Accepted Manuscript

Secure integration of IoT and Cloud Computing

Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta

PII: S0167-739X(16)30694-X
DOI: http://dx.doi.org/10.1016/j.future.2016.11.031
Reference: FUTURE 3237

To appear in: *Future Generation Computer Systems*

Received date: 5 August 2016
Revised date: 8 November 2016
Accepted date: 28 November 2016

Please cite this article as: C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and Cloud Computing, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.11.031

Secure integration of IoT and Cloud Computing

Christos Stergiou [1], Kostas E. Psannis [1], Byung-Gyu Kim [2], Brij Gupta [3]

[1] Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki, Greece
[2] Department of Information Technology (IT) Engineering at Sookmyung Women's University, Korea
[3] National Institute of Technology Kurukshetra, India
Corresponding author email: kpsannis@uom.edu.gr

Abstract - Mobile Cloud Computing is a new technology which refers to an infrastructure where both data storage and data processing operate outside of the mobile device. Another recent technology is Internet of Things. Internet of Things is a new technology which is growing rapidly in the field of telecommunications. More specifically, IoT related with wireless telecommunications. The main goal of the interaction and cooperation between things and objects which sent through the wireless networks is to fulfill the objective set to them as a combined entity. In addition, there is a rapid development of both technologies, Cloud Computing and Internet of Things, regard the field of wireless communications. In this paper, we present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e Cloud Computing and IoT) in order to examine the common features, and in order to discover the benefits of their integration. Concluding, we present the contribution of Cloud Computing to the IoT technology. Thus, it shows how the Cloud Computing technology improves the function of the IoT. Finally, we survey the security challenges of the integration of IoT and Cloud Computing.

Keywords **- Internet of Things, Cloud Computing, Mobile Cloud Computing, Security, Privacy.**

I. INTRODUCTION

In n telecommunication fields there is a new technology called Internet of Things (IoT). The Internet of Things (IoT) is "the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, permitting these objects to gather and interchange data" [1] [2]. IoT technology is the next major step in the new technology sector, but with the great difference that it carries massive changes in business functionality. Over the next years, a flare in the number of connected devices as well as located sites, and the functions they will perform, is expected.

In addition, the main strength of the IoT idea is the high impact that it will have on several aspects of the everyday-life and behavior of potential users. The most obvious effects of the Internet of Things, as a private user could observe, would be visible in both domestic and working fields. In the first case, some examples of the possible application scenarios in which the new paradigm, that is the Internet of Things, will play a leading role in the near future are domotics, e-health, assisted living, and enhanced learning [3] [4]. In the second case, business users could observe the similar consequences which are traceable in some fields such as logistics, intelligent transportation of people and goods, automation and industrial manufacturing, and business/process management.

The Internet of Things is composed of three main parts:

1. The "things" (objects).
2. The communication networks that connect them.
3. The computer systems using data streaming from and to objects.

For example, home security systems already allow you to check remotely the locks on your doors, and thermostats in the house. But what if it was possible to act proactively on your behalf? Imagine you opened the windows to ventilate your house before arriving, based on your personal preferences, weather conditions, and the distance from your house.

To summarize, the Internet of Things is a type of network of some physical objects or things which, embedded with software, electronics, sensors and connectivity that enables them, achieves greater value and service by exchanging data with manufacturers, operators and some other connected devices [5]. Thus, the intensive computations and the mass storage, which are supported by clouds, are often inefficient. Some examples include the limitations of storage, communication capabilities, energy and processing. Such inefficiencies motivate us to combine the technology of Mobile Cloud Computing (MCC) and the Internet of Things. As an emerging technology, Mobile Cloud Computing integrates multiple technologies for maximizing capacity and performance of the existing infrastructure [6].

Moreover, there is another technology, called Mobile Cloud Computing (MCC), which improved through the recent years by a new generation of services which is made its appearance, based on the concept of the "cloud computing" which aims to provide access to the information and the data from anywhere at any time by restricting or eliminating the need for hardware equipment [7]. More specifically, Mobile cloud computing is defined as an integration of cloud computing technology and mobile devices in order to make mobile devices resourceful in terms of computational power, memory, storage, energy, and context awareness. Also, Mobile cloud can be defined as a contemporary approach to innovative services for firms and institutions [8]. Mobile cloud computing is the outcome of interdisciplinary approaches, which consists of mobile computing and cloud computing [9]. The term mobile cloud is generally referred to in two perspectives: (a) infrastructure based, and (b) ad-hoc mobile cloud. In infrastructure based mobile cloud, the hardware infrastructure remains static, and provides services to the mobile users. As a result of the operations of Cloud Computing, it could be used as useful bases for both Internet of Things and Video Surveillance technologies and could provide improvements on their functions.

The rest of the paper is organized as follows. In section 2 there is a review of the related research which deals with the technology of Internet of Things and Cloud Computing and their integration. Section 3 discusses in detail the technology of Internet of Things and some of its basic functions. Moreover, section 4 presents and analyzes the Cloud Computing technique, and its characteristics. Section 5 illustrates the integration of the Internet of Things technology and the Cloud Computing technology, and surveys some of their benefits. Finally section 6 provides the conclusions of the current paper, and offers new possibilities for the development of future work.

II. Related Research Review

For the purpose of this paper we study and analyze previous literature which has been published in the field of cloud computing and Internet of Things, and their integration. The following paragraphs present the papers which contributed significantly in our study.

To begin with, a survey of the different security risks that pose a threat to the cloud is presented in [10]. Also, in [10] was given a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system. Moreover, an exploration of the roadblocks and solutions to provide a trustworthy cloud computing environment presented in [11]. Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbate security and privacy challenges.

Concerning the integration of Internet of Things and Cloud Computing, there have been made some previous studies. A propose of a new platform for using cloud computing capacities for provision and support of ubiquitous connectivity and real-time applications and services for smart cities' needs is given in [12]. Additionally, a presentation of a framework for data procured from highly distributed, heterogeneous, decentralized, real and virtual devices (sensors, actuators, smart devices) that can be automatically managed, analyzed and controlled by distributed cloud-based services shown in [12]. In order to realize the full sharing, free circulation, on-demand use, and optimal allocation of various manufacturing resources and capabilities, the applications of the technologies of IoT and CC in manufacturing are investigated in [13]. Furthermore, a CC- and IoT-based cloud manufacturing (CMfg) service system (i.e.,CCIoT-CMfg) and its architecture are proposed, and the relationship among CMfg, IoT, and CC is analyzed. And finally, the advantages, challenges, and future works for the application and implementation of CCIoT-CMfg are discussed in [13]. The [14] mainly focuses on a common approach to integrate the Internet of Things (IoT) and Cloud Computing under the name of CloudThings architecture. Also, in [14] review the state of the art for integrating Cloud Computing and the Internet of Things, and examine an IoT-enabled smart home scenario to analyze the IoT application requirements. At the end, the CloudThings architecture, a Cloud-based Internet of Things platform which accommodates CloudThings IaaS, PaaS, and SaaS for accelerating IoT application, development, and management proposed in [14]. Furthermore, a presentation and discussion about some of the integration challenges of Iot and Cloud Computing that must be addressed to enable an intelligent transportation system to address issues facing the transportation sector such as high fuel prices, high levels of CO2 emissions, increasing traffic congestion, and improved road safety are shown in [15].

A presentation of an approach to the development of Smart Home applications by integrating Internet of Things (IoT) with Web services and Cloud computing are shown in [16]. The approach focuses on: (1) embedding intelligence into sensors and actuators using Arduino platform; (2) networking smart things using Zigbee technology; (3) facilitating interactions with smart things using Cloud services; (4) improving data exchange efficiency using JSON data format. Also, it is shown an

implementation of three use cases to demonstrate the approach's feasibility and efficiency, i.e., measuring home conditions, monitoring home appliances, and controlling home access. The [17] presents a Cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A Cloud implementation using Aneka, which is based on interaction of private and public Clouds is also presented in [17]. Finally, it concludes the IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community. Internet of Things (IoT) becoming so pervasive that it is becoming important to integrate it with cloud computing because of the amount of data IoT's could generate and their requirement to have the privilege of virtual resources utilization and storage capacity, but also, to make it possible to create more usefulness from the data generated by IoT's and develop smart applications for the users. This type of integration is referred to as Cloud of Things in [18]. With IoTs, anything can become part of the Internet and generate data. Moreover, data generated needs to be managed according to its requirements, in order to create more valuable services. For the previous purpose, integration of IoTs with cloud computing is becoming very important. This new paradigm is termed as Cloud of Things (CoTs) and it is presented in [19]. The [20] focuses in the attention of the authors on the integration of Cloud and IoT, which is what we call the CloudIoT paradigm. Also, many works in literature have surveyed Cloud and IoT separately and, more precisely, their main properties, features, underlying technologies, and open issues in [20]. However, these works lack a detailed analysis of the new CloudIoT paradigm, which involves completely new applications, challenges, and research issues. The [21] focuses on some of the key challenges involved in CoT and the proposal of smart gateway based communication. Cloud of Things, requires smart gateway to perform the rich tasks and preprocessing, which sensors and light IoTs are not capable of doing. Finally, the [22] presents a survey of integration components: Cloud platforms, Cloud infrastructures and IoT Middleware. In addition, some integration proposals and data analytics techniques are surveyed as well as different challenges and open research issues are pointed out.

Finally, we study integration algorithms and methods about the aforementioned technologies. In [23] the authors focus on Fuzzy C-Means based segmentation algorithms because of the segmentation accuracy they provide. Furthermore, the algorithms which have been studied need long execution times. Also, the authors of [23] accelerate the execution time of these algorithms using Graphics Process Unit (GPU) capabilities. At the end, the authors reach the achievement performance enhancement by up to 8.9x without compromising the segmentation accuracy. The main aim of the [24] is to perform a review of the basic methods used for such techniques and finding the emerging trends of the research in this area. The authors of [24] primary focus on summarize some well-known methods of face recognition in video sequences for application in biometric security and enumerate the emerging trends. The [25] in order to address the challenge of the lack of investigating on effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms and applications, surveys the state-of-the-art of social media networks security and trustworthiness particularly for the increasingly growing sophistication and variety of attacks as well as related intelligence applications. Also, the authors of [25] highlighted a new direction on evaluating and measuring the fundamental and underlying platforms. Furthermore, the authors propose a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing, which is essential for social media ecosystem.

Table 1 lists the findings and the concepts examined in each paper. In more detail, in Table 1 could observe independently for each related review that have been studied useful information related to the year which published, the exact authors, and as a conclude for each paper the problems and the solutions which they deal with.

Year	Author	Problems	Solutions
2010	H. Takabi et al **[11]**	• Unique aspects exacerbate security and privacy challenges of Cloud Computing.	• Explores the roadblocks and solutions to providing a trustworthy Cloud Computing environment.
2011	S. Subashini & V. Kavitha **[10]**	• How safe is a Cloud Computing environment is. • Enterprise customers are still reluctant to deploy their business in the cloud. • Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market.	• A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. • Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. • Different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.
2013	J. Gubbi et al **[17]**	• Fueled by the recent adaptation of a variety of enabling wireless technologies, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. • The need for data-on-demand using sophisticated intuitive queries increases significantly.	• A Cloud centric vision for worldwide implementation of Internet of Things. • Cloud implementation using Aneka, which is based on interaction of private and public Clouds. • Expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.
2013	G. Suciu et al **[12]**	• Cloud Computing and Internet of Things (IoT) are two of the most popular ICT paradigms. • The convergence between cloud computing and IoT has become a hot topic over the last few years.	• A new platform for using cloud computing capacities for provision and support of ubiquitous connectivity and real-time applications and services for smart cities' needs. • A framework for data procured from highly distributed, heterogeneous, decentralized, real and virtual devices that can be automatically managed, analyzed and controlled by distributed cloud-based services.
2013	J. Zhou et al **[14]**	• User with a novel means of communicating with the Web world through ubiquitous object-enabled networks presented by Internet of Things. • Cloud Computing enables a convenient, on demand and scalable network access to a shared pool of configurable computing resources..	• A common approach to integrate the Internet of Things (IoT) and Cloud Computing under the name of CloudThings architecture. • An IoT-enabled smart home scenario to analyze the IoT application requirements.
2013	M. Soliman et al **[16]**	• Smart Home minimizes user's intervention in monitoring home settings and controlling home appliances.	• An approach to the development of Smart Home applications by integrating Internet of Things (IoT) with Web services and Cloud computing..
2014	M. Aazam et al **[18]**	• Everything is going to be connected to the Internet and its data will be used for various progressive purposes. • Internet of Things (IoT) becoming so pervasive that it is becoming important to integrate it with cloud computing.	• IoT's and cloud computing integration is not that simple and bears some key issues. Those key issues along with their respective potential solutions have been highlighted.
2014	M. Aazam et al **[21]**	• Integration of Internet of Things with Cloud Computing is gaining importance, with the way the trend is going on in ubiquitous computing world. • Internet of Things (IoT) becoming so pervasive that it is becoming important to integrate it with cloud computing.	• Integration of IoT with Cloud Computing, referred here as Cloud of Things, requires smart gateway to perform the rich tasks and preprocessing, which sensors and light IoTs are not capable of doing. • Focuses on some of the key challenges involved in CoT and the proposal of smart gateway based communication.
2014	F. Tao et al **[13]**	• Internet of Things (IoT) and cloud computing (CC) have been widely studied and applied in many fields, as they can provide a new method for intelligent perception and connection from M2M, and on-demand use and efficient sharing of resources, respectively.	• A CC- and IoT-based cloud manufacturing (CMfg) service system and its architecture are proposed. • The advantages, challenges, and future works for the application and implementation of CCIoT-CMfg are discussed.
2015	A. Botta et al **[20]**	• Cloud computing and Internet of Things (IoT) are two very different technologies that are both already part of our life. • A novel paradigm where Cloud and IoT are merged together is foreseen as disruptive and as an enabler of a large number of application scenarios.	• Integration of Cloud and IoT, which is called the CloudIoT paradigm. • A new CloudIoT paradigm, which involves completely new applications, challenges, and research issues.
2015	J. A. Guerrero Ibanez et al **[15]**	• Performance of transportation systems is of crucial importance for individual mobility, commerce, and for the economic growth of all nations. • It is imperative to improve the safety and efficiency of transportation.	• Integration challenges of IoT and CC that must be addressed to enable an intelligent transportation system to address issues facing the transportation sector.
2016	M. Diaz et al **[22]**	• Internet of Things comprises many interconnected technologies like RFID and WSAN in order to exchange information. • The limitations of associated devices in the IoT require a	• A survey of integration components: Cloud platforms, Cloud infrastructures and IoT Middleware.

		technology like Cloud Computing to supplement this field.	
2016	M. Aazam et al **[19]**	• It is becoming very difficult to manage power constrained small sensors and other data generating devices. • Data generated needs to be managed according to its requirements, in order to create more valuable services.	• Integration of IoTs with cloud computing is becoming very important – Cloud of Things. • CoTs provide means to handle increasing data and other resources of underlying IoTs and WSNs.
2016	M. Alsmirat et al **[23]**	• Big revolution in information technology that is used to diagnose many illnesses and saves patients lives. • Image segmentation is a mandatory step in many image processing based diagnosis procedures.	• Fuzzy C-Means based segmentation algorithms provide segmentation accuracy. • Accelerate the execution time of Fuzzy C-Means algorithms using Graphics Process Unit (GPU) capabilities.
2016	B. B. Gupta et al **[24]**	• Face recognition from video has gained attention due to its popularity and ease of use with security systems based on vision and surveillance systems. • Automated video based face recognition system provides a huge assortment of challenges as it is necessary to perform facial verification under different viewing conditions.	• Perform a review of the basic methods used for such techniques and finding the emerging trends of the research in this area. • Summarize some well-known methods of face recognition in video sequences for application in biometric security and enumerate the emerging trends.
2016	Z. Zhang et al **[25]**	• Social media security and trustworthiness issues have become increasingly serious. • Lack of investigating on effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms and applications.	• Survey on the state-of-the-art of social media networks security and trustworthiness particularly for the increasingly growing sophistication and variety of attacks. • Highlight a new direction on evaluating and measuring those fundamental and underlying platforms. • Propose a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing.

Table 1: Mapping problems against referenced solutions.

III. INTERNET OF THINGS

The Internet of Things is a network of devices that transmit, share, and use data from the physical environment to provide services to individuals, corporations, and society. The objects-things function either individually or in connection with other objects or individuals, and have unique IDs (identifiers). Also, the Internet of Things has different applications in health, transport, environment, energy or types of devices: sensors, devices worn/carried (wearable), e.g. watch, glasses, home automation (domotics).

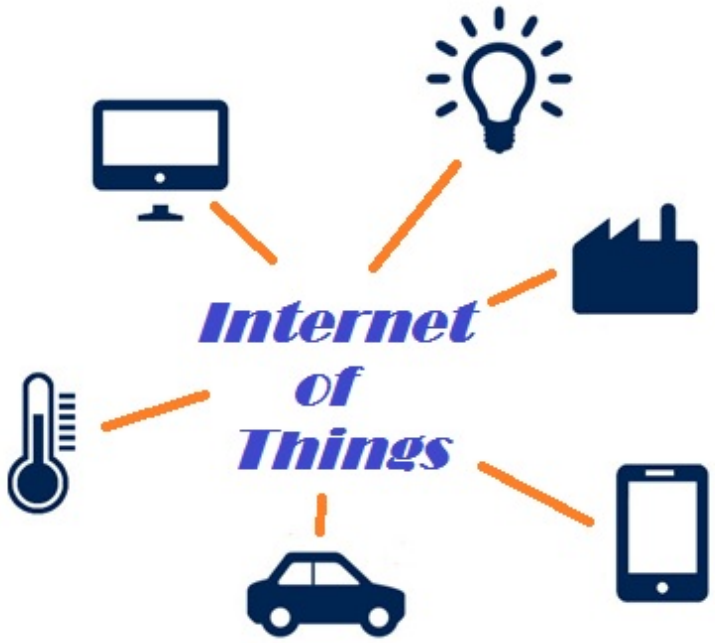

Figure 1: Internet of Things Technology.

3.1. Internet of Things: Advantages of the data

What does it mean when the devices and sensors are networked together and communicate with each other? How can the Internet of Things affect our daily life? GPS systems, alarm systems, and thermostats, all send and receive constant feeds to monitor and automate activities in our daily lives [26]. And the not so obvious: Mosaic, cups, clothes and other everyday objects can also join network to send and receive data over the Internet.

Opportunities where the streaming data will create new markets in order to inspire positive change or to enhance existing services are examined by businesses. Some examples of sectors that are at the heart of these developments are listed below [27]:

a) Smart solution in the bucket of transport: Smart solutions in the bucket of transport, achieve a reduction of traffic on the roads, reduce fuel consumption, set priorities in vehicle repair programs, and save lives.
b) Smart power grids incorporating more renewable: Smart power grids incorporating more renewables improve system reliability, and reduce the charges consumers, thus providing cheaper electricity.
c) Remote monitoring of patients: Remote monitoring of patients provides easy access to health care, improves the quality of services, increases the number of people served, and saves money.
d) Sensors in homes and airports: Sensors in homes and airports, or even in your shoes or doors, improve safety by sending signals when left unused for a certain period of time or when used in the wrong time.
e) Engine monitoring sensors that detect & predict maintenance issues: Engine monitoring sensors that detect and predict maintenance issues, improve inventory replenishment, and even define priorities in scheduling maintenance work, repairs, and regional operations.

3.2. Internet of Things Security

IoT security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things. The Internet of Things involves the increasing prevalence of objects and entities – known, in this context as things -- provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices [28] [29].

The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. IoT products are often sold with old and unpatched embedded operating systems and software. Furthermore, purchasers often fail to change the default passwords on smart devices -- or if they do change them, fail to select sufficiently strong passwords. To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be monitored to identify potential anomalous traffic, and action should be taken if there is a problem.

Security experts have warned of the potential risk of large numbers of unsecured devices connecting to the Internet since the IoT concept was first proposed in the late 1990s. In December of 2013, a researcher at Proofpoint, an enterprise security firm, discovered the first IoT botnet. According to Proofpoint, more than 25 percent of the botnet was made up of devices other than computers, including smart TVs, baby monitors and other household appliances [28].

3.3. Internet of Things Security model

In the field of Internet of Things technology there are System models and initial conditions considered are as similar as that of [30]. A wireless network model with a source-destination pair, N trusted relays and J eavesdroppers $\left(J \le 1\right)$ are considered. Assume that the global CSE is available. The eavesdropper channel, source encoding schemes, decoding schemes and cooperative protocol are considered to be public, only source message is assumed to be confidential. In this paper, the discussion is limited to two main cooperative schemes: decode-and-forward (DF) and amplify-and-forward (AF) [31].

Decode-and-forward (DF)

There are two main stages in DF. Source broadcasts its encoded symbols to its trusted relays using the first transmission slot in Stage 1. When transmitting the symbol *x*, the received signals at the *N* relays are given by,

$$y_r = \sqrt{P_s} h_{SR}^* x + n_r \quad (1)$$

where P_s is the transmit power of source and n_r is the noise vector at relays [31].

In Stage 2, all the trusted relays that successfully decode the message, re-encode the message and cooperatively transmit the re-encoded symbols to the destination by using the second transmission slot. Each relay transmits a weighted version of the re-encoded symbol. When transmitting the symbol $\tilde{x}$, the received signal at the destination is given by,

$$y_d = h_{RD}^{\dagger} w\tilde{x} + n_d \quad (2)$$

while the received signal at the eavesdroppers is expressed in vector form as,

$$y_e = H_{RE}^{\dagger} w\tilde{x} + n_e \quad (3)$$

The transmit power budget for Stage 2 is considered to be P - P_s where P is the total power for transmitting one symbol and P_s is the transmit power of source [31].

Amplify-and-forward (AF)

AF is also a two-stage scheme as that of DF. Stage 1 is the same for both AF and DF, except that the transmit power can be different. The trusted relays forward the signals that are received during Stage 1 to the destination, using the second transmission slot in Stage 2. That is, each relay transmits a weighted version of the noisy signal that they received during Stage 1. The transmitted signals of all

relays are denoted by the product of $diag\{w\}y_r$, where w is the weight vector and y_r is given by (1). The received signal at the destination is given by [30],

$$y_d = \sqrt{P_s} h_{RD}^{\dagger} diag\{w\} h_{SR}^{*} x + h_{RD}^{\dagger} diag\{w\} n_r + n_d \quad (4)$$

The received signals at the eavesdroppers, in a vector form, is denoted by [26],

$$y_e = \sqrt{P_s} H_{RE}^{\dagger} diag\{w\} h_{SR}^{*} x + H_{RE}^{\dagger} diag\{w\} n_r + n_e \quad (5)$$

where P_s is the transmit power of source, n_r is the noise vector at relays and x is the received signal. Also, equations (4) and (5) generated from (1) and (2), and (1) and (3) respectively.

Additionally, another security challenge in IoT is the encryptions algorithm. The RSA algorithm, which is the most commonly used public key algorithm in the Internet, can be used in sensor networks with the assistance of a Trusted Platform Module (TPM), which costs less than 5% of a common sensor node [32]. Thus, the memory has been measured for a fully authenticated handshake with 2048-bit RSA keys. This type of handshake has the largest memory requirements since it needs more code and buffer space for the client's *Certificate* and *CertificateVerify* messages. The memory increased its use because the code basically contains hundreds of statements form *buffer[x] = 0xff*. The use of this encryption algorithm in IoT's security could provide better communication privacy in its functionality.

IV. Cloud Computing

Cloud computing provides computing, storage, services, and applications over the Internet. In general, to render smartphones energy efficient and computationally capable, major changes to the hardware and software level are required. This entails the cooperation of developers and manufacturers. [33]. Mobile cloud computing is defined as an integration of cloud computing technology with mobile devices in order to make the mobile devices resource-full in terms of computational power, memory, storage, energy, and context awareness. The technology of Mobile Cloud computing is the outcome of interdisciplinary approaches combining mobile computing with cloud computing. Thus, this transdisciplinary domain is also referred as mobile cloud computing [33].

There are two perspectives in which the term Mobile Cloud refers: a) infrastructure based, and b) ad-hoc mobile cloud. In the infrastructure based mobile cloud, the hardware infrastructure remains static and also provides services to the mobile users. Nevertheless, there are several applications which utilize cloud resources, but the usage is limited to only storage and application-specific services such as Apple's Siri (voice based personal assistant) and iCloud storage service.

Figure 2: Cloud Computing Technology.

4.1. Cloud Computing Features

As all technologies, so the Cloud Computing technology has some features which determine its function. These features are analyzed and outlined subsequently.

Storage over Internet

Storage over Internet can be defined as a technology framework that uses Transmission Control Protocol/Internet Protocol (TCP/IP) networks to link servers and storage devices, and to facilitate storage solution deployment. The Storage over Internet technology is also known as Storage over Internet Protocol (SoIP) technology. With the combination of the best storage and networking industry approaches, SoIP provides high-performance and scalable IP storage solutions [34] [35] [36].

Service over Internet

The main objective of the Service over Internet is to be committed to help customers all over the world in order to transform aspirations into achievements by harnessing the Internet's efficiency, speed and ubiquity [34] [35].

Applications over Internet

The programs which can be written to do the job of a current manual task, or virtually anything, and which perform their job on the server (cloud server) via an internet connection rather than the traditional model of a program that has to be installed and run on a local computer are the Cloud Applications, or as a scientific definition Applications over Internet. Some examples of powerful programs which run in the cloud and they perform incredible feats of computing for the oblivious user who only needs an internet connection and a browser, are google applications, internet banking, and Facebook [34] [35] [37].

Energy Efficiency

As a definition, the Energy Efficiency is a way of managing and restraining the growth in energy consumption. By delivering more services for the same energy input or for the same services for less energy input may be something more energy efficient. As an example, when a Compact Florescent Light (CFL) bulb uses less energy (1/3 to 1/5) than an incandescent bulb to produce the same amount of lights, the Compact Florescent Light (CFL) is considered to be more energy efficient [34] [35] [37].

Computationally Capable

The services of computational clouds are leveraging the computationally intensive and ubiquitous mobile applications which have been enabled by the technology of Mobile Cloud Computing. Thus, a system is considered as computationally capable when it meets the requirements to provide us the results we want, by making the right calculations [34] [35].

4.2. Mobile Cloud Computing trade offs

Mobile Cloud Computing has some disadvantages-limitations which should be eliminated over the years in order to achieve a better and more ideal use. A number of businesses, and especially the smaller ones need to be aware of these limitations before going in for this technology.

Security

One major issue of the Mobile Cloud Computing is the security issue. Before someone adopts this technology, they should know that all the company's sensitive information would be surrender to a third-party cloud service provider. This could potentially put the company in great risk. Hence, someone must be absolutely sure that they would choose the most reliable service provider, who will keep the information completely safe [38] [39].

Connectivity

Internet connection is critical to Mobile Cloud Computing. Thus, the user should be certain that there is a good result before opting for these services. Since someone owes a mobile device which is connected to the internet has become the norm in the wireless world of today, Mobile Cloud Computing has a very large potential user base [40].

Performance

Another major concern of the Mobile Cloud Computing pertains to its performance. Some users feel performance is not as good as in native applications. Thus, checking with one service provider and understanding their track record is advisable [41] [42].

Latency (Delay)

In mobile cloud computing, latency (sometimes referred as turnaround time) is defined as the time involved in offloading the computation and getting back the results from the nearby infrastructure or cloud.

Privacy

Data privacy is important and is one of the main bottlenecks that restrict consumers from adopting mobile cloud computing. Therefore, to gain consumers trust in the mobile cloud, the application models must support application development with privacy protection, and implicit authentication mechanisms [39] [43].

4.3. Mobile Cloud Computing Security Issues

Cloud computing security or cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers [44]. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community) [45] [46]. There are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced by cloud providers (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud) [38] [48]. The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

4.4. Cloud Computing Security model

In order to provide secure communication over the network, encryption algorithm plays an important role. It is a valuable and fundamental tool for the protection of the data. Encryption algorithm converts the data into scrambled form by using "a key" and only the user have the key to decrypt the data. Regarding the researches that have been made, an important encryption technique is the Symmetric key Encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. In this encryption technique the most used algorithm is the AES [49] [50].

AES (Advanced Encryption Standard) is the new encryption standard recommended by NIST to replace DES algorithm. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. The AES algorithm block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [51] [52].

A part of the AES algorithm represented in this work. This algorithm uses the original key consists of the number of bytes in any case, which are represented as a 4x4 matrix.

Algorithm

```
Cipher(byte[] input, byte[] output)
{
        byte[4,4] State;
        copy input[] into State[] AddRoundKey
        for (round = 1; round < Nr-1; ++round)
        {
                SubBytes ShiftRows MixColumns AddRoundKey
        }
        SubBytes ShiftRows AddRoundKey
        copy State[] to output[]
}
```

AES algorithm considered as better than others for a number of reasons, which is follows [53]:

- ✓ AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.
- ✓ Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- ✓ This algorithm has speedy key setup time and good key agility.
- ✓ It requires less memory for implementation, making it suitable for restricted-space environments.
- ✓ The structure has good potential for benefiting from instruction-level parallelism.
- ✓ There are no serious weak keys in AES.
- ✓ It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
- ✓ Statistical analysis of the cipher text has not been possible even after using huge number of test cases.
- ✓ No differential and linear cryptanalysis attacks have been yet proved on AES.

Additionally, there is an important encryption technique from the Asymmetric key Encryption. In Asymmetric key encryption, two keys, private and public keys, are used. Public key is used for encryption and private key is used for decryption [49] [50].

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [54].

The RSA algorithm which studied in this work uses a key generator that provides two large primes. Those primes are used in order to procced the encryption mode. The two large primes represent the two types of keys that we use in decryption and encryption, the public key and the secret key.

Algorithm

Key Generation: KeyGen(p, q)

Input: Two large primes – p, q

Compute $n = p \cdot q$

$\varphi(n) = (p - 1)(q - 1)$

Choose e such that $\gcd(e, \varphi(n)) = 1$

Determine d such that $e \cdot d \equiv 1 \bmod \varphi(n)$

Key:

public key = (e, n)

secret key= (d, n)

Encryption:

$c = m^e \bmod n$

where *c* is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product [44].

The equation given $c_i = E(mi) = mi^e \bmod n$, then we have the following:

$$(c1 \,.\, c2) \bmod n = (m1 \,.\, m2)^e \bmod n$$

V. IoT and Cloud Computing Integration

Moreover, a new generation of services, based on the concept of the 'cloud computing', has made its appearance in the last few years with the purpose of providing access to the information and the data from any place at any time, thus restricting or eliminating the need for hardware equipment. The term 'cloud computation' is defined as the use of computing logistical resources, as well as the software level, through the use of services transported over the Internet. Nowadays, cloud computing services comprise one of the world's largest areas of competition between giant companies in the IT sector and software [55]. Cloud Computing is a technology which can be set as a base technology in the use of IoT.

More specifically, Mobile Cloud Computing is defined as an integration of cloud computing technology with mobile devices so as to make the mobile devices resourceful in terms of computational power, memory, storage, energy, and context awareness. Mobile Cloud Computing is the outcome of interdisciplinary approaches, combining mobile computing and cloud computing [56]. In addition, Cloud computing provides computing, storage, services, and applications over the Internet. The technology of Mobile Cloud Computing is the outcome of interdisciplinary approaches, combining mobile computing with cloud computing. Thus, this transdisciplinary domain is also referred as Mobile Cloud Computing [57].

Some of the main features of the Cloud Computing technology which relate to the characteristics of both Internet of Things are: a) Storage over Internet, b) Service over Internet, c) Applications over internet, d) Energy efficiency and e) Computationally capable. Tables 2 lists the features of Mobile Cloud Computing regarding the convenience this technology offers when combined with the characteristics of IoT.

Internet of Things characteristics	Storage over Internet	Service over Internet	Applications over Internet	Energy efficiency	Computationally capable
Smart solution in the bucket of transport	**X**	**X**	**X**		**X**
Smart power grids incorporating more renewable	**X**	**X**		**X**	**X**
Remote monitoring of patients		**X**	**X**		**X**
Sensors in homes and airports	**X**	**X**	**X**	**X**	**X**
Engine monitoring sensors that detect & predict maintenance issues		**X**	**X**	**X**	**X**

Table 2: Contributions of Cloud Computing in Internet of Things.

Table 2 lists the features of Cloud Computing technology regarding the convenience this technology offers. Also, it enumerates the main features of the Internet of Things technology. The main purpose of Table 2 is to show which of the specific features of Cloud Computing technology, related more and improve the features of Internet of Things technology. As we can observe from Table 2, the feature of IoT which affected more by the features of Cloud Computing is "Sensors in homes and airports". Regarding the Cloud Computing, the feature which affected more are "Service over Internet" and "Computationally capable". As a general conclusion, we can observe that those two technologies contribute more each other in many of their features.

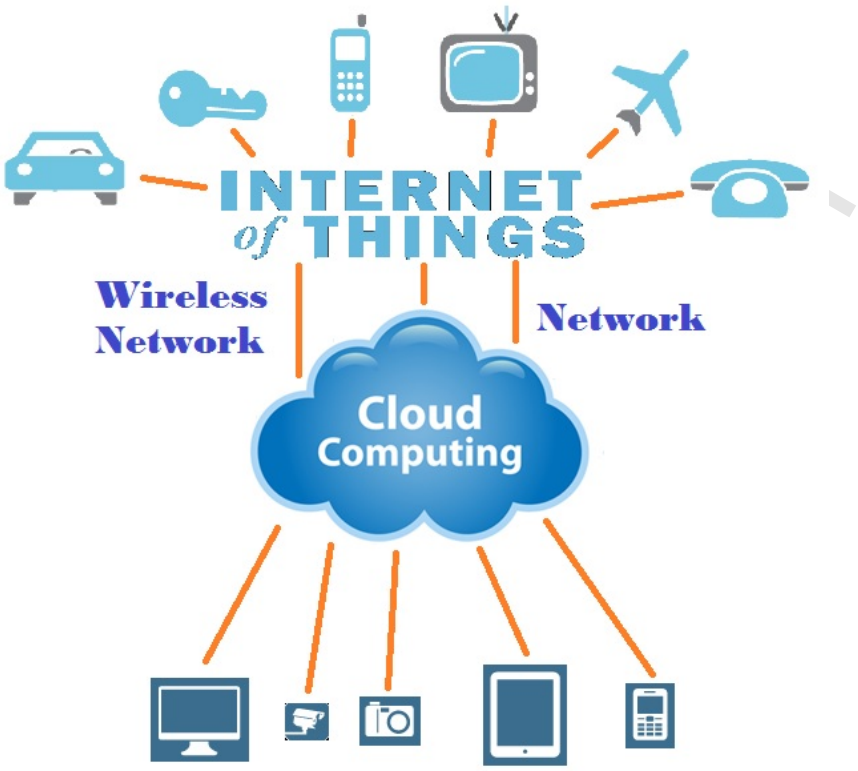

Figure 3: IoT & Cloud Computing Integration.

Through the integration of IoT and Cloud we have the opportunity to expand the use of the available technology that provided in cloud environments. Applications and information that use the Internet of Things technology with this integration can be used through the cloud storage. The integration of IoT and Cloud technologies represented in Figure 3. The cloud offers to mobile and wireless users to access all the information and the application that needed for the IoT connectivity.

5.1. Security issues in IoT and Cloud Computing integration

There is a rapid and independent evolution considering the two words of IoT and Cloud Computing. To begin with, the virtually unlimited capabilities and resources of Cloud Computing in order to compensate its technological constrains, such as processing, storage and communication, could be a benefit for the Internet of Things technology [58]. Also, the IoT technology extends its scope to deal with real world things in a more distributed and dynamic manner and by delivering new services in a large number of real life scenarios, might be beneficial for the use of Cloud Computing technology. In many cases, Cloud can provide the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement the latter [20].

Through the integration of IoT and Cloud Computing could be observed that Cloud Computing can fill some gaps of IoT such the limited storage and applications over internet. Also, IoT can fill some gaps of Cloud Computing such the main issue of limited scope. Based in motivations such those referred previously and the important issue of security in both technologies we can consider some drivers for the integration. The security issue of this integration has a serious problem. When critical IoT applications move towards the Cloud Computing technology, concerns arise due to the lack of trust in the service provider or the knowledge about service level agreements (SLAs) and knowledge about the physical location of data. Consequently, new challenges require specific attention as mentioned in surveys [59] [60] [61]. Multi-tenancy could also compromise security and lead to sensitive information leakage. Moreover, public key cryptography cannot be applied at all layers due to the computing power constraints imposed by the things. These are examples of topics that are currently under investigation in order to tackle the big challenge of security and privacy in Cloud Computing and IoT integration [20].

Subsequently, some challenges about the security issue in the integration of two technologies are listed [20].

a) Heterogeneity. A big challenge in Cloud Computing and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications [62].
b) Performance. Often Cloud Computing and IoT integration's applications introduce specific performance and QoS requirements at several levels (i.e. for communication, computation, and storage aspects) and in some particular scenarios meeting requirements may not be easily achievable [63] [64].
c) Reliability. When Cloud Computing and IoT integration is adopted for mission-critical applications, reliability concerns typically arise e.g., in the context of smart mobility, vehicles are often on the move and the vehicular networking and communication is often intermittent or unreliable. often intermittent or unreliable. When applications are deployed in resource constrained environments a number of challenges related to device failure or not always reachable devices exists [65].
d) Big Data. With an estimated number of 50 billion devices that will be networked by 2020, specific attention must be paid to transportation, storage, access, and processing of the huge amount of data they will produce. The ubiquity of mobile devices and sensor pervasiveness, indeed call for scalable computing platforms [66].
e) Monitoring. As largely documented in the literature, monitoring is an essential activity in Cloud environments for capacity planning, for managing resources, SLAs, performance and security, and for troubleshooting [67].

IoT & Cloud Computing security challenges	Heterogeneity	Performance	Reliability	Big Data	Monitoring
Internet of Things		**X**	**X**	**X**	**X**
Cloud Computing	**X**	**X**		**X**	

Table 3: Affects of IoT & Cloud Computing security challenges.

Table 3 lists the two technologies that we study in this paper and the challenges of their integration that arising from our study. These challenges related to the security issue in the integration of two aforementioned technologies and they listed in detailed in *subsection 5.1*. As we can observe from Table 3, the both technologies have two common main challenges of their integration which are Performance and Big Data. Additionally, we can observe that Internet of Things technology related to more challenges (4) than the Cloud Computing technology (3).

5.2. Proposed Efficient IoT and Cloud Computing security model

As we can infer, by taking advantage of the reasons which AES algorithm provides better secure in Cloud Computing and the two models that give benefits in security issues in IoT we can propose a new method that uses those benefits in order to improve the security and privacy issues in the integration of two technologies.

The AES algorithm provides the ability to have speed key setup time a good key agility. So, if we use this algorithm in the functionality of DF model, we could have a trusted relay method with an encryption of a speed key setup. Therefore, instead the trust relay use that DF and AF methods provide we can seize also there no serious weak keys in AES and so we could have a beneficial security use of the encryption in the integrated new model. Moreover, we can take advantage the less memory which AES needs for implementation that makes it for restricted-space environments. Thus, we can seize the transmit power that the AF model provides and as a result we can have a better and more trusted transmission. In the way of transmission, when the symbol $\tilde{x}$ transmitted with the use of DF model, the received signal at destination is given by the equation (2), which mentioned in previous section.

With this proposed model we can extend the advances of Internet of Things and Cloud Computing, by developing a highly innovative and scalable service platform to enable secure and privacy services. Through this research we can propose the following algorithm which extends the security advances of both technologies.

Key Generation: KeyGen(p, q)
Input: Two large primes – p, q
Compute n = p . q
buffer(n) = (p - 1)(q - 1)
Choose e such that gcd(e, buffer(n)) = 1

In which algorithm the equation method that contains hundreds of statements of the form *buffer[x]=0xff* is combined. With the use of this new type of RSA algorithm in the encryption process, we can conclude that a higher level of communications' security can be provided in the functionalities of the IoT.

Key:
public key = (e, n)
secret key= (d, n)
Encryption:
c = me mod n
where *c* is the cipher text and m is the plain text.

Also, as a proposal of this work could be the following part of algorithm which uses the original key consists of 128 bits/16 bytes which are represented as a 4x4 matrix. With the use of this part of AES algorithm we can draw that data which encrypted with 128bit (or 16 bytes) can be have better encrypted as an 4x4 matrix in order of providing a better use of communication privacy.

```
Cipher(byte[] input, byte[] output)
{
        byte[4,4] State;
        copy input[] into State[] AddRoundKey
        for (i=4; i<44; i++)
        {
                T = W[i-1];
                if (i mod 4 = = 0)
                        T = Substitute (Rotate (T)) XOR RConstant [i/4];
                W[i] = W[i-4] XOR T;
                SubBytes ShiftRows MixColumns AddRoundKey
        }
        SubBytes ShiftRows AddRoundKey
        copy State[] to output[]
}
```

Characteristics	Developed	Key length	Rounds	Certifications	Speed
AES	1998	128, 192 or 256 bits	10, 12 or 14	AES winner, CRYPTREC, NESSIE, NSA	Very fast
RSA	1977	1024-4096 bits	1	PKCS#1, ANSI X9.31, IEEE 1363	Very fast

Table 4: Comparison of AES and RSA algorithms.

Table 4 lists the key characteristics of the two encryption algorithms which have been studied and used in order to use them for the experimental proposal. The key characteristic which is more important is their Speed in which both algorithms are very fast. The key characteristic in which there is a relative difference is the Rounds, where AES needs 10, 12 or 14 rounds instead of the RSA that needs only 1.

5.3. Experimental results

Considering the benefits of the security models and algorithms of Internet of Things and Cloud Computing technologies we can observe that we can have a beneficial use of integration those two technologies. Instead of the wide use of IoT we can take advantage that Cloud Computing security through the AES algorithm performs consistently well in both hardware and software platforms under a wide range of environments. This use could be possible for all type of platforms and DSPs. Furthermore,

the new integrated technology could has good potential for benefiting from instruction-level parallelism and will support any type of block sizes and key sizes that are multiples of 32 and used both of IoT and Cloud Computing. Also, each transmitted signal through the new technology can transmitted as a relay and trusted signal with a weighted version of the re-encoded symbol. By the use of RSA algorithm we can take advantage the two keys encryption in order to provide better secure in the use of the new model.

Through this integration we can achieve some useful functions, i.e. we can use the Cloud-based IoT service in order to connect sensors and also made them capable to share the sensor readings with others, reducing the security issues. Furthermore, another useful function is that we can use the HTTP protocol in order to send data between IoT things and the Cloud Computing applications. Moreover, some of the key advantages and challenges that can be defined from this integration are: 1) Both the physical hardware manufacturing resource and software manufacturing can be intelligently perceived and connected into the wider networks with the support of IoT technologies. 2) The collected information and data can be communicated and transmitted between M2M under the support of specific IoT technologies. 3) The collected and transmitted information can be processed and computed according to specific requirements under the support of different Cloud Computing service, and some useful data and decision information can be intelligently generated and obtained.

However, many other challenges and other benefits remains to be addressed through the integration of Internet of Things and Cloud Computing regarding the security issues, but also regarding the hole use of both technologies together.

AES Characteristics	Key length	Rounds	Certifications	Speed
Internet of Things	X		X	X
Cloud Computing	X	X	X	
IoT & CC integration	X	X	X	X

Table 5: AES contribution in IoT and Cloud Computing.

RSA Characteristics	Key length	Rounds	Certifications	Speed
Internet of Things	X		X	X
Cloud Computing	X	X	X	
IoT & CC integration	X	X	X	X

Table 6: RSA contribution in IoT and Cloud Computing.

The Tables 5 and 6 exhibiting the key characteristic of the two encryption algorithms that used in order to achieve integration of the technologies of IoT and Cloud Computing concerning the security issue. Table 5 presents which of the key characteristics of AES encryption algorithm contributes both IoT and Cloud Computing technologies, and at the end how completely contributes the integration model of IoT and Cloud Computing. Subsequently, Table 6 presents which of the key characteristics of RSA encryption algorithm also contributes both IoT and Cloud Computing technologies, and at the end how completely contributes the integration model of IoT and Cloud Computing too.

VI. CONCLUSION

The Cloud Computing technology offers many possibilities, but also places several limitations as well. Cloud Computing refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. In this paper, we present a survey of Internet of Things Technology, with an explanation of its operation and use. Moreover, we present the main features of the Cloud Computing and its trade offs. Cloud Computing refers to an infrastructure where both data storage and data processing happen outside of the mobile device. Also, the Internet of Things is a new technology which is growing rapidly in the field of telecommunications, and especially in the modern field of wireless telecommunications.

The main goal of the interaction and cooperation between things and objects sent through the wireless networks is to fulfil the objective set to them as a combined entity. In addition, based on the technology of wireless networks, both the technologies of Cloud Computing and Internet of Things develop rapidly. In this paper, we present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e Cloud Computing and IoT) in order to examine the common features, and in order to discover the

benefits of their integration. Concluding, the contribution of Cloud Computing to the technology IoT, and it shows how the Cloud Computing technology improves the function of the IoT was presented. At the end, the security challenges of the integration of IoT and Cloud Computing were surveyed through the proposed algorithm model, and also there is a presentation of how the two encryption algorithms which were used contributes in the integration of IoT and Cloud Computing. This can be the field of future research on the integration of those two technologies. Regarding the rapid development of both technologies the security issue must be solved or reduced to a minimum in order to have a better integration model. These security challenges that surveyed in this paper could be the sector for further research as a case study, with the goal of minimizing them.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and feedback which was extremely helpful in improving the quality of the paper.

REFERENCES

[1] Luigi Atzori et al, "The Internet of Things: A survey," Computer Networks, no. 54, p. 2787–2805, 28/10/2010.

[2] Sandip Roy et al, "A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things," International Journal of Advanced Science and Technology, pp. 23-32, 01/03/2015.

[3] Swan, Melanie (8 November 2012). "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". Sensor and Actuator Networks 1 (3): 217–253. doi:10.3390/jsan1030217.

[4] Mohammad A. Alsmirat; Yaser Jararweh; Islam Obidat; Brij B. Gupta, “Internet of Surveillance: A Cloud supported Large Scale Wireless Surveillance System,” the Journal of Supercomputing, Springer, 2016.

[5] J. Mongay Batalla and P. Krawiec, “Conception of ID layer performance at the network level for Internet of Things”, Springer Journal Personal and Ubiquitous Computing, Vol.18, Issue 2 (2014), Page 465-480.

[6] Y. Kryftis, G. Mastorakis, C. Mavromoustakis, J. Mongay Batalla, E. Pallis and G. Kormentzas, “Efficient Entertainment Services Provision over a Novel Network Architecture”. To be published in IEEE Wireless Communications Magazine, 2016.

[7] M. R. Rahimi et al, “Mobile Cloud Computing: A survey, State of Art and Future Directions”, Mobile Networks and Applications, Volume 19, Issue 2, pp. 133-143, 01/04/2014.

[8] T. Keskin and N. Taskin, "A pricing model for cloud computing service" 47th Hawaii International Conference on System Science, pp. 699-707, 01/10/2014.

[9] S. Fremdt, R. Beck and S. Weber, "Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility" 46th Hawaii International Conference on System Sciences, pp. 1025-1034, 01/10/2013.

[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 1, no. 34, pp. 1-11, 11/07/2010.

[11] Hassan Takabi and James B.D. Joshi, «Security and Privacy Challenges in Cloud Computing Environments», IEEE COMPUTER AND RELIABILITY SOCIETIES, pp. 24-31, 01/11/2010.

[12] George Suciu et al, "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," in 2013 19th International Conference on Control Systems and Computer Science, Bucharest, 2013.

[13] Fei Tao et al, «CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System», IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, vol. 2, no. 10, pp. 1435-1442, 02/05/2014.

[14] Jiehan Zhou et al, «CloudThings: a Common Architecture for Integrating the Internet of Things with Cloud Computing», in Huazhong University of Science and Technology, Wuhan, 2013.

[15] Juan Antonio Guerrero Ibáñez et al, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies," IEEE Wireless Communications, pp. 122-128, 01/12/2015.

[16] Moataz Soliman et al, "Smart Home: Integrating Internet of Things with Web Services and Cloud Computing," in 2013 IEEE International Conference on Cloud Computing Technology and Science, Oulu, 2013.

[17] Jayavardhana Gubbi et al, «Internet of Things (IoT): A vision, architectural elements, and future directions», Future Generation Computer Systems, pp. 1645-1660, 24/02/2013.

[18] Mohammad Aazam et al, "Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved," in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST), Islamabad, 2014.

[19] Mohammad Aazam et al, "Cloud of Things: Integration of IoT with Cloud Computing," Springer International Publishing, pp. 77-94, 01/01/2016.

[20] Alessio Botta et al, "Integration of Cloud Computing and Internet of Things: a Survey," Journal of Future Generation Computer Systems, pp. 1-54, 14/09/2015.

[21] Mohammad Aazam et al, «Smart Gateway Based Communication for Cloud of Things», in 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Public Internet of Things, Singapore, 2014.

[22] Manuel Díaz et al, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, pp. 99-117, 25/09/2015.

[23] Mohammad Alsmirat; Yaser Jararweh; Mahmoud Al-Ayyoub; Mohammed A. Shehab; B. B. Gupta, "Accelerating Compute Intensive Medical Imaging Segmentation Algorithms Using GPUs," MTA, Springer, 2016.

[24] B. B. Gupta, D. P. Agrawal, Shingo Yamaguchi, "Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security," IGI Global Publisher, USA, 2016.

[25] Zhiyong Zhang, Brij B. Gupta, "Social media security and trustworthiness: Overview and new direction," Future Generation Computer Systems, Elsevier, 2016.

[26] Oliver Niggemann, Gautaman Biswas et al, "Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control," International Workshop on the Principles of Diagnosis (DX), pp. 185-192, 01/08/2015.

[27] J. M. Batalla, "Advanced multimedia service provisioning based on efficient interoperability of adaptive streaming protocol and high efficient video coding," Journal of Real-Time Image Processing, pp. 1-12, 24/04/2015.

[28] M. Rouse, "IoT security (Internet of Things security)," IoT Agenda, 01/11/2015. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. [Accessed 27/07/2016].

[29] N. Park & N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," Sensors 2016, vol. 1, no. 16, pp. 1-20, 24 12 2015.

[30] Lun Dong, Zhu Han, Athina P. Petropulu and H.Vincent Poor. Improving Wireless Physical Layer Security via Cooperating Relays. IEEE Transactions on Signal Processing, VOL. 58, No. 3, March 2010.

[31] Aparna K Nair et al, "Analysis of Physical layer Security via Co-operative Communication in Internet of Things," International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015), no. 24, p. 896 – 903, 1 1 2016.

[32] W. Hu, H. Tan, P. Corke, W.C. Shih, S. Jha, Toward trusted wireless sensor networks, ACM Transactions on Sensor Networks 7 (2010) 5:1–5:25.

[33] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27–31, 2011.

[34] G. Md Whaiduzzaman et al, "A Study on Strategic Provision of Cloud Computing Services", The Scientific World Journal, pp. 1-8, 15/6/2014.

[35] Garg SK, Versteeg S, Buyya R. "A framework for ranking of cloud computing services". Future Generation Computer Systems. 2013;29(4):1012–1023.

[36] Georgios Skourletopoulos et al, "An evaluation of cloud-based mobile services with limited capacity: a linear approach," Soft Computing, pp. 1-8, 27/2/2016.

[37] L. Villars et al, "The Critical Role of the Network in Big Data Applications", IDC Analyze th Future, pp. 1-12, 1/4/2012.

[38] P. Viswanathan, "Cloud Computing – Is it Really All That Beneficial?," abouttech, 07/07/2012. [Online]. Available: http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm. [Accessed 24/01/2015].

[39] Florian Pfarr et al, "Cloud Computing Data Protection – A Literature Review and Analysis," 47th Hawaii International Conference on System Science, pp. 5018-5027, 01/10/2014.

[40] S. Andersson et al, «A study of the advantages & disadvantages of mobile cloud computing versus native environment», Blekinge Institute of Technology, Karlskrona, 2013.

[41] Sabine Fremdt et al, "Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility," 46th Hawaii International Conference on System Sciences, pp. 1025-1034, 01/10/2013.

[42] Blog: Follow what's happening at Get Cloud Services, "Mobile Cloud Computing – Pros and Cons", GetCloud Services, 23/12/2014. [Online]. Available: https://www.getcloudservices.com/blog/mobile-cloud-computing-pros-and-cons/. [Accessed 24/01/2015].

[43] R. C. Elaine Shi et al, "Implicit Authentication through Learning User Behavior," Information Security, no. 6531, pp. 99-113, 01/01/2011.

[44] Mohammad Haghighat et al, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," Expert Systems with Applications, vol. 11, no. 42, pp. 7905-7916, 30/11/2015.

[45] Madhan Kumar Srinivasan et al, "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment," ICACCI '12 Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 470-476, 03/08/2012.

[46] B. B. Gupta, Omkar P. Badve, "Taxonomy of DoS and DDoS Attacks and Desirable Defense Mechanism in a Cloud Computing Environment," Neural Computing & Applications, Springer, 2016.

[47] Y. Mamoon, ""Swamp Computing" a.k.a. Cloud Computing," WEB Security Journal, 28/12/2009. [Online]. Available: http://security.sys-con.com/node/1231725. [Accessed 27/07/2016].

[48] Rizwana Shaikha & Dr. M. Sasikumar, "Data Classification for achieving Security in cloud computing," Procedia Computer Science, no. 45, p. 493 – 498, 1 3 2015.

[49] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[50] Randeep Kaur & Supiya Kinger, "Analysis of Security Algorithms in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, 1 3 2014.

[51] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[52] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[53] Abha Sachdev & Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications, vol. 9, no. 67, pp. 19-23, 1 4 2013.

[54] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[55] The NIST definition of cloud computing, National Institute of Standards and Technology. [Accessed 24/07/2015].

[56] Christos Stergiou & Kostas E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey," INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT, pp. 1-12, 11/03/2016.

[57] Huang D. Mobile Cloud Computing. IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter 2011; 6(10): 27–31.

[58] N. Park et al, "Symmetric Key-Based Authentication and the Session Key Agreement Scheme in IoT Environment," in Computer Science and its Applications, 330 ed., Berlin, Springer Berlin Heidelberg, 2015, pp. 379-384.

[59] Bhattasali, T., Chaki, R., Chaki, N., 2013. Secure and trusted cloud of things. In: India Conference (INDICON), 2013 Annual IEEE. IEEE, pp. 1–6.

[60] Simmhan, Y., Kumbhare, A. G., Cao, B., Prasanna, V., 2011. An analysis of security and privacy issues in smart grid software architectures on clouds. In: Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, pp. 582–589.

[61] Synapse Internet of Things Cloud, 2014. https://www.synapse-wireless.com/snap-components/iot.

[62] Grozev N. & Buyya, R., 2014. Inter-cloud architectures and application brokering: taxonomy and survey. Software: Practice and Experience 44 (3), 369–390.

[63] Jeffery K., 2014. Keynote: CLOUDs: A large virtualisation of small things. In: The 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014).

[64] Rao, B. P., Saluia, P., Sharma, N., Mittal, A., Sharma, S. V., 2012. Cloud computing for Internet of Things & sensing based applications. In: Sensing technology (ICST), 2012 Sixth International Conference on. IEEE, pp. 374–380.

[65] He, W., Yan, G., Xu, L. D., May 2014. Developing vehicular data cloud services in the iot environment. Industrial Informatics, IEEE Transactions on 10 (2), 1587–1595.

[66] Dobre, C., Xhafa, F., 2014. Intelligent services for big data science. Future Generation Computer Systems 37, 267–281.

[67] Aceto, G., Botta, A., de Donato, W., Pescap`e, A., 2013. Cloud monitoring: A survey. Computer Networks 57 (9), 2093–2115.

Christos Stergiou was born in Thessaloniki, Greece. Currently, he is an undergraduate student in the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece. Christos received a degree in Informatics and Computer Engineering from Technological Educational Institute of Western Macedonia, Annex of Kastoria (Greece); an MSc degree in Wireless Communication Systems from the Department of Technician of Wired and Wireless Networks of Brunel University (UK).

Kostas E. Psannis was born in Thessaloniki, Greece. Kostas received a degree in Physics from Aristotle University of Thessaloniki (Greece), and the Ph.D. degree from the Department of Electronic and Computer Engineering of Brunel University (UK). From 2001 to 2002 he was awarded the British Chevening scholarship sponsored by the Foreign & Commonwealth Office (FCO), British Government. He was awarded, in the year 2006, a research grant by IISF (Grant No. 2006.1.3.916). Since 2004 he has been a (Visiting) Assistant Professor in the Department of Applied Informatics, University of Macedonia, Greece, where currently he is Assistant Professor (& Departmental LLP/Erasmus-Exchange Students Coordinator and Higher Education Mentor) in the Department of Applied Informatics, School of Information Sciences. He is also joint Researcher in the Department of Scientific and Engineering Simulation, Graduate School of Engineering, Nagoya Institute of Technology, Japan. He has extensive research, development, and consulting experience in the area of telecommunications technologies. Since 1999 he has participated in several R&D funded projects in the area of ICT (EU and JAPAN). Kostas Psannis was invited to speak on the EU-Japan Co-ordinated Call Preparatory meeting, Green & Content Centric Networking (CCN), organized by European Commission (EC) and National Institute of Information and Communications Technology (NICT)/ Ministry of Internal Affairs and Communications (MIC), Japan (in the context of the upcoming ICT Work Programme 2013) and International Telecommunication Union (ITU) SG13 meeting on DAN/CCN, July 2012, amongst other invited speakers. He has several publications in international Conferences, books chapters and peer reviewed journals. His professional interests are: Multimodal Data Communications Systems, Haptic Communication between Humans and Robots, Cloud Transmission/Streaming/Synchronization, Future Media-Internet of Things, Experiments on International Connections (E-ICONS) over TEIN3 (Pan-Asian), Science Information Network (SINET, Japan), GRNET (Greece)-Okeanos Cloud, and GEANT (European Union) dedicated high capacity connectivity. He is Guest Editor for the Special Issue on Architectures and Algorithms of High Efficiency Video Coding (HEVC) Standard for Real-Time Video Applications (2014), Journal of Real Time Image Processing (Special Issue). He is Guest Editor for the Special Issue on Emerging Multimedia Technology for Smart Surveillance System with IoT Environment (2016), The Journal of Supercomputing (Special Issue). He is Guest Editor for the Special Issue on Emerging Multimedia Technology for Multimedia-centric Internet of Things (mm-IoT) (2016), Multimedia Tools and Applications (Special Issue). He is currently GOLD member committee of IEEE Broadcast Technology Society (BTS) and a member of the IEEE Industrial

Electronics Society (IES). He is also a member of the European Commission (EC) EURAXESS Links JAPAN and member of the EU-JAPAN Centre for Industrial Cooperation.

Byung-Gyu Kim has received his BS degree from Pusan National University, Korea, in 1996 and an MS degree from Korea Advanced Institute of Science and Technology (KAIST) in 1998. In 2004, he received a PhD degree in the Department of Electrical Engineering and Computer Science from Korea Advanced Institute of Science and Technology (KAIST). In March 2004, he joined in the real-time multimedia research team at the Electronics and Telecommunications Research Institute (ETRI), Korea where he was a senior researcher. In ETRI, he developed so many real-time video signal processing algorithms and patents and received the Best Paper Award in 2007. From February 2009 to February 2016, he was associate professor in the Division of Computer Science and Engineering at SunMoon University, Korea. In March 2016, he joined the Department of Information Technology (IT) Engineering at Sookmyung Women's University, Korea where he is currently an associate professor. In 2007, he served as an editorial board member of the International Journal of Soft Computing, Recent Patents on Signal Processing, Research Journal of Information Technology, Journal of Convergence Information Technology, and Journal of Engineering and Applied Sciences. Also, he is serving as an associate editor of Circuits, Systems and Signal Processing (Springer), The Journal of Supercomputing (Springer), The Journal of Real-Time Image Processing (Springer), The Scientific World Journal (Hindawi), and International Journal of Image Processing and Visual Communication (IJIPVC). He also served as Organizing Committee of CSIP 2011 and Program Committee Members of many international conferences. He has received the Special Merit Award for Outstanding Paper from the IEEE Consumer Electronics Society, at IEEE ICCE 2012, Certification Appreciation Award from the SPIE Optical Engineering in 2013, and the Best Academic Award from the CIS in 2014. He has been honored as an IEEE Senior member in 2015. . He has published over 150 international journal and conference papers, patents in his field. His research interests include software-based image and video object segmentation for the content-based image coding, video coding techniques, 3D video signal processing, wireless multimedia sensor network, embedded multimedia communication, and intelligent information system for image signal processing. He is a senior member of IEEE and a professional member of ACM, and IEICE.

Dr. B. B. Gupta received PhD degree from Indian Institute of Technology Roorkee, India in the area of Information and Cyber Security. He has published more than 90 research papers (including 03 book and 14 chapters) in International Journals and Conferences of high repute including IEEE, Elsevier, ACM, Springer, Wiley Inderscience, etc. He has visited several countries, i.e. Canada, Japan, China, Malaysia, Hong-Kong, etc to

present his research work. His biography was selected and publishes in the 30th Edition of Marquis Who's Who in the World, 2012.

He is also working principal investigator of various R&D projects. He is serving as associate editor of IEEE Access, Associate editor of IJICS, Inderscience and Executive editor of IJITCA, Inderscience, respectively. He is also serving as reviewer for Journals of IEEE, Springer, Wiley, Taylor & Francis, etc. Currently he is guiding 10 students for their Master's and Doctoral research work in the area of Information and Cyber Security. He is also serving as guest editor of various reputed Journals. Dr Gupta is also holding position of editor of various International Journals and magazines. He has also served as Technical program committee (TPC) member of more than 20 International conferences worldwide. Dr. Gupta is member of IEEE, ACM, SIGCOMM, The Society of Digital Information and Wireless Communications (SDIWC), Internet Society, Institute of Nanotechnology, Life Member, International Association of Engineers (IAENG), Life Member, International Association of Computer Science and Information Technology (IACSIT). He was also visiting researcher with Yamaguchi University, Japan in January, 2015. His research interest includes Information security, Cyber Security, Mobile/Smartphone, Cloud Computing, Web security, Intrusion detection, Computer networks and Phishing.

Research Highlights:

- Presentation of Internet of Things and Cloud Computing technologies which focus on security issues.
- Integration benefits of Internet of Things and Cloud Computing technologies.
- Part of AES algorithm is presented for the improvement of the security issue, resulting from integration of Internet of Things and Cloud Computing technologies.
- Contribution of AES and RSA algorithms in the integration of Internet of Things and Cloud Computing technologies.