Problems in Adopting Middleware for IoT : A Survey

Marcos Gregório, Roberto Santos, Cléber Barros and Geiziany Silva
CESAR – Recife Center for Advanced Studies and Systems
Recife, Brazil
e-mail:{demarcosluiz, robertosf90, cleberbarros.ti, geiziany.mendes}@gmail.com

***Abstract* – In this paper, we present initial concepts of Internet of Things (IoT), whose technology combines Internet and day-to-day objects. We present, as well, the concept of middleware, which is a piece of software that connects software and hardware. After studying several scientific publications, we cover and analyze problems and challenges identified in the implementation of middleware for IoT. Applying knowledge acquired from these documents, we list the principal, recurring problems in adopting middleware for IoT, presenting and describing these problems in detail. Finally, we conclude on how these problems can affect and harm the adoption of middleware for IoT.**

Keywords: Internet of Things; Middleware; Heterogeneous network.

I. INTRODUCTION

The term "Internet of Things" was possibly introduced in 1999, during a lecture delivered by the British innovator Kevin Ashton at Procter & Gamble (P&G) [1]. According to Ashton, computers are very dependent on humans. His idea is that "things" could generate information without needing a human being. He claims that this would bring many benefits to the industry and to humanity, such as, increased information extraction, increased productivity, reduced losses in the energy economy, improvements in security and education, and much more.

In the IoT environment, we have heterogeneous devices and networks. These differences, as well as the complexity, may potentially increase with new technologies. The middleware for IoT facilitates the use of these devices and takes into account their heterogeneity to protect the software from the changes that would be needed to adapt to each device the software is connected to [2]. The IoT changes the way that we understand the world, using sensors to continuously monitor the environment around us, providing more information about traffic, weather, health, fleet management, vehicle control, allowing the Information Systems to provide value-added information for every single person.

The adoption of middleware helps to avoid some common problems in IoT development, such as:

- Hides the heterogeneity of hardware components, operation systems and communication protocols
- Interconnects parts running in distributed locations
- Provides uniformly high level of standard interfaces for developers and application integrators, making these applications easy to build, reuse and inter-operate
- Provides a set of common services to perform various general purpose functions, avoiding repeated efforts of the developing team [3]

However, in spite of the benefits, the adoption of middleware for IoT also brings problems. This paper presents a vision of the most common problems in adopting middleware for IoT based on the work done by different authors.

The rest of the paper is structured as follows. In Section II, we present an overview of the main concepts of IoT. In Section III, we present a review of the concepts related to middleware. In Section IV, we present the most common problems when middleware is adopted in IoT development. Finally, Section V presents the conclusion and final considerations.

II. INTERNET OF THINGS

Internet of Things is a new technology that is growing and gaining prominence. Every year several new devices are developed and software is applied to this new concept. However what is IoT and when did this term appear?

IoT is a technological revolution that has been growing increasingly since 2009. The tendency is to last for much greater time [4]. Even so, according to IDC, by the end of 2020, there will be somewhere around 30 billion devices connected to the IoT world and the IoT market will see an elevation of approximately seven billion dollars [5].

As previously mentioned, IoT is a new way to use applied technology in devices and applications, which allows for communication between day-to-day objects (e.g. washing machines, refrigerators, air conditioning units) to the Internet, for the purpose of supplying access to real-world information. [6].

IoT can also be defined as a dynamic global network infrastructure with auto-configuration capabilities based on standard communication protocols, which are inter-operable and virtual, in which things have physical attributes and virtual personalities use intelligent interfaces being seamlessly integrated into the information network [7].

IoT has the ability to contribute to society by better integrating devices and people, because the amount of

 ISBN: 978-1-61208-505-0

information made available by IoT is enormous, and based on this information decisions that will bring benefits to the entire world population can be taken.

Figure 1. Connection between "things" using the Internet [7]

Figure 1 illustrates all connections between "things" with the Internet. Another feature of IoT is that it allows things and people to be connected anywhere, anytime, with anything or anyone.

As mentioned above, IDC says that in the coming years, there will be over 20 billion devices. Because of that immense amount and variety of devices, they will vary according to their physical characteristics, features and manufacturers. This enormous diversity causes the IoT to be seen from different viewpoints [8].

The differences in these viewpoints refer mainly to the differences between developers of devices, specifically everyday objects. From the point of view of the developer, this is owing to the fact that each developer has his or her favorite programming language, and, as is well known, each language has special features. In order to abstract the language and the complexity that the developer used to access the service provided, one of the best solutions is to use the middleware.

III. MIDDLEWARE

Middleware is a layer or set of software sub-layers interposed between levels of operational and communicative application [9]. The middleware has several features, the primary being to hide details from different technologies, protocols, network environments, data replication, and parallelism. Another feature of middleware is to exempt the programmer from issues that are not directly linked to final application, because middleware masks the heterogeneity of computer architectures, operating systems, programming languages, and network technologies [10]. In other words, middleware acts as the glue. The goal is to connect different systems, abstracting the diverse heterogeneous hardware components, operating systems and communication protocols, as well as to provide an immense amount of interfaces for developers to integrate the final application.

In recent years, middleware obtained greater importance in its use. Deuged says that this is due to the fact that the middleware simplifies the development of new services, old integrations, and new technologies [11].

Companies and business corporations are increasingly using middleware as a solution for connecting their old systems. Because their applications are old and often inherited, the integration of new systems becomes totally impractical financially, and integration is often prohibited due to several factors, for example, to ensure data security. Proper functioning of the features is one of the most important motives that prohibit the integration. However, with the use of middleware, the integration with the different departments and systems becomes easier and its cheaper maintenance [10].

The future of the IoT will consist of a variety of sensors connected to a network that will store all information for all users [10]. The article says, as well, that the IoT must be supported by middleware that enables consumers and IoT developers to interact in a friendly manner.

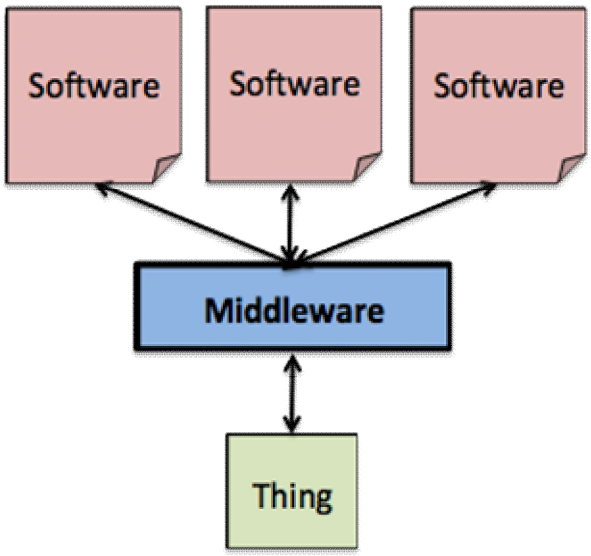

Figure 2. Interaction between software and things using middleware [12]

Figure 2 illustrates how the IoT works with middleware. The idea is that middleware will support a lot of different software and allow for connection with "things."

However, even with all these features and benefits, using middleware with the IoT may present some challenges, such as inter-operability, scalability, abstraction, spontaneous interaction between "things," distributed infrastructure, security, privacy, and variety of middleware types [10].

Regarding the problems cited above, the proposed article focuses on citing the main problems in the use of the IoT

 ISBN: 978-1-61208-505-0

with middleware. The problems and difficulties listed in this article result from studies conducted by researchers.

IV. PROBLEMS/DIFICULITIES WITH MIDDLEWARE FOR IOT

A. *Security problems in IoT plataforms*

Everything indicates that the IoT will have a great impact on humanity because of the fact that it uses objects from our everyday lives. Despite all the benefits that can be gained with this technology, one topic that demands a lot of attention is security in the IoT. This security problem has even been the subject the BlackHat and DEFCON conference on issues related to hacking [13].

In a report published by [14], 70% of the IoT devices are vulnerable to attack. The study was based on the top ten devices most currently used. It found 250 flaws [15]. On average, 25 vulnerabilities were found per each device tested. The top vulnerabilities highlighted were:

- Privacy concerns
- Insufficient authorization
- Lack of transport encryption
- Insecure web interface
- Inadequate software protection

The following scenario illustrates how complicated the problem is: suppose a person is driving his or her car and suddenly, without receiving the driver's command, the steering wheel turns alone and the driver loses control of the car, causing a serious accident. This situation may eventually become reality, as hackers recently broke into a state-car system and took full control of direction [16]. In addition, other functions may be affected in the event of an invasion in the car system, such as turning off the seatbelts or triggering the airbag. Research also suggests that the traditional platforms of Web and data networks may suffer from Denial of Service (DoS) attacks.

A major concern in the development of middleware for the IoT has been to try to avoid security problems and data theft, seeing that the IoT does not refer only to computers, but also to multiple devices, "things," which eventually will be exposed to attacks.

A survey of low-level protocols to ensure security and privacy in centralized and distributed scenarios of IoT is presented in [17], and the research community aims to improve the protocols constantly in order to address these security challenges.

In [18] an analysis and review of available platforms for IoT and a vision regarding security and privacy are presented.

As seen above, the negative impacts caused by this problem lead to one of the primary reasons that security problem in IoT should be looked into with caution and care.

Middleware developers need to be attentive to this major concern as regards the creation of new platforms for IoT. The lack of well-defined protocol security could jeopardize the advances in IoT and adoption by companies and users [31]. A security barrier can be imposed based on the limitations of the infrastructure of IoT itself, which still needs to evolve in this direction so that it can have a more solid basis for the possibility of more robust implementations.

Figure 3 shows that security has different levels of complexity and scale in the case of security and privacy [19]. This article does not aim to explain in detail the greater security as a whole, but it is important to show that IoT security needs to be studied and analyzed with great care and attention, because, as previously explained, any error or security problem would cause the device in question to be discontinued, or, in worse cases, the company that developed the device could suffer loss or lawsuit.

Figure 3. The five primary reasons that cause IoT security vulnerabilities [19]

B. *Support of application developers*

It is known that the IoT is growing quite, as previously stated, and the number of devices is predicted to reach alarming numbers in 2020. In order to promote a greater increase and acceleration in the development of devices, IoT applications should have middleware with simple APIs for the desired features, preferably with high levels of abstraction. Moreover, these APIs should be developed and made available in a standard way, as far as possible, so that the development of new applications and devices will be more efficient and effective [18].

Mineraud says that most IoT platforms currently offer a public API to use services. According to the same, the APIs are generally based on RESTful principles allowing the use of common operations, such as: PUT, GET, PUSH, or

 ISBN: 978-1-61208-505-0

DELETE. These four operations provide support and interaction of devices connected to the platform. But not all platforms include the REST API to help and facilitate the development of web services [18].

To mitigate the above problem, many platforms provide open source libraries to carry out the connections of different programming languages to the APIs available in the middleware. Mineraud is still more emphatic in stating that these links do not make a significant improvement on developer support, seeing that these libraries offer only basic functions such as access keys [18].

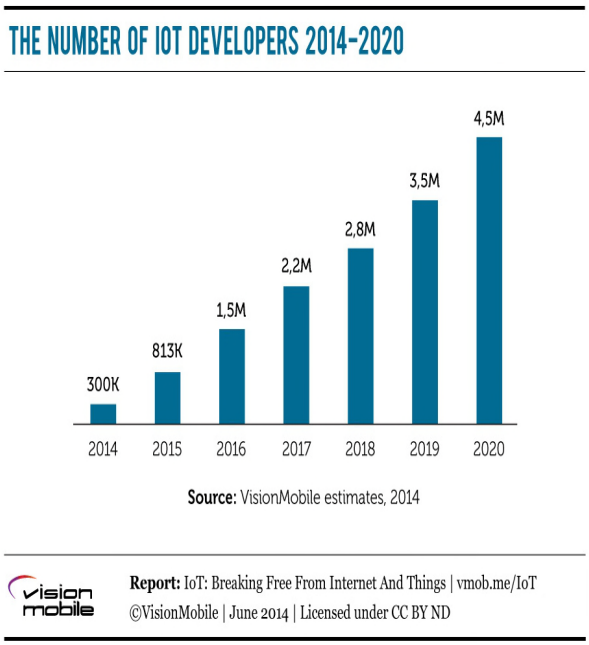

Figure 4. Number of IoT developers [30]

Figure 4 shows that the number of IoT developers is constantly growing, which means that application developer support is more complicated, because the problem affects not only the larger growth of IoT devices, but also the larger growth of IoT developers.

Finally, Mineraud concludes by starting, "We believe that this approach should be more generalized within IoT solutions to maximize usability of the services provided by the IoT platforms."[18]

C. *Processing and data sharing*

The volume of data used in IoT platform tends to be large, and the applications typically present requirements which need to be met in real time. This volume of data presents a stream of unlimited data, which often varies according to time. Because of this variability, data can be unreliable and incomplete, and there is not a desirable quality and information regarding communication loss account [20]. It is also worth mentioning that this data is represented in various shapes and models. The example is a great challenge to use directly the low-level data that the sensors of the devices generate without having a data model and knowledge.

The information and knowledge behind the data collected are the core and basis of the wealth produced by IoT. Therefore, the processing devices and data sharing must be developed to ensure that the data captured by the IoT can be used in various applications. Today, IoT solutions do not support processing and data sharing in a dynamic format. However, it remains possible to combine multiple simple applications in a dynamic format, provided that the URI to the source of the desired information is known. However, it represents a very challenging technique for application developers and platforms IoT [21].

The Ericsson IoT framework provides mechanisms for virtual integration that can be combined with dynamic sites to analyze statistical data. Furthermore, different techniques of processing and data sharing are adapted for IoT. According to Tsai et al. [22], mining technology research data for the IoT try to improve the processing and sharing of large data stream generated by IoT devices.

D. *Privacy concerns*

Many IoT devices collect personal information such as name, address, date of birth, health information, and even credit card numbers. Those concerns are multiplied when one adds in cloud services and mobile applications that work with the device [23]. Too much personal information is collected, and it is very common that this information is not properly protected. In the end, users are not given the choice to allow what type of data will be collected.

According to The Open Web Application Security Project (OWASP) [24], in order to verify if the IoT device has privacy concerns, it is necessary to determine the following:

- Whether all data types that are being collected by the device are identified,
- Whether the device and its various components collect only what is necessary to perform its function,
- Whether identifiable information can be exposed when not properly encrypted while at rest on storage mediums and during transit over networks,
- Who has access to personal information that is collected,
- Whether data collected can be de-identified or anonymized,
- Whether data collected is beyond what is needed for proper operation of the device and whether the end-user has a choice for this data collection,
- Whether a data retention policy is in place.

An IoT device can ensure the privacy concerns by minimizing the data collection, anonymizing the collected

 ISBN: 978-1-61208-505-0

data or giving the end user the ability to decide what data is collected [25]

E. Integration detection technologies and activation

The essence of the IoT platform is to establish a connection detecting and triggering heterogeneous systems with different capabilities and limitations. In the absence of a common standard of communication and detection, different suppliers become accustomed to the vice of writing and implementing their own interaction patterns and implement different sets of communication protocols. Thus, the IoT platform ends up having multiple and different protocols available. Unfortunately, as a result, IoT platform value has increased. This increase grows proportionally with the amount and versatility of the devices supported by the platform. An ideal platform for IoT must provide a group or set of protocols for communication that are standardized and thus every device 'manufacturer can choose the set of protocols that best adjustment in the device.[27]

For a quiet and harmonious integration with detection and actuation of IoT devices, it is essential to define standardized protocols for all devices, for example, in the manner done today with constrained devices by IEFT [27] and communications ETSI M2M and 3GPP [28]

However, the current solutions found for IoT bring a different approach to the issue of different devices. Usually the question of interoperability with others devices in IoT is guaranteed through the implementation of a gateway, which usually features an expanded capacity with the help of plug-ins that make it possible to support new devices in a IoT platform, thus not featuring a standardization of protocols. In order to accelerate integration of new pattern models devices, such as those recommended in the Smart Objects Guidelines [29], they should be integrated in a broad and systemic way [30].

V. CONCLUSION AND FINAL CONSIDERATIONS

The IoT presents numerous benefits to consumers and has the potential to change the ways that people interact with technology.

After a brief explanation of IoT and middleware this survey proposes to clarify the difficulties in adopting middleware for IoT development.

From all exposed difficulties and problems in this research, we realize that the security problem in IoT platforms, presented in section 4, is the difficulty that requires the greatest attention from the IoT developers. Software for IoT involves distribution and data sharing, thus increasing the risks of data theft.

From a security and privacy perspective, the introduction of sensors and devices into currently intimate spaces such as the home, the car, wearable objects, or everyday things to detect and share observations about us increasingly deserves special attention and concern.

There is no denying the utility of middleware assists IoT development, but we have to be aware of some concerns about the difficulties and problems that this survey covers in its study.

For future researches, there is good opportunity to apply solutions to all problems listed above or, perhaps, to choose security as the problem most relevant to the use of middleware for IoT.

REFERENCES

[1] K. Ashton, That 'Internet of Things' Thing [Online]. Available from: http://www.rfidjournal.com/articles/view?4986 2016.08.11

[2] Z. Shirin, Middleware for Internet of Things, University of Twente, November 2013

[3] K. Sacha, "Introduction to Middleware", 2003. Available at http://middleware.objectweb.org/index.html. 2016.08.11

[4] IDC, Worldwide Internet of Things (IoT) 2013-2020 Forecast: Billions of Things, Trillions of Dollars, October2013.

[5] IDC, Worldwide Internet of Things Spending by Vertical Markets 2014-2017Forecast, February 2014.

[6] P. Guillemin and P. Friess, "Internet of things strategic research roadmap," The Cluster of European Research Projects,Tech., September 2009, Available at http://www.researchgate.net/publication/267566519_Internet_of_Things_Strategic_Research_Roadmap 2016.08.10

[7] X. Feng, T. Y. Laurence, W. Lizhe and V. Alex., Internet of Things

[8] L. Atzori and A. Iera, G. Morabito, The Internet of Things: A Survey, Computer Networks., , p.2787-2805, October, 2010

[9] C. Aércio, A. Carlos and F. Ana Paula, "A Study on Middleware for IoT," International Conference on Internet Computing. Athens., pp.32-37, 2016.

[10] C.D Igill and W.D. Smart, Middleware for robots? In: AAAI Spring Symposium on Intelligent Distributed and Embedded Systems. Stanford Proceedings. Stanford:2002

[11] S. De Deugd, R. Carroll, K. Kelly, B. Millett and J. Ricker, SODA: service oriented devide architecture, IEEE Pervasive Computing., pp. 94-96, 2006

[12] M. Koster (2014, May 28). Design Patterns for an Internet of Things [Online]. Available from: https://community.arm.com/groups/internet-of-things/blog/2014/05/27/design-patterns-for-an-internet-of-things 2016.08.11

[13] P. McMillan (2014, Aug 7). DEFCON [Online]. Available: https://defcon.org/images/defcon-22/dc-22-presentations/Mcmillan/DEFCON-22-Paul-Mcmillan-Attacking-the-IOT-Using-timing-attacks.pdf 2016.08.11

[14] D. Miessler. (2014, Jul 7) [Online]. Available: http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284 2016.08.11

[15] N. Dhanjani (2014). Abusing the Internet of Things [Online]. Available: https://www.blackhat.com/docs/asia-14/materials/Dhanjani/Asia-14-Dhanjani-Abusing-The-Internet-Of-Things-Blackouts-Freakouts-And-Stakeouts.pdf 2016.08.11

[16] NIC Videos (2014, jan 7) What is IPV6. [Online] Available: https://www.youtube.com/watch?v=_JbLr_C-

HLk&list=PLQq8-9yVHyObGmdqA-aD_QaLrZaC_tkOI 2016.08.10

[17] R. Roman, J. Zhou and J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279, towards a Science of Cy- ber Security and Identity Architecture for the FutureInternet. doi:http://dx.doi.org/10.1016/j.comnet.2012.12.018. URL http://www.sciencedirect.com/science/article/pii/ S1389128613000054 2016.08.10

[18] Mineraud, Julien, et al. "A gap analysis of Internet-of-Things platforms." arXiv preprint arXiv:1502.01181 (2015).

[19] S. Schuermans and M. Vakulenko (2014, Jun 26). IoT: Breaking Free From Internet and Things [Online] Availabre from: http://www.visionmobile.com/blog/2014/06/who-will-be-the-ios-and-android-of-iot 2016.08.11

[20] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future di- rections, Future Generation Computer Systems 29 (7) (2013) 1645–1660. doi:10.1016/j.future.2013.01.010. URL http://dx.doi.org/10.1016/j.future.2013.01.010

[21] A. Maarala, X. Su and J. Riekki, Semantic data provisioning and reasoning for the internet of things, in: Internet of Things (IOT), 2014 International Conference on the, 2014, pp. 67–72. doi:10.1109/IOT.2014.7030117.

[22] C.-W. Tsai, C.-F. Lai, M.-C. Chiang and L. Yang, Data mining for internet of things: A survey, Communications Surveys Tu- torials, IEEE 16 (1) (2014) 77–97. doi:10.1109/SURV.2013. 103013.00206.

[23] Internet of things HPE Security Research Study, Craig Smith and Daniel Miessler, HPE Fortify, June 2014

[24] OWASP. (2016, Feb 5) Top 10 2014-I5 Privacy Concerns [Online]. Available: https://www.owasp.org/index.php/Top_10_2014-I5_Privacy_Concerns 2016.08.10

[25] H. Kate et al. OWASP IoT Top Ten Infographic avaliable at https://www.owasp.org/images/8/8e/Infographic-v1.jpg 2016.08.10

[26] C. Bormann, A. Castellani and Z. Shelby, CoAP: An application protocol for billions of tiny internet nodes, IEEE Internet Com- puting 16 (2) (2012) 62–67. doi:10.1109/MIC.2012.29.

[27] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. d. Abeele, E. D. Poorter, I. Moerman and P. Demeester, IETF stan- dardization in the field of the Internet of Things (IoT): A survey, Journal of Sensor and Actuator Networks 2 (2) (2013) 235–287. doi:10.3390/jsan2020235.

[28] T. Klinpratum, C. Saivichit, A. Elmangoush and T. Magedanz, To- ward interconnecting M2M/IoT standards: interworking proxy for IEEE1888 standard at ETSI M2M platform, in: The 29th International Technical Conference on Circuit/Systems Com- puters and Communications, 2014

[29] IPSO Alliance, Ipso smartobject guideline, Tech. rep., Internet Protocol for Smart Objects (IPSO) Alliance (2014). URL http://www.ipso- alliance.org/ technical-information/ipso- guidelines 2016.08.10

[30] S. Satyadevan, B. Kalarickal and M. Jinesh, Security, trust and implementation limitations of prominent iot platforms, in: S. C. Satapathy, B. N. Biswal, S. K. Udgata and J. K. Mandal (Eds.), Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Vol. 328 of Advances in Intelligent Systems and Computing, Springer International Publishing, 2015, pp. 85–95. doi:10. 1007/978- 3- 319- 12012- 6_10.

[31] R. Roman, J. Zhou and J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279, towards a Science of Cy- ber Security and Identity Architecture for the Future Internet. doi:http://dx.doi.org/10.1016/j.comnet.2012.12.018. URL http://www.sciencedirect.com/science/article/pii/ S1389128613000054 2016.08.12

 ISBN: 978-1-61208-505-0