Internet of Things - IOT Interoperability and Challenges

Muhammad Jawad Hamid Mughal¹, Mohammad Faisal², Mehr E Munir³

¹ Department of Computing and Engineering Sciences, SZABIST, Dubai
² Faculty of Computer Science and IT, University of Malakand, Pakistan
³ Department of Electrical Engineering, Iqra National University, Peshawar, Pakistan

¹jawadhamid242@gmail.com, ²mfaisal_1981@yahoo.com

Corresponding Author: Muhammad Jawad Hamid Mughal.

https://doi.org/10.26782/jmcms.2019.08.00025

Abstract

Internet of things is a concept that associate world with tech-systems to communicate in a manner that is easy and automated. Over past decade the idea became true focus for researchers and industrial domains. IOT is a technology of future that is rapidly growing every day with perceptions, providing humans control and update of things. The awareness of devices interaction and communication is coming from years but still struggling to be accepted by industries and organization due to lack of standardization. This study addresses IOT platforms limitations and interoperability challenges through reviewing scholarly papers. Also internet of things history and cloud computing role in IOT are briefly described.

Keywords: Internet of Things, Interoperability, Cross domain, Framework, RFID.

I. Introduction

There is no proper definition for IOT, the name itself contains meaning – all the devices (things) interacting to each other via medium (internet) over pre-defined manufacture’s platforms. Internet of thing give logical nature for all connected devices through internet and establish communication structure. Things belong to our environment from small to large connected to internet collaborating and exchanging information are members of IOT, that is reducing human interaction with machines, providing access to device to make discussions. Idea to control electric devices remotely was initiated in 1990’s [X] and still is in phase of full deployment in various areas like logistics, smart homes, environment, wireless sensors etc. Sensors provides platform between devices and users to interact, also change raw data for device to specific machine format to understand easily. All data transfer between connected devices performed through appropriate medium (wired or wireless) e.g. fiber, Bluetooth, RFID, IEEE 802.11 etc. IOT is widely spread approach and becoming a requirement everywhere. Wired medium is known as a reliable medium for
communication, IOT devices can also be connected through wire but it cannot be set up everywhere.

Involvement of IOT proven beneficial towards industries, academic, financial and transport sectors. Things includes all the objects not only that are considered by humans everyday but other products like gadgets, landmarks, clothes, food items, specialized equipment, fruits, plants, transport etc. listed under IOT. Architecture of IOT is basically classified into applications, transpiration and processors [XIII].

In this paper we discussed short background of IOT, detailed literature review of research papers – identifying IOT platforms and challenges. Further discussed few IOT applications, cloud computing with IOT and design comparison table.

Background

Things started connecting since 1989 (internet birth). First internet device (toaster) was created by John Romkey in 1990 that can perform function (ON, OFF) through internet. Steve Maan created wear cam in 1994. Kevin Ashton, executive director of Auto-ID Center in MIT suggested the name “Internet of Things” (1999) and also created RFID same year. It was later (2003) installed in US army program (Savi). In 2005 articles about IOT and its future were cited and same year report on IOT was published by International Telecommunications Union. [X, XIII]

II. Literature Review

Amelie Gyrard and et al had briefly discussed on communication between IOT applications based under different domains and proposed a framework called “M3 Framework”.

M2M is one way of communication between machines. IOT applications do not interpret data, as there are domains specify and not interoperable due to different set of concept in domain area, domain experts do not share it publically. Paper describes M3 framework design to build interoperable cross domain IOT applications. Steps includes – understanding multiple domains platform, attaching additional information to heterogeneous domains, choosing common names for M3 to define senor measurement.

No interoperability in IOT application is due to lack of standardization, belonging to technologies, data formats, platforms etc. Cross domain IOT application interaction is useful for many reasons. Paganelli et al. give ideal to develop Web of things applications for we services but forget to combine domains. Cross domains interoperability has some limitations which are describe in this paper are that: combine different set of concepts of cross domain but did not specify which one, difficulties face in combining domains.

Solution for the limitation, M3 framework is designed by authors. Framework consists of several layers communicating with each other’s internally. Perception layer deals with physical devices like actuators, sensors, RFID tags etc. Data acquisition layer receives sensor data from devices in SenML format and convert it on the basis of M2M measurement concepts. Persistence layer stores
information of domains. Knowledge management layer has job to indexing, reusing, designing and merge domain knowledge. Reasoning layer uses reasoning engine to deduce knowledge. Knowledge query layer has to run queries. Application layer give output to users screen.

The M3 framework consists of following steps. User provides an input and framework consider an application templates fulfill user needs. In next step user will pick one of the provided templates. Framework by its self will generate the template chosen by the user earlier to design IOT application. After then user will send data and data will be converted by M3 converter. Next reasoning engine will run with rules of selected template and triple store will store the data. In next step framework will generate the query using M3 SPARQL. Finally result will be displayed to user [III].

In the whole paper author describe about IOT devices and there limitations that every devices has its own separate domain. Different domain device are not compatible to communicate with each other unless they bring in to same domain. Paper proposed a framework for cross domain interoperability and has been tested on android platform.

Article discussed about the middle layer that perform as a platform for the connectivity of IOT devices. Platform should have the information about IOT devices provider, manufacture, developers and user whom will be using this devices. Different platforms are evaluated, rather they fulfill user requirements or not. Gap analysis will highlight the flaws in today’s solution and will help them to improve their IOT ecosystem for future.

Internet of Things moves traditional environment towards smart environment such as: smart houses, smart cities, smart cars etc. Now days there are many solutions that interconnect home appliances to communicate. Article compares all the features of IOT applications and platforms that provide an important role to connect device to the cloud. Main theme of the article is to demonstrate the gap analysis of current platforms in respect of their capacities. To fill these gaps and evaluate the limitation of different platforms, authors conducted survey from the experts of national Finnish IoT program to find the future issue of IOT platforms and on the basis of these issues they pointed some suggestion to fill the gaps.

Section 2 listed almost 39 available IOT platforms in a table manner. Columns represent the characteristics of the platforms mentioned in rows. Color codes are used to clarify the platform characteristic. Green indicates “meets expectation”, red for “miss match” user expectation and orange for partial expectation. This will give a quick and summarized view of the platform and will ease the selection.

Characteristics summarized in the table are presented in this section. Several dimensions are covered in gap analysis which identifies the functionality of IOT platforms.

Integration of sensing and actuating technologies: Different IOT devices communicate through sensors and actuators with different protocols. An IOT
platform should provide a set of standardized protocols after that device manufacture will choose one of the protocols.

**Data Ownership:** We analyze that when data is stored over the cloud, most of the time data owner do not have full access control and data is stored is raw format at the back end without any encryption. End user requires authentication key to get read and write permission. Authors present an ideal for future IOT platforms that data owner should have rights to give access to predefined resources and end user will have control on raw data. Before sending data to cloud (PaaS) data owner can encrypt the data.

**Data processing and data sharing:** Data processing in IOT is a big challenge because of real time requirement. Sometimes IOT data is unreliable and incomplete. Multiple data steams can be process and combine virtually in an application if URL of one is known; this is difficult task for application developers. Security and privacy mechanisms must be develop in IOT platform for the protection of data stream.

**Support of application developers:** Developers should be provided streamlined APIs (quality) by IOT platforms. Development of future APIs shall uniform for all platforms. APIs usually perform basic operations like DEL, GET, PUT but these operations are interactive only to the connected devices.

**Toward IOT ecosystem formation:** To process IOT ecosystem, the platforms should be able to adopt new features and should be easy for developers to expend applications based on the platforms. Cross IOT domains that server as a single ecosystem to provide application services and new feature products, for this IOT broker is needed which will provide services sharing, space and time to different platforms.

**Dedicated IOT marketplaces:** Cloud based software’s are available at the software marketplace. These applications can be easily found on Apple store or Google play. Store support for paid applications is provided to end users. Some IOT platforms have dedicated stores for applications, few provides publically shared applications and other charge users for cloud storage. According to McKinsey companies produce massive amount of data by business but only use or process normal amount of data; they should use this sensor data for the prediction and produce more business. However they need expert analyst for this development and such IOT marketplace will give boost to business to business interaction. Windows Azure is an example of successful model for business that provides business a platform to share their data which will allow application developers availability at huge amount of data [V].

The article analyze gap between IOT platforms and evaluate multiple numbers of available IOT platforms based upon their capabilities.

Authors in this paper discussed about the security issue in IOT system. As IOT is one of the most wanted interconnected devices network now days, that connects different devices and enable communication between them. Anything connected to the internet must have security issue. Authors proposed a conceptual model “APPARATUS” for
IOT security which is architecture oriented model and considers IOT system as cluster of connected networks (nodes).

One of IOT vision was provided in 1991 by Weiser, he said that most technologies will merge with environment. There are number of security issues already be described like algorithms used in for encryption in embedded device are weak. Effective way of for system security is to do security practice at development stage. Also identify security issues and requirements at requirement gathering stage. Security requirements for any IOT system should be same. APPARATUS model gather information from IOT system architecture to identify security issue.

Architecture of a system provides information about network topologies and nodes in networks where as some features of IOT systems are not expressed like users etc. To know the limitation “micro world” concept is used, that analysis’s the system in managed environment. APPARATUS can easily be integrated to existing security frameworks that are been using for many years for security analysis.

Authors discussed some related work about security requirements that have been used in development stage for security analysis. Security challenges are define in Gurgens paper about embedded system. He says for embedded systems security tool have to be made that fitted to their needs. Framework to evaluate security in IOT system Ge introduce graphical model of security that evaluates IOT system in levels. The framework is not limited to only one system same as APPARATUS model. Diaz said many IOT tasks depend on cloud. He further said that IOT will act as a middle layer that will send all data to cloud for processing.

APPARATUS model will help the designers to easily fetch security requirements from IOT system structure. APPARATUS model first step of security inspection is that from where the security needs are found in IOT system. Secondly provide full security analysis to IOT system. IOT structure is defined as a cluster of multiple nodes that are connected. Each node has their own properties that they perform in a system. APPARATUS is defined in to two concepts: IOT nodes and Network connections.

Properties of IOT nodes are defined as: Identification:An ID is assigned to each stakeholder to identify their properties and roles in respective nodes of IOT system. Aspect:Specifies the node either it’s a single physical node or produced of multiple sub nodes. Layer:Some architecture identify five layers, some identify seven layers. As a reasoning model APPARATUS choose three layers of architecture. It provides properties that are necessary for security of IOT system. Type: Describe the type of node. Device could be wearable, server or sensor etc. Attribute: It defines the capability of a node. Node that can only sends the information to the network cannot perform any other task. Other node can only receive the information. Whereas node that can do both send and receive information is best suited node in IOT system. When node in IOT system performs multiple tasks that node is produced by multiple sub nodes.
Input & Output: Input data is processed by nodes to produce an output result. IOT nodes are connected to each other through network connection. Network medium can be wireless or wired [IX].

Author K.E Psannis and et al have well described about limitations of IOT, Mobile Cloud Computing MCC, advantages of MCC and MCC in business. IOT technology is the part future where everything will be communication to each other through internet. IOT generates massive amount of data which is send to their destination via cloud. MCC includes mobile devices having some additional advantages.

IOT is not limited to specific number of devices. IOT structure needs dedicated support for access the services. Humans and things can be connected anywhere at any time through internet. Components of IOT exchange information without human which consume a lot of energy to complete task. The term Green IOT is used which means to save energy while communicating. Some limitation of technologies that are used is IOT are discussed in this paper. For example:

**Architecture technology:** that gives connectivity able to perform interactivities between distributed systems. Architecture model should be capable for providing interoperability for different systems.

**Data Storage:** Capacity of data coming from IOT devices is growing day by day which requires more space.

**ID technology:** Every IOT device should have unique ID. Device ID also helps to differentiate between characteristics of the devices.

Organization need there data to be secure. Encryption technologies are used to secure data but future goal is to make data more secure by using efficient encryption algorithms.

Implementing software for distributed systems in a difficult task. Database with high performance which allows the management of the large amount of data gathered through the interaction between devices and humans connected to different network is required by IOT.

MCC has same characteristics as CC only devices are mobile. In this section of paper author handsomely describes few important advantages of MCC. Flexible architecture that provides full services to users. Architecture model consists of four main services i.e. Saas, PaaS, IaaS and data center. Each service is paid and charge per usage. MCC gives unlimited data storage on cloud through internet. In MCC data storage and data processing are performed on cloud which reduces processing of data on mobile device. 4G technology is capable to receive and transfer huge amount of data to cloud in less time. Major advantage of CC is that all the hardware component like storage, servers are offered by service providers. User’s requests to central processors of cloud with a unique ID. Operator at cloud side required user for authentication. Requested data is delivered to cloud and service is provided to subscriber. Cloud based service providers, users are provided security model for data privacy and security. Software installation and updating is done vendors. Demand to increase services, storage are deployed quickly by vendors. Data backup is taken by
the service provider and in case of any disaster data recovery is easy. Cloud applications are easy to use from anywhere and at any time. Applications can be accessible from any location without any device or place restrictions, just need to be connected to the internet. MCC applications can be accessible offline through HTML 5, which give user good experience with the application even the device is not connected to the internet. Battery time is also a limitation, to improve battery time large and complex computation tasks can be processed on cloud servers.

In past few years IOT and MCC provide great technical advantages to business. List of IOT applications that give business a great support in service sector. In logistics if vehicles and product packets of different things communicates to each other and share their location, weight gives new business trend. Health and care sector using IOT device can access real time information of patient [VI].

Sejun Lee and et al explain more intensively about IOT devices that are used in smart homes. With their great work they had proposed a concept of auto configuration of DNS for IOT devices. IOT enable devices to connect, communicate with each and do sharing through cloud. In IOT smart homes some devices with high specification e.g. washing machine, LCD etc. are known as high capacity devices. Other devices are low capacity devices e.g. light, sensors – requires less computation but are useful for management and monitoring purpose. When device request to connect to the internet – IP address, subnet mask gateway and DNS are automatically assigned to that device. At some level DNS still need to be configured manually. In IOT structure manual configuration of DNS is time taking task due to the large number of connected devices.

Ipv6 Stateless concept is that device will automatically assign IP to itself without getting it from DHCP server. Devices by default had some configuration known as factory configuration which includes device category like TV, Fridge, Mobile and device models (name of manufacture, ID) IOT device gets DNS search list from RA (Router Advertisement) or DHCPv6. Auto DNS name configuration procedure is divided in to two phases. First IOT device as host receives DNSSL through RA or DHCPv6 and check if it is valid. Then look for DAD (Duplicate Address). Node Information query is sends by router to host in the same subnet. Host replies with NI to get DNS name. Then router saves IOT device DNS information in DNS server. Control device get DNS list from DNS server and can monitor and control IOT device through DNS name [XII].

Interoperability

Amelie and et al has well described the importance of semantic web technologies for IOT based applications. In IOT device are connected to each other and communicate with each other through the internet. All devices are domain specifies – devices with different domain are not able to interact with each other. Due to specific domain limitation M2M application are not interoperable.

This research provides unified system that enables the interoperability semantic IOT applications. Authors designed SWoT (Semantic Web of Things) generator that will provide the developers of IOT application a template with all required files to implement semantic web IOT applications. Main idea of providing
this approach to IOT developers is that they will not use their own models nor interpret data by designing own set of rules.

**Machine to Machine Measurement M3 Framework:** Purpose of SWoT is to ease work of developers and help to implement IOT projects. SWoT generator design templates for IOT applications using inputs (sensors) and domain knowledge provided by developer. SWoT generator is an important component of M3 framework. The framework consists of three steps. First information about sensor and domain as an input is given by the developer to SWoT generator to create SWoT template. Template is necessary for IOT application implementation and also has information for interoperable domains. In the next step developer attach additional data information with M3 converter to get M3 data which will be needed in next step. In last step developer gets concluded M3 data. SPARQL (query language of semantic web) query executes and domain information fetch from template is loaded by developer.

**IOT application template dataset:** SWoT generator make SWoT template by demanding dataset of IOT application. Domain knowledge is needed for IOT plans. Generating new templates are easy; just need input dataset and domain knowledge.

**Interoperable domain knowledge:** For designing templates for SWoT applications without interoperable data and set of rule it is difficult task. For this we should have the knowledge of cross domains, datasets and rules about IOT data.

**Designing, Developing and Running the Application:** Design phase help developer to select application that has to be deploying by template through semantic web query. At developing stage developer loads the program with data and rules and arranges data to implement application. Running level application gets run time input by end users.

Authors show the benefits of their work by use cases. Cloud developer can easily use M3 framework. Developers select template by choosing inputs, domains and download the SWoT template. Then they use M3 converter. If developer is not use to Jena then it would be difficult task for him. Jena is a kind of framework use to implement web applications. Few code lines need to be coded to load M3 data. All required information by template is loaded and query is executed available in M3 template. Lastly developer will display result in user interface. Cross domain applications are designed by combination data sets and set of rules of two different domains.

**Assisting IOT Projects:** SWoT generator help in projects to design IOT application through proposed template with multiple domain knowledge. Below figure 1 shows detailed knowledge about the implementation of interoperable IOT applications with the help of M3 framework.
Like smart home lights are switched off if no one is present. In healthcare scenario continue information of patient such as blood pressure, heart rate etc. is observed and alert is send to doctor if needed. SWoT template can also assist with healthcare and can implement smart application which can suggest a medicine or treatment through interoperable knowledge of domains [1].

Amelie et al have gently described the importance of semantics and its integration with IOT based architectures in this paper. Authors work hard and designed semantic engine which can help to integrate different constituents of IOT architecture such as: Cloud, smart phones and machine to machine gateways. Billions of heterogeneous devices needs to communicate with each other to share information which is only possible with cross domain integration and interoperable IOT applications. Authors said they go through the recent work and underlined some points for future IOT applications i.e. interoperability among different domains, data summarization and ease the development. Semantic engine can perform such task and can be integrate with components of IOT structure mentioned above.

Main purpose of semantic engine is to accept components of the architecture as introduced in beginning. To design IOT application on small devices with limited CPU, memory and power - we need to filter and fetch only what is need to construct the application. Below figure 2 shows five components of semantic based architecture.
Five components of the architecture are defined as; Template catalogue is a collection of defined templates with already selected interoperable domain concepts. This mechanism is important for interoperability between apps, data explanation and IOT apps easy development. Converter attaches additional information to data. Data is collected from different projects. To explain interoperable data unified language is applied in converter. This mechanism is important for data explanation and IOT apps easy development. Reasoning engine gather the complexity out of IOT data. This mechanism is important for data explanation. Data is queried in query engine that will be used in the next phase. This mechanism is important for IOT apps easy development. At last phase application is used by users. The mechanism should fulfill the different requirements of people.

Authors further discussed about embedding cloud, mobile and gateway with semantic engine and advantages of architectures. In cloud-IOT architecture application downloads the required template and additional sensor data is attached with converter. After that rules are loaded to the application and data executes in query engine. User friendly interface can be designed as a final application. Advantage of cloud-IOT architecture is to interpret data from internet when privacy is not the priority. In mobile-IOT and gateway architecture first internet connection is required to get the template from template catalogue. After downloading the template remaining components are executed connectionless. Mobile-IOT and gateway architecture gives advantage of local data processing instead of sending sensor information to the cloud. Reduce the network traffic and increase the data privacy.

Zhexuan et al have proposed an application layer solution for different devices to communicate. First, the information about the device provides by current specifications are used and place them in the middleware of proposed architecture. Secondly, user will be able to create and execute different tasks by using different web technologies. This structure will enable the interoperability without any change in the existing technologies.
In coming years IOT is expected to bring change in the way of communication between devices. Every object will be provided internet connectivity to interact with other device and introduce new services for the end users. Author highlighted very important scenario of new devices launching. With new devices arrival, new tasks also take place that how to provide interaction between heterogeneous technologies. Few well known standards are defined for interoperability i.e. Bluetooth, Universal Plug and Play UPnP etc. When different standards interact with each other for communication they had agreements before sharing their services which makes it difficult to connect devices dynamically. Solution is to create adopters of each standard and extend them to others but the solution also has some drawbacks. If there are any changes in one standard, the adopter has to be modified according to the changes. To provide interoperability for N standard, N numbers of adapters needs to be generated. Bridge between standards can also be the solution [XIV]. Author advice the use of Service layer where all devices are mapped to semantic service and service should linked with OWL. Benefit to this is that it does not require any extra effort from device production. The framework explains the interoperability of different device services. OWL’s stands for Ontology Web Languages and is designed to represent knowledge about things and relations between them.

### III. Cloud Computing and IOT

Required services consumed from providers as planned ahead over the internet in known as cloud computing. Companies can start with small resources and increase depend later if required. Cloud computing is new technology for hosting and supplying service (SaaS, PaaS, IaaS etc) but the idea behind this is not new, in 1960 John McCarthy [XI] already said that in future computing services will be accessible to users publically.

![Figure 3: Cloud and IOT Devices](VIII)
Connected devices ratio crossed the number of humans and projected number of things connected in 2020 is 24 billion, handling that amount of data is not an easy task. Devices have their default storage but its limited – storing that huge and growing amount of data needs permanent, reliable, secure rental service that can provide additional data storage and processing speed [VIII]. Cloud computing integration with IOT can leads to solve much problems faced against storage limitation, data integrity, security, QoS and resources allocations etc.

**Table 1:** Effecting Factors Comparison

| Sr # | Variables | Diff. Platforms | Diff. Equipment’s | Diff. Versions/Time Of Purchase | Diff. Operating Systems | Diff. Protocols | Diff. Programming Languages |
|------|-----------|-----------------|-------------------|---------------------|------------------------|----------------|---------------------------|
| 1    | IOT       | Hardware / Software both lies on platform. Thus, platform is so called a combination of Hardware and Software. Platform might be a stage of specific hardware / software, each device has their own platforms which defer from each other. | Equipment’s are used in device for a specific purpose. Every device has their brand equipment’s. | IOT includes devices all over the universe. People buy them, company’s purchase them, all are not purchase at the same time, thus version of device also change with the time. | All devices which connect to the internet are IOT devise. Those devices don’t use same OS. | Protocols are used for communication purpose in between IOT devices. Some relies on TCP/IP, some on UDP etc. | Java, C, Python, JavaScript, Swift, PHP, C# |

*Copyright reserved © J. Mech. Cont.& Math. Sci.*  
*Muhammad Jawad Hamid Mughal et al.*

315
## Cloud Computing

| 2 | Many platforms are provided by cloud vender; out of which three are the main platforms. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). All of the above are On-Demand Service / Pay as go – per usage. | Distributed data centers are the combination for many Servers, Routers, and Switches etc. Each of them consists of different equipment’s depend upon the requirements. | Hardware / Software are not purchase for server rooms at the same time. If required so they are purchased. E.g. data storage space decreasing so vender will purchase a new storage. Purchase date / version will be change. | Cloud computing at the backend is the combination of distributed data centers, consists of many servers, switches, routers etc. All of these have their own separate operating system. | Gossip protocol use for failure detection, messaging, monitoring. Connectionlessness n/w protocol. State Routing Protocol SRP etc. | SQL, Oracle for Database. Go procedural language created by Google. GFM domain-specific language and many more. |

## Interoperability

| 3 | Computers, mobiles, tablets, sensors, wrist watch, MACbook, iPod, smart watch, IP cameras etc. | RAM, ROM, storage devices, smart touch screen, 3D touchscreen, mic, monitors, camera lenses etc. | Purchasing time should not affect the inter communication between device unless the latest version supports previous versions. | Microsoft, MAC, Linux, Unix, Android, IOS. | Interconnectivity between different devices through internet using separate protocols. | Different languages can communicate through cloud but there should a combine storage, rather than even single device having separate language or OS will have separate storage e.g. icloud and android backup. |
IV Limitations

The idea of technology “IOT” is to minimize gaps between physical things and to be more interactive in a way – they can exchange relevant data consuming lesser time. Although in past decade lots of research have been done in this area which in a result provide different sectors i.e. organizations, Gov. Sectors, logistics, home automations, smart cities etc. much benefits. On other side there are few limitations faces in IOT paradigm that causes applications to perform tasks on time.

Multiple challenges in IOT includes; data management, as all connected things are breeding lots of data every sec which is difficult for existing infrastructure to deal with. Data mining, as data is increasing day by day which needs to be process / analysis using data mining tools. Other than traditional data (plan text, tables) IOT data also contains streaming data i.e. location, temperature, chemical changes etc. which is challengeable task for data mining tools to address immediately. Security challenge, as rapidly growing IOT network - security threats are also increasing. IOT has security issues due to lack of encryption, web interfaces are not secure, less software protection and authorization. To prevent against IOT security concerns developers should integrate security solution, include firewalls etc. into product and educate users to use built-in devices security features [IV].

IOT architecture is also a challenge for service based things in terms of cost and performance. Large number of devices connected in a networks leads to scalability issue in multiple aspects i.e. managing and transferring data etc [VII].

V. Conclusion and Future Work

IOT technology bringing massive variations in daily live, help devices get connected with other manufacturing device to ease and reduce human effort. Besides the advantages there are few flaws in the technology. Lake of standardization and different platforms, every manufacture have their own built-in platform that leads to difficulty while establishing connections and exchanging information. Rather than using third party platforms, a platform should be implement that is compatible with all different manufactured devices which can make things interoperate and provide more secure medium. A set of rules should be listed for devices that want to join IOT area before get connected. Talking further, IOT is a method of bringing thing under a single umbrella and when things increases the transfer rate also increase, for that reason high bandwidth internet is recommended because appropriate medium for IOT is wireless.

References

I. A. Gyrard, C. Bonnet, K. Boudaoud and M. Serrano, "Assisting IoT Projects and Developers in Designing Interoperable Semantic Web of Things Applications," 2015 IEEE International Conference on Data Science and Data Intensive Systems, Dec 2015.
II. A. Gyrard, S. K. Datta, C. Bonnet and K. Boudaoud, "A Semantic Engine for Internet of Things: Cloud, Mobile Devices and Gateways," 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 8-10 July 2015.

III. A. Gyrard, S. K. Datta, C. Bonnet and K. Boudaoud, "Cross-Domain Internet of Things Application Development: M3 Framework and Evaluation," 3rd International Conference on Future Internet of Things and Cloud, 24-26 August 2015.

IV. In Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431-440, July-August 2015.

V. J. Mineraud, O. Mazhelisb, X. Suc and S. Tarkomaa, "A gap analysis of Internet-of-Things platforms," Computer Communications, Vols. 89-90, pp. 5-16, March 2016.

VI. K.E. Psannis, S. Xinogalos and A. Sifaleras, "Convergence of Internet of things and mobile cloud computing," Systems Science & Control Engineering, vol. 2, no. 1, pp. 476-483, May 2014.

VII. L. D. Xu, Wu He and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233 - 2243, November 2014.

VIII. M. Aazam, I. Khan, A. A. Alsaffar and E.-N. Huh, "Cloud of Things: Integrating Internet of Things with Cloud Computing and the Issues Involved," in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, Islamabad, Pakistan, 2014.

IX. M. H. F. A. P. E. K. C. Mavropoulos O., "Apparatus: Reasoning About Security Requirements in the Internet of Things," Advanced Information Systems Engineering Workshops, vol. 249, pp. 219-230, June 2016.

X. P. S. V. Daniel, V. and R. A. , "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in International Conference on Science, Engineering and Management Research (ICSEMR 2014), Chennai, India, 2014.

XI. Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7-18, April 2010.

XII. S. Lee, J. (. Jeong and J. Park, "DNS Name Autoconfiguration for IoT Home Devices," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, pp. 131-134, April 2015.

XIII. S. Madakam, R. R. and S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, pp. 164-173, January 2015.

XIV Z. Song, A. A. Cardenas and R. Masuoka, "Semantic Middleware for the Internet of Things," 2010 Internet of Things (IOT), 30 Dec 2010.