A Study for taking an approach in Industrial IoT based Solution

Kazi Hassan Shakib¹ and Farhin Faiza Neha ²

¹,² CUET, Raozan-4349

¹kazishakib98@gmail.com and ²farhinfaiza@gmail.com

Abstract. In present era demand for small and portable electronic devices which supports internet connectivity is increasing all around the world and across all industries. These IoT based devices are gaining popularity because of their ease of use. These devices also provide powerful interoperability and feasibility in almost all situation. We can use Internet of Things (IoT) as a great instrument for achieving the desire of connecting people and devices everywhere all the time and in all situations. IoT builds a network of different types of devices such as small handheld devices, vehicles, home appliances etc. that are connected together. This network is incorporated with small sensor nodes, wireless connectivity and actuators for collecting data from adjacent environment and transfer data seamlessly to the base station without any computer or human interaction. Though Internet of Things (IoT) is a primitive term which has greatly attracted the attentions of researchers and academicians it is now getting limited by a number of factors such as flexibility, interoperability, concurrency, scalability and addressing issues. In this paper we will discuss how to make approach when we will go for IoT based solutions considering several parameters such as cost effectiveness, profit generation, maintenance, security etc. In which projects IoT based solutions will be feasible considering. Its network infrastructure, architecture, processing power and scalability.

Keywords: Internet of Things (IoT), network infrastructure, architecture, scalability, scale-up, Random Forest, KNN-classifiers, COCOMO-II, Walston-Felix model, RFID.

1. Introduction
In 1999, The term IoT was first presented by Kevin Ashton of Proctor and Gamble. He used the word and linked the idea of using radio frequency identification (RFID) to allow computers to manage all individual things [1]. Presently because of the advancement of technology different types of embedded system, wireless sensor networks, control system, automation has changed the definition of IoT. It has been anticipated that the number of IoT devices will have thirty folds increment between 2009 and 2020, thus by the end of 2020 the number of connected devices will be approximately 26 billion [2]. Internet of Things is a recent communication concept that imagines an upcoming world where our daily used objects such as cars, consumer product, industries will become collaborative via internet connection, microcontrollers, transmitter-receivers, sensors, nodes and robust data analysis. In recent time IoT is
getting more attention due to the advancement of wireless technology. IoT is a tool to use different technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Machine to Machine (M2M), Vehicular to Vehicular (V2V) communications and will make all devices connected to internet for continuously collecting and updating data as per requirement [3].

![Figure 1. Google search trends since 2010 for terms IoT. The relative value 0 to 100 represents search interest.](image)

The future of our internet will summarize a considerable number of devices that will provide data to the end user through various communication protocols and unique addressing schemes [4]. Both industry and academic persons have explained IoT in a number of different ways. According to International Telecommunications Union, IoT is a universal framework for the data society that will interconnect both physical and virtual things for driving profit and also will push on interoperable data correlating progress [5]. The main concept of IoT is establishing connection between physical world and virtual world by connecting all devices through internet which will communicate with the users of the system. Though, Internet of Things will come up with tons of new and exciting opportunity increased amount of data and device will cause scalability issue. It may also cause new threats new threats such as security risks, risks of malware attack, information heft and many more. Therefore, for any project we should first go for existing embedded mechanical based solution. Before going to IoT based solution a robust Quality Assurance (QA) process is mandatory considering fatal risk issues that may cause loss of fortune, data or even life [6].

![Figure 2. Technological Evolution of IoT [5](image)](image)

![Figure 3. The Top 10 IoT Segments in 2018-based on 1,600 real IoT project [6](image)](image)
We can say that, both IoT based technology and usage and number of IoT based applications for example Smart Cities (23%), Connected Industry (17%) and Connected Buildings (12%) are the top three IoT projects are increasing day by day. So, we should focus on finding out whether these projects are going to affect our personal life and public safety directly. It is necessary finding out that whether IoT based solutions are feasible for these projects. IoT uses sensors for collecting information from local environment which may cause security issue. We use sensors in our everyday life for example Smartphones which is the vital component of our daily life use different types of sensors such as GPS, Accelerometer, GPS receivers etc. for doing various functions continuously but most of the people do not know it.

1.1. Case Study
Some of the examples of IoT based solutions are smart homes and offices, e-health and assisted living which play a vital role in a person’s personal and professional life and greatly help to shape the world in future in which we live now. IoT includes variety of devices starting from wearable low-powered devices like fitness bands to devices that provide medical help to home appliances to automobiles.

In the city of Padova, Italian IoT based smart city project has been deployed which uses most advanced communication technology so that it can manage administration service of the city for the people [7]. Hence, IoT based solutions are considerable in such systems when there is extremely large variety of devices, link layer technologies, and services.

Canary smart security system is an example of IoT based device consists of video, audio, motion detection, night vision, a siren, and air quality, temperature, and humidity sensors into a single device. Canary security system is used to keep the house safe from intruders by detecting motions and persons. A user may be far away from his home but he can control and see who is entering or leaving his house and can close the main security gate or shut down the electronic equipment using his smartphone by the help of this smart app system [8].

Another example of such devices is kolibree smart toothbrush which is also a smartphone-based application helps parents to monitor and improve their kids’ and their own tooth brushing habits. Children master oral hygiene through playing games. We can also send data which is stored on the memory card of the smartphone to dentists for necessary inspection when any trouble arises [9].

1.2. Background of IoT
Most important part of IoT is communicating with various devices by connecting through internet. It might also have many other characteristics such as sensing, mobility, memory, image processing and many more.
Figure 6. Overview of Internet of Things [5].

The above figure is an example of an IoT prototype taken from [5]. If devices are close enough internet is not mandatory for transferring data. They can communicate using protocols like Bluetooth and ZigBee. We can say a device is IoT device based on some characteristics according to ITU-T Recommendation [10].

Table 1. Characteristics of the Internet of Things.

| Characteristics      | Description                                                                 |
|----------------------|-----------------------------------------------------------------------------|
| Interconnectivity    | All devices must be connected for information interchange.                  |
| Heterogeneity        | Different IoT devices may use different network, protocols or hardware but they must remain connected. |
| Dynamic changes      | The state of the device (Device states: connected, disconnected, waking up, and sleeping) may change frequently or quantity of the device may fluctuate. |
| Enormous scale       | The quantity of the devices will be larger in future for enabling communication between machine to machine rather than machine to human. |
| Things-related Services | It will provide services like protection and semantic consistency amongst physical and virtual things. |

According to ITU we can define IoT using three terms that is connection between any devices or things in any place at any time.

1.3. IoT Architecture
The basic architecture of IoT contains few stages such as device, gateway connectivity, data processing and cloud or user interface. In first stage, physical devices collect unprocessed data from surroundings and convert it into processed data. Actuators converts energy into motion and sensors receives and responds to a signal and acts like a transducer. Sensors connect to edge gateway using protocols like Modbus, Bluetooth, Wi-Fi, Near Field Communication (NFC), Zigbee etc. Edge gateway converts data from analog to digital using data acquisition besides data aggregation.
Data is acquired by Internet gateway and cloud is connected by using advance messaging queuing protocol (AMQP), web sockets, message queuing telemetry transport (MQTT), constrained application protocol (COAP), fog computing, event hubs etc. Finally, data is stored in a database or simply in cloud and cloud application controls rest of the communication with the users.

2. Literature Review

Google search trends in Figure 1 from June, 2010 to June, 2020 show us that, IoT solutions are gaining popularity day by day. Especially in the last decade people’s interest involving “IoT” and “Interest of Things” has increased rapidly.

Bestoun S. Ahmed at el. [11] performed a systematic study based on Quality Assurance for IoT based solutions. During this study author tried to answer multiple research questions that were raised while trying to assure quality of IoT based solutions. Based on these questions papers with a number of 478 pages are analysed and issues such as privacy, security, performance, interoperability, legislation, integration, behaviour of the system under a network connection, heterogeneity are classified from QA point of view. In this study papers that were published between 2009-2017 was considered for finding out a large number of evidences about quality assurance of IoT based solutions. But this paper does not directly indicate the sectors where and when we should go for IoT based solutions. The selection procedure of 478 papers also have been shown in this study. IoT means connection between various types of devices. These devices may use variety of hardware, protocols etc. heterogeneity issue is making research and development of QA methods more challenging. For this reason, developing a general testing strategy for all IoT based solutions is difficult. Another important thing is for producing devices at low cost vendors are sacrificing security aspect of the devices. IoT system designers always deal with the difficulty that whether to design the system with a lot of low costs sensors which may cause vulnerability to the security of the system or rather high-performance nodes having advanced feature like encryption capability impacting the overall costs. So, before going to IoT based solutions we should keep in mind these problems.

Energy efficiency of IoT based device has become a matter of concern for both scientists and researchers of this field. Giving sufficient energy to all these devices has become a great issue of concern for researchers as number of IoT based devices are getting huge day by day. So, we need to think a realistic approach so that we can easily decide for which sectors we should go for IoT based solutions. If a problem can be solved using embedded traditional solution, we don’t need to go for an IoT based solution. We will go for an IoT based solutions when communication between large number of devices

![IoT Architecture](image_url)
is needed for example smart city [12] and also based on several parameters such as cost effectiveness, profit generation, maintenance, security etc.

Ray et al.[13] performed a systematic survey on the architecture of existing IoT based applications such as Service oriented architecture (SOA), Home Health Hub IoT (H³ IOT) platform, Machine to Machine (M2M) based distributed architecture, Distributed IoT/IoE , Social IoT, DTLS employed security architecture, Media-aware Traffic Security (MTSA) architecture etc. which paved the way for researchers solving real life problems by building Internet of Things notions. Unfortunately, how these architectures can be used effectively ensuring quality are not discussed in this paper.

Perera et al. [14] had performed a research on the context awareness issues of IoT based system in terms of security, privacy and quality of data processed. Context awareness means the ability of a system that can acquire data from the surroundings through sensors and can take decision depending on the situation. Through this context awareness process there is a possibility that we can check the quality of the system. However, when and in which areas this intelligent IoT can be used which has context awareness ability is not discussed in this paper. Before issues of context awareness computing for IoT based system, we need to keep in mind that big data can cause a great problem. Since, fields are growing in numbers understanding, learning, processing big data and giving appropriate decision can be a challenging issue for intelligent IoT system.

Gubbi et al. [15] performed a systematic study based on application domain, architecture, cloud centric IoT and future challenges such as Energy efficient sensing, Secure reprogrammable networks and privacy, Quality of service (QoS), New protocols, Participatory sensing, Data mining, GIS based visualization etc. Among them QoS and security-based issues are discussed briefly. While implementing IoT based solutions we need to consider these future challenges.

Another research [16] depending on energy consumption of IoT device author represented a framework of IoT workflow. This framework shows us energy is consumed mainly in four stages i.e. sensing, networking, pre-processing, storing and analysing. Though IoT based applications are getting popularity as a source of saving energy, its own energy efficiency is at stake. Because huge amount of energy is needed for areas where IoT based systems are expanding at a large scale. Author proposed a solution for saving energy as the above-mentioned stages are important for working of IoT smoothly. Three determinants for supporting IoT based devices are energy efficiency, security and privacy. Before going into IoT based solutions we need to consider these factors. We need to implement these solutions without affecting environment’s resources i.e. energy much.

In another document [17] author defined IoT from the point of view of different stakeholders i.e. ETSI, ITU, IETF, NIST, OASIS, W3C, CASAGRAS project, IERC, CISCO, HP and many more. Author tried to clear the confusion and lack of awareness about the definition of IoT that was created due to the diversity of research on IoT. This document also gives an outline about the basic architectural requirements of IoT. But there is no direct indication about when we should go for IoT based solution based on people’s demand and society’s interest.

Security is one of the most important issue that we need to think when we go for an IoT based solution. Though there are many advanced algorithms for ensuring digital security, but many of them are not compatible for IoT world. Because IoT devices are constrained with limited power supply, processing cycles and memory usage. So, we need to consider these issues before going into a IoT based solution. Otherwise, it may hamper the progress of IoT in implementing Smart City, Smart Home and Smart Infrastructure, etc. Existing authentication procedure are at stake because of the characteristics of IoT devices that we discussed in Table 1 such as heterogeneity in terms of devices, topology, communication and different security protocols used in IoT. In [18] author proposed a security scheme based on Elliptic Curve Cryptography scheme and Lamport’s OTP algorithm through which two-factor authentication among devices can be achieved. Moreover, this strategy can be implemented in real-time IoT networks.

Samaniego at el. [19] tried to solve the security issue of IoT devices by implementing block-chain as service for IoT. Here, each valid transaction is stored as a block. It starts with an initial block and as a
new set of nodes does come to action, the hash value of the previous one gets pushed to the system. Therefore, if anyone with malicious intent makes any sort of change to the previous block all recipients in the mentioned block will be able to notice. So, we can say that block-chains are tamperproof distributed transaction ledger. Moreover, it solves the issue of network latency and constrained interaction with sensors and actuators by implementing fog centric IoT system. So, we can use the concept of block-chain while implementing IoT based solution. But block-chain creates costs rise up the project overhead.

The problem arises from using this IoT based devices is dealing with security threats, maintenance (scaling up-to expand/make bigger industrial approach), inter-dependency between layers and devices, to use and co-relate these devices and to maintain viable profit margin and minimizing costs to actually make an better and bigger industry-oriented automated devices. So, turning a single mechanical/embedded device and connecting to a server controlling thousands of devices creating Big Data problem consisting real-time analysis and maintaining huge bulk of sensor data may not seem a good decision in most of the cases. IoT with Big-Data analysis will create greater cost. So there lies an issue of solving a problem with costly and not profit oriented IoT solutions or just keeping it as mechanical or embedded singly monitored system as before.

As for security threat analysis it arises because of data lose due to climate change or inter-dependency on gateway connectivity or malicious hacking/by thousands of viruses such as ransomware, botnet, Advanced Persistent Threats (APT), Identity theft, Denial of Service (DoS), mirai (virus attack) and the loss of continuous sending of real time sensor data due to device vulnerability.

Lonzetta et al. [20] discussed about low energy Bluetooth which is a wireless technology used for interchanging information. Though, it uses short wavelength for transferring information at short distance its security is at stake. Bluetooth Low Energy (BLE) is a simpler version of classic Bluetooth which are used in low powered IoT devices for example in sensors, heart rate monitors and fitness devices. These devices are merge with Bluetooth (v4.0) standard in 2010 by Bluetooth special interest group (SIG). BLE exchanges small amount of data periodically and in other cases remains in sleep mode. As, they consume low power they are vulnerable to security issue.
3. Methodology

In this paper, we will analyse to make an approach so that can be taken in IoT for predicting to take a project and analysing beforehand. There are two approaches that can be taken for going for a project in IoT solutions.

Firstly, naïve solution can be taken in this matter with less features by calculating project estimation, overhead and the risk factor, COCOMO II model, Static-multivariable models' example: Walston and Felix development model [21] at IBM consisting the source code and effort to generalize the cost with the equation:

\[ E = 5.2 L^{0.91}, \text{where } D = 4.1 L^{0.36} \text{ and } I = \sum_{i=1}^{29} w_i x_i \]  

[The productivity index has 29 variables].

The problem arises as it goes for localizing and not including the hardware and other cost relatively.

Secondly, we can go for Machine Learning approach where this is a classification problem to decide to go for IoT solution or not from training the machine with the feature list. For the classifier being KNN-classifier (easy to interpret) that predicts the test data will be classified in which decision group. There may arise boundary problem in separating the decision vector and classify properly as the dataset and problems such as missing data may occur, so it may not be easily separable with varied factors associated with it.

Another good implementation of classifier can be Random forest classification (normalization isn’t needed like in Kernelized SVM) as there arises situations like scale up or not in every phase of the industrial process rather than naïve bayes classifiers.

It gives better result in globalizing the result creating best fit model for the features helping the model to overcome over-fit and under-fit the feature data.

The reason we are using Random-forest classifier is that it uses majority voting on bootstrap aggregation(bagging) of features and data as without pruning the feature column and randomized sample taken grows so in this classification problem it will be highly effective. As we will be working with industrial data so missing data in certain aspect can act and be an important issue while determining the result as well. So, without overfitting data it will give a good result in best-fitting the bootstrapped models and then aggregating into a good decision in decision tree.
4. Conclusion
In this paper, we discussed the approaches to analyse IoT based solutions and whether to go for it or not. There are problems associated with IoT solutions like security threats, maintenance in scale up or scale down decisions, energy efficiency problem [16], storage problem, analysis of these huge amount of sensor data, data manipulation in middleware, trust issue [22]. So, for cost minimization and profit maximization we need to understand when to go for IoT based solution. We had an approach that concludes this problem and give the industry experts a feature analysis that would ensure a better solution in solving this issue.

5. Future Work
For future work we will focus on implementing a better naïve solution for better calculation and machine learning approach to analyse better algorithms (based on experimental results) to efficiently classify stacking of devices for IoT based solution or to go for mechanical/embedded singly monitored system mentioning important efficient features to classify. We will also work on a good dataset made up from industry response.
6. References

[1] Ashton, K. (2009). That ‘internet of things’ thing. *RFID journal*, 22(7), 97-114.

[2] Frey, R. M., Xu, R., & Ilic, A. (2015). A novel recommender system in IoT. In *2015 5th International Conference on the Internet of Things (IOT 2015): Seoul, South Korea, 26-28 October 2015*. IEEE.

[3] Yan, B. N., Lee, T. S., & Lee, T. P. (2015). Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): A co-word analysis. *Scientometrics, 105*(2), 1285-1300. LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21.

[4] Vermeeren, O., & Friess, P. (Eds.). (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.

[5] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers, 17*(2), 243-259.

[6] Forbes Homepage, https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iot-growth/#15c8016b3ecc, last accessed 2020/06/21.

[7] Mehmoord, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Communications Magazine, 55*(9), 16-24.

[8] Canary Homepage, https://canary.is/, last accessed 2020/06/21.

[9] Kolibree Homepage, https://www.kolibree.com/en/kolibree-toothbrush-app, last accessed 2020/06/21.

[10] Sector, I. T. S. (2012). ITU-T Recommendation Database.

[11] Ahmed, B. S., Bures, M., Frajtak, K., & Ceny, T. (2019). Aspects of quality in Internet of Things (IoT) solutions: A systematic mapping study. *IEEE Access, 7*, 13758-13780.

[12] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal, 1*(1), 22-32.

[13] Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences, 30*(3), 291-319.

[14] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials, 16*(1), 414-454.

[15] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660.

[16] Singh, U., & Chana, I. (2019, July). Energy Efficient Solutions for IoT Based Applications. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1287-1292). IEEE.

[17] Minerwa, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative, 1*(1), 1-86.

[18] Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015, February). One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)* (pp. 1-6). IEEE.

[19] Samaniego, M., & Deters, R. (2016, December). Hosting virtual iot resources on edge-hosts with blockchain. In *2016 IEEE International Conference on Computer and Information Technology (CIT)* (pp. 116-119). IEEE.

[20] Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks, 7*(3), 28.
[21] Amanullah, Abdus Salam, Abdullah Khan, Samad Baseer. (2016, December). A Comparative Study Software Cost Estimation Using COCOMO-II and Walston-Felix models. In 2016 IEEE International Conference on Innovations & Software Engineering (ICONICS 2016).

[22] Qusay Idrees Sarhan (2016). Internet of things: a survey of challenges and issues. In 2018 Int. J. Internet of Things and Cyber-Assurance, Vol. 1, No. 1, 2018