Management Capabilities for Mobile and IoT Devices: An Evaluation Framework

A. Achtaich, R. Mazo, N. Souissi, C. Salinesi, O. Roudies

Abstract*—recent experienceindicates that mobile and connected devices are increasingly becoming a key enabler of advanced services and applications. Specifically in the case of the enterprise, they represent a land of opportunities to grow in efficiency and quality with reduced costs and time-to-market. However, mobile and IoT also exposes enterprises to new challenges, such as security and safety risks, scale, heterogeneity, resources constraints, or context fluctuations. This paper introduces an evaluation framework that elicits the needed capabilities to enroll, control, and manage mobile and IoT devices, towards properly integrating them with the organization workflow, in accordance with internal policies. To demonstrate the usability of the framework, the paper presents a comprehensive review of Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) solutions. A preliminary evaluation is conducted with various companies to prove the framework's relevance, ease of use and completeness.

***Index Terms*—IoT, mobile devices, enterprise, management capabilities, requirements, framework, security, BYOD.**

I. INTRODUCTION

The Internet of Things [1] is a land of opportunity for believers and supporters of the Connected Enterprise. Experience already shows that smartphones, smart appliances, wearables, sensors and actuators can be brought together to deliver advanced services to customers, partner institutions, and actors of the enterprises themselves. The software applications behind these services allow basic operations like controlling a product lifecycle from the producer all the way to the customer, to more complex ones like starting the car when the smartphone of the employee is close or preparing the conference room for a meeting by turning on the lights, opening the curtains, and lunching the appropriate presentation. The IoT is also a big source of data. The volume of services, the amount of data, and the given opportunities provided by the IoT continue to grow. However risks and difficulties expand at the same time too. When implementing IoT strategies, enterprises are confronted with new management challenges. On the one hand, because of their mobile nature, IoT devices require special attention: access to IoT nodes shall be secured, the use of constrained resources optimized, heterogeneous devices shall be able to communicate, access to shared confidential content and applications shall be controlled and the state and usage of devices monitored.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Achtaich*, Univ. Mohammed V- Rabat, Emi, Siweb Team - Rabat, Morocco.
R. Mazo, GIDITIC, Universidad Eafit, Medellin,, Colombia
N. Souissi, ENSMR, Département Informatique - Rabat, Morocco
C. Salinesi, CRI, Université Panthéon Sorbonne, Paris, France
O. Roudies, Univ. Mohammed V- Rabat, EMI, SIWEB Team - Rabat, Morocco.

On the other hand, connected devices come in very large number and diversity, they are constantly solicited, and they can be physically present everywhere. With 6.4 billion objects connected in 2016, and a market value estimated to grow up to $4 billion in 2019 [2], managing IoT becomes a distinctive challenge, and for the enterprise, a real and critical concern. Therefore, adopting a platform with unique specifications to manage the fleet of mobile and connected devices is needed. It is thus quite important to understand the main capabilities that such solutions shall provide, while taking into account the specific circumstances of each enterprise.

Hence, the contribution of this paper consists in an evaluation framework that elicits the main capabilities which should be provided for the management of a fleet of connected devices. The purpose of the framework is to be used as a guidebook to assist organizations and practitioners with the specification of capabilities of a fleet management solution or with the evaluation of existing ones. Furthermore, the paper illustrates the use of the framework through a detailed example, by confronting 4 Enterprise Mobility Management (EMM) suits and Unified Endpoint Management (UEM) suits with the proposed framework.

The evaluation framework was preliminary evaluated through a survey that included the participation of large scale companies. The evaluation validated the concerns related to the personal use of mobile and IoT devices in the enterprise, and proved the relevance, the diversity and the completeness of the capabilities elicited in the framework.

Section 3 describes the research methodology followed in this paper. Section 4 introduces the opportunities brought by mobile and IoT use in the enterprise, as well as the risks it entails. Section 5 presents the evaluation framework, which describes the main capabilities that should be considered for mobile and IoT management. Section 6presents the leading EMM and UEM platforms. Section 7 presents the results of the comparative study. Section 8 summarizes the results of the preliminary evaluation, before concluding in section 8.

II. RELATED WORK

The management of mobile and IoT devices, in the special case of the enterprise, is a topic that has only been tackled few times in the literature. Secondary studies are especially rare to find.Concerning mobile management, K. Heinrich and K. Gerhard[3] defined in their book the main aspects related to mobile managements, introduced security issues, demonstrated the business impact of mobility and evaluated few mobile device management products. In [4], the authors introduced the fundamentals of mobile computing, aswell as some of its management aspects. While authors in[5]display the current status of mobile management related technologies, along with issues and challenges.

With regards to IoT, Oprea, et al. [6] present a map of the main challenges related to the adoption of IoT devices in the enterprise, without much to say about how these issues shall be tackled. Most IoT management related works available are focused on one of the aspects proposed in the framework presented in this paper, like security[7],context-awareness[8], or heterogeneity management[9]. Some contributions were more focused on the evaluation of management aspects of EMM or UEM solutions. For example, in [10], the authors propose a review from a security perspective. They evaluate device management's security capabilities by modeling a threat and applying a security requirements engineering methodology. Also, Disterer & Kleiner[11] discuss organizational issues related to the use of personal devices at work, present technical approaches and propose solutions. Finally, the authors in [12] overview the state of mobile devices security in critical infrastructures, as well as practices and trends in mobile device security including access control, next-generation firewall, Bring you Own Device (BYOD) control mechanism, confidentiality, integrity, and availability.However, to the best of our knowledge, none of the proposals introduces a complete template for manager to build, invesigate or choose the necessery features for a management soluition. Also, nonecollect and analyse the existing functionalities of enterprise mobility and IoT management suits. The available documentation related to this field is mainly composed of white papers, reports or blog posts.

III. METHODOLOGY

As stated in the introduction, the goal of this paper is to propose an evaluation framework of capabilities for the management of fleets of connected devices, for the benefit of engineers and practitioners, willing to implement a management solution within the organization. To reach this goal, the methodology used to collect theoretical data and validate it can be summarized in three phases as follows:

Preliminary phase: In order to elaborate the evaluation framework, brainstorming sessions based on conclusions drawn from the literature [13][14][15][16][17][18] were conducted. In this phase, the selection was restricted to secondary studies, where efforts have already been made to synthesize the main issues around mode and connected device's integration and management, specifically in the enterprise.

Analyze phase: In order to demonstrate its usability, the Framework was used to compare leading Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) solutions. They are designed by the experts in the mobile and IoT field, like VMware, Blackberry, and IBM. Even more, they are widely adopted by companies all around the world, and capitalize on user's constant feedback and assessment. Therefore, in our opinion, they are exhaustive and representative of the most relevant fleet management features. This analysis gives an example of one of the many possible uses of the Framework,

Preliminary evaluation phase: The framework is presented to assess its usability for each of the participant companies.

IV. OPPORTUNITIES AND IMPLICATIONS OF MOBILE AND IOT IN THE ENTERPRISE

Fleets of connected devices are not completely new to the enterprise. As a matter of fact and as Figure 1 illustrates, computers—desktops then laptops—were historically the first devices which integration in the enterprise needed to be managed [19]. More recently, mobile devices delocalized business related activities too by providing remote access to emails, applications and data. New services such as collaborative applications, platforms for real time access and sharing of content and tailored user specific applications are examples of these services. Nowadays, the IoT encompasses all devices that connect to the internet; including desktop and laptop computers, and smartphones, tablets and the like, but also kinds of embedded systems (e.g., sensors and actuators in connected vehicles, buildings, machine tools, containers, etc.). Overall, they create a global infrastructure that enables smart advanced applications at the service of the enterprise. This section demonstrates how the integration of fleets of connected devices has modified the dynamics within the enterprise. It also displays the risks this choice entails. For the sake of originality, we will concentrate on fleets of mobile and IoT devices.

A. Towards Mobile Device Management in the Enterprise

Typically, mobile devices are used in companies to send emails, transfer files, access internal applications, or communicate with team members. For instance, GlaxoSmithKline, a leading company in the healthcare industry, deployed more than 31000 iPads for its consultants in 180 countries to provide access from any location to corporate resources [20]. The integration of such devices in the workplace presents a great opportunity for enterprises. Return on experience indicates that it may increase productivity, efficiency, quality and sales, reduce the time and cost of several operations and improves customer relationships [21]. Nevertheless, an enterprise is a very sensitive environment where mobile device also added a new layer of complexity. First, mobile devices store sensitive confidential data. Being mobile, they move outside the boundary of the company, and thus can be stolen, used by third parties, and therefore data can leak or be disclosed to unauthorized parties and services used non properly. Second, mobile devices are exposed to malware that can reach the whole IT infrastructure and even worst almost any other internal resources, including critical ones. Finally, the unsupervised access to the internal network can cause traffic infiltrations. As a result, managing mobile devices is a critical issue for any enterprise that cares about its safety and business continuity [22].

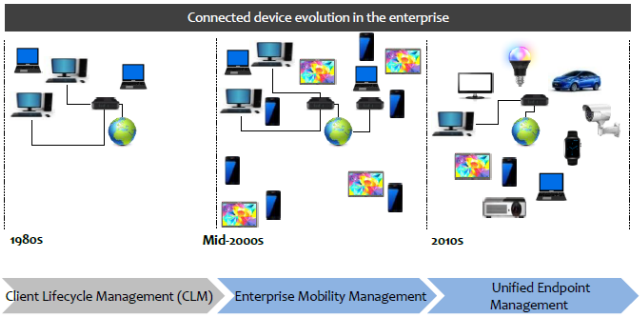

Figure 1: Connected device evolution in the enterprise

B. Towards Unified Endpoint Management in the Enterprise

Today, there is a combinatorial explosion of the number and diversity of connected objects in enterprises, from health monitoring microchips, to distributed vending machines, or distance sensors. But at the same time, connected objects become more and more practical and powerful. As a matter of fact, Gartner indicates that 4.9 Billion objects were connected in 2015 and that this number will be multiplied by 5 in the next four years [23].

An example of use of IoT is the one of Coca Cola's fountain drink dispensers. After witnessing a decline in their fountain drink dispenser market, the Coca Cola lunched the "Coca-Cola Freestyle" [24]. This new kind of connected dispenser, which involves of 3000+ dispensers, consisted in a drink factory that lets customers pick the beverage of their choice, making them more customer-driven, and more efficient.

The IoT opens new revenue to organizations by enabling innovative services through advanced business models, increased efficiency and productivity through real-time insight and maintenance, and saved unnecessary costs through predictive diagnosis and dynamic self-adaptation. Connected objects hold countless amounts of information. Integrating them in the enterprise and connecting them with each other presents enormous business opportunities. However, like mobile devices, incorporating IoT technologies in the framework of the enterprise represents major challenges. The increased demand for the internet jeopardizes the user experience and efficiency. Thus, insuring the availability of services and applications becomes vital to preserve the productivity and quality guaranteed by the enterprise. Security is a major concern for enterprises, since any weak node on a network could compromise the entire infrastructure. Physically compromised connected objects—Stolen or lost—are a primary leak of confidential content, which endanger the enterprise's privacy and reputation.

V. A FRAMEWORK OF CAPABILITIES

Many enterprises witness the fact that employees bring their own devices (BYOD) [11]. Contrary to devices that are purchased and distributed by the companies themselves it is absolutely impossible to control whether these devices are produced by different constructors or operate with various operating systems. Furthermore, IoT devices bring a wider disparity in formats and protocols. However, if BYOD is not prohibited or controlled, and IoT is not standardized, then **communication** in this heterogeneous environment becomes a real issue. Besides, connected devices have limited hardware and software **resources**. Yet, they continuously collect great amounts of data that shall be stored, examined, and processed. This increases the risks of failures, like short memory, low processing and battery depletion. Connectivity is another concern; for most of the operations they handled, connected objects need an internet connexion to synchronize data, download or communicate with other devices.

Remote resource allocation through cloud-computing can eventually solve some resource related issue, but it creates new **security** concerns. Indeed, sensitive data could be victim to malicious activity and at be disclosed to unauthorized users. Security is not a new concern, but it takes a whole new level of complexity now that the number of connected devices has multiplied. A single malware can have a wider scale and impact, especially when the device contains valuable sensitive **data** that should be protected in private containers and encrypted.

Besides, connected objects are context aware; in other words, they are designed to **adapt** their services according to their own perception of their surroundings. Many different kinds of context information can be monitored to achieved that; changes that may occur over time, the performance of the devices and their applications, the interactions between the different stakeholders and the network state.All of these attributes and others should be observed and **monitored**, either to produce reports, when the environment is stable, or to trigger recovery plans or reconfigurations when inconsistencies or exceptions are captured.

Considering the opportunities brought to the enterprise thanks to smart devices, and the risks that it implies, it is crucial for organizations to locate the main sources of challenge, and prepare the necessary tools to control to preserve the stability, security and integrity of the devices and resources.

Therefore, an evaluation framework that elicits the capabilities that should be satisfied for a proper management of a fleet of connected devices was developed. Its ultimate purpose is to be used as a guiding tool to assist organizations with the integration of a fleet management solution, but it can also be of use to build a solution that fits the organization requirements, to evaluate existing proposals or to access its market positioning.

In the following, we identify the capabilities that these solutions should satisfy, to properly supervise the integration of connected devices, depending on the needs of the enterprise.

security, resource management, content management, monitoring and adaptation.

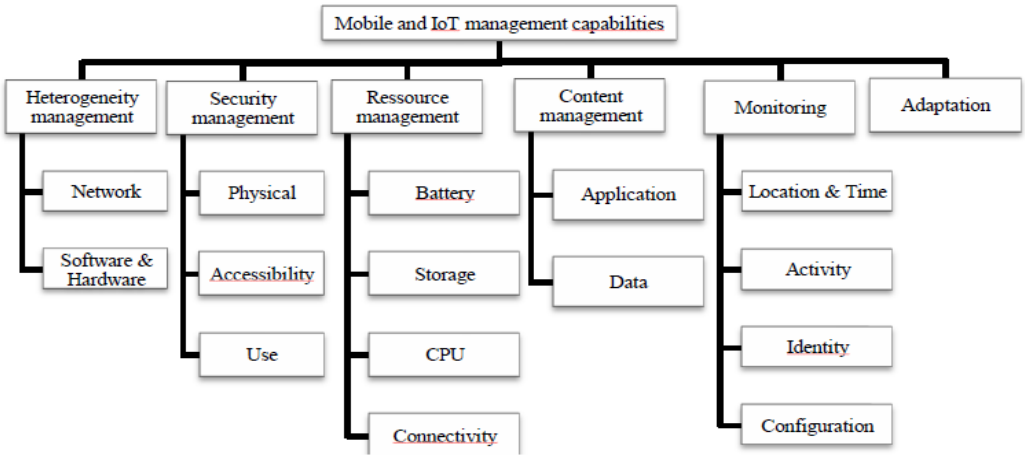

Figure 2: Capabilities that should be insured by EMM and UEM

A. Heterogeneity Management

Connected devices bring a disparity in hardware components, software languages and communication protocols. Therefore, to enable the efficient and seamless interconnectivity of these devices, organizations are now expected to bridge the gap between diverse formats and protocols, with the help of smart gateways and middleware platforms, to provide advanced applications.

Software &hardware: Employees use their personal devices for professional tasks. This includes mobile devices like smartphones or tablets, but also wearables and other sensors. These devices are usually built by different constructors and are meant to be used with various operating systems like Android, iOS, Windows mobile and IoT, Linux, Blackberry, Contiki, LiteOS and RiotOS. Managing interoperability should be a priority for organizations, in order to develop applications that exploit the multitude of available devices, and achieve the promise of IoT.

Network: Connected objects collect and exchange information using different communication technologies. NFC, Bluetooth, RFID and ZigBee are used for short range communications, while GSM, Wi-Fi, or Ethernet, among other technologies, can be used to connect devices in a Local, Metropolitan or Wide area networks. The implications of this heterogeneous environment are a challenge for the enterprise, which should be a concern for the management platform.

B. Security Management

One of the most critical concerns in any company is the security of its computing devices and the confidentiality of its data and information. IoT exposes companies to a whole new level of vulnerabilities, such as unsecured public networks, uncontrolled connections through private networks, malware penetration to the local infrastructure through weak nodes, unrestrained access to corporate data and unauthorized users. It is only a matter of time before hackers locate and exploit vulnerabilities offered by the various entry points offered by the multitude of devices and applications in a corporation network. Guaranteeing the security of devices and their content should thus be a priority.

- **Physical:** Physical security refers to the implementation of the necessary mechanisms and policies that restrict the physical access to mobile or IoT resources. Physical threats can occur either from the user of the device himself, by disclosing confidential data, or from an unauthorized party, who unofficially accessed the device, or stole or found it lost.
- **Accessibility:** Accessibility security refers to the measures put in place to protect organizations from unauthorized or unlawful access to internal resources. These are targeted by cyber-criminals in hopes that the network crashes or who aim for the organization's confidential data or credentials. Illicit access to resources could target:
  - devices, routers or servers to disable the network provider (DoS)
  - IP addresses, MAC addresses or emails, which can lead to identity theft, thereby gaining illegitimate advantages (Spoofing)
  - a collection of devices with the purpose of taking control and distributing malware (Botnets)
  - Confidential data, which can be leaked to public, disclosed to third parties or held for blackmail (Leakage and discloser)
  - Files and documents to alter their content (Change)
  - Bank and accounting credential for a cyber-robbery (Cyber-robbery)
- **Use:** Usage security aims to protect organizations from a wrongful manipulation of a connected device. Whether it is for professional or personal purposes, users usually connect to external servers through an internet access. These resources are prone to contain malicious software, which could infiltrate and infect the private network of the organization.

Another misuse of connected devices is the alteration of the installed software or OS, by installing applications that have a direct impact on the OS's settings, or by deleting those responsible for usage regulations, which are intrinsic to the operating system.

C. Resource management

Connected devices are highly solicited, and generate a large amounts of data. Some of which is latency sensitive, and other might require heavy processing and analysis. However, low processing capabilities, short memory, small space storage and battery depletion are among the many intrinsic features of these same devices. A reasonable compromise between efficient usage and profitable resource management should be determined by a supervision platform.

- **Battery drain:** The majority of connected devices are powered by batteries, thus monitoring their state is crucial for service durability. Delivering optimal battery life, while reducing power consumption, is the main concern of enterprises in terms of battery management.
- **Storage:** Computers, smartphones and smart devices continuously generate and collect data of different types. Some of it is large and typically accessed sequentially, like pictures or videos captured by smartphones and other smart devices. Other data is small and unstructured, generally supplied by sensor logs and measures. Smartphones are rather more advanced in terms of storage capacity compared to IoT devices, which may have 4K, 96K or in best cases 256K of memory. Choosing the appropriate storage option and properly managing it is therefore a crucial task for the enterprise to maintain the performance of the fleet.
- **CPU:** While some connected devices preform a limited amount of processing on small sensed data, like it is the case of smart sensors, others handle more considerable streams, and are expected to deliver a high performance capability, which is, for example, the case of mobile and automotive devices. Therefore, in order to fit the performance needed for each specific application, it is essential to be able to configure the processor, by adjusting, reducing or boosting its features. Furthermore, with the help of powerful resources, like cloud platforms and smart gateways [25], connected device's capacities can be empowered. The main challenge lies in allocating the right resource to the right device, all while ensuring the overall performance and energy efficiency.
- **Connectivity:** Devices must be connected to access and share data, synchronize, and communicate with other devices and applications. The IoT depends thus very much on the Internet, even for the most basic operations. However, internet connections are not always guaranteed. This is even true with mobile telecommunication technologies like 3G and 4G, which can sometimes fall short in coverage. To overcome these issues, management platforms should take advantage of internet access when this one is available, with respect to other constraints. On the other hand, other communication mechanisms, like Bluetooth, should be able to sustain objects connectivity, to realize the needed operations.

D. Content Management

Corporate data is precious and very sensitive. Unfortunately, it is sometimes easily accessible via devices when they fall into the wrong hands. Meticulous measures should be taken by the management solutions to regulate access, manipulation and sharing. Furthermore, for mobile devices and wearables, applications are generally distributed via app market places where users can download all kinds of applications, for business and for personal usage. The acquisition of applications should be controlled and the boundaries between personal and professional applications should be clear.

- **Application management**: Application management provides the foundation for industry specific applications and addresses the concerns related to the access, security and control of all applications that run on devices. In order to do so, application management should face the following challenges:
  - providing the organization's specific applications; first by supporting the environment to create and deploy these applications, then by implementing or embracing a marketplace for the distribution and supply, with the help of the user or directly by automatically updating the device;
  - securing user's access to applications, and application's access to internal resources;
  - configuring devices with application related policies;
  - monitoring the activity of applications in order to insure their compliance with the enterprise rules, and their conformity with the rest of the devices in the fleet.
- **Data management:** Data management provides secure storage, access and diffusion of corporate data on a fleet of devices. This module addresses the following:
  - Access to data is a first concern; proper distribution channels and sharing protocols should be carefully and specifically chosen;
  - deploying the policies to secure access, transit and storage of data needs to be put in place in order to restrict illegitimate manipulation of data and separate different types of content; and
  - monitoring the status of the data is substantial to insure consistency and accuracy.

E. Monitoring

Every company has internal policies that define and portray a strict behavioural and functional setup for its employees, including their use of personal devices within the company. In this sense, CIOs and IT managers make sure that devices are constantly monitored to guarantee that they comply with the rules. User activity, device state and connectivity, and environment conditions, are all considered relevant.

- **Location & Time monitoring:** Thanks to embedded sensors, some connected devices like computers, mobile devices, wearables and cars can be traceable, thus determining the location of their owner. Monitoring time and location could enable organizations adjust device configuration depending on the level of trust granted to the location in question, or to a certain time frame.
- **Activity monitoring:** Activity monitoring focuses on analysing the state of the device. Through the embedded smart sensors, the management platforms should be able to detect the surroundings of the user like brightness or temperature, recognize presence, predict user activity from calendar, and even be aware of the behaviour of other devices in the fleet. Furthermore, it should be possible to track usage characteristics, user communication logs, consumption, battery level and so one.
- **Identity monitoring:** To determine the level of trust and the configuration category granted to a device, it should be possible to track any alteration in its identity. Connected device's identity is defined by a list of parameters. First, user identity, if any, which refers to the personal information about users as well as their status and profile group. Then, device hardware characteristics, which include constructor information, embedded sensors, storage capacity, etc. And finally, software identity, which involves supported OS, supported languages, default application, etc.

- **Configuration monitoring:** The management platform should be concerned with the compliance of a configuration in a given context, with the internal policies. Then, amongst the valid configurations that could be applied on a device, chooses the most appropriate.

F. Adaptation

Monitoring the context of connected devices enables the platform to detect when inconsistency occurs. If and when this happens, the management platform should be capable of launching a new configuration, one which corresponds to the new state. In the case of an unauthorized location or time frame, adapting the device consists of blocking certain privileges. In the case of suspicious activity or unauthorized use, the adaptation could lead to a complete shutdown of device access. And finally, if the configuration of the device changes manually, by the user himself, the platform could reset the previous configuration, or propose a new one.

VI. OVERVIEW OF THE APPROACHES

Introduced under the name Mobile Device Management (MDM), **Enterprise Mobility Management (EMM)** platforms emerged in the mid-2000s. EMM organized the use of mobile devices in the professional context. The success of these platforms proved very legitimate since they allowed corporations to better integrate mobile technologies in their IT infrastructure, by applying configurations for groups of users, securing storage, accessing and using corporate information and applications in a consistent way with the rest of the information systems, monitoring the use of resources, and finally producing more reliable activity reports on employees.

Four EMM sub-categories can be distinguished [26]: (1) **Mobile Device Management (MDM)** platforms "support centralized control of an entire fleet of smartphones and other mobile devices by applying and ensuring pre-defined configurations" [27]; (2) **Mobile Application Management (MAM)** platforms secure applications in a container, from which policies and data storage can be provided and controlled [28]; (3) **Mobile Identity (MI)** systems ensure that only trusted registered devices are allowed to access enterprise applications and data [26]. And finally, (4) **Mobile Content Management (MCM)** platforms secure the business content that is stored on mobile devices.

When first introduced, MDM handled mobile devices, content and applications. Later, the three features split to offer independent functionalities under the umbrella of EMM. A consequence was that companies that needed to lock down their documents with policy-based controls opted for MCM only. The same goes for businesses which only concern is managing applications (MAM).

Unified Endpoint Management (UEM) platforms provide a holistic environment to control all end-user devices, including desktops, laptops, tablets, smartphones, wearables and IoT [29]. UEM was first created to fill the gap between client lifecycle management solutions for computers and EMM solutions for mobile devices into one platform. Eventually, the number and diversity of endpoints in the enterprise expended, thus new devices needed to be discovered, monitored and eventually integrated to the company's fleet of devices. Managing vending machines, printers, sensors and wearables requires a broad range of features, sometimes similar to EMM's. Among these new functionalities one can for instances quote: device enrolment, data security, application and content distribution, and device configuration.

In order to understand the contribution of EMM and UEM platforms, the paper focuses on studying the leading solutions, which are considered the most mature, dynamic and qualified to represent the best of EMM and UEM capabilities [29]. The selection includes Airwatch, MobileIron, MaaS360 and BlackBerry® Enterprise Mobility Suite.

Airwatch has been topping the list of Gartner Magic Quadrant for Enterprise Mobility Management Suites for the last 6 years [26]. Besides, it is the world's largest EMM and UEM provider in terms of revenue and Market Share [30]. The company was founded in 2003 and acquired by VMware in 2014 for approximately $1.181B [31].

In 2006, iPhones and Androids had recently been introduced into the workspace, but the market lacked of infrastructure built around these devices to protect data and guarantee a required level of security. **MobileIron** was a pioneer in managing mobile devices, and later, IoT in the enterprise. In the last years, it was ranked best-in-class for its management, security and its operating environment [32], a world leader in mobility services [33] and the fastest growing EMM and UEM vendor [34].

MaaS360 is an IBM platform that provides IT organizations with the necessary tools to monitor and control devices, applications and content. MaaS360 was recognized by several entities for its exceptional IT support [35], and its strong overall performance and ease of use [33].

After merging with Visto, a provider of mobile messaging services for mobile operators, Good Technology, also an expert in email products for mobile professionals [36], converted to managing and securing mobile data and devices in business environments. It has been a **BlackBerry®** company since 2015, and has extended its services in order to cover the broad scope of IoT [37].

VII. RESULTS OF THE COMPARATIVE STUDY

This section reviews the management solutions presented in the previous section according to the framework of capabilities presented above. First, an overview of the main capabilities, as implemented by all solutions, is introduced, then, ina summary of our findings is presented for each solution. The check sign (✓) denotes the support of the capability by a given solution. The uncheck mark (x) denotes lack in the implementation of the capability. And the comment specifies a particular observation about (+strengths) or (-shortcomings).

A. Heterogeneity Management

Management platforms are multitenant and cross platform; they manage the various operating systems used into the corporate environment including Windows, Macs, Linux, Blackberry, iOS, and Android. Some platforms do not support all the major OSs thought. Airwatch and MobileIron do not support Linux, and Blackberry is not compatible with newer versions of Windows and Mac.

Thanks to the components described in Figure 3, notably, Datacentre services, EMM and UEM solutions provide end-to-end integration mechanisms that allow devices to communicate with the IT infrastructure [38][39][40].

Nevertheless, IoT environments are still under development, and every new operating system requires adding specific separated incremental capabilities, which increases the cost and diversity of the overall solution. Only major and mature operating systems like chrome OS [41] or Windows 10 can be supported. Devicesimplementvarious communication technologies. Some of them can directly connect to the internet via Wi-Fi; others rely on mobile telecommunication technologies like 4G, short range communication technologies using Bluetooth of NFC, and some use Z-ware or ZigBee protocols. This heterogeneity, managed partially by the smart gateway –presented in **Figure 3**, complicates peer to peer communications between devices, which is an important basis of collaborative work.

To support communication between the administration interface and devices of different hardware and software characteristics, several components are required:

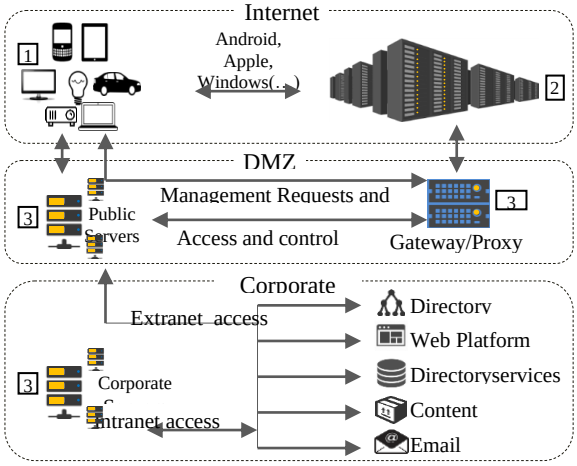

Figure 3: Standard Architecture of EMM and UEM platforms

B. Security

One of the main priorities of UEM and EMM platforms is insuring the security of devices, applications and documents. This goal is partially reached through the distributed architecture of the overall platform represented in **Figure 4** The main components of this architecture are described below.

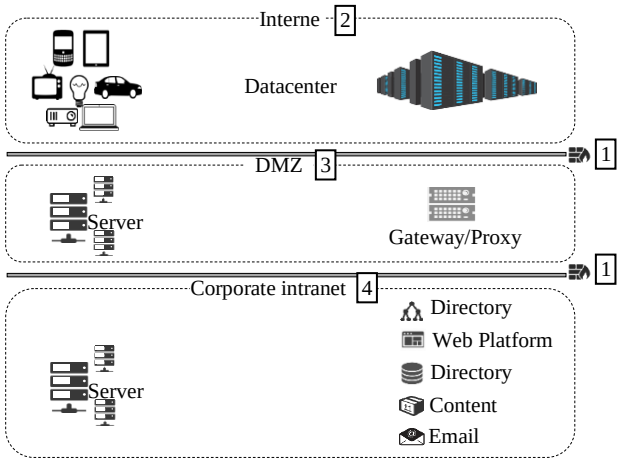

Figure 4 : The Network Architecture of EMM and UEM platforms

C. Resource management

Some of the actions triggered by UEM and EMM solutions take into consideration the state of hardware resources like the battery, the storage or the processing capacity. However, they do now fix the problem of mobile and IoT devices constrained resource. Even more, as reported by customers, the agent application on these devices consumes battery life, internet data, and memory.

D. Content management

A few years ago, the IT infrastructure was strictly composed of devices provided by the company to its employees. Security and confidentiality issues were limited and correctly identified. Today, personally owned devices are allowed to connect to the resources of a company. This new concept added another level of complexity to the management cycle. Also, outside users such as contractors, guests, clients, or other third parties sometimes need to access the corporate resources using their own devices. In this case, content and app control becomes an issue.[42][43].

E. Monitoring

One of the most important assets of using IoT in the enterprise is their ability to collect real-time information. EMM and UEM are aware of this reality. Nevertheless, only basic information is collected, which narrows the field for intelligent services.[44][45].

F. Adaptation

Context information collected from endpoints can trigger simple reconfiguration. MobileIron constrains network access depending on device's current state, (i.e. the running OS, the level of encryption, the applications running on device, etc). Airwatch defines "hot zones" as locations or times where features, content, network access and security settings are adjusted [46]. For multi-user devices, switching from one profile to another leads to a complete reconfiguration, in order to respond to the particular needs of each category of users. Identity checking could also lead to OS or content updates, to redefine application access policies or to launch or block certain battery draining processes. Smart adaptations however are missing in these platforms.

G. Comparatif study

The management platforms depicted above are all leaders, thus, they all cover most of the management aspects that we propose. The diversity of communication protocols is still unmanaged. This is a serious drawback especially in the era of IoT, where devices support various communication protocols, but need to interact nevertheless. EMM and UEM suits do not fix the issues related to limited resources, opposite to that, they are reported to contribute to the drainage of battery, memory and bandwidth. Finally, when compared with the nature and quantity of data that can be collected from devices, the adaptation alternatives offered by the management platform remain very modest. The specificities of each solution can be summarized as follow.

- Airwatch performance in all management aspect is notable, especially for big companies that need to manage a large number of diverse devices, and needs the solution to work hand in hand with the company's existing infrastructure.

- Blackberry offers a comprehensive and modular solution to satisfy the needs of those who want an all-in-one and end-to-end solution, and those who are interested in specific capabilities. Their portfolio includes devices, OS and management platforms. However, the features supported by its native component are richer than the ones proposed across other platforms.
- Compared with other solutions, MobileIron is exclusively focused on mobile and IoT fleet management. Apart from few shortcomings mentioned in Table 1, MobileIron answers the needs of customers who need to manage specific aspects within the company workflow (Docs@work, AppConnect, AppTunne, etc). Among all solutions, MobileIron has been reported to be the most user-friendly, easy to implement and most reactive to O updates.
- IBM MaaS360 offers its customers a wider portfolio of features by integrating its EMM and UEM solutions with a variety of other IBM services. However, the mobile and IoT management platforms are two different solutions which are still not integrated. The SaaS nature of the MaaS360 solutions can be a drawback for customers in need of a hybrid or on-premise deployment.

	Heterogeneity		**Security**			**Resource Management**	**Content**		**Monitoring**	**Adaptation**
	Software & Hardware	Network	Physical	Accessibility	Use		AM	DM		
Airwatch	+ Supports QNX, chrome OS and Tizen	x	✓	✓	✓	x	✓	-Rigid on-premise infrastructure	✓	
MobileIron	- Lacks support for Linux, Mac OS X	x	✓	✓	-Lacks native anti-malware	x	✓	+Protects data in unmanaged folders	-Missing reporting and analytics dashboard	x
Maas360	✓	x	-Lacks SAML support	✓	✓	x	-App wrapping and analytics weak	-SaaS Only	✓	x
BlackBerry	-Lacks support Linux.	x	✓	✓	✓	x	✓	✓	-Inferior analytics for non-Blackberry devices	x

Table 1 : Comparison of leading EMM and UEM solutions

VIII. PRELIMNARY VALIDATION

In this paper, a framework that elicits the main capabilities which ought to be provided for the management of a fleet of connected devices was presented. To demonstrate one of the many ways it can be employed, the framework was used to evaluate and compare leading EMM and UEM suits.

As a preliminary validation for our proposal, a survey was conducted. First, a pilot version of the survey was distributed and answered by two companies, then the answers were analysed by our team and the questions improved. A second and final version was then distributed to a larger sample. The questions were classified in 4 categories. The first one is introductory; it is meant to determine the decision authority of the participants, the nature and penetration rate of mobile and IoT devices in their respective companies and whether the latter uses a management platform. The goal of the second category of questions is to confirm the benefits brought to the company through the use of these devices, as well as the risks they entail. In this category,two questions were added in the second version of the survey, an open question to provide insight on the main reasons the company have decided to adopt a management solution to manage its fleet of mobile and IoT devices, and another one to assess their level of satisfaction about it. The third category of questions aims to evaluate the coverage of the framework. Consequently, the capabilities introduced in this paper were compared to the ones implemented in each company, and an open question invited the participants to complete, if necessary, the list of capabilities, with others that are relevant to their company. And finally, a forth category was added in the second version of the survey to assess the usability of the framework. The first question interrogates the companies that already use a management platform about the capabilities they would consider from the framework, to upgrade their current version. Then the second question concerns companies that haven't adopted a solution yet, to determine their willingness to use our framework as a guiding tool to choose the appropriate solution that best fits their needs. And finally, one open question to understand how the framework could be used in the company. The survey was created using the "SurveyMonkey" tool, and was broadcasted by email. 10 correspondents from 10 different companies answered (Algo Consulting, Microsoft, Rich Oxygen, Original,

Forbes Magazine, ATJ Consulting, OCP, Hidden Founders, the Moroccan Minitère de l'industrie, du Commerce, de l'Investissement et de l'EconomieNumérique and Nestlé),70% of which have senior positions in their respective companies (CEOs, CTOs,CIOs, Information Technology Directors,MIS Directors,Project Plannings, etc), 20% work in middle management (Managers, Architects,Senior Database Administrator and Engineers, etc), and the rest are employees, thus represent end users.

All stockholders use laptops and smartphones at work. 60% of them also use their smartwatch. The senior representatives indeed confirmed that the use of personal mobile and IoT devices at work have increased productivity, enabled new services and insured employee attainability. However, they also expressed their concern regarding the confidentiality of content, as well as the security of the company's IT resources.

While 70% of participant companies addressed these concerns by adopting a mobile and IoT management solution, only half of them asserted that they are satisfied with the capabilities offered.

According to the participant stakeholders, our framework helped in the following cases:

- While they were not completely satisfied with the capabilities offered by their management solutions, the managers could not diagnose the exact features that were lacking. Through the framework, 80% were not satisfied with service durability, 40% complained about device performance when running a fleet management solution and 60% expressed their intention in mining the gap between devices that collaborate while using different communication protocols.
- Amongst the companies that were content with their current platforms, 40% would consider upgrading their version to enable managed devices to adapt to alterations in their context in order to deliver advanced services and 20% would appreciate that all devices communicate regardless of the communication technology they use.
- 2 out of 3 companies that do not use any specific software to manage mobile and IoT devices would consider our framework to evaluate the market solutions.

In conclusion, however selected with different ratios, all the capabilities proposed in the framework were chosen by at least one company, proving the relevance of them all. Furthermore, none of the stakeholders mentioned other capabilities that are important to their companies, other than the ones provided by the framework, thus proving its completeness.

IX. CONCLUSIONS

Mobile and IoT has revolutionized the way people and objects interact, especially in the workplace. Employees can now communicate, perform their usual tasks and use corporate applications anytime, at any place, more efficiently and with fewer costs. Moreover, integrating IoT in the enterprise enables advanced smart applications that monitor business processes, provide real-time insights and interventions, enhances CRM, and contribute to strategic improvements based on predictive analytics of generated big data. However, it does not come without few drawbacks; heterogeneity of devices, potential theft of corporate resources and confidential information, maintenance, and unregulated use pose serious problems to the enterprise.

This paper sheds the light on the fundamental functions that enterprises should be able to carry out to insure remote device management. It includes discovering and establishing communication with various types of devices, securing access to content and corporate resources, distributing and protecting access to files and applications, conserving limited hardware resources, maintaining internet connectivity, monitoring user activity and device performance, and reconfiguring when necessary to maintain compliance with internal policies[47]. The paper is mainly concerned with the Airwatch, MobileIron, Maas360 and BlackBerry EMM and UEM solutions, which offer the necessary tools to properly integrate mobile and IoT devices with the organization workflow.

Managing IoT devices in the enterprise is practically new with significant room to improve in order to reach its full potential. Some of the possible capabilities may include collaboration; the IoT creates a global infrastructure, where all devices can interact. The platforms could go beyond the management of collaborative tasks and applications, to a dynamic allocation of resources. Devices could merge camera footage for 360° visuals, lend memory for running certain programs, delegate tasks before complete depletion of energy, or momentary share processors for the analysis of data. Another opportunity includes cognitive adaptations; thanks to cloud infrastructures, enterprises are able to archive colossal amounts of data. The management platforms could put together various types of monitored information, like location, videos, time, social network feed, or user browsing preferences, and learn better ways to solve problems. A good example of this capability would be the Comma Car [48]. Through analyzing the data, the platform could discover patterns and behaviors, which can be very significant for the enterprise in terms of processes optimization, user experience enhancement, and behaviour prediction.

ACKNOWLEDGMENT

This work was supported by the Moroccan « Ministère de l'EnseignementSupérieur, de la Recherche Scientifique et de la Formation des Cadres », by the « French Embassy in Morocco », and by the « InstitutFrançais du Maroc ».

REFERENCES

1. I. T. Union, "Overview of the Internet of Things," 2012.
2. ASDReports, "Mobile Device Management (MDM) Market worth $3.94 Billion by 2019," 2014. [Online]. Available: https://www.asdreports.com/news-2621/mobile-device-management-mdm-market-worth-394-billion-2019.
3. K. Heinrich and K. Gerhard, *Mobile Device Management*, 2012 (27 a. 2012.
4. J. Hommes, *Mobile Device Management*. GRIN Verlag, 2012.
5. M. M. Yamin and B. Katt, "Mobile device management (MDM) technologies, issues and challenges," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19*, 2019, pp. 143–147.
6. S. Oprea, B. G. Tudorica, A. Belciu, and I. Botha, "Internet of Things, Challenges for Demand Side Management," *Informatică Econ.*, vol. 21, no. 4, 2017.
7. iridhara Raam, *Securing endpoints to improve IT security*. ACM, 2018.
8. M. V. Moreno, M. A. Zamora, and A. F. Skarmeta, "An IoT based framework for user-centric smart building services," *Int. J. Web Grid Serv.*, vol. 11, no. 1, p. 78, 2015.

9. H. Li, Y. Tian, Y. Liu, T. Li, and W. Mao, "UAI-IOT Framework: A Method of Uniform Interfaces to Acquire Information from Heterogeneous Enterprise Information Systems," in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 724–730.
10. K. Rhee, W. Jeon, and D. Won, "Security requirements of a mobile device management system," *Int. J. Secur. its Appl.*, vol. 6, no. 2, pp. 353–358, 2012.
11. G. Disterer and C. Kleiner, "Using Mobile Devices with BYOD," *Int. J. Web Portals*, vol. 5, no. 4, pp. 33–45, Jan. 2013.
12. C. Vorakulpipat, C. Polprasert, and S. Siwamogsatham, "Managing Mobile Device Security in Critical Infrastructure Sectors," in *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*, 2014, pp. 65–68.
13. G. Santucci, C. Martinez, and D. Vlad-câlcic, "The Sensing Enterprise," *FInES Work. FIA 2012*, pp. 1–14, 2012.
14. V. Raychoudhury, J. Cao, M. Kumar, and D. Zhang, "Middleware for pervasive computing: A survey," *Pervasive Mob. Comput.*, vol. 9, no. 2, pp. 177–200, 2013.
15. G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, and E. Ayday, "A survey on information security threats and solutions for Machine to Machine (M2M) communications," *J. Parallel Distrib. Comput*, vol. 109, pp. 142–154, 2017.
16. M. A. Abbasi, Z. A. Memon, T. Q. Syed, J. Memon, and R. Alshboul, "Addressing the Future Data Management Challenges in IoT: A Proposed Framework," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, 2017.
17. S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the IoT Resources: Fundamentals, Requirements, Comprehensive Review and Future Directions," *IEEE Commun. Surv. Tutorials*, pp. 1–1, 2018.
18. F. G. Furtmüller, "An Approach to Secure Mobile Enterprise Architectures," *Int. J. Comput. Sci. Issues*, vol. 10, no. 1, pp. 329–336, 2013.
19. B. Michelson and Bruce, *Closed loop lifecycle planning : a complete guide to managing your PC fleet*. Addison-Wesley, 2007.
20. VMware-AirWatch, *GlaxoSmithKline Increases Employee Productivity Across the Globe with AirWatch*. 2015.
21. P. Callewaert, C. Combes, A. Choukhman, B. Van Der Heijden, B. Joosten, and T. De Jaeger, "Key takeaways to advance in mobile," 2013.
22. N. Leavitt, "Today's Mobile Security Requires a New Approach," pp. 16–19, 2013.
23. C. Pettey, "Gartner Says Two-Thirds of Enterprises Will Adopt a Mobile Device Management Solution for Corporate Liable Users Through 2017," 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2213115.
24. T.-A. Blakely, "The Amazing Technology Behind the Coca-Cola Freestyle Soda Fountains," 2015. [Online]. Available: http://blogs.air-watch.com/2015/10/coca-cola-freestyle-mobile-innovation/#.WFKeNlXhDIU.
25. M. Aazam and E.-N. Huh, "Fog Computing and Smart Gateway Based Communication for Cloud of Things," in *2014 International Conference on Future Internet of Things and Cloud*, 2014, pp. 464–470.
26. C. Terrence, R. Smith, C. Silva, B. Taylor, J. Girard, and M. Basso, "Magic Quadrant for Enterprise Mobility Management Suites Market Definition / Description," no. June. pp. 1–12, 2015.
27. D. Beimborn and M. Palitza, "Enterprise App Stores for Mobile Applications-Development of a Benefits Framework," *Amcis*, pp. 1–11, 2013.
28. Kony, "Mobile Application Management," 2012.
29. R. Smith, B. Taylor, C. Silva, J. BhatMan, T. Cosgrove, and J. Girard, "Magic Quadrant for Enterprise Mobility Management Suites," 2016. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-390IMNG&ct=160608&st=sb.
30. F. Gabrielle, "AirWatch Surges Ahead With Largest EMM Market Share Worldwide," 2015. [Online]. Available: https://www.vmware.com/ca/en/company/news/releases/AirWatch-Surges-Ahead-With-Largest-EMM-Market-Share-Worldwide.
31. L. Cheng and H. Sliwinski, "VMware Completes Acquisition of AirWatch (NYSE:VMW)," 2014. [Online]. Available: http://www.vmware.com/company/news/releases/vmw-newsfeed/VMware-Completes-Acquisition-of-AirWatch/1812214.
32. H. Haile, "DCIG's 2014 MANAGEMENT MOBILE DATA BUYER'S GUIDE," 2014.
33. C. Kane, "The Forrester Wave ™: Enterprise Mobile Management," 2015.
34. S. K. Crook, "Worldwide Enterprise Mobility Management Software 2014-2018 Forecast and 2013 Vendor Shares," 2014.
35. MaaS360, "MaaS360 Named SIIA Software CODiE Award Finalist in Two Categories | MaaS360 by Fiberlink," 2014. [Online]. Available: http://www.maas360.com/news/press-releases/2014/maas360-named-siia-software-codie-award-finalist-in-two-categories/.
36. K. Marney, "So far, so good for tech start-up," *USA Today*, 2002. [Online]. Available: http://usatoday30.usatoday.com/money/covers/2002-05-07-goodtech.htm.
37. Trefis Team, "BlackBerry's Good Technology Acquisition Is Smart, Does It Impact Its Valuation? - Forbes," 2015. [Online]. Available: http://www.forbes.com/sites/greatspeculations/2015/09/08/blackberrys-good-technology-acquisition-is-smart-does-it-impact-its-valuation/#2bb98591694a.
38. J. Ormond, S. Wheeler, and O. Martin, "Microsoft cloud services and network security | Microsoft Docs," 2016. [Online]. Available: https://docs.microsoft.com/en-us/azure/best-practices-network-security.
39. P. Kodeswaran, S. Mukherjea, P. G. Naldurg, V. Ramakrishna, and A. Seshadri, "Dynamic enterprise boundary determination for external mobile devices," 2016.
40. B. Brannon, "The New Era of EUC Is Here: Introducing Unified Endpoint Management," 2016. [Online]. Available: http://blogs.air-watch.com/2016/08/vmworld-news-euc-unified-endpoint-management/#.WGU_k1XhDIV.
41. L. Angela, "VMware and Google Expand Partnership to Enable Enterprise-Wide Management of Chrome Devices," *Marketwired*, Palo Alto, CA, 22-Aug-2017.
42. M. Dunkerley, "Breaking Down Unified Endpoint Management," *AirWatch*, 2016. [Online]. Available: http://blogs.air-watch.com/2016/09/breaking-unified-endpoint-management/#.WGWJ0VXhBhE.
43. MobileIron, "Mobile Content Management (MCM) Software | MobileIron," 2015. [Online]. Available: https://www.mobileiron.com/en/solutions/mobile-content-management-mcm.
44. L. Norville, "AirPatrol brings context awareness to AirWatch EMM - AirWatch Blog," 2014. [Online]. Available: http://blogs.air-watch.com/2014/11/airpatrol-brings-context-awareness-airwatch-emm/#.VnqDKBXhDIU.
45. J. F. G. Jr., "Mobile Device Management System Privacy Impact Assessment (February 2015)," 2015.
46. IBM, "Combating security threats with endpoint security intelligence and control," 2016.
47. [47] A. Achtaich, N. Souissi, R. Mazo, O. Roudies, and C. Salinesi, "A DSPL Design Framework for SASs: A Smart Building Example," *EAI Endorsed Trans. Smart Cities*, vol. 2, no. 8, p. 154829, Jun. 2018.
48. [48] G. Hotz, "we are comma.ai," 2016. [Online]. Available: http://comma.ai/.

AUTHORS' PROFILES

AsmaaAchtaich, received her engineering degree in Computer science from Ecole Nationale de l'IndustrieMinérale (ENIM) in Rabat. She is currently pursuing a PhD degree in Ecole Mohammadiad'Ingénieurs (EMI) – Université Mohammed V and Université Paris 1 - Panthéon Sorbonne. Her research interests include Internet of Things, Requirements engineering and Software product lines.

Raul Mazo, is an Associate Professor at Université Paris 1 - Panthéon Sorbonne and a Visiting Professor at Eafit University. His research interests include (Dynamic) Product line engineering, Self-adaptive systems, and Software and Requirements engineering. He received a PhD in Computer Science from Université Paris 1 - Panthéon Sorbonne.

NissrineSouissi, is a professor at the MINES-RABAT School, Morocco. She obtained a PhD in computer science from the University Paris-Est Créteil in 2006, France and an engineer degree in computer engineering from Mohammadia School of Engineers in 2001, Morocco. Her research interests include process engineering, business process management and data management.

Camille Salinesi, is a Professor at Université Paris 1 Panthéon Sorbonne. His research interests include requirements engineering, strategic alignment and product lines. Salinesireceived a PhD from Université Paris 6, Pierre et Marie Curie.

OunsaRoudies, is a Professor of Computer Science at Ecole Mohammadiad'Ingénieurs (EMI), Université Mohammed V. She is the head of Siweb Research Team which specializes in Information System Engineering. Her research interests include Information system management, Project management and Design science research.