A., Magesh, E., & Lunagariya, R. (2015, December). Mobile based home automation using Internet of Things (IoT). In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2015 International Conference on (pp. 340-343). IEEE.

[15] Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Generation Computer Systems, 78, 1040-1051.

[16] Skouby, K. E., & Lynggaard, P. (2014, November). Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services. In Contemporary Computing and Informatics (IC3I), 2014 International Conference on (pp. 874-878). IEEE.

[17] Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An information framework for creating a smart city through internet of things. IEEE Internet of Things journal, 1(2), 112-121.

[18] Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. Procedia computer science, 52, 1089-1094.

[19] Giang, N. K., Lea, R., Blackstock, M., & Leung, V. (2016, December). On building smart city iot applications: A coordination-based perspective. In Proceedings of the 2nd International Workshop on Smart (p. 7). ACM.

[20] Krylovskiy, A., Jahn, M., & Patti, E. (2015, August). Designing a smart city internet of things platform with microservice architecture. In Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on (pp. 25-30). IEEE.

[21] Melis, A., Prandini, M., Sartori, L., & Callegati, F. (2016, September). Public transportation, IoT, trust and urban habits. In International Conference on Internet Science (pp. 318-325). Springer, Cham.

[22] Devi, Y. U., & Rukmini, M. S. S. (2016, October). IoT in connected vehicles: Challenges and issues—A review. In Signal Processing, Communication, Power and Embedded System (SCOPES), 2016 International Conference on (pp. 1864-1867). IEEE.

[23] Garofalaki, Z., Kallergis, D., Katsikogiannis, G., Ellinas, I., & Douligeris, C. (2017, December). A DSS model for IoT-based intelligent transportation systems. In 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) (pp. 276-281). IEEE.

[24] Al-Dweik, A., Muresan, R., Mayhew, M., & Lieberman, M. (2017, April). IoT-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems. In Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on (pp. 1-6). IEEE.

[25] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. In Exploring the convergence of big data and the internet of things (pp. 141-154). IGI Global.

[26] Bhatt, C., Dey, N., & Ashour, A. S. (Eds.). (2017). Internet of things and big data technologies for next generation healthcare.

[27] Negash, B., Gia, T. N., Anzanpour, A., Azimi, I., Jiang, M., Westerlund, T., ... & Tenhunen, H. (2018). Leveraging fog computing for healthcare iot. In Fog Computing in the Internet of Things (pp. 145-169). Springer, Cham.

[28] Habte, T. T., Saleh, H., Mohammad, B., & Ismail, M. (2019). IoT for Healthcare. In Ultra Low Power ECG Processing System for IoT Devices (pp. 7-12). Springer, Cham.

[29] Qiu, T., Liu, X., Han, M., Li, M., & Zhang, Y. (2017). SRTS: A self-recoverable time synchronization for sensor networks of healthcare IoT. Computer Networks, 129, 481-492.

[30] Sony, P., & Sureshkumar, N. (2019). Concept-Based Electronic Health Record Retrieval System in Healthcare IOT. In Cognitive Informatics and Soft Computing (pp. 175-188). Springer, Singapore.

[31] Thramboulidis, K., & Foradis, T. (2016). From Mechatronic Components to Industrial Automation Things-An IoT model for cyber-physical manufacturing systems. arXiv preprint arXiv:1606.01120.

[32] Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. IEEE Industrial Electronics Magazine, 11(1), 17-27.

[33] Breivold, H. P., & Sandström, K. (2015, December). Internet of Things for Industrial Automation--Challenges and Technical Solutions. In Data Science and Data

Intensive Systems (DSDIS), 2015 IEEE International Conference on (pp. 532-539). IEEE.

[34] Deshpande, A., Pitale, P., & Sanap, S. (2016). Industrial automation using Internet of Things (IOT). International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(2), 266-269.

[35] Mekala, M. S., & Viswanathan, P. (2017, August). A Survey: Smart agriculture IoT with cloud computing. In Microelectronic Devices, Circuits and Systems (ICMDCS), 2017 International conference on (pp. 1-7). IEEE.

[36] Li, J., Gu, W., & Yuan, H. (2016). Research on IOT technology applied to intelligent agriculture. In Proceedings of the 5th International Conference on Electrical Engineering and Automatic Control (pp. 1217-1224). Springer, Berlin, Heidelberg.

[37] Patil, K. A., & Kale, N. R. (2016, December). A model for smart agriculture using IoT. In Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), 2016 International Conference on (pp. 543-545). IEEE.

[38] Ko, S., Song, H., Cho, Y., Chung, J., Kim, S., Yim, D., ... & Smith, A. (2018, March). LoRa network performance comparison between open area and tree farm based on PHY factors. In Sensors Applications Symposium (SAS), 2018 IEEE (pp. 1-6). IEEE.

[39] Mushtaq, S. (2018). SMART AGRICULTURE SYSTEM BASED ON IOT AND IMAGE PROCESSING. International Journal of Advanced Research in Computer Science, 9(1).

[40] Wu, Z., Li, S., Yu, M., & Wu, J. X. (2015, April). The Actuality of Agriculture Internet of Things for Applying and Popularizing in China. In Proceedings of the International Conference on Advances in Mechanical Engineering and Industrial Informatics, Zhengzhou, China (pp. 11-12).

[41] Rathore, M. M., Ahmad, A., Paul, A., Wan, J., & Zhang, D. (2016). Real-time medical emergency response system: exploiting IoT and big data for public health. Journal of medical systems, 40(12), 283.

[42] Li, N., Sun, M., Bi, Z., Su, Z., & Wang, C. (2014). A new methodology to support group decision-making for IoT-based emergency response systems. Information systems frontiers, 16(5), 953-977.

[43] Chowdary, S. M. B., Manash, E. B. K., Krishna, J. G., Kothapalli, C. D., & Rao, M. M. (2017). EFFICIENT SMART EMERGENCY RESPONSE SYSTEM FOR FIRE HAZARDS USING IOT.

[44] El Kafhali, S., & Salah, K. (2017). Efficient and dynamic scaling of fog nodes for IoT devices. The Journal of Supercomputing, 73(12), 5261-5284.

[45] Collina, M., Corazza, G. E., & Vanelli-Coralli, A. (2012, September). Introducing the QEST broker: Scaling the IoT by bridging MQTT and REST. In Personal indoor and mobile radio communications (pimrc), 2012 ieee 23rd international symposium on (pp. 36-41). IEEE.

[46] Desai, P., Sheth, A., & Anantharam, P. (2015, June). Semantic gateway as a service architecture for iot interoperability. In Mobile Services (MS), 2015 IEEE International Conference on (pp. 313-319). IEEE.

[47] Sarkar, C., SN, A. U. N., Prasad, R. V., Rahim, A., Neisse, R., & Baldini, G. (2015). DIAT: A scalable distributed architecture for IoT. IEEE Internet of Things journal, 2(3), 230-239.

[48] Yasumoto, K., Yamaguchi, H., & Shigeno, H. (2016). Survey of real-time processing technologies of iot data streams. Journal of Information Processing, 24(2), 195-202.

[49] Wang, L., & Ranjan, R. (2015). Processing distributed internet of things data in clouds. IEEE Cloud Computing, 2(1), 76-80.

[50] Anagnostopoulos, T., Zaslavsky, A., & Medvedev, A. (2015, April). Robust waste collection exploiting cost efficiency of IoT potentiality in smart cities. In Recent Advances in Internet of Things (RIoT), 2015 International Conference on (pp. 1-6). IEEE.

[51] Kawabata, H., Ishibashi, K., Vuppala, S., & de Abreu, G. T. (2017). Robust relay

selection for large-scale energy-harvesting IoT networks. IEEE Internet of Things Journal, 4(2), 384-392.

[52] Vogel, B., & Varshney, R. (2018, October). Towards designing open and secure IoT systems: insights for practitioners. In Proceedings of the 8th International Conference on the Internet of Things (p. 36). ACM.

[53] Ciuffoletti, A. (2017). OCCI-IOT: an API to deploy and operate an IoT infrastructure. IEEE Internet of Things Journal, 4(5), 1341-1348.

[54] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[55] Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015, October). Network-level security and privacy control for smart-home IoT devices. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on (pp. 163-167). IEEE.

[56] Oravec, J. A. (2017, July). Emerging "cyber hygiene" practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. In Professional Communication Conference (ProComm), 2017 IEEE International (pp. 1-5). IEEE.

[57] Lee, H., & Kobsa, A. (2017, March). Privacy preference modeling and prediction in a simulated campuswide IoT environment. In Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on (pp. 276-285). IEEE.