International Business Management 10 (17): 3807-3811, 2016
ISSN: 1993-5250

Internet-of-Things (IoT) as Engine of Growth for the Economy

[1]Nomahaza Mahadi, [1]Imran Fazley Ibrahim, [2]Azizul Yadi Yaakop, [3]Zailin Zainal Ariffin
[1]International Business School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
[2]School of Maritime Business and Management,
Universiti Malaysia Terengganu, Terengganu, Malaysia
[3]Faculty of Defence Studies and Management,
National Defence University of Malaysia, Kuala Lumpur, Malaysia

Abstract: The Internet-of-Things (IoT) is set to bring a major change in the way we conduct our lives and business in the near future. The contribution to the economy is expected to be significant as internet connections will not only be limited to humans to other people but it will also involve the real physical world as well. Machines will no longer be confined to their respective networks and the IoT trend will provide the potential for machines to self-learn as well. This study will discuss the potential economic significance of the IoT trend and the impact that an environment of connected devices have had in our businesses and daily lives. At the end of the study, the discussions on the implementation of IoT and its risks will be provided.

Key words: Internet-of-things, innovation, technology, economy, Malaysia

INTRODUCTION

Businesses are constantly looking out for opportunities that will be able to give them an edge in a very competitive market environment. A company's ability to react to any situation that may present itself to the business could possibly affect the profits and losses that could significantly affect the business' future and its growth (Omar *et al*., 2015). One of the ways that a company can do this is through the use of technology. Technology has certainly played a very big role in improving business performances. In the post industrial revolution era, it is very clear that the prosperous nations are among those who have a very clear technological lead. The GDP growth rates of the developed countries compared to the others are also very striking (Schilling, 2013). While the developed countries were able to almost double their GDP in the period from 1969-2011, the other countries were only able to improve by about 50% from their levels in the 1970s.

The internet has been usually known as a network of connections between IP addresses. These IP addresses serve as a unique identifier to nodes (i.e., computers) which serves as the channel for human operators to communicate with other people or retrieve and send data from and to a database. Visualization of partial internet network in 2005 can be seen below (Acculation, 2015) (Fig. 1).

Fast forwarding to present time, personal computers are no longer the major shareholders in terms of internet

Fig. 1: Visual representation of internet connections (Acculation, 2015)

connection. Mobile devices (smartphones, tablets, wearables) have been steadily gaining ground and are on track to take over the computer as major channel to get connected to the internet (Anthony, 2013). The next major step will be the Internet of Things (IoT) where humans will also need to share the internet space with other connected devices as well. IoT is roughly used to define the connection between physical things in the real world to the internet allowing these devices to interact with the environment around them (Mashal *et al*., 2015). The potential value adds from IoT devices are expected to reach US $1.9 Trillion dollars by 2020 (Gartner Inc., 2013). By >50 billion devices are expected to be connected to the internet (Haubenwaller and Vandikas, 2015) and this will provide opportunities and also challenges to the

Corresponding Author: Nomahaza Mahadi, International Business School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

businesses around the world. Therefore, this conceptual paper aims to bring a new perspective to the understanding of IoT's importance to the business environment as a whole and identify the requirements and resources needed to implement IoT for businesses. This paper will also examine the potential issues and challenges of IoT and suggest some potential solutions to the issues faced.

MATERIALS AND METHODS

Overview of IoT and its impact: IoT is a result of a natural progression of recent technological advancements. The introduction of technologies such as improved miniaturization and increasing computing power has allowed for an explosion of interconnected devices that are using a common communication protocol through the internet (Glova *et al*., 2014). The connected devices not only improves online communication between people, people and devices but it also helps devices to communicate to other devices through the use of embedded solutions and wireless identification technologies. This development has led to increasing collaborative efforts which have resulted in changing values in the business environment. The changing values are having an impact on the way products and services are marketed challenging traditional business models. Chief among the changes needed is for businesses to seriously consider including the data management tools into their strategic decisions. A major challenge will be for businesses to realize the potential in integrating their various business operations in a more collaborative environment.

Other than businesses, the IoT development is also causing a rethink in people's socialization process (Shaev, 2014). The two major areas that are most affected is the separation between the real world and the virtual world is becoming narrower as technology begins to meld into our lives through the smartphones that we carry or through the increasing influence of social media as a form of communicating and increasing prominence and our own attachment to connected objects. Being able to communicate with machines means that for some, the need for human company may no longer be an important factor. When it comes to rules and regulations, the authorities are still in the difficult initial phase of setting it up (Oriwoh *et al*., 2013). There is recognition early on that the deployment of IoT will need to be guided by specific set of rules to prevent abuse. There are already a number of potential security issues identified that will need to be dealt with. More elaboration on this will be done later. Chief among these concerns are in the areas of security and also ownership of accountability and liabilities. For example, the ability to handle increasing complexity while managing the transfer of functionality, particularly from the mechanical domain to the information technology and electronics domains has long been an issue facing system designers (Griffin, 2010; Bradley *et al*., 2015). As technology has evolved, along with the ability to create increasing volumes of information, the challenges for designers have increased, requiring the wider communication and integration of knowledge and understanding across and between individuals.

On the one hand, IoT constitutes a network of physical objects (things) with embedded technology used for internal interactions within the network and for interactions between things and environment. Examples include various built-in sensors, smart home technology and cutting edge means of communication such as weight control management programs, photographic and video devices, alarms, dictionaries, scanners, games etc. A key factor seen to fulfil the full potential of an IoT environment is having devices that more autonomous and smarter than what the current available technologies (Kyriazis and Varvarigou, 2013). It is argued that real world dynamics will put a great strain on the processing application of connected devices and objects and make the system error prone and unpredictable in its performance. The ability for these devices to learn and self-improve will greatly help resolve these performance issues.

RESULTS AND DISCUSSION

Implementation requirements of IoT: The shift towards IoT will result in an environment that combines various aspects of technologies with the world around it. Using various types of sensors with suitable controls and regulations and topped up with a sound system management, a whole new set of possibilities has been made available (Borgia, 2014; Bradley *et al*., 2015) (Fig. 2). It is clear that the management of the network in the IoT is going to be a very complex arrangement. By looking at examples building architecture and city planning management systems, a somewhat similar arrangement for the computer network has been proposed (Hernandez-Bravo and Carretero, 2014). With this concept, the management involves the utilization of a pattern concept instead of individual units in the network. Before this a traditional way of looking at networks is through the use of tree diagrams or hierarchical structures to represent the different levels involved in the network. But the problem with this view is

that the structure puts a limit on the type of complexity that can be represented. In particular the types of decisions that can be made are limited by the number of options presented. By using a pattern concept, there is an element of reasoning presented where the process will have a larger view on the issue that needs to be decided upon.

The proliferation of connected devices will not only add to the complexity of the network of connected devices but also increases the need for data-on-demand significantly. It is possible that a localized central computer may not be able to handle the load and will need some help from other resources to process the data more efficiently. Cloud computing can be a good solution for this pressing problem (Gubbia *et al*., 2013) (Fig. 3).

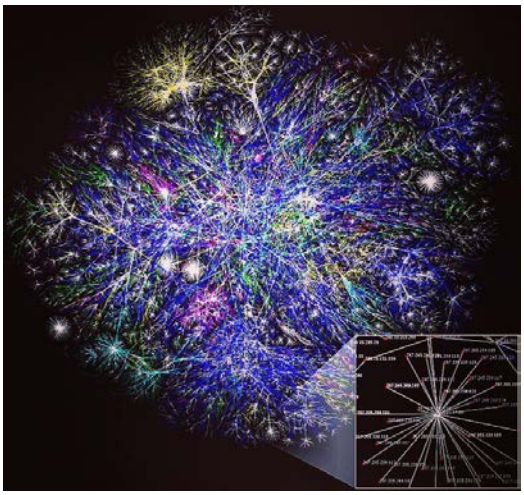

Fig. 2: The emerging IoT scene (Borgia, 2014)

Application development for IoT systems is also a very challenging issue to address (Patel and Cassou, 2015). Consider a building environment where there a set number of floors with a set number of rooms in each floor. Each of the rooms in the buildings may have different types of sensors with the similar aim of monitoring safety and security of its inhabitants. Due to the large number of possible combinations of devices that can occur, it will almost be impossible for the system designer to consider all possible scenarios to prepare for. A proposed solution to this complexity is the modular approach where instead of designing systems for devices, it might be more efficient to design for function and scale up the function with more devices as necessary.

Through the development of opening up communication between devices taking place, there is also a concern on unauthorized access (Nguyen *et al*., 2015). Current security protocols employ either one of these two approaches when it comes to security, asymmetric and

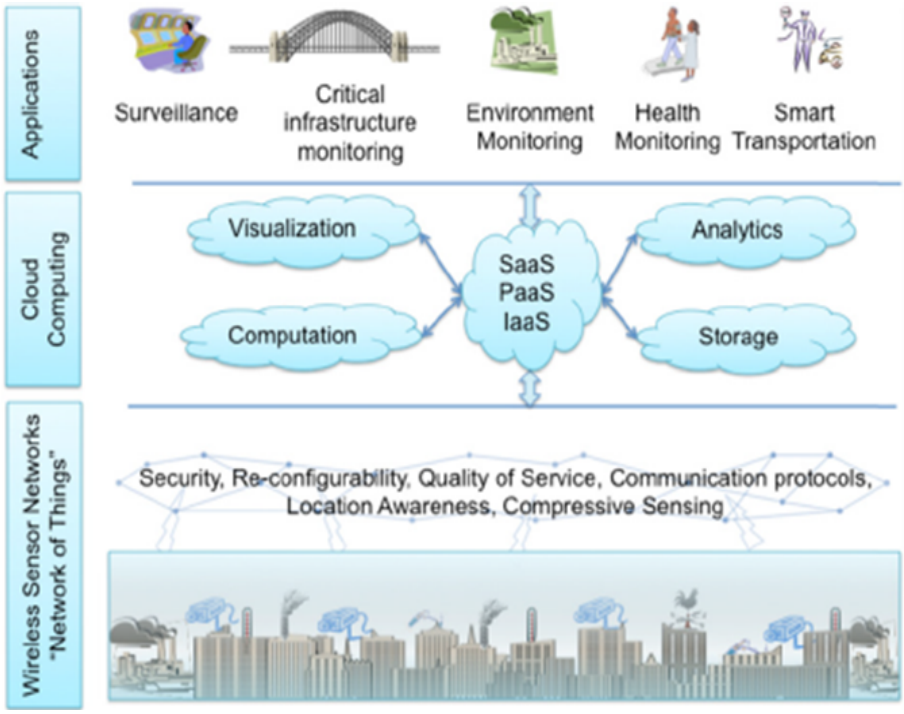

Fig. 3: Conceptualized IoT system with cloud computing (Gubbia *et al*., 2013)

symmetric approaches. Both methods have their pros and cons but both are not fully capable of providing absolute protection against new found threats in the IoT environment. As such there is a proposal for a combination of both approaches to offer a better form of defence. What is certain however is that heavy research is still being done in this new area of computer science.

Issues to consider: When dealing with an IoT, there are several issues that will need to be considered which can be categorized into two groups. These groups are the demand factor and supply factor. With the supply being factors related to businesses and the demand coming from the consumer end. For the demand side, both public and private consumers may share the same concerns when it comes to inter-connected devices and these areas are in the aspect trust, security and privacy. Consider a scenario where a network is established by connecting devices together to allow communication between one devices to another. Additional devices are only able to connect to the network provided it is a trusted device. While the intuition for this thought is easily understood, the implementation of such a concept is a challenge and highly complex for machines. By examining human behaviour of giving trust based on the reputation of the person, a similar approach to handle trust between connected nodes in a network known as the Trust Reputation Model (TRM) was introduced.

In order to mitigate concerns related to trust issues, a comprehensive trust management system has been proposed (Yan *et al*., 2014). In this TRM, an IoT system is thought to have 3 different layers, physical perception layers involving the device capabilities to receive information from their external environments, network layers involving all the networked connections to transmit and receive data and application layer which provides the required services to the end users. In all three layers, it is important that data integrity is verified and well secured. Both the integrity and security of data in the network are closely related considering most of the sources will be from external parties. Among the areas where the data verification and security is crucial will be in communication and storage, computation time, scalability and the security system itself.

For the supply side, it is important for businesses to have the building blocks of an IoT system in place. The essential IoT technologies are device identification, network, middleware, cloud and IoT applications (Lee and Lee, 2015). The company will then need to evaluate the system architecture that is the best fit for them and proceed to build the ecosystem required. It cannot be denied that any technology no matter how promising will to have its value demonstrated in dollar terms before a business decision to allow the technology to get off (Lee and Lee, 2015). The IoT will require a lot of investments from the enterprises and so a proper valuation of the feasibility of the project will need to be carried out. Another challenge of IoT is providing communication and collaboration among heterogeneous objects and information system to produce useful services. It is expected that the number of interconnected devices will reach 50 billion by 2020. Managing such a huge number of devices and systems requires unparallel scalability and improved performance of IoT (Mashal *et al*., 2015).

Similar to other business decisions when weighing options, it is in the best interest of companies to conduct their own assessment and measure the potential returns on investments before they can fully commit to the project. The company will need to make an evaluation of the investments required, establish an ROI timeframe and also implement a monitoring system to ensure that the newly acquired resource is able to help improve business.

CONCLUSION

Internet of things is trend that looks set to revolutionize all aspects of our lives in the near future. With a market value exceeding US trillions of dollars, there is a big potential for the trend to generate huge returns for businesses and also generate a lot of new jobs as well. It is a relatively new field and no company can claim to own a significant share of the market yet. Opportunities are a plenty for both the hardware and software providers. For Malaysian companies, the opportunity is in the software side as this area does not require a big company setup and can generate higher margins for the company's bottom line. However, the risk on the enterprise is the lack of regulation which has the potential to derail any investments made companies in case the capital outlay is made in the wrong direction.

In order to counter the negative reception that consumers both private and businesses alike, a revolutionary end user application or new device will be needed to turn around the perception. By offering the market new ways and insights to reap the benefit of this new technology the rate of acceptance will be much higher. There is an element of caution that must be placed against all this optimism for the new trend. As we begin to open up to accept the flood of new information, the chances of having a compromised security also increase. Business ethics also becomes an issue as we walk a fine

line between democratizing data and also outright privacy violation. The internet of things is a force that has come to stay and as we take the baby steps into a new frontier it would be wise to look forward to the promised opportunities but also keep the guards up against possible unknown threats lurking around the corner.

REFERENCES

Acculation, 2015. Internet map: Network data visualization example. https: //www. acculation. com/blog/2015/01/30/internet-map-network-data-visualization/.

Anthony, S., 2013. The demise of Microsoft's monopoly and the PC market, by the numbers. http://www.extremetech.com/computing/161666-the-demise-of-microsofts-monopoly-the-pc-market-by-the-numbers.

Borgia, E., 2014. The internet of things vision: Key features, applications and open issues. Comput. Commun., 54: 1-31.

Bradley, D., D. Russell, I. Ferguson, J. Isaacs, A. MacLeod and R. White, 2015. The internet of things-The future or the end of mechatronics. Mechatronics, 27: 57-74.

Gartner Inc., 2013. Newsroom. http://www.gartner.com/newsroom/id/2636073.

Glova, J., T. Sabol and V. Vajda, 2014. Business models for the internet of things environment. Procedia Econ. Finance, 15: 1122-1129.

Griffin, M.D., 2010. How do we fix system engineering? Proceedings of the 61st International Astronautical Congress, September 27-October 1, 2010, Prague, Czech Republic, pp: 1-9.

Gubbia, J., R. Buyya, S. Marusic and M. Palaniswami, 2013. Internet of things (IoT): A vision, architectural elements and future directions. Future Generat. Comput. Syst., 29: 1645-1660.

Haubenwaller, A.M. and K. Vandikas, 2015. Computations on the edge in the internet of things. Procedia Comput. Sci., 52: 29-34.

Hernandez-Bravo, A. and J. Carretero, 2014. Approach to manage complexity in internet of things. Procedia Comput. Sci., 36: 210-217.

Kyriazis, D. and T. Varvarigou, 2013. Smart, autonomous and reliable internet of things. Procedia Comput. Sci., 21: 442-448.

Lee, I. and K. Lee,q 2015. The Internet of Things (IoT): Applications, investments and challenges for enterprises. Bus. Horizons, 58: 431-440.

Mashal, I., O. Alsaryrah, T.Y. Chung, C.Z. Yang, W.H. Kuo and D.P. Agrawal, 2015. Choices for interaction with things on internet and underlying issues. Ad Hoc Networks, 28: 68-90.

Nguyen, K.T., M. Laurent and N. Oualha, 2015. Survey on secure communication protocols for the internet of things. Ad Hoc Networks, 32: 17-31.

Omar, S.S., R. Ramlan, K. Ahmad and C.S. Wei, 2015. Small business growth: A review of literature from the tipping points and social network perspectives. Adv. Sci. Lett., 21: 1089-1093.

Oriwoh, E., P. Sant and G. Epiphaniou, 2013. Guidelines for internet of things deployment approaches-The thing commandments. Procedia Comput. Sci., 21: 122-131.

Patel, P. and D. Cassou, 2015. Enabling high-level application development for the internet of things. J. Syst. Software, 103: 62-84.

Schilling, M.A., 2013. Strategic Management of Technological Innovation. 4th Edn., McGraw-Hill, New York, USA., ISBN-13: 978-0078029233, Pages: 336.

Shaev, Y., 2014. From the sociology of things to the internet of things. Procedia-Social Behav. Sci., 149: 874-878.

Yan, Z., P. Zhang and A.V. Vasilakos, 2014. A survey on trust management for internet of things. J. Network Comput. Applic., 42: 120-134.