Outlook on moving of computing services towards the data sources

Farzaneh Akhbar[1], Victor Chang[2], Yulin Yao[3], Víctor Méndez Muñoz[4]

[1] Istanbul Technical University, Maslak, Istanbul, Turkey. M.f.akhbar@gmail.com
[2] *Xi'an Jiaotong Liverpool University, China. ic.victor.chang@gmail.com*
[3] Independent Researcher, Southampton, UK, yulinyao.forever@gmail.com
[4] Universitat Autònoma de Barcelona, UAB, Spain. victor.mendez@uab.es

Keywords: Big Data, Internet of Things, Nano Data Centres, Cloud Computing.

Abstract: The Internet of things (IoT) is potentially interconnecting unprecedented amounts of raw data, opening countless possibilities by two main logical layers: become data into information, then turn information into knowledge. The former is about filtering the significance in the appropriate format, while the latter provides emerging categories of the whole domain. This path of the data is a bottom-up flow. In the other hand, the path of the process is a top-down flow, starting at the strategic level of business and scientific institutions. Today, the path of the process treasures a sizeable amount of well-known methods, architectures and technologies: the so called Big Data. On the top, Big Data analytics aims variable association (e-commerce), data mining (predictive behaviour) or clustering (marketing segmentation). Digging the Big Data architecture there are a myriad of enabling technologies for data taking, storage and management. However the strategic aim is to enhance knowledge with the appropriate information, which does need of data, but not vice versa. In the way, the magnitude of upcoming data from the IoT will disrupt the data centres. To cope with the extreme scale is a matter of moving the computing services towards the data sources. This paper explores the possibilities of providing many of the IoT services which are currently hosted in monolithic cloud centres, moving these computing services into nano data centres (NaDa). Particularly, data-information processes, which usually are performing at sub-problem domains. NaDa distributes computing power over the already present machines of the IP provides, like gateways or wireless routers to overcome latency, storage cost and alleviate transmissions. Large scale questionnaires have been taken for 300 IT professionals to validate the points of view for IoT adoption. Considering IoT is by definition connected to the Internet, NaDa may be used to implement the logical low layer architecture of the services. Obviously, such distributed NaDa send results on a logical high layer in charge of the information-knowledge turn. This layer requires the whole picture of the domain to enable those processes of Big Data analytics on the top.

1 INTRODUCTION

IoT as a technology relies on machine to machine communication through the internet. Embed systems of various kinds of devices gather data from the environment for more interpretation and information extraction. Since, the involved environment with technology becoming bigger, IoT theoretical limit is as big as the internet itself. The IoT are pervasive to our day-to-day lives, people can get to the internet and get connected to each other through small sensors on different smart and portable devices. RFID, NFC, Wi-Fi, Bluetooth are various types of local area connection that IoT can be used (Atzori et al., 2010; Gubbi et al., 2013). In this way, IoT can break down boundaries in all areas to enable "anytime, anywhere, anyone, and anything" access (Welbourne et al, 2009). In the top-down path information is coming to the strategic level, enabling new ways of market penetration, collecting a wide range of information from the underlying data infrastructure. Similarly, challenges are encountered such as designing the appropriate architecture and data centre to prepare networking and security (Domingo, 2012).

Cloud computing has a complementary role for IoT and currently they are inextricably linked (Gubbi et al., 2013). Cloud computing can provide the virtualization facilities to help device applications for integrating their utility computing, monitoring devices, storage devices, analytics tools and visualization platforms. In this case, what enables applications and users to access applications on demand anytime, anyplace and anywhere is the utility-based model of cloud computing. While blending this characteristic of Cloud with IoT, data could be gathered as much as intended.

In this paper, apart from the fact of providing an overview about cloud computing and internet of things, we discuss issues and challenges when, cloud and IoT collaborate with each other for a better proficiency. We focus in the possibilities of moving computing service towards the data sources and new high level applications of Big Data in the information-knowledge logical layer. The idea of this multiple layered clouds is not new. NaDa approach was proposed several years ago (Vytautas et al., 2009) to improve video streaming services taking advantage of the in-transit machines of the IP providers. The same concept has been applied to other applications, for example in P2P clouds based in nano centres (Babaoglu et al., 2012). More recently, multiple layered clouds can solve several IoT applications with nano and micro data centres in front of the conventional cloud infrastructure (Petri et al., 2014). The contribution of the present work is to describe de possibilities of a generic logical architecture for Big Data applications, composed of a data-information layer in the IoT and NaDa infrastructure and an information-knowledge layer in the Cloud. For example, a market segmentation system selects target information from NaDa in-transit data. Then, it sends the result of this filter processing to a cloud computing storage. On the top, a cloud application is obtaining clustering of market segmentation from the whole domain statistics. The two main logical layers are break down as follows. Section 2 by suggesting an IoT architecture in four physical layers, we aim to give a new approach to fill research gaps. In Section 3 we describe current integration of IoT and cloud, as well as key research problems in data size and security constrains, disaster recovery and categories of cloud services to IoT. Section 4 is focusing the NaDa alternative to some of the problems found in Section 3, particularly what is related to data management. It details the main idea of moving computing services towards the IoT data sources. Section 5 summarizes a questioner to professionals. We conclude in Section 6.

2 INTERNET OF THINGS

Internet of Things (IoT) contains a wide range of smart objects, connected through the internet via sensors, exchanging data and information update. According to Vermesan et al. (2011), internet of things is the biggest community right after the internet itself. “Things” in internet of things could refer to any devices which have the ability to switch to the internet with unique IP addresses. IoT enlarge internet connectivity beyond customary devices like computers, laptop and smartphones to a diverse range of devices and things of daily life and industry. Such devices have integrated embedded systems to control operations. Besides, it is relevant that embedded systems can communicate and interact with the exterior environment, via the Internet. This definition include everything from heaters, cell phones, doors, people and animals, security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and any items which can be identified with unique IP addresses. In summary, they are called IoT or internet of everything (Gubbi et al, 2013).

IoT can be regarded the extended version of the virtual Internet into the physical arena. This can be illustrated by the spatially distributed devices, enabling local sensing and remote actuation (Atzori et al., 2010; 2012; Miorandi et al., 2012). Most important IoT facilities are physical establishments, sensors, software and radio frequency identification (RFID). These facilities help things or physical objects in IoT to collect, send and receive data back and forth in machine to machine, machine to man and both converse communications.

Majority of IoT objects use RFID technology. RFID is widely used for tracking objects, people, and animals (Miorandi et al., 2012). RFID system architecture is signed by a split of simple RFID tags and considerable infrastructure of networked RFID readers. This approach optimally supports tracking physical objects within obvious boundary such as warehouses or data centres, but limits the sensing power and disposal flexibility that acquire new infrastructure or architecture in IoT. A more suitable model for the Internet of Things can be illustrated by considering the technological requirements; demands on the services; and finally decentralized systems of smart objects, autonomous physical/digital objects supplement with sensing, processing, and network abilities. In contrast to RFID tags, smart objects carry a patch of logical facilities that

let them feel their local situation and cooperate with human users. They sense, log, and process what's occurring around their environment, act based on their smart, intercommunicate with each other, and exchange information with end users or people. By perceiving RFID properties, architecture can be developed in such a way that data warehouses are closer to these sensors (Kortuem et al., 2010).

Another characteristic should be considered for constructing a new architecture in IoT is, how objects communicate with each other. Machine to Machine communication is how objects make interactions. This kind of communication paradigm provides ubiquitous connectivity between devices, plus an ability to communicate autonomously without human intervention. In IoT machine-to-machine communications enable remote sensors to gather data in the first layer of IoT architecture and sends it wirelessly to a network in the next layer, where it lead to hubs and next routed through the Internet, maybe to a server such as an application or personal computer for more analyse. At that point, the data is analysed and acted upon, according to the software in place and this is how IoT infrastructure work (Gassis et al., 2012; Rui et al., 2015).

2.1 Architecture for the Internet of Things

The IoT architecture contains different layers. However, there are several ways of modelling the IoT layer infrastructure. To ensure the architecture can be adopted easily, four key layers are proposed as follows: sensor layer, network layer, platform layer and application layer. As Figure1 shows, first layer belongs to physical objects like sensors. This sensor layer consists of a Wireless Sensor Network (WSN), RFID reader, and M2M terminals to collect various data from environments. Gathered data from things or objects in first layer going to the second layer where gateways and hubs lead data to the internet and clouds for more processes and storage in central servers.

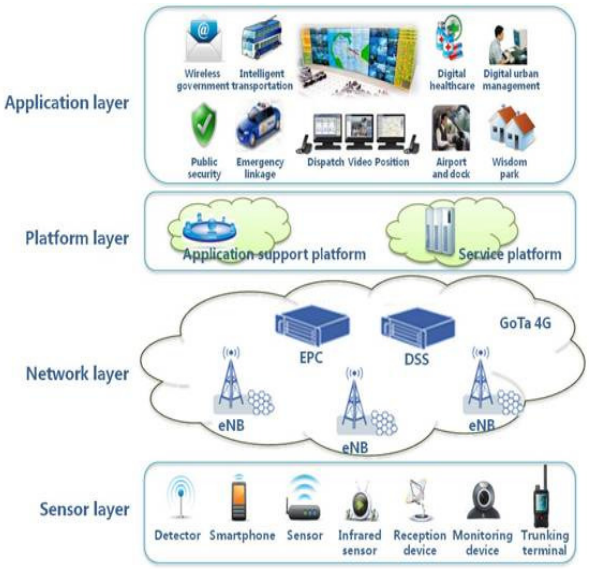

Figure1 : Internet of Thing Architecture

Platform layer or the Internet of Services (IoS) involves the analysis of Big Data uses open platforms and interface architectures to support user's requests in the last layer. What is important for users in the last layer is, real-time statistics and historical analysis reports from the gathered data from sensors, till they could react to anomalies, occurrences or other events appropriately and quickly as soon as they occur, so we need such a platform to satisfy these needs for maximizing IoT potential and that is the topic for our paper (Ning et al, 2015).

Last layer is where end users exist. In this layer there are screen displays with friendly and graphical user interfaces, the virtual infrastructure for utility computing, integrating applications, monitoring devices,

analytics tools which allow users access real-time analysis reports. Furthermore, we have visualization platforms and client delivery in this layer. The utility-based model, cross-platform and mobile management facilitate that cloud computing offers in this layer will enable end users to access applications as needed at anytime, anyplace and anywhere.

In this paper, we propose that the "ideal" IoT platform can transfer data faster with less energy consumption and latency and higher level of security. Although there are lots of work in literature, such as generic survey on IoT or gaps in IoT (Atzori et al., 2010; 2012; Miorandi et al., 2012; Gubbi et al., 2013), few of survey papers focus on problems of clouds and IoT interconnection on real world. This is an important area of investigation because cloud can provide on demand capabilities in terms of infrastructure, but also in the interconnection of services, services and data, opening the opportunity to the top-down applications of Big Data, the logical level of information-knowledge.

3 INTERNET OF THINGS AND CLOUD COMPUTING

The first step of the integration needs accommodation of Clouds capabilities with IoT, which needs "mediators" to connect both. In other words, objects in IoT connect with each other through clouds on the internet, and new applications may take advantage of the emerging knowledge of such integration. This combination helps IoT reach its feasibility and maximize its potential. Cloud computing provides an important means of supporting flexible traffic growth and reducing application deployment costs, since users will not buy extra software or hardware with increased user demands equivalent to the pay as you go model for clouds.
Cloud architecture in IoT, refers to systems where software is involved in the delivery of computing and storage capacities as a service. Cloud computing architecture can be divided into the front end and the back end. The front end can be reached by the users who can access to the cloud via an interpreter or interface like a web browser. The cloud itself is the back end of cloud computing architecture, encompasses various servers, computers and data storage devices. Figure 2 shows that data collected by objects go back end clouds after passing hubs, to data centres. Cloud architectures aim to design software applications according to use on demand Internet services access. Adoption to cloud architectures can be designed for such that computing infrastructure is utilized only when it is required. For example, to process a user request, ask the imperative resources on-demand like: servers, platform and storage, and then perform a specific computation.

On the other hand, cloud computing has capability of big data management in IoT (Zaslavsky et al. 2013). Thus, the cloud back end, may also support a wide range of big-data applications of the information-knowledge logical layer, where the whole IoT domain is aggregated to provide these new applications. Without the technology of cloud, IoT could not manage huge amount of data producing by it's everywhere objects. Nowadays, IoT penetrates to all aspects and angles of industry, even normal peoples' daily life and breaking down the boundaries. This means we encounter with really big data in ubiquities IoT, where objects collect data anywhere, anytime with big Variety (range in type and source of data), Volume (size of the data) and Velocity (frequency of data generation) via the implanted sensors (Chang, 2015). Hence, cloud computing can serve as the platform to collect, process and analyze data in IoT in order to enable high level big data applications (variable association, data mining, clustering and so on).

Cloud computing plays the front end role in the IoT for data management by connecting assets, people, products and services together in order to satisfy real-time decisions need to streamline information flow. Hence, the use of IoT may boost asset performance, reduce supply chain risks, empower people and guarantee product quality and integrity. More objects can be connected together by the use of Cloud. However, there are areas that users need to be aware of, such as reduced cost of quality and compliance, greater return on innovation, a better quality of services and a better quality of experiences.

More objects in IoT mean more data flow streams. Data after being collected, filtered and processed to the significant information, needs storage and is often stored in data centres. Cloud data centres can be designed to accommodate to store the increasing amount of data. To limit over-capacity, companies should focus on retrieving and using data generated by the IoT cost effectively. The reason is that IoT menacing can generate huge amounts of data from distributed sources, so transferring the entire amount of data to a single location for more processing will not be technically and economically feasible. Sine cloud data centres have, the more distributed capacity in comparison with central data centres relied on TCP/IP network only (Gill et al., 2011);

this can be done by locating data centres in different geographical points. While IoT data come from multitudes of sensors, the facility requires even more bandwidth than current capacity of distributed cloud data centres. It means we need new version of data centres with better performance and capacity.

Another reason in which current cloud data centres are less capable is, big data of IoT need a better management, preparation and security. Current data centre and architecture of IoT, cannot not answer the rapid growth of data size. Data of IoT come from embedded sensors in different locations. Due to the nature of data sharing and backbone implementation required for the involved hardware and software with the gathered data, we need just-in-time operations (Gubbi et al., 2013; Jin et al., 2014) to decrease freight delays and delivery schedule failures. Since the majority of data is collected by RFID technology, so wireless resource management should be optimized to reduce power consumption and meet the mobility requirements of objects. For example, the uplink/downlink bandwidth required for different communication of machine-to-machine communication or man-to-man communication, which exists among IoT objects through clouds.

The management of big data security in IoT and Cloud collaboration require having a high level of security which can resist external attacks and unauthorized access. This approach could be strengthened by empowering software engineering approach. The whole process can be validated with designing such a framework to secure the technical design and applications, accurate administration and policies associated with recommended methods (Chang et al., 2016 a). This can be used to design an architecture, to help IoT successfully adopt with Cloud services and platforms. Implementing security hardware and software solution for clouds in IoT at data centres will be useful for all types of services.

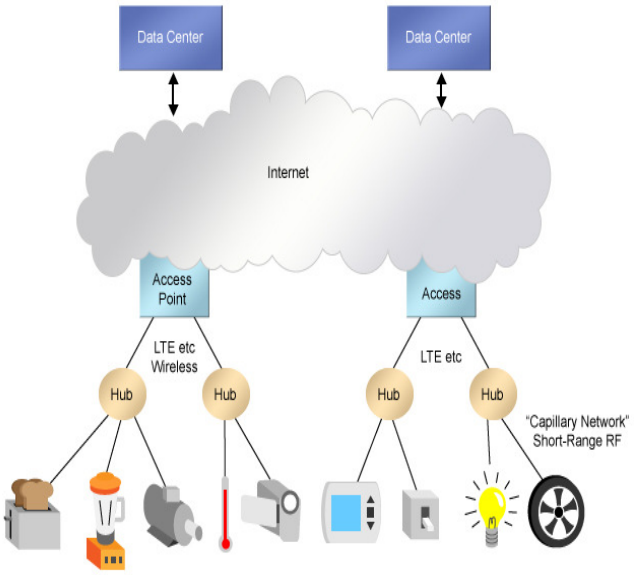

FIGURE 2: Current Place of Data Centres in Internet of Things Architecture

In our suggested architecture various security categories have been considered based on the selected literature (Jara et al., 2010; Zhou et al., 2011). These categories include:

- Build system in a way could protect themselves security automatically, in adoption with other software applications.
- Reach wireless network security (LAN, MAN, GAN) and platform security include Virtualization, Operating Systems and systems software.
- Making network security convergence, where social networks, multi-network media infrastructures and technologies can overlap.
- Provide system service security, data security, good service delivery, privacy, open source software security, web services security and etc.

3.1 Cloud Computing Classification in IoT

Computing Clouds are commonly classified into Public Clouds, Private Clouds and Hybrid Clouds, but in this area there is some kind of new model which is different from private, public or even hybrid. This new model is Community cloud and is one of the issues in a business framework in internet (Chang et al., 2014). New issues always bring new needs to accommodate and adoption with previous applications and frameworks. By adding community cloud to the cloud computing and then over to IoT infrastructure, we have to consider its needs in IoT architecture (Kortuem et al, 2010; Muñoz et al., 2013).

IoT uses public cloud for services such as server, data storage, application access and many others. This helps involve end users to get free from hardware/software purchasing, maintenance and management, when they use public clouds such as Amazon EC2 or S3. Apart public clouds, we have private clouds which are custom-built used internally to ensure only users with authorized access. Private clouds can offer computing power services individually or in collaboration with other cloud environments, using a special pool of physical computing resource. However, under the private cloud model, the cloud is only accessible by a single private company or organization, securing them with a greater control and privacy (Garcia et al., 2014).

A hybrid cloud is a combination of private and public cloud due to use their both advantages concurrently. This combination is done for giving the organization the opportunity of flexible use of the various services in both private and public cloud environment. With this merging, end user or company profit is as follows:

- Use a public development platform that sends data to a private cloud or a central data center–based application
- Use a number of SaaS (Software as a Service) applications and negotiate data between private and data centre resources in central servers.
- Privatize a business process as a service for only the eternal users.

After these all, community cloud is the last type of cloud. A community cloud is not a combination of previous three clouds, since it does not possess all properties of private, public or hybrid clouds. However, it contains some special characteristic of them simultaneously. For example, it can send data publicly, but give local access permission to end-users.

Since then, cloud architecture in IoT contain all of these four types of clouds, so applications and object should have such an ability to use and access them appropriately and it provides new issues in IoT architecture itself.

3.2 Big Data Disaster Recovery in IoT's Clouds

Advantages cloud computing can offer for big data should not be ignored. Among the proficiencies for large amount of data, disaster recovery, has special significance. There is plenty of literature considering the privacy and security of big data in cloud computing or IoT (Atzori et al., 2010; Gubbi et al., 2013; Subashini and Kavitha, 2011; Wang et al. 2010). While there is a less attention to the disaster recovery in private, public or hybrid clouds for restoring data in a precarious and risky situation, in a case, there are not enough or suitable backup. The importance of disaster recovery for big data make us to think to a new architectures or structures for taking backup of data for assuring data lost prevention, in unexpected situations, such as dying central hard disk or maybe even natural phenomenon or fire. In Chang's (2015) multi-purpose approach, the DR service allows data to be restored to multiple places, with multiple methods, to ensure the data recovery at very high percentage. In our suggested architecture, NaDas with their capabilities make chance for getting automatic back up and smart storage. This ensure us, all data and services can be restored back to normal as soon as possible if disasters / serious accidents happen (Riggins et al., 2015; Chang, 2015).

3.3 Cloud Computing Services in IoT

Scientists, define cloud computing as a service oriented framework. These services allow IoT collaborates with Cloud Computing infrastructure. Similarly, there are challenges to be resolved. Cloud includes software, platform and infrastructure as services. For use this service efficiently, we need a framework and application to be able to interconnect with them, appropriate (Cheng et al., 2016; Karagiannis et al., 2015).

Software as Services (SaaS): Using various ranges of software as much as you want, anytime, anywhere just by accessing internet, without installing and maintaining. Although, SaaS making software usage easier, but security and availability and performance still alive among challenges, in cloud computing.

Platform as Service (PaaS): For using applications and services we need a hostess, to develop and run them and cloud host you as a platform based on application or other services you ask to use. There are lots of literature giving a try to improve this capability of clouds based on current topics, but still there are gaps for adaptation and data safety.

Infrastructure as a service (IaaS): Accessing to computing facilities, virtually or physically, is what IaaS provides it. Making network connections, bandwidth, IP addresses and load balancers are some capabilities of IaaS. Cloud brings all this services even from one server/machine or maybe from multitude servers. This service model works with other two SaaS and PaaS.

By considering all mentioned above, NaDa may help IoT to use cloud services to be more secure with a better quality. In our new proposed architecture, NaDas, data centres can be allocated to fewer groups of end-users manage their data. Different layers of services in NaDas can communicate with each other and services can be offered in a peer to peer form, so request- response in IoT service will get a higher quality. In other words, an end user's NaDa could not get a response from its request, since this request will send to NaDas in the near distance. The reason is that NaDas can disperse in small distance everywhere, sent request will be responded again, sooner than, it sent to central data centres.

4 NANO DATA CENTERS IN INTERNET OF THINGS

Large-scale data processing can pose challenges for current IoT model, since the surges and increased demands can make IoT services subject to delay and downgrade of the service. In the previous data processing, some of encountering difficulties can be summed up as:

- Overlapping of requested resources.
- Large scale distribution of demanding machine or applications.
- Obligatory of processes can run on different machines, which one or more than of those machines fail or stop to work due to any reason:
    1. Process of releasing all machines after process ending in good manner to back them to their stable situation
    2. Scale out the process to other machines in a case
    3. Process requirement like bandwidth or memory capacity increase, calculation of waiting time if processes face with any problem and so many others.

In hence, we need Cloud architectures be able to solve such challenges and then replicate them in technology, which work based on clouds like IoT (Chang and Ramanchandran, 2016).

In our proposed model of IoT architecture that needs to deal with rising amount of data, our focus is on data centre design and management. In the new architecture, previous data centre will replace with nano data centres through clouds. In current IoT architecture, data centre stands at the platform layer, but by using cloud nano and micro data centre, we could bring them closer to sensors to overcome the latency of data transmission's cost and latency to a central server in far geographical places. Further, we can also reduce all other different cost cause by sending data back and forth through the paths among end users. All in all NaDas could solve lots of risk and problems of IoT, in advance. It could give solution to mentioned issues in the previous paragraph. For example, in new model since users have their data centre, there will be no problem with memory capacity or bandwidth amount. In the worst case if, some user's requests need more capacity than

the user NADa it could access its request by asking its neighbour, via peer to peer communication. Also, by replacing NaDa with a central data center, there will no anxious about recourse overlapping, cause in most case NaDa connected to end user could satisfy its customer's request or pass it to its nearest neighbour, so we will access pool of resources to guarantee no resource shortage.

NaDa has been presented as a working version of distributed data centres in cloud computing in our previous research (Akhbar and Tolga, 2015). It is an appropriate solution for a wide range of IoT applications with large amount of data management. However, not all the IoT use cases can fit in the only NaDa approach. The non-coalescent data access pattern does not fit well in this paradigm. Non-coalescent pattern typically gets data, processing, and as part of the output of the processing it is giving the next data object to be accessed. Actually, the high level Big Data applications are usually becoming to the non-coalescent, thus the need of using NOSQL database and artificial intelligence techniques to provide an efficient processing. For these reasons the Big Data applications from the strategic level (data mining, associated variables or clustering) will still remain in a (1) filtering processing to extract relevant information from the NaDa and (2) transfer such reduced data to classical cloud centres, in order to turn information into knowledge. But this is the top-down Big Data applications. The users of the IoT devices can live with a bottom-up model placed in NaDas clouds, without traditional cloud centres.

NaDas implanted on already present computing elements in clients houses such as TV, receivers, wireless modems, gateways, etc; virtually or physically. In this case we will have a new architecture at IoT and little change on different layer contents. As you can see on figure 3 NaDas move to the lower layer at IoT architecture on hubs and other gateways, which data encounter with after being collected by sensors and start the journey to internet. By comparing Figure 2 and figure 3, we can see obviously how NaDa is closer to the hardware layer and this less distance will reach impressive better quality of services.

Another question is, "what is the best version of NaDas for providing a maximum level of quality of services?" Based on our last investigations (Farzaneh and Tolga, 2015), we need to adjust NaDas properties based on our necessities and goals. We could use the saturation points from our previous research for adjusting NaDa on IoT, too, since IoT use could computing infrastructure in same.
For example, our research proves by considering 1 gigabyte of memory capacity for NaDa, QoS reach maximum point in compassion with central data centres or even NaDas with other memory capacities (Granados et al., 2014).

5 QUESTIONNAIRE FOR 300 PROFESSIONALS

In order to understand the impact, benefits and risks for organizations adopting IoT, a large scale survey has been used. Questionnaires have been distributed to 1000 professionals who have related experience with IoT and Cloud. The aim is to understand the general consensus rather than the deep analysis of a chosen area, similar to a large scale survey conducted by Chang et al (2016 b). Altogether 400 professionals working in different areas of Cloud Computing have answered questionnaires and have provided their rationale, explanations and spending to improve their security solutions and adoption of large scale Cloud security services. Similarly, the best practice approach can allow anyone to adopt and in this case, the same approach ahs been adopted for IoT investigations. Questions are based on multiple choices followed by a space to allow participants to provide open ended answers, so that more insider knowledge can be obtained. Figure 3 shows the demographics of 300 respondents, which are equally distributed in major sectors. Information Technology has the highest percentage of 28%, followed by Higher Education with 20%, others with 15%, healthcare with 13% and the jointly lowest of finance and consulting with 12% each. All the respondents have at least 5 years of IT experience through their experiences, advanced research or services.

Figure 4 shows results of number of respondents answering the benefits of IoT adoption with NaDas. The number one factor for the benefit is the easy accessibility, since the respondents feel that they can connect to the internet at anywhere they go and it is convenient for their work and communications with others. The number second factor is integrations with mobile devices, since many services are online and users have developed habits of using mobile phones to access these services, as an increasingly number of respondents can access the internet and apps on their smart phones. Future proofs and cost-savings have highly similar number of respondents and both contribute to the last two factors. In terms of people voting others, there are more than ten types of answers and are grouped under the category of "others".

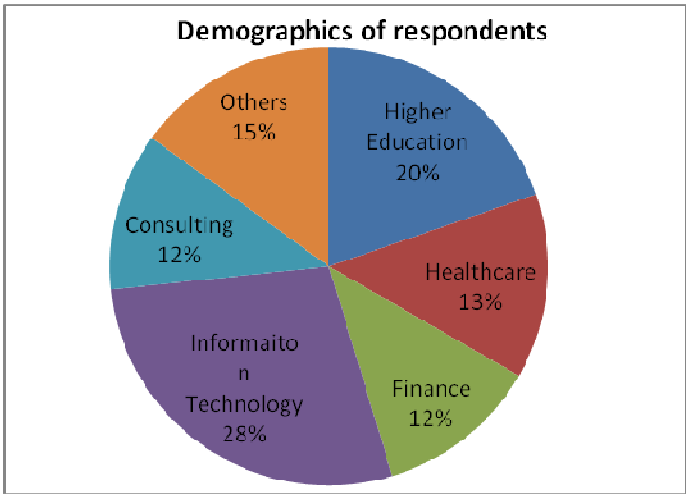

Figure 3: Demographics of respondents

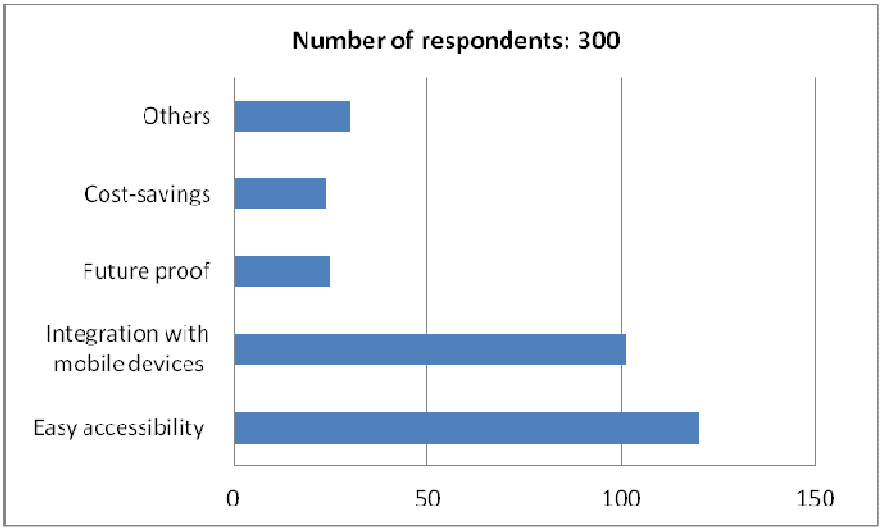

Figure 4: Number of respondents answering the benefits of IoT adoption with NaDas

Figure 5 shows the results of number of respondents answering the challenges of IoT adoption with NaDas. Privacy and security remain the number one factor since there is a growing concern that if many devices can connect to each other and also connect to the internet, it is easier for the hackers to gain unauthorized access and also spread malicious files in the shared network. The probability of receiving attacks, phishing and hacking may also arise (Chang et al., 2016 a; 2016 b). Hence, any prototypes that can implement large scale penetration testing and ethical hacking will be useful for the future development. All data and activities should be protected to keep users status anonymous. Quality of service (QoS) and data loss/recovery are the joint second factor since both are important. If QoS is low, performance, accessibility and security can be unsatisfactory Data loss and recovery are essential as explained in previous sections, since all data should be able to be retrieved and made alive if large scale attacks destroy data. Other factors are less to be concerned based on our feedback although integrations with other technologies, costs and other factors can be considered.

The use of large scale questionnaires can help us validate our proposal for IoT adoption, particularly NaDas development to ensure that all services can stay connected, be always available and can recover data, as well as provide a strong defence against all types of attacks and hacking. Factors for benefits and challenges have been discussed in detail so that more analysis can be followed up.

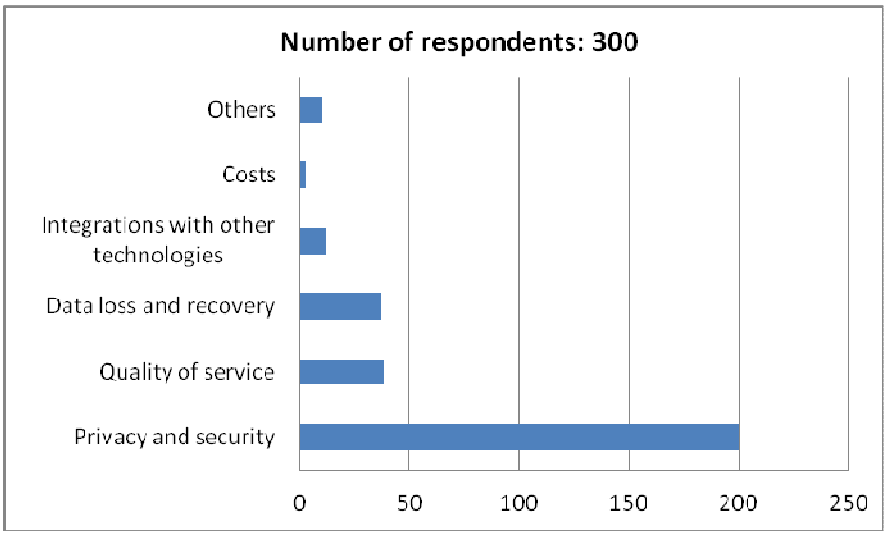

Figure 5: Number of respondents answering the challenges of IoT adoption with NaDas

6 CONCLUSIONS AND FUTURE WORK

Combining cloud computing infrastructures with ubiquitous IoT allow more objects to be connected to the internet, to process data, share results and allow individuals to be well-informed with the latest trends and businesses to stay competitive. The benefit of doing so can produce a large amount of data. On the other hand, the management of big data processing and analytics for IoT architecture has become an important challenge among researchers, since there are issues such as shortage in services, security concerns and quality of services yet to be improved. Problems in IoT and cloud computing collaboration mean that a new version of IoT platforms should be designed and made available. Other approach includes proposing a new framework and architecture will be deployed in order to access higher quality of data management and request-and-response model.

With this perspective and studying previous work on literature, we take a look from a new angel at current IoT architecture model and try to give a new model, to solve various problems. Since, previously we do an investigation on cloud computing data centres and gain nano data centres, some kind of distributed data centres, with better performance, we conclude, could replicate it over IoT, too. With the extensive use of NaDas make changes in IoT architecture, and move most of its data centres form platform layer, the third layer to a lower layer, which is a network layer. This movement could make a revolution on big data management, QoS and QoE. See Figure 6 for details. The results from Section 5 can support our case since there is a strong evidence that IoT adoption for NaDa is popular and within the strategic plans for 300 professionals that we have surveyed on. However, challenges such as privacy and security, quality of services and finally data loss and recovery should be resolved right before the wide adoption of IoT for NaDa.

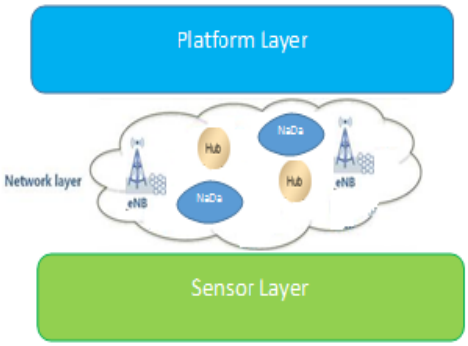

Figure 6: New Architecture of IoT, When Placing Central Data Centres at Platform Layer, with NaDas in Network Layer

Future work of this research includes investigation of a new architecture that uses specific IoT simulator, and undertake experiments in real settings of IoT (such as smart cities) to demonstrate a proof-of-concept for a NaDa architecture. More data analysis based on our survey will be presented to support the effectiveness of adopting IoT for NaDas. More work is required to demonstrate that NaDa architecture can replace the current version of data centres. We hope our paper helps other researchers to have a deeper look at IoT architecture by considering the emerging new challenges of IoT technology, for managing increasing size and huge input amount of data, security and privacy problems, which involved with the IoT structure.

REFERENCES

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, *56*(16), 3594-3608.

Babaoglu, O., Marzolla, M., & Tamburini, M. (2012, March). Design and implementation of a P2P Cloud system. In ACM Proceedings of the 27th Annual ACM Symposium on Applied Computing (pp. 412-417).

Chang, Victor, Robert John Walters, and Gary Wills. The development that leads to the Cloud Computing Business Framework. *International Journal of Information Management* 33.3 (2013): 524-538.

Chang, V. (2014), The business intelligence as a service in the cloud. *Future Generation Computer Systems* 37 (2014): 512-534.

Chang, V. Towards a Big Data system disaster recovery in a Private Cloud. *Ad Hoc Networks* 35 (2015): 65-82.

Chang, V. A Cybernetics Social Cloud. *Journal of Systems and Software* (2016), in press.

Chang, V., and Ramachandran, M. Towards achieving Data Security with the Cloud Computing Adoption Framework. IEEE Transactions on Services Computing 9(1) (2016).

Chang, V., Kuo, Y-H, and Ramachandran M. Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems* 57 (2016 a): 24-41.

Chang, V., Ramachandran, M., Yao, Y., Kuo, Y. H., & Li, C. S. A resiliency framework for an enterprise cloud. International Journal of Information Management, 36(1), (2016 b): 155-166.

Cheng, Xiaoyan, and Guoqing Dang. The P2P communication technology research based on Internet of things. Advanced Research and Technology in Industry Applications (WARTIA), 2014 IEEE Workshop on. IEEE, 2014.

Domingo, Mari Carmen. "An overview of the Internet of Things for people with disabilities." Journal of Network and Computer Applications 35.2 (2012): 584-596.

Farzaneh Akhbar, Tolga Ovatman, “Quality of Service Trade-offs Between Central Data Centersvvand Nano Data Centers”, Accepted in 5th International Conference on Cloud Computing and Services Science, 2015 Lisbon, Portugal.

Gazis, Vangelis, et al. Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things. Informatics (PCI), 2012 16th Panhellenic Conference on. IEEE, 2012.

Gill, P., Jain, N., & Nagappan, N. (2011, August). Understanding network failures in data centers: measurement, analysis, and implications. In *ACM SIGCOMM Computer Communication Review* (Vol. 41, No. 4, pp. 350-361).

Gubbi, Jayavardhana, et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29.7 (2013): 1645-1660.

Granados, Jose, et al. "Towards energy-efficient HealthCare: An Internet-of-Things architecture using intelligent gateways." *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on*. IEEE, 2014.

Jara, A. J., Zamora, M., & Skarmeta, A. F. (2010, January). An architecture based on internet of things to support mobility and security in medical environments. In *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE* (pp. 1-5). IEEE.

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An information framework for creating a smart city through Internet of things. *Internet of Things Journal, IEEE*, *1*(2), 112-121.

Karagiannis, Vasileios, et al. "A Survey on Application Layer Protocols for the Internet of Things." *Transaction on IoT and Cloud Computing* 3.1 (2015): 11-17.

Kortuem, Gerd, et al. "Smart objects as building blocks for the internet of things." *Internet Computing, IEEE* 14.1 (2010): 44-51.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*,*10*(7), 1497-1516.

Ning, Huansheng, et al. "Guest Editorial Special Issue on Big Data Analytics and Management in Internet of Things." Internet of Things Journal, IEEE 2.4 (2015): 265-267.

Ubeda Garcia, Mario, et al. Integration of Cloud resources in the LHCb Distributed Computing. *J. Phys.: Conf. Ser.*. Vol. 513. 2014.

Muñoz, Víctor Méndez, et al. "Rafhyc: An architecture for constructing resilient services on federated hybrid clouds." *Journal of Grid Computing* 11.4 (2013): 753-770.

Petri, I et al., "In-Transit Data Analysis and Distribution in a Multi-cloud Environment Using CometCloud," Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Barcelona, 2014, pp. 471-476.

doi: 10.1109/FiCloud.2014.84

Riggins, Frederick J., and Samuel Fosso Wamba. "Research Directions on the Adoption, Usage, and Impact of the Internet of Things through the Use of Big Data Analytics." System Sciences (HICSS), 2015 48th Hawaii International Conference on. IEEE, 2015.

Rui, Jiang, and Sun Danpeng. "Architecture Design of the Internet of Things based on Cloud Computing." *Measuring Technology and Mechatronics Automation (ICMTMA), 2015 Seventh International Conference on*. IEEE, 2015.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, 1, 9-52.

Vytautas Valancius, Nikolaos Laoutaris, Laurent Massoulié, Christophe Diot, and Pablo Rodriguez. 2009. Greening the internet with nano data centers. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09). ACM, New York, NY, USA, 37-48.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In IEEE *INFOCOM, 2010 Proceedings IEEE* (pp. 1-9).

Welbourne, Evan, et al. "Building the internet of things using RFID: the RFID ecosystem experience." *Internet Computing, IEEE* 13.3 (2009): 48-55.

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). Sensing as a service and big data. arXiv preprint arXiv:1301.0159

Zhou, L., & Chao, H. C. (2011). Multimedia traffic security architecture for the internet of things. *Network, IEEE*, *25*(3), 35-40.