## INTRODUCTION

The need of "*cloud*" support has become inefficient due to the intensive computations, the mass storage, and the security issues. Some examples include limited storage capacity, communication capabilities, energy and processing. Inefficiencies like these have motivated us in order to find a model for the combination of CC and other technologies such as Internet of Things and Big Data. As a "*base*" technology, Cloud Computing consolidates various technologies and applications to get the maximum capacity and performance of the existing infrastructure (Kryftis et al., 2016; Stergiou & Psannis, 2016; Stergiou et al., 2018b).

Mobile Cloud Computing improved through the recent years by a new generation of services based on the concept of the "*cloud computing*", which aims to provide access to the information and the data from anywhere at any time, and simultaneously restrict or eliminate the need for hardware equipment (Rahimi et al., 2014; Stergiou & Psannis, 2016; Stergiou & Psannis, 2017b; Stergiou et al., 2018f). In particular, Mobile Cloud Computing (MCC) could be defined as an integration of Cloud Computing (CC) technology and mobile devices in order to make mobile devices resourceful in terms of computational power, memory, storage, energy, and context awareness (Fremdt et al., 2013; Keskin & Taskin, 2014; Haung, 2011; Stergiou et al., 2018c). As a result of the operations of Cloud Computing, it could be used as useful base for several technologies, such as Internet of Things (IoT), Big Data (BD) and Surveillance Systems, and could provide improvements on their functions.

Therefore, 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. Although cloud is useful for computing and storage (Rahimi et al., 2014; Stergiou & Psannis, 2017a; Stergiou et al., 2018d), the traditional computation offloading techniques cannot be used directly for smartphones because these techniques are generally energy-unaware and "*bandwidthhungry*".

Furthermore, the term "*cloud computation*" is defined as "*the use of computing logistical resources by using services transported over the internet*" (Stergiou & Psannis, 2016; Stergiou & Psannis, 2017b). Nowadays, Cloud Computing services constitute one of the world's largest areas of competition between giant companies in the IT sector and software (Mell & Grance, 2011). However, Cloud Computing 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 (Rahimi et al., 2014; Mell & Grance, 2011; Haghighat, 2015). Thus, as the MCC is the outcome of CC it faced the same security and privacy challenges and issues.

In addition to this, CC additionally used to be a base technology for other technologies due to its types of services (Stergiou & Psannis, 2016; Stergiou et al., 2018b; Plageraset al., 2017). One of those is the Big Data (BD). BD is a term used to describe the expected, due to the connected to the Internet devices, rapid increase in the volume of data production. Subsequently, these large amounts of data could be defined as "*a broad term for data sets so large or complex that traditional data processing applications are inadequate*" (Stergiou et al., 2018b). Furthermore, BD is often associated to the use of predictive analytics or certain advanced methods to extract knowledge from the data. Rarely, are also related to a particular size of set of data (Hilbert & López, 2011; Fu et al. 2015). Precision in BD could result in more confident decision making, and better decisions may drive in increased operational efficiency, reduced costs, and minimized risk (Hilbert & López, 2011). From this scope, it can be observed that BD is now equally important both for business and internet. This happens because more information drives to

more accurate analysis (Stergiou & Psannis, 2016). The real problem is not that the large amounts of data have been obtained, but whether they have any value or not. Hopefully, by predicting that organizations would be able to acquire information from any source, harness the relevant data, and analyze them in a specific way in order to get quick answers, the following should be achieved: 1) reduce costs, 2) reduce time, 3) produce new items and optimize their offerings, and 4) take more ingenious decisions (Stergiou & Psannis, 2017b).

Regarding Security and Privacy issues and challenges in the field of CC and particularly of MCC, and in order to succeed a 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 in order to decrypt the data. Regarding the researches that have been made in the field, 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 algorithm (Stergiou & Psannis, 2017b; Kumar et al., 2011; Kaur & Kinger, 2014; Negi et al. 2013).

AES (Advanced Encryption Standard) is the high developed encryption standard recommended by NIST aiming to replace the older 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. Also, AES has been carefully tested for many security applications (Huang, 2011; Stergiou et al., 2018d; Singh & Kinger, 2013; Gupta et al. 2016).

The rest of the paper is organized in 6 sections as follows. In section 2 we present previous work that address challenges and solutions related to Mobile Cloud Computing. Section 3 provides a comparative analysis of the previous works which we have studied offering a brief analysis about evolution of the number of researches that have been made through the years. In section 4 we offer a brief literature analysis of CC and MCC. In section 5 we discuss the outcomes of the literature study and additionally we propose an algorithm method as an indicated solution for Security and Management challenges. Final conclusions and future research directions are given in section 6.

## BACKGROUND

For the purpose of this paper we study and analyze previous literature which has been studying two aspects, Security and Privacy Management in MCC and Security and Privacy of MCC. In addition to this, we also present some former works of our research group which have been made in field of CC in general. All the papers presented with ascending form, from the older to the newest. The following paragraphs present the papers which contributed significantly in our study.

### A. Security & Privacy Management in MCC

Initially, the papers that deal with the Security and Privacy issues of Management in MCC are illustrated [23-34]. As we can realize there are several works in this field. More particular, Angin et al. (2010) propose an entity-centric approach for an IDM model in Cloud environment. The proposed approach based on two aspects: a) active bundles, and b) anonymous identification. The active bundles include a payload of Personally Identifiable Information, privacy policies and a virtual machine that enforces the policies and additionally the active bundles use a set of protection mechanisms in order to protect themselves. As regard the anonymous identification, they use it with the aim to mediate interactions between the entity and the Cloud services using entity's privacy policies. Moreover, the authors present the main characteristics of the approach which are: a) independent of third party, b) provides minimum

information to the Service Provider, and c) provides ability to use identity data on untrusted hosts. Then, Doukas et al. (2010) demonstrate the implementation of a mobile system that enables electronic healthcare data storage, update and retrieval using CC. The proposed mobile application based in Google's Android OS and offers management of patient health records and medical images. This system was evaluated with the use of Amazon's S3 cloud service. Finally, the authors summarize the details of the implementation and then present initial results of the system in practice. Moreover, Dinh et al. (2011) survey the MCC technology, which could help the general readers to have an overview of the MCC including the definition, the architecture, and the applications. Also, this work presents the issues, the existing solutions, and the recent approaches of the MCC technology. At the end, the authors discuss a number of future research directions of the MCC. Through Habib et al. (2011) propose a multi-faceted Trust Management system architecture for a cloud computing marketplace, with the aim to support the customers in reliably identifying trustworthy cloud providers. The proposed system offers means to identify the trustworthy cloud providers in term of different attributes that assessed by multiple sources and roots of trust information. Furthermore, Prasad et al. (2012) presents a sort survey of MCC evolution and additionally explains how CC and Mobile Devices could be combined with good terms for future opportunities, implications and legal issues for developing countries. In another research, Shiraz et al. (2012) try to review the existing Distributed Application Processing Frameworks, also known as DAPFs, for SMDs in MCC domain. The main objective of this work is to highlight issues and challenges to existing DAPFs in developing, implementing, and executing computational intensive mobile applications within MCC domain. Thus, through this work the authors propose a thematic taxonomy of the current DAPFs, and then they review current offloading frameworks by using thematic taxonomy, and analyze the implications and critical aspects of current offloading frameworks. Finally, this work puts forward open research issues in distributed application processing for MCC that remain to be addressed. Also, Kim & Park (2013) proposes a trust management approach by making an analysis of user behavioral patterns for a reliable MCC. So, the authors suggest a method in order to quantify a one-dimensional trusting relation count on the analysis of telephone call data from Mobile Cloud Environment. Subsequently, it is enhanced trustworthiness of data production, management, and overall application. Whaiduzzaman et al. (2014) present a state-of-the-art survey of vehicular Cloud Computing. More detailed, the authors present a taxonomy for vehicular Cloud in which special attention has been devoted to the extensive applications, Cloud formations, key management, inter-Cloud communication systems, and broad aspects of privacy and security problems. Additionally, this work illustrates the design of an architecture for Vehicular Cloud Computing, itemize the properties required in vehicular Cloud which support the proposed model. In order to achieve their goal, authors compare the proposed mechanism with normal Cloud Computing and then discuss about open research issues and the future directions. Additionally, Khalil et al. (2014) discuss the limitations of the state-of-the-art Cloud Identity Managements with respect to mobile clients. In particular, the authors demonstrate that the current IDMs are vulnerable to three attacks. As a result of their research, the authors propose and validate a new IDM architecture dubbed Consolidated IDM that countermeasures these attacks. Through their experimental results the authors illustrates that CIDM offers its clients with better security guarantees and that it has less energy and communication overhead compared to the current IDM systems. Furthermore, Ali et al. (2015) offer a detailed survey of the security issues that arise due to the very nature of Cloud Computing. Furthermore, this work presents a number of recent solutions offered in the literature with the aim to counter the security problems. In addition, there is a brief view of the highlighted security vulnerabilities in the Mobile Cloud Computing. Then, Rittinghouse & Ransome (2009) discuss about the evolution of the computing as regarding the historical perspective, with focus on advances which primarily led to the evolution of the Cloud Computing. Additionally, there is a survey of some of the critical components that are vital in order to make the Cloud Computing paradigm feasible. The authors by addressing a number of particular legal and philosophical problems try to conclude with a hard look at all the successful Cloud Computing vendors. Finally, Mollah et al. (2017) try to present the major security and privacy issues and challenges in the field which have grown much interest among the

academia and research community. Also, they try to illustrate reports of recent works of literature. Moreover, they present a comparative analysis of the literature works based on different security and privacy requirements, and concluding they present the open issues in the field.

### B. Security & Privacy of MCC

Subsequently, the papers that deal with the Security and Privacy issues of the MCC are illustrated. Starting from the oldest, a survey of the various security issues that pose a threat to the Cloud as presented by the work of Subashini & Kavitha (2011). The survey that illustrated in this work could be more specific to different security problems which have emanated due to the nature of the service delivery models of a Cloud Computing system. Continuously, Liang et al. (2011) propose a Security Service Admission Model based on Semi-Markov Decision Process in order to model the system reward for the Cloud provider. Initially, through this work try to define the system states by a tuple represented by the numbers of Cloud users and the associated to them security service categories, and the current event type. Then, the authors derive the system steady-state probability and service request blocking probability with the use of their proposed model. Then, Hada et al. (2011) propose a trust model for Cloud architecture which uses mobile agent as security agents to acquire useful information from the virtual machine that the user and the service provider could utilize with the aim to keep track of privacy of their data and virtual machines. In the proposed model the security agents can dynamically move through the network, replicate themselves according to the requirement, and perform the assigned tasks like accounting and monitoring of virtual machines. Also, Popa et al. (2013) propose a framework with the aim to secure the data transmitted between the components of the same Mobile Cloud Application, and with the aim to ensure the integrity of the applications at the installation on the mobile device and when being updated. Furthermore, the proposed framework of this work allows applying different security properties to various kinds of data and not the same properties to all the data processed by the application. In addition to this, the proposed approach takes into account the user's preferences and the mobile device performances. Moreover, Hashizume et al. (2013) discuss and identifies the main vulnerabilities in CC systems, and the most important threats that found in the literature related to CC technology and its environment, as well as to identify and relate vulnerabilities and threats with possible solutions. Suo et al. (2013) with the aim to facilitate the emerging domain of MCC security and privacy, in brief review the advantages and system model of MCC, and pay attention to the security and privacy in the MCC. At the end, the authors provide the current security and privacy approaches, by deeply analyzing the security and privacy problems from the aspects of mobile terminal, mobile network and Cloud. Additionally, Shahzad & Hussain (2013) present a comprehensive literature review of MCC and the security and privacy issues that MCC faced. Also, the authors present a complete understanding analysis of MCC, in where they explain its architecture, advantages and applications. At the end, the authors conclude that their research is significant useful for the mobile service providers, and thus they can improve the security technologies and mechanisms used for Cloud security in order to minimize the user's security concerns. Then, Khan et al. (2013) illustrate particular efforts that have been devoted in research organizations and academia in order to build secure MCC environments and infrastructures. Thus, in the spite of the efforts, there are a number of loopholes and challenges that still exist in the security policies of MCC. The authors through the literature review conclude in three things that discussed in this work. Firstly, they highlight the current state of the art work which proposed to secure MCC infrastructures. Secondly, they identify the potential problems. Finally, they provide taxonomy of the state of the art. Furthermore, Zhang et al. (2017) propose a novel technique that called "match-then-decrypt", in which a matching phase is also presented before the decryption phase. The proposed technique operates by computing special components in ciphertexts, which are used in order to perform the test that if the attribute private key matches the hidden

access policy in ciphertexts without decryption. Moreover, in this work there is a proposal of a basic anonymous ABE construction, and then obtain a security-enhanced extension based on strongly existentially unforgeable one-time signatures. More specifically, the authors conclude that the formal security analysis and performance comparisons indicate that their proposed solutions simultaneously ensure attribute privacy and improve decryption efficiency for outsourced data storage in MCC. Finally, Jiang et al. (2018) initially identify that the scheme that proposed in former work of Tsai and Lo, which was privacy aware authentication scheme for distributed MCC services, fails to achieve mutual authentication. The authors of this work conclude to this regarding it is vulnerable to the service provider impersonation attack. In addition to this, the authors state that the former scheme also suffers from some minor design flaws, including the problem of biometric measure, wrong password, and fingerprint login, no user revocation facility when the smart card is lost or stolen. At the end, they offer some a number of suggestions in order to avoid the aforementioned design flaws in future design of authentication schemes.

### C. Research group's previous works in CC & MCC

At this point there will be present a number of former works which deal with problems and solutions in the field of Cloud Computing in general. More particular, some of them deal with problems and solutions in the field of Mobile Cloud Computing. Starting again from the oldest, Stergiou & Psannis (2016) try to combine the MCC and IoT with the Big Data with the aim to examine the common characteristics and in addition to discover which of MCC and IoT benefits improve the operation of BD applications. Also, the authors of this work present the contribution of MCC and IoT individually to Big Data. Moreover, Stergiou et al. (2018a) present a survey of Internet of Things and CC focusing on the security problems of both of them. More particular, the authors try to combine these technologies aiming to examine the common features, and also aiming to discover the benefits of their integration. At the end, there is a presentation of the contribution of Cloud Computing to the IoT. So, this work illustrates how the Cloud Computing improves the functionality of Internet of Things, and additionally, surveys the security challenges of the integration of Cloud Computing and Internet of Things. Continuously, Stergiou & Psannis (2017a) present a survey of Big Data and Cloud Computing, illustrating their basic characteristics, and focusing on the security and privacy problems of both of them. Regarding this, the authors try to combine the functionality of Big Data and Cloud Computing aiming to examine the frequent characteristics, and in addition to this to discover the benefits which are related in security problems of their integration. Furthermore, Stergiou & Psannis (2017b) survey Cloud Computing and Big Data technology, and their major characteristics, focusing on the security and privacy problems of both of them. Particularly, the authors combine the functionality of two technologies aiming to examine the common characteristics, and additionally to discover the benefits related in security issues of their integration. Then, there is a presentation of a novel method of an algorithm that can be used for the purpose of improving Cloud Computing's security through the use of algorithms that can offer more privacy in the data related to Big Data. At the end, there additionally a survey about the challenges of the integration of Cloud Computing and Big Data related to their security level. Also, Stergiou et al. (2018b) in order to achieve a type of network that will offer more intelligent media-data transfer new technologies were studied. Thus, the authors initially studied the use of various open source tools of Cloud Computing analyzers and simulators. So, the authors after they measure the simulated network performance with CloudSim simulator, they use the Cooja emulator of the Contiki OS aiming to confirm and access more metrics and options. In particular, in this work there is an implementation of a network topology from a small section of the script of CloudSim with Cooja, so that the authors could test a single network segment. The results that have been produced of the experimental procedure illustrate that there are not duplicated packets received during the whole procedure. Finally, Stergiou et al. (2018e) propose a novel system for Cloud Computing integrated with Internet of Things as a base scenario for Big Data. Moreover, the authors try to establish an architecture relaying on the security of the network with the aim

to eliminate the security issues. The solution proposed in this work installs a security "*wall*" between the Cloud server and the outer Internet, aiming to eliminate the privacy and security problems. As regard the main goal of this paper a sort survey of IoT and Cloud Computing also presented, focusing on the security issues of both of them. Additionally, the authors state that through their study conclude that Cloud Computing could offer a more "*green*" and efficient "*fog*" environment for sustainable computing scenarios.

## LITERATURE COMPARATIVE ANALYSIS

Taking into account the Related Research Review Section we realized that the study of MCC's Security and Privacy issues become more popular in the research and academic community over the recent years. We have come to the above conclusion counting on our study of several works in the field of Security and Privacy of Mobile Cloud Computing. The main balk of these works presented in Related Research Review Section. Consequently, there is a need for further research in this area as the growing numbers studied indicate.

As we can observe, the last four years the interest of the researchers has increased considerably compared to the previous decade. Figure 1 illustrates the growth of studies in Security and Privacy Management in Mobile Cloud Computing through the years. Equally important Figure 2 represents the growth of studies in Security and Privacy of Mobile Cloud Computing through the years.

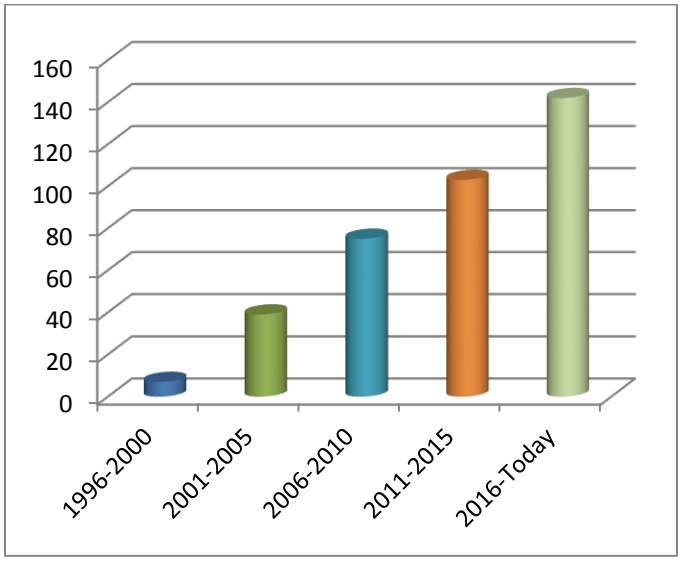


*Figure 1. Growth of works made in Security and Privacy Management in Mobile Cloud Computing over the years*

*Table 1. Related research work's challenges and issues of the Mobile Cloud Computing technology*

| Year | Author | Challenge/Issue |
|---|---|---|
| 2009-08 | J. W. Rittinghouse & J. F. Ransome (2009) | • Cloud reliability to users<br>• Users desired outcomes of the Cloud<br>• Levels of trust in Cloud environment |
| 2010-09 | C. Doukas et al (2010) | • Sharing and management of medical information resources through mobile healthcare systems |
| 2010-11 | P. Angin et al (2010) | • Entities authentication to service providers<br>• Entities multiple accounts associated with multiple service providers |
| 2011-01 | S. Subashini & V. Kavita (2011) | • Cloud environment safety<br>• New Cloud model targeting to improve the existing one |
| 2011-04 | H. Liang et al (2011) | • Increased number of Critical and Normal Security service users<br>• Allocate Cloud resource aiming to maximize the system rewards with the considerations of the Cloud resource consumption and incomes generated from Cloud users. |
| 2011-10 | H. T. Dinh et al (2011) | • Low bandwidth of Mobile Cloud Computing<br>• Availability of Mobile Cloud Computing<br>• Heterogeneity of Mobile Cloud Computing<br>• Computing offloading of Mobile Cloud Computing<br>• Security of Mobile Cloud Computing<br>• Enhancing the efficiency of data access of Mobile Cloud Computing<br>• Context-aware mobile Cloud services of Mobile Cloud Computing |
| 2011-11 | S. M. Habib et al (2011) | • Not consistent descriptions in Service Level Agreements among Cloud providers<br>• Uncertain reliably identifying trustworthy Cloud providers for the customers |
| 2011-12 | P. S. Hada et al (2011) | • Major need of bringing reliability, transparency and security in Cloud model for client satisfaction |
| 2012-10 | M. R. Prasad et al (2012) | • Cloud Computing challenges: Performance, Security & Privacy, Control, Bandwidth Costs, Reliability<br>• Mobile Cloud Computing legal issues |
| 2012-11 | M. Shiraz et al (2012) | • Users expectation to run computational intensive applications on Smart Mobile Devices in the same way as powerful stationary computers<br>• Establishment of distributed application processing platform at runtime which requires additional computing resources on Smart Mobile Devices |
| 2013-01 | D. Popa et al (2013) | • Use of MCC increases security risks and privacy invasion<br>• MCC application model not well-defined |
| 2013-06 | A. Shahzad & M. Hussain (2013) | • Security and privacy risks faced be MCC uses<br>• Architecture and Cloud service delivery models issues<br>• Mobile Cloud infrastructure issues<br>• Mobile Cloud communication channel issues |
| 2013-07 | H. Suo et al (2013) | • Security and privacy issues and challenges in MCC |
| 2013-07 | A. N. Khan et al (2013) | • Security threats have become a hurdle in the rapid adaptability of the MCC paradigm |
| 2013-12 | M. Kim & S. O. Park (2013) | • MCC architecture, design and implementation need to be improved due to limited computing capability and storage issues<br>• Trust management approach for reliable MCC |
| 2013-12 | K. Hashizume et al (2013) | • Risk of outsourcing data to third party Cloud providers<br>• Cloud Computing inherits many technologies security issues |
| 2014-02 | M. Ali et al (2014) | • Services provided by third party Cloud providers entail additional security threats<br>• Migration of user's assets outside the administrative control in the Cloud environment escalates the security concerns. |
| 2014-03 | I. Khalil et al (2014) | • Mobile devices are easy to be compromised<br>• Mobile users store Personal Identifiable Information in unprotected text files, cookies and applications<br>• Limitations of state-of-the-art Cloud Identity Management Systems with respect to mobile clients |
| 2014-04 | Md. Whaiduzzaman et al (2014) | • Traffic management and road safety by instantly using vehicular resources<br>• Vehicular Cloud Computing security challenges: Authentication, Secure location & localization, Securing vehicular communication, Vehicular public key infrastructure, Data security, Network heterogeneity, Access control |
| 2017-02 | Y. Zhang et al (2017) | • Each decryption usually requires many pairings and the computation overhead grows with the complexity of the access formula<br>• Existing schemes suffer a serve efficiency drawback and not suitable for MCC where users may be resource-constrained |
| 2017-04 | M. B. Mollah et all (2017) | • Data security challenges<br>• Partitioning and offloading security challenges<br>• Virtualization security challenges<br>• Mobile Cloud applications security challenges<br>• Mobile devices security challenges<br>• Privacy challenges |
| 2018-06 | Q. Jiang et al (2018) | • A previous proposed scheme of Tsai & Lo fails to achieve mutual authentication and withstands all major security threats |

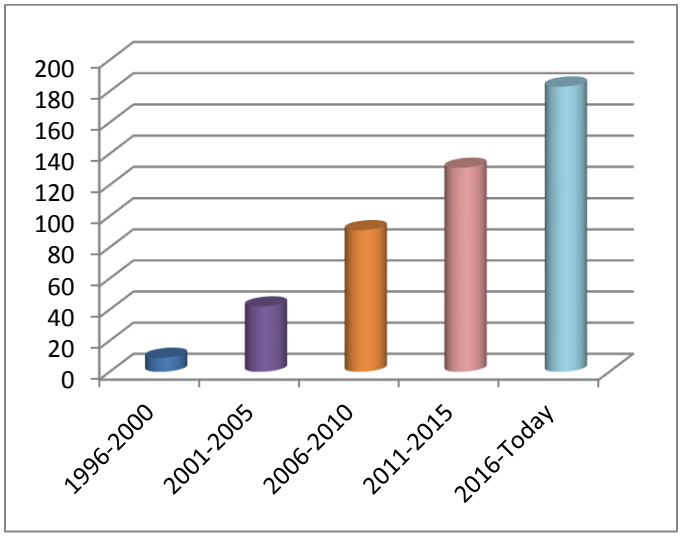


*Figure 2. Growth of works made in Security and Privacy of Mobile Cloud Computing over the years*

The study of previous works motivates us to survey the Security and Privacy challenges and issues of the Mobile Cloud Computing technology. Thus, count on the major works related to Security and Privacy challenges and issues we have tried to figure out them in Table 1.

Table 1 lists the major challenges and issues which we have distinguished from the related works. Through Table 1 we can figure out which are the major issues and challenges of the Mobile Cloud Computing that have been addressed by the literature.

## INTRODUCING TO CLOUD COMPUTING

CC offers abilities and functions such as 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 levels are required. This causes the cooperation of developers and manufacturers (Rahimi et al., 2014).

### A. Features

As all technologies, so the CC technology has a number of characteristics which determine its operation. These characteristics are represented and outlined below.

***CC(a):*** *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*" (Whaiduzzaman et al., 2014; Garg et al., 2013).

***CC(b):*** *Service over Internet*
The Service over Internet has as major objective is to "*help customers all over the world in order to transform aspirations into achievements by harnessing the Internet's efficiency, speed and ubiquity*" (Whaiduzzaman et al., 2014; Garg et al., 2013).

***CC(c):*** *Applications over Internet*
Cloud Applications, or as scientific known as Applications over Internet, are the programs which have been written to do the job of a current manual task, or virtually anything, and which perform their job on the server through an internet connection (Whaiduzzaman et al., 2014; Garg et al., 2013).

***CC(d):*** *Energy Efficiency*
Energy Efficiency could be defined as "*a way of managing and restraining the growth in energy consumption*" (Whaiduzzaman et al., 2014; Garg et al., 2013). By delivering more services for the same energy input or for the same services for less energy input may be something more energy efficient (Whaiduzzaman et al., 2014; Garg et al., 2013).

***CC(e):*** *Computationally Capable*
The services of computational clouds are leveraging the computationally concentrated and ubiquitous mobile applications which have been enabled by the technology of MCC. Thus, a system can be considered as computationally capable when it meets the requirements to offer us the results we want, by making the right calculations (Whaiduzzaman et al., 2014; Garg et al., 2013).

### B. Security on Cloud Computing

CC security is an evolving sub-domain of computer security, network security and information security. It makes an allusion to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of CC.

CC technology offers through its storage solutions to users and industries various capabilities with the aim to store and process their data in third-party data centers (Haghighat et al., 2015). Thus, by aiming to offer secure communication through the network, encryption algorithm plays a vital role. As regards 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 (Kumar et al., 2011; Kaur & Kinger, 2011; Stergiou et al., 2018g; Gupta & Badve, 2017).

AES (Advanced Encryption Standard) is the newest encryption standard and the more reliable, recommended by NIST to replace DES algorithm. The only effective scenario of attacking in AES is the Brute force attack, in which the attacker tries to test all the characters combinations to unlock the encryption. AES encryption model is fast and flexible, and in addition, it can be implemented on different platforms (Singh & Kinger, 2013).

### C. Mobile Cloud Computing trade offs

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

***CC(l-a):*** *Security*
One major issue of the MCC 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 (Stergiou & Psannis, 2016; Viswanathan, 2012; Pfarr et al., 2015; Stergiou et al.,2018g; Gupta et al., 2016).

***CC(l-b):*** *Connectivity*
Internet connection is critical to CC. 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, CC has a very large potential user base (Stergiou & Psannis, 2016; Almrot & Andersson, 2013).

***CC(l-c):*** *Performance*
Another major concern of the CC 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 (Stergiou & Psannis, 2016; Fremdt et al., 2013; GetCloud Services, 2014).

***CC(l-d):*** *Latency (Delay)*
In CC, 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 (Stergiou & Psannis, 2016; Li et al., 2017).

***CC(l-e):*** *Privacy*
Data privacy is important and is one of the main bottlenecks that restrict consumers from adopting CC. Therefore, to gain consumers trust in the Cloud, the application models must support application development with privacy protection, and implicit authentication mechanisms (Stergiou & Psannis, 2016; Pfarr et al., 2014; Shi et al., 2010).

### D. Challenges outcomes by combining Cloud Computing with other technologies

When critical applications, such as the 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 (Botta et al., 2016; Bhattasali et al., 2013; Simmhan et al., 2011). 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 integrating Cloud Computing with other technologies (Botta et al., 2016; Book, 2018; Stergiou et al., 2018g; Gou et al., 2017).

Subsequently, some challenges about the security issue in the integration of Cloud Computing with other technologies are listed below (Botta et al., 2016).

a) Heterogeneity. A big challenge in Cloud Computing integration with other technologies is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications (Grozev & Buyya, 2014).
b) Performance. Often Cloud Computing integration with other technologies 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 (Rao et al., 2012).
c) Reliability. When Cloud Computing integration with other technologies is adopted for mission-critical applications, reliability concerns typically arise. When applications are deployed in resource constrained environments a number of challenges related to device failure or not always reachable devices exists (He et al., 2014).
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 (Dobre & Xhafa, 2014).
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 (Aceto & Botta, 2013).

### E. Cloud Computing as base technology for Big Data

Cloud Computing (CC) is a new generation of services which aims to provide accessibility to information and data from any place at any time. With this kind of novel technology there is no limitation and no further need for hardware equipment. The recent years, Cloud Computing services compose one of the major areas in the world of competition among the giant companies in the field of IT and software (Mell & Grance, 2011; Skourletopoulos et al., 2017; Dorgham et al., 2018).

More specifically, Cloud Computing is consisted of a technology of internet services providing remote use of hardware and software. As a result, the users of Cloud Computing could have access to information and data from any place at any time. In the concept of Cloud Computing there is another technology called Mobile Cloud Computing (MCC) that refers in general concept to in two prospects (Stergiou et al., 2018f): a) infrastructure based, and b) ad-hoc mobile cloud. In the prospect of infrastructure based mobile cloud, the infrastructure of the hardware is still static and delivers services to the mobile users

(Stergiou et al., 2018c; Batalla et al. 2016). Particularly, MCC is defined as "*the integration of Cloud Computing and Mobile technology in order to make any type of mobile devices resourceful in terms such as computational power, memory, storage and energy*" (Stergiou & Psannis, 2017b). Regarding the usage of Cloud services in Mobile devices many types of services could be processed through it. Thus, high quality media could be transmitted through Cloud environment progressed in applications which were installed and operated in Cloud.

Considering this Cloud Computing could be settled as a base technology to operate other technologies such as Big Data and consequently to be accomplished an integration of Cloud and Big Data (Haghighat et al., 2015; Garg et al., 2013). In addition to this, Cloud Computing also used to be a base technology for others technologies due to its type of services (Stergiou & Psannis, 2016; Stergiou et al., 2018d).

As already mentioned, one of those is Big Data (BD). Big Data used to describe the surprisingly rapid increase in volume of data in structured and unstructured form. It is a broad term for data sets so large or complex that traditional data processing applications are inadequate. Furthermore, Big Data often refers to the use of predictive analytics or certain advanced methods to extract value from data. Rarely, it also refers to a particular size of data set (Hilbert & López, 2011; Fu et al., 2016). Precision in Big Data could result in more confident decision making, and better decisions may lead to an increased operational efficiency, reduced costs, and minimized risk [18]. From this scope we realize that the Big Data is now equally important both for business and internet. This happens because more information leads to more accurate analyses (Stergiou & Psannis, 2016). The real problem is not that you have acquired large quantities of data, but whether it has any value or not. Hopefully, by envisaging that the organizations would be able to obtain information from any source, harness the relevant data and analyze it with the aim to get quick answers, we will achieve the following: 1) to reduce costs, 2) to reduce time, 3) to produce new products and to optimize their offerings, 4) to make more intelligent decisions (Stergiou & Psannis, 2017a; Stergiou & Psannis, 2017b).

## RESEARCH OUTCOMES & PROPOSED SOLUTIONS

*Table 2. Literature challenges in the field of Mobile Cloud Computing*

| ***Literature work*** | ***Challenges*** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *Privacy* | *Security* | *Trusted environment* | *Bandwidth* | *Environment limitations* | *Management* | *Reliability* | *User authentication* | *Efficiency* |
| **Rittinghouse & Ransome, 2009** | | | X | | | X | X | X | |
| **Doukas et al., 2010** | | | X | | | X | | | |
| **Angin et al., 2010** | X | X | | | | X | | X | |
| **Subashini & Kavitha, 2011** | | | X | | X | X | | | |
| **Liang et al., 2011** | | X | X | | | X | X | X | |
| **Dinh et al., 2011** | | X | X | X | | | X | | X |
| **Habib et al., 2011** | | X | X | | | | X | X | |
| **Hada et al., 2011** | | X | X | | | | X | | |
| **Prasad et al., 2012** | X | X | | X | | X | X | X | |
| **Shiraz et al., 2012** | | | | | X | X | | | X |
| **Popa et al., 2013** | X | X | | | X | X | | | |
| **Shahzad & Hussain, 2013** | X | X | X | | X | | X | | |
| **Suo et al., 2013** | X | X | X | | | | | | |
| **Khan et al., 2013** | | X | | | X | | | | |
| **Kim & Park, 2013** | | | X | X | X | | X | | X |
| **Hashizume et al., 2013** | | X | X | | | | X | X | |
| **Ali et al., 2015** | | X | X | | X | X | X | | |
| **Khalil et al., 2014** | | | X | | X | X | X | X | |
| **Whaiduzzaman et al., 2014** | | X | | | | X | X | X | X |
| **Zhang et al., 2017** | | | X | X | X | | | | X |
| **Mollah et al., 2017** | X | X | | X | | | | | |
| **Jiang et al., 2018** | | X | X | | X | | | X | |

Table 2 presents the challenges that have been addresses by the literature work which we have studied. As we could observe most of the works that we have studied focus on the "*Trusted environment*" which in our opinion is the major issue of the Mobile Cloud Computing, and as a result the "*Security*" issue is most popular in the literature work. Additionally, concerning the rest of the challenges we come to the conclusion that the "*Reliability*" and the "*Management*" are also basic issues that need to be addressed. More detailed, through the number of 22 works that we have stood out the statistic results are the following: Privacy 6 of 22, Security 15 of 22, Trusted environment 15 of 22, Bandwidth 5 of 22, Environment limitations 10 of 22, Management 11 of 22, Reliability 12 of 22, User authentication 9 of 22, Efficiency 5 of 22. Equally important, the less mentioned issues are the "*Bandwidth*" and the "*Efficiency*" which are really vital for the functionality of the Mobile Cloud Computing technology.

Regarding this, we could realize that more researches need to be done in the field in order to find better solutions aiming to improve Bandwidth and Efficiency of MCC.

Thus, based on previous works (Stergiou et al., 2018b; Stergiou & Psannis, 2017a; Stergiou et al., 2018f; Stergiou et al., 2018c; Stergiou et al., 2018d; Stergiou & Psannis, 2017b; Plageras et al., 2017; Stergiou et al., 2018a; Stergiou et al., 2018e) the optimal solution in order to achieve a reliable and trusted environment with a more "*safe*" authentication and encryption for the users the MCC system have to adapt the AES encryption algorithm.

The AES algorithm has variable key length of 128, 192, or 256 bits, with default 256 bits. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible algorithm, and it can be implemented on various platforms especially in small devices, such as mobile devices. Also, AES has been carefully tested for many security applications (Singh & Kinger, 2013). As a result, the AES algorithm provides the ability to have speed key setup time a good key agility. So, if we use this algorithm we could have a trusted relay method with an encryption of a speed key setup. Therefore, instead the trust relay use 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. Similarly, 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 AES offers and as a result we can have a better and more trusted transmission in a MCC environment (Stergiou & Psannis, 2017b; Singh & Kinger, 2013; Stergiou et al., 2018e; Gupta, 2018).

Count our study and the reliability of AES encryption algorithm for a MCC environment we suggest the following part of pseudocode based on the AES encryption algorithm.

*Table 3. Suggested pseudocode based on the AES encryption algorithm*

**Algorithm 1**

```
input -> byte[]
byte[] + R.Key -> state[]
for 6 to 66
  W[i-1] -> T
  if i mod 6 = 0
                rotate T + 6
      W[i-6] / T -> W[i]
      R.Key+1
      i+1 -> i
Row +1 -> Row
state[] -> output[]
```

With this proposed method we can extend the advances of MCC, in particular when it integrates with other technologies like IoT and Big Data, by developing a highly innovative and scalable service platform to enable secure and privacy services. Through tour research we can propose the algorithm 1 which extends the security advances of MCC environment, especially when integrates with other technologies. As a proposal of this work could be this part of pseudocode algorithm which uses the original key consists of 128 bits/16 bytes which are represented as a 6x6 matrix.

### F. Experimental Results

Compared our proposed method with the existing one we come to some measurements that have been through time and showing the benefits of our proposed method.

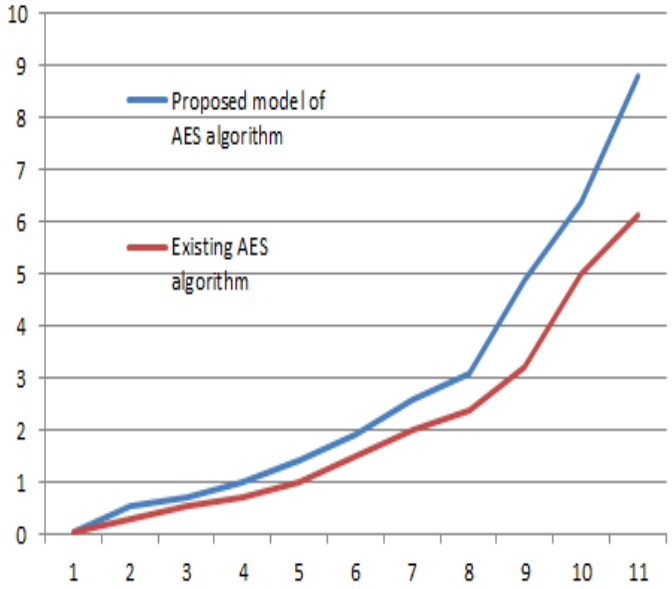


*Figure 3. Security level of encryption algorithms of measurement used for the study of AES model algorithm*

As we can observe by Figure 3 the more often is the combined use of the algorithms, the higher level of security of the data usage we get every time. The upper line represents our proposed model of AES algorithm and the other (down line) represents the existing AES algorithm. Based on Figure 3 we can also figure out that our proposed method is over from the existing model regarding the higher security level of encryption that it can achieve through the time.

## CONCLUSION & FUTURE DIRECTIONS

The MCC technology provides a number of possibilities, but additionally places several challenges and issues that need to be addressed as well. Mobile Cloud Computing refers to an infrastructure where data, applications and information could be processed through a mobile device, but simultaneously outside of the mobile device. The main objective of the use of MCC is to decrease the use of stronger hardware and to have the access to data and applications, and in many times to more computational power, from every place and in any time, through a mobile device.

With our study, in regard on the huge benefits of the Mobile Cloud Computing technology, we try to achieve a more safe and trusted environment for the MCC users in order to operate the functions, and transfer, edit and manage data and applications. This could be achieved proving a novel method count on the AES encryption algorithm, which is, according to our study, the most relevant encryption algorithm to a Cloud environment.

Furthermore, we try to define the most important issues and challenges in the field of Mobile Cloud Computing technology by presenting a number of the most significant works related to MCC through the last eight years.

As a future work, we could focus to find novel ways to achieve a better integration MCC with other technologies, focusing on security algorithms and all the challenges that the technologies faced on security level. Regarding the rapid development of Cloud technology the security issues of Mobile Cloud Computing must be solved or reduced to a minimum in order to have a better and safer model. The security challenges and issues that surveyed in this work 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


Aceto G., Botta A., de Donato W., Pescape A., (2013) "Cloud monitoring: A survey", Elsevier, Computer Networks, vol. 57, issue: 9, pp. 2093–2115, June 2013.

Ali M., Khan S. U., Vasilakos A. V., (2015) "Security in cloud computing: Opportunities and challenges", Elsevier, Information Sciences, vol. 305, pp. 357-383, February 2015. [DOI: 10.1016/j.ins.2015.01.025]

Almrot E., Andersson S., (2013) "A study of the advantages & dis-advantages of mobile cloud computing versus native environment", Digitala Vetenskapliga Arkivet, Bachelor Thesis in Software Engineering, Blekinge Institute of Technology, Karlskrona, May 2013.

Angin P., Bhargava B., Ranchal R., Singh N., Linderman M., (2010) "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", in Proceedings of 29th IEEE International Symposium on Reliable Distributed Systems, 31 October-3 November 2010, New Delhi, India. [DOI: 10.1109/SRDS.2010.28]

Batalla J. M., Mastorakis G., Mavromoustakis C. X., Zurek J., (2016) "On cohabitating networking technologies with common wireless access for Home Automation Systems purposes" IEEE Wireless Communications, vol. 23, issue: 5, pp. 76-83, October 2016. [DOI: 10.1109/MWC.2016.7721745]

Bhattasali T., Chaki R., Chaki N., (2013) "Secure and trusted cloud of things", In Proceedings of INDICON Annual IEEE India Conference, 13-15 December 2013, Mumbai, India. [DOI: 10.1109/INDCON.2013.6725878]

Blog: Follow what's happening at Get Cloud Services, "Mobile Cloud Com-puting – Pros and Cons", GetCloud Services, 23/12/2014. [Online]. Available:

https://www.getcloudservices.com/blog/mobile-cloud-computing-pros-and-cons/. [Accessed 24/12/2017].

Book, (2018) “Secure data outsourcing scheme in cloud computing with attribute-based encryption”, International Journal of High Performance Computing and Networking, vol. 12, issue: 2, pp. 128-136, January 2018.

Botta A., de Donato W., Persico V., Pescape A., (2016) “Integration of Cloud Computing and Internet of Things: a Survey”, Journal of Future Generation Computer Systems, vol. 56, pp. 1-54, March 2016. [DOI: 10.1016/j.future.2015.09.021]

Dinh H. T., Lee C., Niyato D., Wang P., (2011) “A survey of mobile cloud computing: architecture, applications, and approaches”, Wireless Communications and Mobile Computing, vol. 13, pp. 1587-1611, October 2011. [DOI: 10.1002/wcm.1203]

Dobre C., Xhafa F., (2014) “Intelligent services for big data science”, Future Generation Computer Systems, vol. 37, pp. 267–281, July 2014.

Dorgham O., Almonani A., Alauthman M., Albalas F., Obeidat A., (2018) “An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms”, International Journal of Cloud Applications and Computing, vol. 8, issue: 2, pp. 96-112, April 2018.

Doukas C., Pliakas T., Maglogiannis I., (2010) “Mobile Healthcare Information Management utilizing Cloud Computing and Android OS”, in Proceedings of 32nd Annual International Conference of the IEEE EMBS 2010, 31 August-4 September 2010, Buenos Aires, Argentina.

Fremdt S., Beck R., Weber S., (2013) “Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility”, in Proceedings of 46th Hawaii International Conference on System Sciences, 7-10 January 2013, pp. 1025-1034, Wailea, Maui, HI, USA.

Fu Z., Ren K., Shu J., Sun X., Huang F., (2015) "Enabling Personalized Search over Encrypted Out-sourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, December 2015.

Fu Z., Ren K., Shu J., Sun X., Huang F., (2016) “Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement”, IEEE Transactions on Parallel and Distributed Systems, vol. 27, issue: 9, pp. 2546-2559, September 2016. [DOI: 10.1109/TPDS.2015.2506573]

Garg S. K., Versteeg S., Buyya R., (2013) “A framework for ranking of cloud computing services”, Future Generation Computer Sys-tems, vol. 29, issue: 4, pp. 1012–1023, 2013.

Gou Z., Yamaguchi S., Gupta B. B., (2017) “Analysis of Various Security Issues and Challenges in Cloud Computing Environment: A Survey”, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, pp. 221-247, 2017.

Grozev N., Buyya R., (2014) “Inter-cloud architectures and application brokering: taxonomy and survey”, Wiley Online Library, Software: Practice and Experience, vol. 44, issue: 3, pp. 369–390. March 2014.

Gupta B. B., Agrawal D. P., Yamaguchi S., (2016) “Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security”, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, 2016.

Gupta B. B., Badve O. P., (2017) “Taxonomy of DoS and DDoS attacks and desirable defence mechanism in a Cloud computing environment”, Springer, Neural Computing and Applications, vol. 28, issue: 12, pp. 3665-3682, December 2017.

Gupta Brij B., (2018) “Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives”, CRC Press, Taylor & Francis, 666 pages, November 2018.

Habib S. M., Ries S., Muhlhauser M., (2011) “Towards a Trust Management System for Cloud Computing”, in Proceedings of IEEE International Joint Conference TrustCom-11/IEEE ICESS-11/FCST-11, 16-18 November 2011, Changsha, China.

Hada P. S., Singh R., Meghwal M. M., (2011) “Security Agents: A Mobile Agent based Trust Model for Cloud Computing”, International Journal of Computer Applications, vol. 36, no. 12, pp. 12-15, December 2011. [DOI: 10.5120/4547-6435]

Haghighat M., Zonouz S., Abdel-Mottaleb M., (2015) “CloudID: Trustworthy cloud-based and cross-enterprise biometric identification”, Expert Systems with Applications, vol. 42, no. 21, pp. 7905-7916, November 2015.

Hashizume K., Rosado D. G., Fernandez-Medina E., Fernandez E. B., (2013) “An analysis of security issues for cloud computing”, Springer, Journal of Internet Services and Applications, vol. 4, no. 5, pp. 1-13, December 2013. [DOI: 10.1186/1869-0238-4-5]

He W., Yan G., Xu L. D., (2014) “Developing vehicular data cloud services in the IoT environment”, IEEE Transactions on Industrial Informatics, vol. 10, issue: 2, pp. 1587–1595, May 2014. [DOI: 10.1109/TII.2014.2299233]

Hilbert M., López P., (2011) “The World’s Technological Capacity to Store, Communicate, and Compute Information”, Science, vol. 332, issue: 6025, pp. 60–65, 2011.

Huang D., (2011) “Mobile cloud computing”, IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27-31, October 2011.

Jiang Q., Ma J., Wei F., (2018) “On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services”, IEEE Systems Journal, vol. 12, issue: 2, pp. 2039-2042, June 2018. [DOI: 10.1109/JSYST.2016.2574719]

Kaur R., Kinger S., (2014) “Analysis of Security Algorithms in Cloud Computing”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, March 2014.

Keskin T., Taskin N., (2014) “A pricing model for cloud computing service”, in Proceedings of 47th Hawaii International Conference on System Science, 6-9 January 2014, pp. 699-707, Waikoloa, HI, USA.

Khalil I., Khreishah A., Azeem M., (2014) “Consolidated Identity Management System for secure mobile cloud computing”, Elsevier, Computer Networks, vol. 99, pp. 99-110, March 2014. [DOI: 10.1016/j.comnet.2014.03.015]

Khan A. N., Mat Kiah M. I., Khan S. U., Madani S. A., (2013) “Towards secure mobile cloud computing: A survey”, Elsevier, Future Generation Computer Systems, vol. 29, issue: 5, pp. 1278–1299, July 2013.

Kim M., Park S. O., (2013) “Trust management on user behavioral patterns for a mobile cloud computing”, Springer, Cluster Computing, vol. 16, issue 4, pp. 725-731, December 2013. [DOI: 10.1007/s10586-013-0248-9]

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

Li J., Huang L., Zhou Y., He S., Ming Z., (2017) “Computation partitioning for mobile cloud computing in big data environment”, IEEE Transactions on Industrial Informatics, Vol. 11 January 2017.

Liang H., Huang D., Cai L. X., Shen X. S., Peng D., (2011) “Resource Allocation for Security Services in Mobile Cloud Computing”, in Proceedings of IEEE Conference on Computer Communications Workshops INFOCOM WKSHPS 2011, 10-15 April 2011, Shanghai, China.

Mell P., Grance T., (2011) “The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology”, National Institute of Standards and Technology Special Publication, pp. 1-7, September 2011.

Mollah M. B., Azad Md. A. K., Vasliakos A., (2017) “Security and privacy challenges in mobile cloud computing: Survey and way ahead”, Elsevier, Journal of Network and Computer Applications, vol. 84, pp. 38-54, April 2017.

Negi P., Mishra A., Gupta B. B., (2013) “Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment”, Cryptography and Security, arXiv preprint arXiv:1304.7073, April 2013.

Pfarr F., Buckel T., (2014) Winkelmann A., “Cloud Computing Data Protection – A Literature Review and Analysis”, in Proceedings of 47th Hawaii International Conference on System Sciences, pp. 5018-5027, 6-9 January 2014, Waikoloa, HI, USA.

Plageras A. P., Stergiou C. L., Psannis K. E., Kim Byung-Gyu, Gupta Brij B., Ishibashi Y., (2017) “Solutions for Inter-connectivity and Security in a Smart Hospital Building”, in Proceedings of 15th IEEE International Conference on Industrial Informatics (INDIN 2017), 24-26 July 2017, Emden, Germany.

Popa D., Cremene M., Borda M., Boudaoud K., (2013) “A Security Framework for Mobile Cloud Applications”, in Proceedings of 11th RoEduNet International Conference, 17-19 January 2013, Sinaia, Romania.

Prasad M. R., Gyani J., Murti P.R. K., (2012) “Mobile Cloud Computing: Implications and Challenges”, Journal of Information Engineering and Applications, vol. 2, no. 7, pp. 7-15, October 2012.

Rahimi M. R., Ren J., Liu C. H., Vasilakos A. V., Venkatasubramanian N., (2014) “Mobile Cloud Computing: A survey, State of Art and Future Directions”, Mobile Networks and Applications, Volume 19, Issue 2, pp. 133-143, April 2014.

Rao B. B. P., Saluia P., Sharma N., Mittal A., Sharma S. V., (2012) “Cloud computing for Internet of Things & sensing based applications”, In Proceedings of IEEE 6th International Conference on Sensing Technology (ICST 2012), pp. 374–380, 18-21 December 2012, Kolkata, India.

Rittinghouse J. W., Ransome J. F., (2009) “Cloud Computing: Implementation, Management, and Security”, CRC Press, 340 Pages - 127 B/W Illustrations, 17 August 2009. ISBN 9781439806807 - CAT# K10347

Shahzad A., Hussain M., (2013) “Security Issues and Challenges of Mobile Cloud Computing”, International Journal of Grid and Distributed Computing, vol. 6, no. 6, pp. 37-50, 2013. [DOI: 10.14257/ijgdc.2013.6.6.04]

Shi E., Niu Y., Jakobsoon M., Chow R., (2010) “Implicit Authentica-tion through Learning User Behavior”, ACM, in Proceedings of ISC’10 13th International Conference on Information Security, pp. 99-113, 25-28 October 2010, Boca Raton, FL, USA.

Shiraz M., Gani A., Khokhar R. H., Buyya R., (2012) “A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing”, IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1294-1313, November 2012.

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 Proceedings of IEEE 4th International Conference on Cloud Computing, 4-9 July 2011, pp. 582–589, Washington, DC, USA.

Singh G., Kinger S., (2013) “Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July 2013.

Skourletopoulos G., Mavromoustakis C. X., Mastorakis G., Batalla J. M., Sahalos J. N., (2017) “An Evaluation of Cloud-Based Mobile Services with Limited Capacity: A Linear Approach”, Springer, Soft Computing, vol. 21, issue: 16, pp. 4523-4530, August 2017. [DOI: 10.1007/s00500-016-2083-4]

Stergiou C. L., Psannis K. E., Gupta B. B., Ishibashi Y., (2018d) "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, In Press, June 2018d.

Stergiou C., Psannis K. E., (2016) "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016. [DOI:10.1002/nem.1930]

Stergiou C., Psannis K. E., (2017a) "Algorithms for Big Data in Advanced Communication Systems and Cloud Computing", in Proceedings of 19th IEEE Conference on Business Informatics 2017 (CBI2017), Doctoral Consortium, 24-26 July 2017a, Thessaloniki, Greece. [DOI: 10.1109/CBI.2017.28]

Stergiou C., Psannis K. E., (2017b) "Efficient and Secure Big Data delivery in Cloud Computing", Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017b. [DOI: 10.1007/s11042-017-4590-4]

Stergiou C., Psannis K. E., Gupta B. B., (2018f) "Advanced Media-based Smart Big Data on Intelligent Cloud Systems", IEEE Transaction on Sustainable Computing, in Press, 2018f.

Stergiou C., Psannis K. E., Gupta B., Ishibashi Y., (2018e) "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, In Press, June 2018e. [DOI: 10.1016/j.suscom.2018.06.003]

Stergiou C., Psannis K. E., Gupta B., Ishibashi Y., (2018g) "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184, September 2018g.

Stergiou C., Psannis K. E., Kim B.-G., Gupta B., (2018a)"Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018a. [DOI: 10.1016/j.future.2016.11.031]

Stergiou C., Psannis K. E., Plageras A. P., Ishibashi Y., Kim B.-G., (2018b)"Algorithms for efficient digital media transmission over IoT and cloud networking", Journal of Multimedia Information System, vol. 5, no. 1, pp. 27-34, March 2018b. [DOI: 10.9717/JMIS.2018.5.1.27]

Stergiou C., Psannis K. E., Plageras A. P., Xifilidis T., Gupta B. B., (2018c) "Security and Privacy of Big Data for Social Networking Services in Cloud", in Proceedings of IEEE conference on Computer Communications (IEEE INFOCOM 2018), 15-20 April 2018c, Honolulu, HI, USA.

Subashini S., Kavitha V., (2011) "A survey on security issues in service delivery models of cloud computing", Elsevier, Journal of Network and Computer Applications, vol. 34, issue: 1, pp. 1-11, January 2011. [DOI: 10.1016/j.jnca.2010.07.006]

Suo H., Liu Z., Wan J., Zhou K., (2013) "Security and Privacy in Mobile Cloud Computing", in Proceedings of 9th International Conference on Wireless Communications and Mobile Computing (IWCMC 2013), 1-5 July 2013, Sardinia, Italy.

Viswanathan P., (2012) “Cloud Computing – Is it Really All That Beneficial?”, abouttech, 7/7/2012. [Online]. Available: http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm. [Accessed 24/5/2017].

Wang C., Ren K., Lou W., Li J., (2010) “Toward publicly auditable secure cloud data storage services”, IEEE network, vol. 24, no. 4, pp. 19-24, July 2010.

Whaiduzzaman Md., Haque M. N., Chowdhury Md R. K., Gani A., (2014) “A Study on Strategic Provision of Cloud Computing Services”, The Scientific World Journal, pp. 1-8, June 2014.

Whaiduzzaman Md., Sookhak M., Gani A., Buyya R., (2014) “A survey on vehicular cloud computing”, Elsevier, Journal of Network and Computer Applications, vol. 40, pp. 325-344, April 2014. [DOI: 10.1016/j.jnca.2013.08.004]

Y. Kumar, R. Munjal, H. Sharma, (2011) “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue: 3, October 2011.

Zhang Y., Chen X., Wong D. S., Li H., You I., (2017) “Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing”, Elsevier, Information Sciences, vol. 379, pp. 42-61, Febrouary 2017. [DOI: 10.1016/j.ins.2016.04.015]