An Enhanced Secured IOT Model for Enterprise Architecture

Conference Paper · March 2020

DOI: 10.1109/ICMCECS47690.2020.247112

4 authors, including:

Ife Olalekan Ebo
Mountain Top University Ogun State Nigeria

Olorunjube Falana
Federal University of Agriculture, Abeokuta

Olumuyiwa Alaba
Tai Solarin University of Education

An Enhanced Secured IOT Model for Enterprise Architecture

Ife Olalekan Ebo
Department of Computer Science and Mathematics
Mountain Top University, Prayer City, Nigeria
ioebo@mtu.edu.ng

Olorunjube James Falana
Department of Computer Science
Federal University of Agriculture, Abeokuta, Nigeria,
falanaoj@funaab.edu.ng

Olutosin Taiwo
Department of Computer Science
University of Kwazulu-Natal, Durban, South Africa,
olutosinoyeleke@gmail.com

Olumuyiwa, Bamidele Alaba
Department of Computer and Information Sciences,
Tai Solarin University of Education,
Ijebu Ode, Ogun State.
alabaob@tasued.edu.ng

2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS) 978-1-7281-3126-9/20/$31.00 ©2020 IEEE 10.1109/ICMCECS47690.2020.247112

Abstract- **Enterprise architecture (EA) is a comprehensive way of helping an organization to achieve its desire objectives. Recent research shows the requirement of EA in small and medium-sized enterprises (SMEs). There is strong empirical evidence affirming that SMEs are a major job creation in any economy. However, the analysis also clearly shows that the sector is very diverse. With the advent of the Internet of Things (IoT), a new paradigm for driving digital innovation in EA has emerged. IoT enabled interactions between machines and devices to communicate globally. It also spurred new digital innovation used to deliver value-added services in a wide range of industries. There is a risk that promoting IoT in EA due to their large contribution to employment, without adequate provision for security may result in a trade-off between quantity and the security of EA. In view of this, this paper proposed an enhanced IoT ecosystem architecture with a security layer to enforce the security policies for each of EA IoT layers. The paper also presents the IoT service business model.**

Keywords: ***Internet of Things, small and medium enterprises, business model,***

I. INTRODUCTION

The enterprise sector is undergoing a remarkable revolution because of the increased complexity, inter-dependencies, emerging technologies, globalization, and change in demands and customer satisfaction. Small and medium enterprises are businesses whose personnel numbers are below certain limits. They stimulate private ownership and entrepreneurial skills and adapt quickly to changing market situation, generate employment, help diversify economic activities and make significant contributions to the economy.

A new paradigm found to be an important part of the future internet because of the rapid advancement of information and communication technologies (ICT) is the Internet of Things (IoT). It represents a wide connection and perception of things, services, networks, and infrastructure. This new technology has changed the interaction between people and objects. IoT integrates different things such as sensors, actuators, and services produced by individuals and companies to support their various applications. It has been seen as a major component of industry 4.0 as a result of the changes it has brought, as well as its ability to gather data via embedded sensors and actuators to produce actionable information [1].

IoT also represents the ubiquitous connectivity concept for businesses, governments and consumers, with their own management, monitoring, statistical computations and data analysis systems. The "things" in IoT may refer to humans, animals or objects. For example, a product with microchip on it to which an internet protocol (IP) can be assigned is capable to transfer data over the internet.

According to Iansiti and Lakhani [2], IoT has significantly changed the ways of doing business by enabling enterprises to develop value-added services with their network of machines and devices, improve their service business models, and enhance their sustainability. Hilton [3] reported that IoT solutions have been marketed and purchased by small, medium and large enterprises, some of which are used for remote asset tracking, factory automation, fleet services, energy or utility management, parking management, facilities management, smart vehicle enablement and many others. Its growth has tremendously increased the number of internet users from 1.158 billion in 2007 to 3 billion in 2014; about 15 billion devices are also connected to the internet in 2014. Lund et. al., predicted that IoT will have about 6% impact on the global economy, and over 24 billion IoT devices will be connected by the year 2025 [4]. The study conducted by Hilton further stated that majority of those devices will belong or be sold by large enterprises rather than SMEs, such that only 25% of the connected devices by 2025 will belong to or be sold by SMEs [3].

SME IoT platform is concerned with the aim of creating business value and customer satisfaction through IoT services. IoT platforms provide the required tools for different enterprises to build and host their applications in low-cost, timely and less programming efforts. Most SMEs managers do not have the expertise or technical know-how to select or develop and deploy their own SME IoT services, thus, they are opened to the ones provided by vendors. Meanwhile, some individuals SMEs and companies (vendors) are developing their own SME ecosystems methodologies for improving business performance and customer satisfaction.

Thus, there is a need to help SMEs in the selection or development and deployment of IoT systems and solutions that are efficient, effective, low-cost, easy, secured and with networkable micro-controllers, which can be used to better serve customers, improve productivity, extend market base, and stay competitive [5] because of the present and predicted low patronage of IoT systems and solutions by SMEs [3].

More so, the increasing numbers of SMEs IoT platforms are characterized with their advantages and challenges, thus, enterprise managers rather subscribe to vendors IoT platforms than build their own in-house. Hence, there is a need to help enterprise managers understand the elements that should make up a SME IoT platform ecosystem and its architectural design in relation to their enterprise services which have been inadequately studied. In the light of the aforementioned, this paper presents a modified SME IoT ecosystem and IoT architecture towards the development of SME IoT and how SMEs managers can plan IoT services with the use of the IoT service business model.

The remainder of this paper is organized as follows: Section 2 discusses the literature review. Section 3 describes the overview of SME ecosystem via a presented modified five-key players that made up the enhanced SME ecosystem. Section 4 describes the improved IoT architecture for service business models; Section 5 discusses the SMEs service business model. Section 6 concludes the work.

II. LITERATURE REVIEW

Several research works have been conducted towards the selection, and adoption of IoT in various fields of human endeavours. Some of the commonly used term in IoT applications includes smart health, smart grid, smart home, smart education, smart industry and smart commerce [6 -12]. IoT has capability of bringing together billions of smart devices, each one providing data that has the ability to act and influence the environment. If such large amount of data are well managed, and process intelligently through smart solutions, it will enhance decision making process and increase business returns.

A business is not a single entity but one that spans across different industries [13]. It is an ecosystem that exists to contribute its quota to the socio-economic environment. For an IoT business ecosystem, it comprises of IoT-related individuals and companies that contributes socially to their environment [14]. According to Amit and Zott [15], the major determinant of the success and wide spread of the importance and use of IoT in the business environment is the emergence and development of the following methodologies:

(1) Artificial Intelligence: this is the tremendous increase in the computer capacity to handle large volume of data (structured or unstructured). It takes in data produced by IoT devices and make actionable decisions about these data, thus, giving IoT devices commands to perform specific tasks.

(2) Machine learning: which consists of algorithms developed to automatically detect Big data, and determine the best IoT device that will tend to produce the desired and optimal result with or without human intervention.

(3) Data Analytics and Data Mining: this is the process of systematically and consistently finding data patterns, relationships and applying them to discover new sets of data.

III. OVERVIEW OF SME IOT ECOSYSTEM

An ecosystem is a collection of systems or a complex network or interconnected system. With an SME ecosystem, enterprises will be able to work together among themselves to support new products and services, improve productivity, extend market and stay competitive [16]. This means that ecosystems are majorly the competitive unit in the IoT, hence, the battle will be between these ecosystems, not between individual companies. An IoT ecosystem creates interdependency among partners in the ecosystem, all partners share the same fate. Individual partners will be successful only if the ecosystem is successful. Since the success of any IoT platform is dependent on the ecosystem, the understanding of the SME IoT ecosystem will help business owners determine the right IoT platforms for their service development and deployment in a quick and low-cost manner.

Every IoT ecosystem consists of four major components, namely: people, hardware, data and process, in which SME IoT ecosystem is not an exception. Based on the survey of literature, this paper discusses two of the major components: people and hardware, as the basis for other two components.

A. Stakeholders/People

According to Bröring et al. [17], an enterprise IoT ecosystem is made up of stakeholders such as things provider, developer, platform provider and users. In the research conducted by Lee [16], he identified five key players of the enterprise ecosystem such as software platform developer, hardware platform developer, network technology developer, application/solution developer, and users and customers. These five players are major contributors to the innovation, expand markets, foster collaboration and help enterprises to stand in the face of competition, while satisfying the users and customers. However, the five key stakeholders do not take care of the security challenges being faced by IoT ecosystems.

Rather than allow individual stakeholder to deal with security issues facing IoT platforms, it is proposed that a separate key player, named security platform developers, be introduced to the ecosystem, to deal with security issues squarely as shown in figure 1. They are centralized to provide the necessary security at every level of development in the ecosystem. Each of these key players is discussed below:

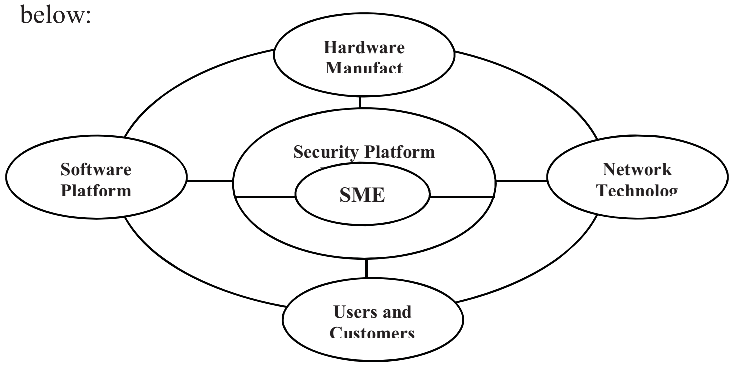

Fig. **1.** The modified five key players of an SME IoT ecosystem

1. Hardware Manufacturer

IoT hardware for SMEs refers to physical components deployed in the smooth running of the SMEs. They include PCs, tablets, smartphones, sensors, actuators, and peripheral devices that are often built from various components. The hardware manufacturers include board manufacturers, gateway device manufacturers, controller developers, sensor manufacturers, device manufacturers, and so on [16]. Hardware consists of things or physical assets that are built with processors, microcontrollers and other components.

Hardware manufacturers have contributed largely to the development of SMEs through IoT by producing prototyping kits and boards, for example, Arduino IoT products, raspberry Pi, Espressif ESP8266, AdaFruit feather boards, littleBits, and so many others. These hardware platforms are easy to use, cost less, small in size and easy to understand and program. Some hardware manufacturing companies include IBM, Arduino, Intel, Raspberry Pi, AT & T etc [18-20].

2. Network Technology Developer

Stakeholders under this category include data network developers, telecom operators, connectivity platform developers and network device manufacturers. They provide avenues for communication between devices/machines on a local or wide area networks. For local networks, they provide short range platforms such as the Bluetooth low energy, Zigbee, radio frequency identification (RFID), near-field communication (NFC) and so on, which are mostly used in industry where low power and low data rate are required. While for a wide area network, they provide low-power wide area (LWPA), Sigfox, LoRa, and the 5G cellular mobile network.

3. Software Platform Developer

IoT Software platform developers include data platform developers, cloud service providers, operating system developers, third-party developers, system integrators and in-house developers. They produce visual platforms using a model-driven approach that enable both professionals and less technical developers to consume IoT services. Their applications provide a customized platform, that reduces complexity in developing IoT systems, prevents data redundancy, and manage data, deployment and security of the system. Their platforms provide services for healthcare, education, e-commerce, finance, transportation, and manufacturing industries. Examples include AWS, IBM Watson, Microsoft Azure, and KPN LoRa [21].

Some developers use various IoT platforms to develop task in a domain-specific application because of the complexity in architecture, protocols and programming languages, time-consuming and distributed nature of IoT systems. They integrate IoT software and hardware platforms to produce different IoT services. For instance, a developer may decide to use Arduino IoT kits alongside with ThingsSpeak platform.

Lee et.al [22] suggests that software platform should be programmable with an easy programming language, provides high level APIs for device management and communication, support simultaneous execution of several IoT applications with different function and allows partner IoT devices to communicate with host device.

4. Security Platform Provider

Based on the review of existing literature, security platforms developer or providers are often combined under the software platform developers [16, 17]. It is pertinent to note that security has been a major challenge facing most enterprise IoT platforms. Bertino [23] stated that IoT systems have high security risk as a result of their lack of well-defined perimeters, highly dynamic, highly heterogynous for communication medium and protocols, and continuous changes because of mobility. Intruders can have access to sensitive information of the customer or business transactions when an enterprise IoT system lacks security.

Thus, the adoption of an enterprise IoT system is hinged on the protection available. In view of this, the potential threat on the security may be improved by establishing Security Platform Providers that with be saddled with the major responsibilities of providing IoT systems security via IoT security protocols such as authentication, authorization, access control, and non-repudiation and incorporating security protection mechanisms such as data encryption, firewalls, and security analytics into the IoT systems.

5. Users and Customers

The major significance of SMEs using IoT systems is to satisfy users and customers in a timely, low-cost, innovation promoting and better service delivery. Thus, users and customers are the major beneficiaries of IoT systems. IoT systems assist users and customers to shop, track and monitor assets, manage office utility, check certain operations and maintain machinery.

B. Hardware

This includes a wide range of devices that are used to manage tasks and functions such as security, data collection, system activation, actions specifications, communication, and detection of support-specific goals and actions. IoT hardware devices include routers, bridges, sensors, actuators, servers, and development boards.

IV. THE ARCHITECTURE OF SME IOT

Enterprise architecture can leverage the interconnectivity of smart devices by grouping them to measure certain data or to form new business models and uses. Architecture has a significant impact on the success of a system, thus its need to be thoroughly looked into. The SME IoT ecosystem discussed in the previous section highlights the key stakeholders and technology needed for the implementation of the architecture of the IoT, as well as ensuring its implementation and continuous update for the provision of IoT services.

Based on the reviewed literature, several architectures have been proposed: three-tier architecture, consisting of the edge, platform and the enterprise tier [24-27]; four-layer architecture and five-layer architecture [28-30]. Lee [16] presented a modified five-layer architecture, replacing the business layer on top of the five-layer architecture with a service management layer to reflect the unique services of enterprise IoT. Other layers are perception layer, network layer, processing layer, and application layer.

In this paper, we presented an improved five-layer enterprise IoT architecture as shown in figure 2 and 3. A security section is added to ensure and enforce the security policies for each of the layers. The improved five-layer architecture is presented as follows.

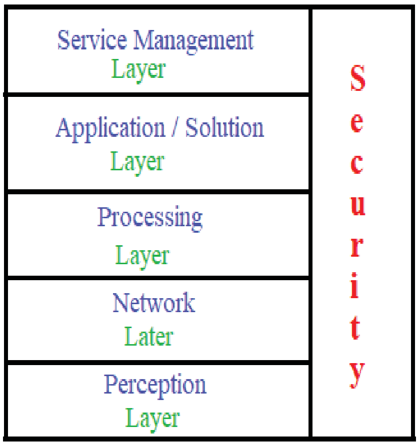

Fig. 2. A modified five-layer architecture of the enterprise IoT.

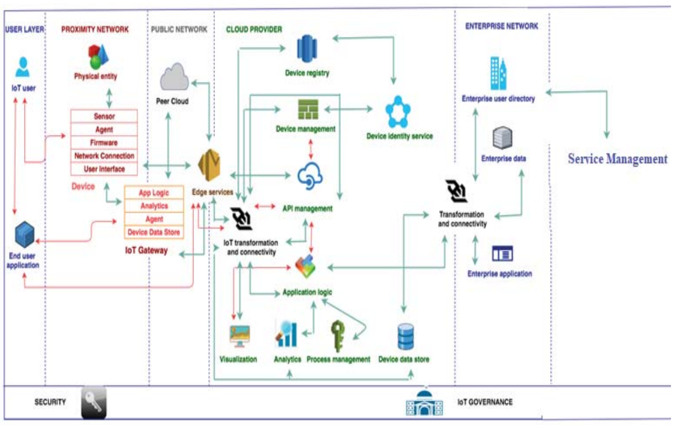

Figure 3: An Improved Enterprise IoT Overview (adapted from IBM [33])

A. Perception Layer

The public networks and proximity are found in this layer. It consists of different sensors, actuators, tags and readers, smartphones, and cameras. This layer encompasses several sensing technologies (e.g. RFID, GPS, WSN, NFC, etc.). They are used to collect data, identify objects, people and gather locations information. Data are collected from a myriad of internet-connected devices and social networks are analyzed to attend to different real-time events. Information gathered are converted to digital signals, which are more convenient for network transmission.

B. Network Layer

In this layer, all the data received from devices are transmitted to the processing layer through the gateway or straight from the device into the Cloud provider, using the edge services and IoT transformation and connectivity. This layer uses various network and communication technologies. It uses media such as 3G/4G/5G, Wifi, Zigbee, Bluetooth, FTTx, UMB, infrared, and so on. Large chunk of data will be carried by the network; hence, it is significant that a reliable and dynamic technology be employed.

C. Processing Layer

This is also known as the middleware layer. It consists of cloud computing providers, database management providers, data analytics and big data. This layer cleanses data, stores it, analyses and process data collected by IoT devices in real-time. It provides API management and visualization and can launch commands of control from the enterprise network to the public one.

D. Application Layer

This layer consists of a set of domain-specific applications that help collects, share and solves user's problems. It consists of the front end of the whole IoT architecture through which IoT services will be exploited by users and customers. It has the data from the enterprise, an enterprise user directory and the applications. The data flow to and from the network using the transformation and connectivity component. The data stored in the enterprise is gathered from structured and unstructured sources of data and real-time data that come from stream computing. The application layer facilitates the development of myriads of enterprise IoT applications. Managers must understand what types of enterprise applications are provided at the application layer.

E. Service Management Layer

This is the top layer of the enterprise IoT architecture responsible for the selection and delivery of IoT services to the enterprise. This layer controls and activities, process and procurers necessary for an organization to plan, design, implement and improve enterprise IoT services. The IoT services are value available to users and customers, to solve their specific problems. These values are measured based on the customers' willingness to pay, use and reuse the services provided by the enterprise.

F. Security and IoT Governance

Security systems and IoT governance have the role to span the architecture's elements to provide policies and control for the data and applications, which are defined and enabled in the whole system.

V. IOT SERVICE BUSINESS MODEL

Several authors have reported different views on service business model [31, 32]. For instance, Amit & Zott [15] described service business model as a new valuable unit that measures the organizations capacity to create, capture and deliver value to end users and customers. Zott et. al [34] described it as a way to create sustainable competitive advantage, while opportunity creation is the major concern of the business [35]. Hence, Ahokangas et.

al [36] stated that service business models are never static and develops continuously through refinement, adaptation, revision and reformulation.

Scholars are of the opinion that gone are the days when a single business model could sustain an enterprise for longer profitability, thus, we need service business model innovation that will retain the market position or gain greater market share [37, 38].

Therefore, based on Ahokangas et. al [38] position, we derived 5 essential components of an enterprise IoT service business model: value proposition, value network, resources, customers/customer relationships and sustainability.

A. *Value Proposition*

This is widely mentioned in several literatures on enterprise service business model [34-35, 39]. This refers to product or service to a target end users or customers, for which they are always willing to pay and use [41]. For IoT services, value proposition should be less expensive both for customers and the enterprise, as well as, generating income for the enterprise. More so, success factors for value proposition include scalability, flexibility, accessibility, efficiency and service quality. Lee [16] reported that when users and customers perceive new products or services, value proposition is derived and adopted. Value proposition also consists of what an enterprise offers to users and customers in return for the product. According to Julius [40], there are value proposition and unique value proposition (UVP). He stated that UVPs are very difficult to locate but once identified, it can be the key to huge success for an enterprise.

B. *Value Network*

This refers to the participants that contribute to the development of IoT products and services. They include partners, device manufacturers, software developers, data scientists, as well as other enterprises. They are usually external parties bringing solutions to the company either in the supplier part or in the distributor part of the value chain.

C. *Resources*

These are the assets, knowledge, human resource, technologies, services, marketing channels, and other intangible assets like goodwill or brand which helps the firm in performing the key activities or attain and manage key partnerships. According to Lee [16], there are two important questions enterprise should ask themselves before developing IoT services, they are:

i. What are the available resources enterprises can make use of to deliver the IoT services?
ii. What the resources that will differentiate between the enterprise and other enterprises (i.e. competitors?.

D. *Customers / Customer Relationships*

These are programs laid by enterprises to support business goals. SMEs can have distinct customer relationship program to address different customer segments. These relationships can take personal interaction or automated platform depending on the enterprise's strategy and segments value and size. Chang and Wills [42] stated that a very strong assistance and support should be made available by the enterprise to create stronger relationship between the parties.

E. *Sustainability*

This is gradually becoming part of the business models, because its major concerned is the ability to ensure continuous growth of the business, the profits, and fulfill both social and environmental responsibilities.

VI. CONCLUSION

In recent years, we have seen few enterprises embracing IoT platforms in spite of the huge benefits that can be derived from it. Majority of the EAs are afraid to adopt IoT platforms due to the paucity of studies, frequent attacks and use of non-standard devices. This makes it very difficult for EA to make an informed decision. This research proposed to fill this gap by proposing a security-conscious IoT ecosystem and IoT service business model essential for the deployment of IoT-enabled services for small and medium enterprises.

REFERENCES

[1] W. H. Dutton, "Putting things to work: social and policy challenges for the Internet of things", info, Vol. 16 Iss 3 pp. 1-21, 2014.

[2] M. Iansiti , K.R. Lakhani, Digital ubiquity: how connections, sensors, and data are revolutionizing business, Harv. Bus. Rev. 92 (11) (2014) 91–99.

[3] Steve Hilton, IoT for small and medium businesses (SMBs) requirements, 2017. Available from https://www.machnation.com/2017/07/26/iot-for-small-and-medium-business-smb-requirements-and-unified-office-case-study/ accessed on 13th February 2020.

[4] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and regional internet of things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand," *International Data Corporation (IDC)*, May 2014.

[5] D. Shin , An exploratory study of innovation strategies of the internet of things SMEs in South Korea, Asia Pac. J. Innov. Entrep. 11 (2) (2017) 171–189 .

[6] Fernandez, F., & Pallis, G. C., Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on* (pp. 263-266). IEEE.

[7] R. Ramakrishnan , L. Gaur , Smart electricity distribution in residential areas: internet of things (IoT) based advanced metering infrastructure and cloud analytics, in: Proceedings of the International Conference on Internet of Things and Applications (IOTA), Pune, 2016, pp. 46–51 .

[8] G. Ghatikar , Internet of things and smart grid standardization, Internet of Things and Data Analytics Handbook, Wiley Telecom, 2017, p. 816

[9] Bhide, VishwajeetHari, and SanjeevWagh. "ilearning IoT: An intelligent self-learning system for home automation using IoT." Communications and Signal Processing (ICCSP), 2015 International Conference on. IEEE, 2015.

[10] Gonzalez-Martínez, J., Bote-Lorenzo, M., Gomez-Sanchez, E., and Cano-Parra, R.: 'Cloud computing and education: A state-of-the-art survey', Computers & Education, 2015, 80, (2015), pp. 132-151

[11] Prifti, L., Knigge, M., Kienegger, H., & Krcmar, H., A Competency Model for "Industries 4.0" Employees. 13th International Conference on Wirtschaftsinformatik, 2017.

[12] Pan G, Qi G, Zhang W, et al., Trace analysis and mining for smart cities: issues, methods, and applications. *Communications Magazine*, IEEE 2013, 51(6), 120-126

[13] J. Moore , Predators and prey: a new ecology of competition, Harv. Bus. Rev. 71 (3) (1993) 75–86 .

[14] O. Mazhelis , E. Luoma , H. Warma , Defining an Internet-of-Things ecosystem, in: S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networking. ruSMART 2012, NEW2AN 2012, Springer, Berlin, Heidelberg, 2012 Lecture Notes in Computer Science, Vol 7469 .
[15] Amit, R., & Zott, C., Value creation in e□business. Strategic management journal, 22(6□7), 493-520, 2001.
[16] Lee In, The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things (7): 10078, (2019) pp. 2542-6605 https://doi.org/10.1016/j.iot.2019.10 0 078
[17] A. Bröring , S. Schmid , C. Schindhelm , A. Khelil , S. Kabisch , D. Kramer , D. Le Phuoc , J. Mitic , D. Anicic , E. Teniente , Enabling IoT ecosystems through platform interoperability, IEEE Softw. 34 (1) (2017) 54–61 .
[18] Omar Valdez-de-Leon, Key Elements and Enablers for Developing an IoT Ecosystem, May 17 2017 available at
[19] G. Gardaševi ´c , M. Veleti ´c , N. Maleti ´c , D. Vasiljevi ´c , I. Radusinovi ´c , S. Tomovi ´c , The IoT architectural framework, design issues and application domains, Wirel. Person. Commun. 92 (1) (2017) 127–148.
[20] K.J. Singh , D.S. Kapoor , Create your own Internet of Things: a survey of IoT platforms, IEEE Consum. Electron. Mag. 6 (2) (2017) 57–68.
[21] Y. Sun , H. Yan , C. Lu , R. Bie , P. Thomas , A holistic approach to visualizing business models for the Internet of Things, Commun. Mob. Comput. 1 (1) (2012) 1–7 .
[22] H. Lee , D. Sin , E. Park , I. Hwang , G. Hong , D. Shin , Open software platform for companion IoT devices, in: Proceedings of the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2017, pp. 391–392 .
[23] Elisa Bertino. 2016. Data Security and Privacy in the IoT. Keynote Summary, *Proceedings of EDBT 2016.* Colin Boyd. 2003. Protocols for Authentication and Key Establishment. In *Information Security and Cryptography*, Springer
[24] M. Popescu, D. Dumitriu and M. Helfert, Adoption, Architecture and Technology of Enterprise IoT Systems – Towards a framework of concerns in IoT environment. Irish Conference on Aritificial Intelligence and Cognitive science, Dublin, 2017
[25] Wu, M., Lu, T., Ling, F., Sun, J., Du, H.: Research on the architecture of internet of things. In: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE (2010)
[26] A. Al-Fuqaha , M. Guizani , M. Mohammadi , M. Aledhari , M. Ayyash , Internet of Things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376 .
[27] I. Mashal, O. Alsaryrah, T.Y. Chung, C.Z. Yang, W.H. Kuo, D.P. Agrawal Choices for interaction with things on internet and underlying issues ad hoc networks, 28 (2015), pp. 68–90
[28] D. Darwish , Improved layered architecture for Internet of Things, Int. J. Comput. Acad. Res. 4 (4) (2015) 214–223 .
[29] S. Madakam , R. Ramaswamy , S. Tripathi , Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (5) (2015) 164–173.
[30] P. Sethi , S.R. Sarangi , Internet of Things: architectures, protocols, and applications, J. Electr. Comput. Eng. 2017 (2017) 9324035
[31] Demil, B., & Lecocq, X., Business model evolution: in search of dynamic consistency. *Long Range Planning*, *43*(2), 227-246, 2010.
[32] Onetti, A., Zucchella, A., Jones, M. V., & McDougall-Covin, P. P., Internationalization, innovation and entrepreneurship: business models for new technology-based firms. *Journal of Management & Governance*, *16*(3), 337-368, 2012.
[33] https://www.ibm.com/developerworks/cloud/library/cl-grush-smart-toothbrush-bluemix-trs/index.html
[34] Zott, C., Amit, R., & Massa, L., The business model: recent developments and future research. Journal of management, 37(4), 2011, 1019-1042.
[35] Teece, D. (2010). Business models, business strategy and innovation. Long Range Planning, 43 (2-3): 172 – 194.
[36] Ahokangas, P., Juntunen, M., & Myllykoski, J., Cloud computing and transformation of international e-business models. A Focused Issue on Building New Competences in Dynamic Environments (Research in Competence-Based Management, Volume 7) Emerald Group Publishing Limited, 2014, 7, 3-28.
[37] Morris, M., Schindehutte, M., & Allen, J., The entrepreneur's business model: toward a unified perspective. *Journal of business research*, *58*(6), 726-735, 2005.
[38] Ahokangas, P., Atkova, I., Moqaddamerad, S., & Juntunen, M. (2015). Bringing futures thinking to business model innovation.
[39] Ahokangas, P., Juntunen, M., & Myllykoski, J., Cloud computing and transformation of international e-business models. *A Focused Issue on Building New Competences in Dynamic Environments (Research in Competence-Based Management, Volume 7) Emerald Group Publishing Limited*, *7*, 2014, 3-28.
[40] Julius F. G. Future business models of an internet of things (ioT) enabled healthcare sector. A master thesis submitted to the department of management and International Business, Oulu Business School, University of Oulu, 2015
[41] M. Dubosson-Torbay , A. Osterwalder , Y. Pigneur , E-business model design, classification, and measurements, Thunderbird Int. Bus. Rev. 44 (1) (2002) 5–23.
[42] Chang, V., and Wills, G.: ‘A University of Greenwich Case Study of Cloud Computing –Education as a Service’: ‘E-Logistics and E-Supply Chain Management: Applications for Evolving Business.’ (2013), pp. 232-244
[43] R. Savjani 5 things to consider before choosing an IoT platform company (2017). Available from https://www.softwebsolutions.com/resources/ IoT- platform-company.html