ISSN 2350 – 0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 2, Issue 10, October 2015

The Internet Of Things: A Survey on Effective M2M Communication

Priyadharshini.SP,Rajesh.R

P.G. Student, Department of Computer Science and Engineering,IFET College of Engineering, Villupuram, Tamilnadu, India
Assistant Professor, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India

ABSTRACT: The term Internet of Things (IoT) is defined as the network of highly connected various kind of devices such as smart sensors, actuators, smartphones, RFID tags, backend servers, etc.. Machine to Machine (M2M) Communication enables those interconnected network of heterogeneous objects to interact and exchange information among each other and therefore creates the IoT environment practically possible. In current perspective, IoT environment which enables a huge network of things to communicate with each other may facing several technical and application issues such as security, privacy concern, decision making support, sensor anonymity, diversity of device applications and so on. In this survey paper, our objective is to provide an analysis of challenges arise during M2M communication of networked devices.

KEYWORDS: Internet of Things (IoT), Machine to Machine (M2M) communication, IoT related technologies, IoT challenges.

I. INTRODUCTION

Internet of Things (IoT) environment emerges due to the advancement in the communication technologies. IoT will revolutionize human lives by bringing lots of automation to everything or devices that are connected to the Internet. Machine to Machine (M2M) Communication made the practical realization of interconnected intelligent devices to communicate information and to coordinate decisions. M2M Communications are realized through a range of technologies and networks of various devices. IoT enables any physical objects to be connected and provides smart communication between those connected devices through M2M communication in order to reduce human intervention. Eventhough the devices connected together in IoT environment generates smartness in information and communication technologies, they still facing several challenges in their technical and application aspects.

A huge amount of interconnected objects as envisioned for the IoT will create a major challenges in terms of security in data exchange, privacy concern, constrained resources, device heterogeneity, sensor anonymity, decision making support and so on. A fundamental challenge in M2M communication is that ever increasing number of connected IoT devices.

According to Ericsson, survey on IoT states that around 50 billion connected devices will exist by 2020. This creates major challenges towards the existing M2M communications in terms of security and privacy of data concern.

More the IoT devices are deployed, the greater our information is at risk. In fact, a rapid growth in number of devices in IoT are vulnerable to security attacks such as denial of service, replay attacks, etc...IoT networks are diverse in terms of device applications and services, which may cause heterogeneity problem due to diversity in data formats during M2M communications. Decision support systems are still a major problem in machine to machine interaction network, i.e, IoT since they highly aim to reduce the human interventions during their communication.

There are several survey papers that describes the IoT technology in various aspects. By utilizing those facts, in this survey paper we provide an analysis of several challenges and the defined technologies to overcome those issues that occurs during M2M communications of IoT.

II. MAJOR ISSUES IN M2M COMMUNICATIONS OF IoT

A. Secured Communication

The IoT offers connectivity for both human-to-machine and machine-to-machine communications. In the near future, everything is likely to be equipped with small embedded devices which are able to connect with internet. Such ability is useful for various domains in our daily life. However, the more the IoT devices are deployed, the greater our information system is at risk. Indeed, a non-negligible number of devices in IoT are vulnerable to security attacks [1].

B. Privacy

As the deployment and development of devices and technologies were increased, an individual's privacy concern has been eliminated.

C. Device Heterogeneity

The heterogeneous nature of IoT devices and its applications raises various challenges in terms of data security and network functionality [1].

D. Availability

Availability of software refers to ability of the IoT applications to provide services for everyone at different places simultaneously [2]. This kind of issue was highly overwhelmed by providing redundancy towards critical services and devices.

E. Performance

M2M communications of IoT highly relies on the performance of those networked devices and their underlying technologies.Decision making support, smart sensing, Quality of Service are some of the performance metrics in IoT that should exhibit the best possible performance.

Apart from these technical and application challenges M2M communications of IoT faces several more issues such as reliability, interoperability, mobility, scalability and so on.

III. RELATED WORK

This section describes about the various perspectives of IoT technologies

"Survey on Secure communication protocols for the Internet of Things"[1]

In this paper, the study of multiple secure, lightweight and attack-resistant solutions for WSNs and IoT based on identified security requirements and challenges are made. Analysis of various existing protocols and techniques are performed in order to provide secured M2M communication of IoT. Heavyweight cryptographic operations i.e. based on RSA and Diffie-Hellman agreement protocols are considered to replace the lightweight operations i.e. using symmetric cryptography [1]. We take advantage of asymmetric cryptographic implementation such as Elliptic Curve Cryptography (ECC) in order to provide highly best possible secured communication over IoT devices.

“Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”[2]

This paper gives an overview of IoT enabling technologies, protocols and applications. The detailed view of several protocols which fit together to deliver the required functionalities is discussed. Provides a good foundation to gain knowledge about various IoT technologies. The interplay between the IoT challenges, cloud computing and fog computing challenges and Big data analytics are discussed [2]. We consider the advantageous feature of horizontal integration among various IoT services which in turn helps for the smart autonomic management, data aggregation and diverse protocol adaptation [2]. Protocol Integration to generate out the better IoT services are considered to overcome the availability challenges.

“A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things”[3]

Extracting higher-level information from the raw sensory data captured by the devices and representing this data as machine-interpretable or human-understandable information has several interesting applications [3]. The requirements and the solutions to the challenges in the process of information extraction are depicted. An integrated IoT analytics tool called Knowledge Acquisition tool (KAT) is presented. KAT can be used to import sensor data from various sources and enables processing the raw sensor data and creating abstractions using the common data analysis methods that are discussed [3].
Heterogeneous of devices and the scalability issues of IoT phase of M2M Communication are mitigated by implementing the analytics tool that helps to transform the raw sensor data into human-understandable and/or machine-understandable through the techniques of higher-level abstractions.

“An Energy Efficient and Reliable Internet of Things”[4]

IOT is going to be a market-changing force for a wide variety of real-time monitoring applications, such as E-healthcare, homes automation system, environmental monitoring and industrial automation as it is supporting to a large number of characteristics and achieving better cost efficiency [4]. Energy Efficiency Reliability (EER) issues and the barriers are analyzed to enhance the development and the deployment of IoT devices.
Reliability is critical for Efficient IoT communication, because unreliable sensing, processing, and transmission can cause false monitoring data reports, long delays, and even data loss, which would reduce people’s interest in IoT communication. Therefore, the rapid growth of IoTcommunication demands high reliability [4].
Local Vote Decision Fusion (LVDF) algorithm is implemented directly to the M2M communications of IoT to achieve a high rate of reliable services.

“Ubiquitous Data Accessing Method in IoT-BasedInformation System for Emergency Medical Services”[5]

The rapid growth in IoT technology has spurred the increase of real-time data which causes difficulty in information storage and accessing which in turn causes the data interoperability problems.
The resource-based data accessing method named Ubiquitous Data Accessing (UDA-IoT) is designed to acquire and process IoT data ubiquitously in order to improve the accessibility of IoT data resources [5].
The UDA-IoT implementation is significant to support decision-making system in emergency services such as medical services. In UDA-IoT model, heterogeneous IoT data are encapsulated in unified format of resources with unique URI so as to be accessed ubiquitously [5].

"Socio-Organism Inspired Model Forming Multi-Level Computational Scheme for Integrated IoT Service Architecture"[6]

This paper deals with decision-support system in IoT objects by extending their functions to obtain an integrated and advanced infrastructure.
It is accomplished by composing an IoT architecture that imitates brain-neural system of living organisms and creating an intelligent framework inspired by human-to-human socio interactions that will serve as a model for machine-to-machine interactions [6].
Multi-Level Computation (MLC) mechanism is implemented at each layer of general IoT architecture to perform intelligent and sensing/actuating behavior.
MLC enables inter-IoT infrastructure function realizing human to human interactions [6].

"Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?"[7]

The future IoT architecture is focused in two different aspects such as Unit IoT and Ubiquitous IoT.
Focusing on special applications, the architecture of Unit Iot is built from man like neural network (MLN) model and its modified model. Ubiquitous IoT refers to the global IoT or the integration of multiple Unit IoTs with ubiquitous characters, and its architecture employs social organization framework (SOF) model [7].
The MLN and SOF models are built to empower the existing IoT architecture to provide the best possible interaction among the devices like human-to-human interactions.

IV. CONCLUSION AND FUTURE WORK

As a result of conducting this survey, this paper describes about the IoTs beneficial functionalities and various IoT technologies implemented. As though IoT provides several feasible gain to reduce human interventions it faces several technical and application challenges in current aspects. Several models and mechanisms are surveyed to overcome those challenges.

Our future work focuses on building a highly feasible IoT architecture which emerges an effective M2M communication among the highly connected physical objects. The integration of all the advantageous mechanisms provided to overcome the IoT challenges are depicted to model an effective IoT environment that performs highly secured communication with the upgraded neural support analysis among the interconnected devices.

REFERENCES

[1] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, "Survey on Secure communication protocols for the Internet of Things", Elsevier Adhoc Networks, Volume 32 Issue C, Pages 17-31, Sep 2015.

[2] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aldehari, Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", IEEE Communications Surveys & Tutorials, 2015.

[3] FriederGanz, Daniel Puschmann, Payam Barnaghi, "A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things", IEEE Internet of Things Journal, Vol 2, No 4, August 2015.

[4] ShyamSundar Prasad, Chanakya Kumar, "An Energy Efficient and Reliable Internet of Things", International Conference on Communication, Information & Computing Technology (ICCICT), 2012.

[5] BoyiXu, Li Da Xu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services",IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014.

[6] YanuariusTeofilusLarosa and Jiann-Liang Chen, Yi-Wei Ma, Sy-Yen Kuo, "Socio-Organism Inspired Model Forming Multi-Level Computational Scheme for Integrated IoT Service Architecture", 2nd Baltic Congress on Future Internet Communications, 2012.

[7] HuanshengNing and Ziou Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?", IEEE Communications Letters, Vol. 15, No. 4, April 2011.