South-East European University

Faculty of Contemporary Sciences and Technologies

Third Cycle Studies

Doctoral Dissertation Topic:

THE PROPOSED MODEL FOR SECURITY IN THE CLOUD, CONTROLLED BY THE IT SECURITY SPECIALIST- END USER

Candidate:

Mr.Sc. Dhuratë Hyseni

Supervisor:

Prof.Dr. Betim Çiço

Tetovo, 2018

Faculty of Contemporary Sciences and Technologies

South East European University, Tetovo, Macedonia.

Supervisor: Prof. Dr. Betim Çiço, South East European University

Date:

01/03/2018

Upon request of Mr. Sc. Dhuratë Hyseni of Ferizaj candidate of the PhD at South-East European University of Tetova Macedonia, Faculty of Contemporary Sciences and Technology, I issue the following:

CERTIFICATE

It is hereby certified that her PhD Dissertation named

THE PROPOSED MODEL FOR SECURITY IN THE CLOUD, CONTROLLED BY THE END USER-ITSS

Was proofread by me Mr. Sc. Sefedin Musliu, Court Authorized Translator/Interpreter of Gjilan And my colleague Robert John Symons, Advocate of Gjilan.

Gjilan, this 13 day of February, 2018

Sefedin Musliu

ABSTRACT

Cloud computing has brought impressive advantages for clients wishing to use cloud services, such as flexibility in managing the space, automatic software updates, easier access to required information, etc. Yet, there is a complex problem regarding security of data in the cloud, which becomes more critical when the data in question is highly sensitive. The encryption of data at rest is considered to be one of the main issues related to security in cloud computing and especially in cloud storage.

Although there is an increase in the usage of the cloud storage services, there is still a significant number of client organizations that lack sufficient trust in third party cloud providers to rely on the sole security they provide. One of the main approaches to overcome this problem is the encryption of data at rest, which comes with its own difficulties such as efficient key management, access permissions, and similar factors.

We propose a new approach to security that will be controlled by the IT security specialist (ITSS) of the company i.e. the file owner. The approach is based on multiple strategies of file encryption, partitioning, and distribution among multiple storage providers, resulting in increased confidentiality since a supposed attacker will need to first obtain parts of a file from different storage providers, know how to combine them, before any decryption attempt. We also show how the proposed approach compares to different enterprise-wide encryption strategies. All details of the strategy used for a particular file are stored on a separate file, which can be considered as a master key for the file contents. Also, we present each strategy with the results and comments related to the completed measurements.

ABSTRAKT

Klaud kompjuting ka sjellur perparësi të jashtzakonshme për klient të cilët dëshirojnë t'i përdorin këto shërbime, e ndër përparsitë kryesore është fleksibiliteti në manaxhimin e hapsirës, përditësimi automatik i softuerëvë dhe qasja e lehtë në informacione të nevojshme. Megjithatë, akoma ekzistonjnë probleme komplekse sa i përket sigurisë së të dhënave në klaud, e që behet akoma më kritike kur janë në pyetje të dhënat e ndjeshmëri të lartë. Kriptimi i të dhënave në përgjithsi duket të jetë njëra nga qështjet kryesore lidhur me sigurinë në klaud dhe në vecanti me hapsirën në klaud.

Përkundër rritjes së përdorimit të shërbimeve të hapsirave në klaud, akoma egziston një numër i madh i organizatave/ kompanive që nuk u besojnë palëve të treta të provajderëve të klaudit dhe sigurinë që ata ofrojnë. Njëra nga qasjet më thelbësore për të tejkaluar këtë problem është kriptimi i të dhënave në përgjithësi e cila poashtu ka edhe vështirësitë e saja e që është manaxhimi i çelsave efiqient, lejimi i qasjes dhe faktor të tjere.

Në këtë rast ne propozojmë një qasje të re të sigurisë që do të kontrollohet nga Specialisti i Sigurisë së IT (ITSS) i kompanisë, p.sh pronari i fajllit. Kjo qasje bazohet në strategji të shumefishta të kriptimit të fajllave, ndarjes dhe shperndarjes nëpër hapsira të ndryshme të provajderëve të ndryshëm duke rezultuar në rritjen e konfidencialitetit meqë sulmuesit e mundshëm do të duhej ti marrin pjesët e fajllit nga hapsirat e provajderëve të ndryshëm, të dijnë ti kombinojnë, parase të fillojnë ti dekriptojnë. Ne poashtu, tregojmë se si qasja jonë e propozuar krahasohet me strategjitë e gjëra të enkriptimit të kompanive. Të gjitha detajet e strategjive të përdorura të ndonjë fajlli ruhen në në një fajll të vecant, i cili mund të konsiderohet dhe si master çelsi i përbajtjes së fajllit. Ne poashtu, paraqesim secilën strategji me rezultatet dhe komentet lidhur me matjet e bëra.

АБСТРАКТ

Употребата на операција Клауд донесе импресивни предности за клиенти кои сакаат да го користат услугите Клауд, како што е флексибилност во управувањето со просторот, автоматско ажурирање на софтверот, полесен пристап до потребните информации, итн. Сепак, има еден сложен проблем во врска со безбедноста на податоците во Клауд, кој станува се повеќе критичен кога податоците во прашање се многу чувствителни. Кодирање на пасивни податоци се смета за еден од главните проблеми поврзани со безбедноста во употребата на операција Клауд, а особено во архивирањето Клауд .

Иако има зголемување на користење на услугата архивирање во Клауд, се уште има голем број на организации на клиенти кои немаат доволно доверба во трети лица даватели на Клауд за да сметат на безбедноста која тие го обезбедуваат. Еден од главните пристапи за да се надмине овој проблем екодирање на пасивни податоци, кој доаѓа со свои тешкотии како што е ефикасно клучно управување, дозволи за пристап, и слични фактори.

Ние предлагаме нов пристап за безбедност, која ќе се контролира од страна на специјалист за ИТ безбедност (ITSS) на компанијата, односно сопственик на датотеката. Пристапот се заснова на повеќе стратегии на кодирање на дадотека, поделба и дистрибуција меѓу повеќе провајдери за архивирање, што резултира со зголемена доверливост додека напаѓачот ќе треба прво да зема делови од датотека од различни провајдери за архивирање, знае како да ги комбинира, пред да се обиде да ги декодира. Ние, исто така покауваме како предложениот приод се споредува со различни стратегии за кодирање со широк потфат. Сите детали за стратегија користени за одредена датотека се чуваат на посебна датотека, која може да се смета како управувачки клуч за содржината на датотеката. Исто така, ви го претставуваме секоја стратегија со резултатите и коментари во врска со извршените мерки

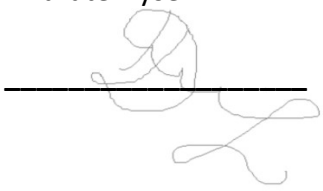
DECLARATION

I declare, that my Dissertation

The Proposed Model for Security in the Cloud, Controlled by the IT Security Specialist- End User

has been written entirely by myself and has not been submitted previously. The research was carried out at the SEEU under the supervision of Prof. Dr. Betim Çiço.

Dhuratë Hyseni



ACKNOWLEDGEMENTS

The work for this PhD dissertation has been challenging and was intense for the rest of three years, and would not have been possible without the intensive help and support of several people whom I would like to thank.

I would like to acknowledge all the professors and peoples who assisted me during my doctoral studies at South East European University.

I'm most grateful to Prof. Dr. Betim Çiço, my advisor, for his great encouragement, advice and guidance professionally and personally. He has provided me the honor and opportunity to work in this PhD dissertation.

Last but not least, I sincerely thank my parents, my husband and my doughter Ema for their sacrifice, understanding, patience, encouragement, love and support during those challenging moments of my studies.

TABLE OF CONTENT

1 INTRODUCTION 18

1.1 MOTIVATION 18
1.2 RESEARCH QUESTIONS 22
1.3 HYPOTHESES 22
1.4 PUBLICATIONS 24
1.5 ORGANIZATION OF THIS DISSERTATION 25

2 FUNDAMENTALS OF CLOUD COMPUTING 27

2.1 CLOUD COMPUTING 27
2.2 FEATURE OF CLOUD COMPUTING 29
2.3 CLOUD SERVICE MODELS 31
2.4 CLOUD DEPLOYMENT MODELS 34
2.5 CLOUD ARCHICETURE DESCRIPTION 36
2.6 SECURITY IN CLOUD INFRASTRUCTURE AND SECURITY RISKS 39
2.6.1 Analysis of threats in cloud environments 39
2.6.2 Security and privacy concerns in cloud services 45
2.7 SECURITY OF IAAS 46
2.8 SECURITY OF PAAS 48
2.9 SECURITY OF SAAS 49
2.10 DATA SECURITY IN CLOUD COMPUTING 53
2.10.1 Data confidentiality 55
2.10.2 Data integrity 59
2.10.3 Data availability 61
2.11 VIRTUALIZATION AND MULTI-TENANCY 63
2.12 DIFFERENT TYPES OF VIRTUALIZATION 65
2.13 DESIGNING SECURE MULTI-TENANCY 68

3 RELATED WORKS 70

3.1 INTRODUCTION 70
3.2 SOLUTION PROPOSED FOR CLOUD SECURITY UNTIL NOW 71
3.2.1 Analysis of the first proposal 71
3.2.2 Analysis of the second proposal 73
3.2.3 Analysis of the third proposal 73
3.2.4 Analysis of the fourth proposal 74
3.2.5 Analysis of the fifth proposal 74
3.2.6 Analysis of the sixth proposal 75
3.2.7 Analysis of the seventh proposal 76
3.2.8 Analysis of the eighth proposal 77
3.2.9 Analysis of the nine proposal 79
3.2.10 Analysis of the ten proposal 81

4 THE ROLE OF CRYPTOGRAPHY FOR CLOUD SECURITY 83

4.1 INTRODUCTION 83
4.2 FUNDAMENTALS ON CRYPTOGRAPHY 83
4.3 CRYPTOGRAPHY IN CLOUD SECURITY 85
4.3.1 The importance and difficulty of encrypting data in the cloud 89
4.4 ENCRYPTION AND DECRYPTION TECHNIQUES 92
4.4.1 Symmetric Cryptography 94
4.4.2 Data Encryption Standard-DES 96
4.4.3 Triple Data Encryption Standard -3DES 97
4.4.4 Advanced Encryption Standard - AES 98
4.4.5 Asymmetric Cryptography 99
4.4.6 Diffie Hellman - DH 99
4.4.7 El Gamal 101
4.4.8 Rivest-Shamir-Adleman RSA 103
4.4.9 Hybrid Cryptography 105
5 PROPOSED MODEL ANALYSIS FOR CLOUD SECURITY CONTROLLED BY END USER-ITSS 108
6 IMPLEMENTING PROPOSED MODEL FOR CLOUD SECURITY CONTROLLED BY END USER-ITSS 111
6.1 IMPLEMENTATION OF THE PROPOSED MODEL 111
6.2 THE STRATEGY OF ENCRYPTION OF THE PROPOSED MODEL 116
7 MEASUREMENTS OBTAINED IN THE PROPOSED MODEL 128
7.1 FIRST PART OF MEASUREMENTS 129
7.1.1 Discussions on obtained measurements, based on our model for first part. 138
7.2 SECOND PART OF MEASUREMENTS 139
7.2.1 Discussions on obtained measurements, based on our model for second part 151
8 CONCLUSION 153
9 REFERENCES 155

LIST OF FIGURES

Figure 1. *Cloud Computing Environment 27*

Figure 2. *Users of Cloud Application Platform 29*

Figure 3. *Cloud computing architecture with an e-mail aplication example. [11]..... 32*

Figure 4. *Cloud Service Reference Architecture [18] 37*

Figure 5. *Security for the SaaS stack [34]..... 50*

Figure 6. *Complexity of security in cloud environment [34]..... 54*

Figure 7. *Data security for proposel model for cloud security 55*

Figure 8. *Cloud security relationship framework 64*

Figure 9. *Steps to implement full virtualization kernel level [69]..... 66*

Figure 10. *Actions taken to implement virtualization the type of paravirtualization kernel leve [69] 67*

Figure 11. *Virtualization Hardware-assisted [69] 68*

Figure 12. *Levels of Abstractions of Cloud Computing..... 71*

Figure 13. *Security objectives for different stakeholders..... 72*

Figure 14. *Basic scheme for communication..... 85*

Figure 15*. Security challenges in major areas of cloud and cryptography role, [92]..... 88*

Figure 16. *Classification of algorithms [113]..... 94*

Figure 17. *The schema of symmetric encryption and deencryption 95*

Figure 18. *Encryption with DES 97*

Figure 19. *The function of AES..... 98*

Figure 20. *The function of DH..... 100*

Figure 21. *RSA processing of Multiple Blocks [123] 104*

Figure 22. *Schema for hybrid function [125]..... 106*

Figure 23. *Hybrid algorithms used in the app. eSiguria 107*

Figure 24. *Proposed model for security in cloud computing controlled by the ITTS [93, 108]..... 109*

Figure 25. *Login form for access..... 111*

Figure 26. *Modules in "eSiguria"* *111*
Figure 27. *The form of configuration of "eSiguria"* *112*
Figure 28. *The form of user configuration.* *113*
Figure 29. *The form of sending documents to the cloud* *113*
Figure 30. *Module of Administration* *114*
Figure 31. *Workflow for the proposed cloud security model* *114*
Figure 32. *Configuration of security for users* *115*
Figure 33. *Partitioned then encrypted data* *117*
Figure 34. *Encrypted then partitioned data* *118*
Figure 35. *Part of code used to present the implementation of Random partitoning* *119*
Figure 36. *Part of code used to present the implementation of Static partitoning* *119*
Figure 37. *Partition Schema based on file size* *120*
Figure 38. *Part of the code providing the implementation of partitions based on the size of file* *121*
Figure 39. *Partitioning and distribution of files to the cloud computing* *122*
Figure 40. *Content of the file ..enc* *123*
Figure 41. *Stream Cipher Diagram[130]* *125*
Figure 42. *Differences between Stream Cipher and Block Cipher* *126*
Figure 43. *Part of the code from eSiguria, for the use Stream Cipher and Block Cipher* ... *127*
Figure 44. *Schema of implementation of Case_I, for algorithm AES used at the first group of measurements.* *130*
Figure 45. *Schema for implementation of CASE_II, for algorithm AES used at the first part of measurements.* *131*
Figure 46. *Graph of the group 1* *135*
Figure 47. *Graph of the group 2.1* *136*
Figure 48. *Graph of the group 2.2* *136*
Figure 49. *Graph of the group 2.3* *137*
Figure 50. *Graph of the group 3* *137*

Figure 51. *Graphic presentation of Case_I and Case_II for symmetric and asymmetric algorithms..... 139*

Figure 52. *Used schema in the second part of measurements for symmetric algorithms. 140*

Figure 53. *Schema used in the second part of measurements for asymmetric algorithms 141*

Figure 54. *Schema used in the second part of the measurements for hybrid algorithms . 143*

Figure 55. *Graphical presentation of measurements for the type of file .doc with size 2969 ..... 147*

Figure 56. *Graphical presentation of measurements for the type of file .doc with size 606 KB..... 147*

Figure 57. *Graphical presentation of measurements for the type of file .pdf with size 606 KB..... 148*

Figure 58. *Graphical presentation of measurements for the type of file .png with size 606 KB..... 148*

Figure 59. *Graphical presentation of measurements for the type of file .mov with size 606 KB..... 149*

Figure 60. *Graphical presentation of measurements for the different type of files 149*

Figure 61. *Graphical presentation of data from the table 12..... 151*

LIST OF TABLES

Table 1. *Data in relation to our proposed model, referring to study [1] and most important elements that are shown above 20*

Table 2. *The way of control and management of models in the cloud computing..... 35*

Table 3. *Overview of cloud related threats as defined by the Cloud Security Alliance [21, 22] 39*

Table 4. *Cloud security threats and some related solutions based on our survey and the CSA documents [21, 22] 42*

Table 5. *Security requirements for different level [33] 52*

Table 6. *Classification of cryptographic algorithms 89*

Table 7. *Explanation for figure 33 and 34 ..... 117*

Table 8. *Block Cipher Modes of Operation [130] 124*

Table 9*. Files used for measurement 128*

Table 10*. Rresults from the measurements of the first part 132*

Table 11. *Results of measurements for the second part 144*

Table 12. *Rezults of measurements for the second par, presented in general 150*

ABBREVIATIONS

The following table describes the significance of various abbreviations and acronyms used throughout the thesis.

Abbreviation	Meaning
IT	Information technology
ISP	internet service provider
CIA	Confidentiality Integrity Availability
CSP	Cloud Serves Provider
CC	Cloud Computing
IT	Information Technology
CSC	Cloud Services Customers
SLA	Service Level Agreement
SOA	service oriented architecture
PDP	Provisional Data Possession
NIST	National Institute of Standards and Technology
SSL	Secure Socket Layer
AWS	Amazon Web Services
SLA	Service Level Agreement
SAAS	Software as a Service
PAAS	Platform as a service
IAAS	Infrastructure as a service
I/O	Input-output
WSS	Web Services Security
CSA	Cloud Security Alliance
VM	Virtual machines
ISMS	Information Security Management Systems
IEEE	Institute of electrical and electronics engineers
SSL	Secure Socket Layer
TLS	Transport Layer Security
AD	Active Directory
VMI	virtual machine introspection
RAIN	Redundant Array of Independent Net-storages
VMM	Virtual Machine Monitor
SOA	service oriented architecture
ACPS	Advanced Cloud Protection System

TCCP	Trusted Cloud Computing Platform
PVI	Private Virtual Infrastructure
TPM	Trusted Platform Modules
POR	Proof of Retrieval
HLA	Homomorphic Linear Authenticator
PDP	Provable Data Possession
MAS	Multi-Agent System
SSLA	Security Service Level Agreements
DH	Diffie-Hellman
TLS	Transport Layer Security
ITSS	IT Security Specialist
PDP	Provisional Data Possession
TPA	Third Party Auditor

CHAPTER I

Part I:

1 INTRODUCTION

1.1 Motivation

Storing data and offering Cloud service make it very attractive to its users, as well as to the ISP (internet service provider). Many different organizations and businesses have gone through this environment or are considering the benefits of it for their businesses. A very important motive was the Global Encryption Study [1].

Global encryption study is the twelfth study sponsored by Tales e- Security - This research is based on two main aspects that we will deal with: first, to tell of the plan to store data in the cloud and secondly the possibility of inventing an effective and trustworthy model of the storing data in cloud. Cryptography is seen as the most powerful part in this field but there is still a gap in organizations because they require maximum protection of sensitive data from inside and outside attacks. Based on this study [4], these are the most important findings in recent years:

- Possible changes in the encryption strategy and managing this strategy in the industry,
- Protection of sensitive data and the possibility of controlling keys in cloud computing,
- Data that should be encrypted and application that enable this service,
- The role of Hardware Security Modules (HSMs) for addressing cloud and managing cases

A large number of companies coming from eleven main countries of the world have taken part in this research. The first steps in the creation encryption strategies in the cloud computing were studied in the USA in 2005, and was then developed all over the world. This research presents different statistics that were collected at the end of each year, and every research undertaken has been based on security factors.

We have closely analyzed some very important elements for the proposed model for providing security in cloud [1]:

The way of storing data by the organizations after they are sent to the cloud:

- 46% of the respondents answered that the encryption was realized before data was send to the cloud, so that the encrypting keys were managed locally by the organization itself,
- 21% of them allow encryption in cloud by keys that are generated and managed locally,
- 37% of them rely completely on the provider offering space in the cloud such as key generation and its management.

Industries that have shown interest on improving the encryption strategies:

Financial services, transportation, Tech & software, health & pharmacy, hospitality, consumer products, public sector and its increase over the years.

Possible attacks that come for sensible data: based on the data it is estimated that the main factor in losing sensible data are mistakes made by employees at 54%. Information related to the management of encrypting keys, which keys are difficult to manage in the encryption process. Starting from the encrypting keys to host services up to the archiving keys and back up data.

The way of organizing data to be stored in the cloud:

- 46% - encryption of data before sent to the cloud as well as managing and generating keys realized locally,
- 37% - encryption of data, generation and management of data is realized by the provider

*Table **1.** Data in relation to our proposed model, referring to study [1] and most important elements that are shown above*

Elements	Support of the proposed model
The way of storing data by the organization after it is sent to the cloud	Our proposed model takes part at the question where data is partitioned and encrypted then sent to the cloud, which got 46% interest by the companies.
Industries which have shown interest in developing a better encrypting strategy	In this part our proposed model offers support for every field we mentioned above.
Possible attacks on sensitive data	After processing the data, 56% of attacks on sensitive data come from the employees. In this context, our proposed model does not allow employees to make such mistakes. It uses security configuration realized by the IT specialist (employee who is well qualified in IT), then the entire communication continues on that configuration for a particular employee.
What keys pose difficulties when managing in the encrypting process	The proposed model makes it possible to store the data by the used strategy. This strategy depends on the type of algorithm used, the cryptography keys, the method of partitioning etc. This file is stored locally to the last user.
The way of organizing data for storing in the cloud	Our proposed model relates to the 46% option of encryption of data which are completed before being send to the cloud. Depending on the strategy used, we have shown them in..CHAPTER 5 & 6.

Shared resources – Cloud computing is known for its increase in reliability and scalability between parties in this environment. Users might be able to buy, sell or rent space depending on their requirements. Shared resources is an important element in cloud computing and the space is offered to the client with a restricted management or control for the client. There are different working clouds. If it requires thread running at the same

domain then it is reasonable to demand the share of joint resources. Although it is not treated by the *Cloud Providers*, it also has its disadvantages, competing for the cloud servers it is related to the performance and as a result there will not be such high performance as in the free clouds, [109].

Massive scalability –The main advantage of cloud computing is scalability; it enables the management of demands coming from clients. The cloud scalability offers an increase of space usage for a particular period of time or different purposes and without any effect on their performance. The infrastructure of scalability can be realized both vertically or horizontally based on the handling of the problem. It is seen by clients as a low cost advantage because they only pay for the space they need to use. There are many possibilities of monitoring scalability offered by the IT for companies but there is an ongoing research of the different algorithms with a possibility of anticipating scalability at any time of use.

Elasticity – It is seen as a possibility of complying with the requirements or needs of the allocated resources. Also the possibility of managing uploads independently by the user and in real time. The use of Elasticity services has the possibility of adjusting and planning the architecture for the increase and decrease of infrastructure in disposition and is thus foreseen for virtual cloud as well. Elasticity is related directly to the service "pay as you go" and companies pay only for the services used. Scalability is treated more in the layer of system application for receiving and removing resources, whereas Elasticity is treated as a possible way of creating space and the adaptation of a request in real time.

Self-provisioning of resources- In cloud computing this alternative is also known as a self-service for the use of services based on needs without taking part of the other parties. Users are free and independent and may use services based on their requests without participation of IT personnel, understandably in the certain limit by the other parties. The services are ready to be used at any time and their use is depended directly by the user, based on his/her needs.

1.2 Research Questions

The main question to be answered in this thesis is the data security in the cloud and reliability of the end user in the cloud. Despite the fact that during the research, many solutions were proposed but no real solution offered a high level of reliability. The open question that led this research is: How do we achieve the implementation of an application that controls the data securely from recent cloud computing users? At the moment, as a solution to the benefit of the end users, it offers data monitoring in the storage process in the cloud. However, this section has added the security mode of the user's latest security, giving them the ability to determine the level of encryption and algorithms and the file partitioning method before being sent to the cloud environment.

To reach the highest level of confidence for the cloud user, this scientific research paper will answer the following questions:

- *What is the proposal for sensitive data security in the cloud computing?*
- *Is this solution the best proposed in comparison with the other solutions?*
- *How difficult is the encryption process in the cloud environment?*
- *What is the level of data encryption offered by the provider?*
- *The role of the server location for data in the cloud environment?*
- *How important are the data security certifications in the cloud?*

1.3 Hypotheses

This thesis investigates three main hypotheses. The main aim is to increase the data security in the cloud controlled by the end user. Stated hypothesis related to our scientific work in this particular field of our dissertation.

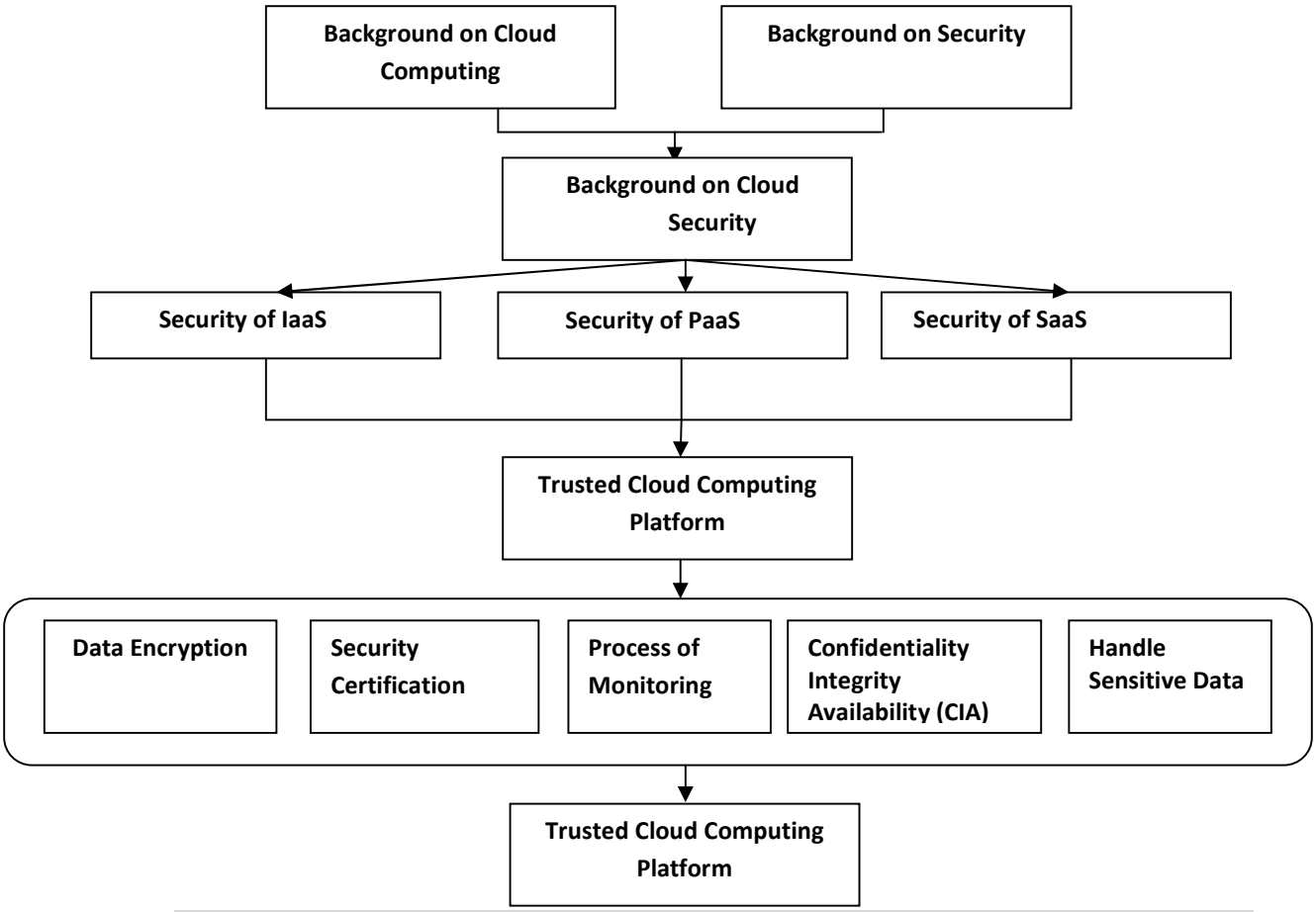
Null Hypothesis: *Defining a suitable model to enhance security in the cloud controlled by the end user- IT Security Specialist*.

This hypothesis is implemented in a way that is based on the security claims in the cloud, claims related directly to the sensitivity of data determined and controlled by the end user, the ITSS. It is implemented and tested for different cases (see VI&VII CHAPTERS for more details.)

Hypothesis II: *Combination of two types of symmetric and asymmetric algorithms, as a suitable solution to provide the data security in the cloud*. Second hypothesis is implemented in the proposed model of Null hypothesis and explained in details for symmetric, asymmetric and hybrid algorithms, as a better solution for in cloud security. It explains the way of applying encryption of data in the cloud, which has been viewed as a challenge for many researches in this field. Another challenge in the field of encryption and the way of managing the encryption keys, which enables these keys to be saved locally or send to the cloud, but before this data is encrypted by the DSA algorithm.

Hypothesis III: *The proposed model for security in the cloud may be implemented safely.* The proposed model for controlling the security in the cloud is implemented in the .Net, explanation regarding the way of implementation and the supported modules offered in chapter V.

The steps followed to implement Research Questions and Hypotheses:



1.4 Publications

Research done for the thesis has been supported by these publicaions:

1. International Journal of Advanced Computer Science and Applications- IJACSA, "*The Proposed Model for Increased Security of Sensitive Data in Cloud Computing*", Dhuratë Hyseni, Besnik Selimi, Artan Luma, Betim Cico, Volume 9 No 2. February 2018.

2. JOURNAL OF NATURAL AND TECHNICAL SCIENCES- JNTS, "*Data Encryption, Partition and Distribution Strategies for User-Controlled Security in the Cloud*", Dhuratë Hyseni, Besnik Selimi, Artan Luma , Betim Cico, (2018)

3. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), "*The Strategy of Cryptography for the Proposed Model of Security in Cloud Computing*", Dhuratë Hyseni , Besnik Selimi , Artan Luma , Betim Cico, 978-1-5386-0814-2/17, IEEE, 2017

4. International Journal on Information Technologies & Security, "*CONCEPTION, DESIGN AND IMPLEMENTATION OF AN INTERFACE FOR SECURITY IN CLOUD CONTROLLED BY THE END USER*", Dhuratë Hyseni, Betim Çiço, Besnik Selimi, (2016)

5. 4th Mediterranean Conference on Embedded Computing (MECO' 2015), "*The proposed model for security in the cloud, controlled by the end user*", Dhurate HYSENI, Betim CICO, Isak SHABANI, (14-18 June 2015)

6. 9th South East European Doctoral Student Conference (DSC'2014) – "*The proposed architecture for security in the cloud, based on safety elements controlled by the user*" Dhurate HYSENI, Betim CICO, 2014

7. 14th Workshop “Software Engineering Education and Reverse Engineering”, Romania - Sinaia, “Data *Security in the Cloud: A Proposed Model*”, Participant, Dhurate HYSENI, Betim CICO, 24 – 30 August 2014

1.5 Organization of this dissertation

The dissertation is organized as follows:

Chapter 2 introduces topics which outline the fundamentals of this field. This includes a component based approach for cloud computing, security in the cloud infrastructure, data security in the cloud, virtualization and multi-tenancy.

Chapter 3 provides an analysis of recent solutions provided for security in the cloud. The chapter analyses all the proposals made, outlines the main idea for the solutions offered and similarities with our proposed model. We have analyzed about ten proposals as a best solution similar to our proposal.

Chapter 4 outlines the role of cryptography in cloud computing. Moreover, it begins with the basics of cryptography, the importance and issues of encrypting and sending them to the cloud. The second part of the chapter explains the techniques of encryption and decryption, then explains symmetric, asymmetric and hybrid algorithms and their application in our proposal.

Chapter 5 is the focal point of this work. It gives a thorough explanation to our proposed model for security control by the ITSS. In addition, it explains the options offered to increase security in cloud computing.

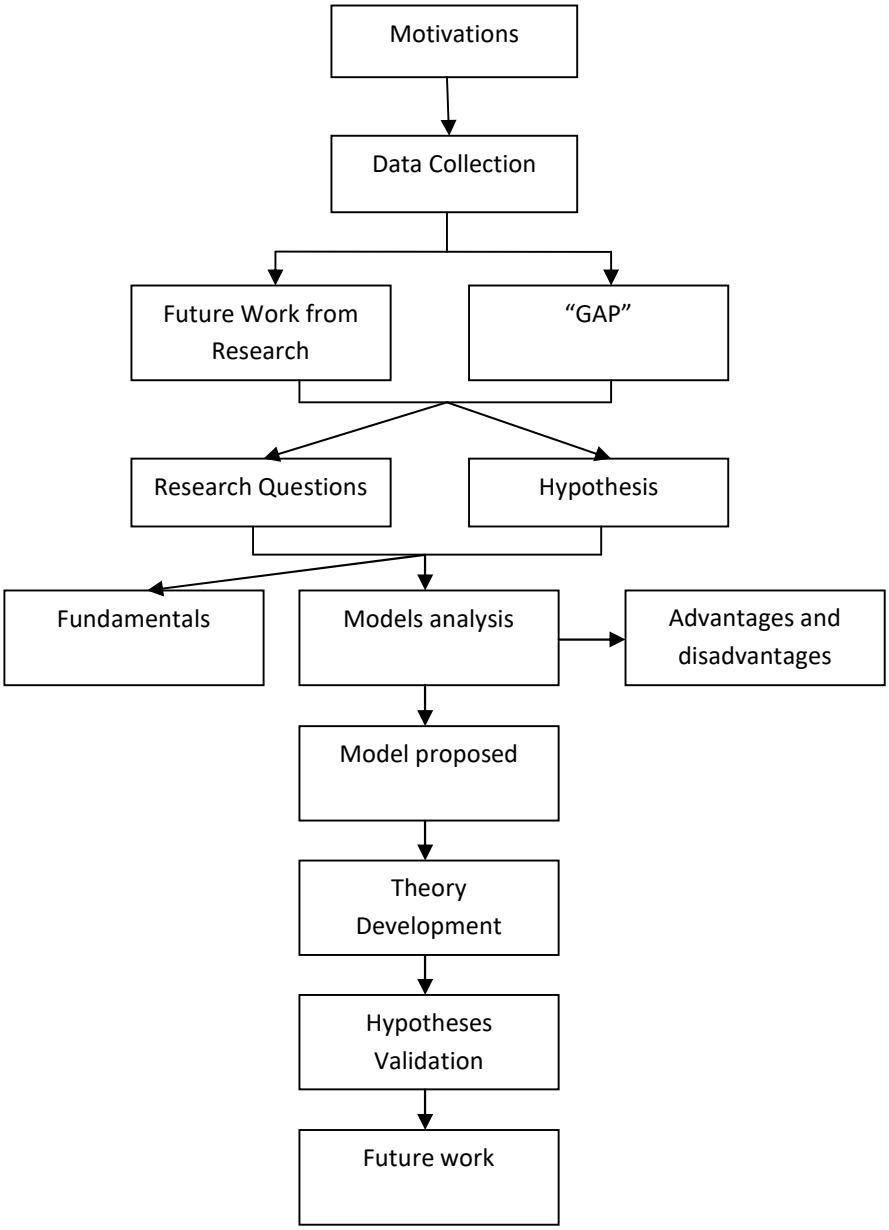
Chapter 6 treats the method of implementing our proposed model in chapter 5. Apart from the explanations of our proposed model it also offers the method of implementation for every model of the application named as “eSiguria” (our proposed model). The second part provides the strategy of encryption used in our model.

Chapter 7 treats the realized measurements of our proposed model. These measurements were divided in two parts, the first part considers two scenarios (for symmetric and asymmetric algorithms), and the other part treats three scenarios (for symmetric, asymmetric and hybrid algorithms). All the results are given in graphs and

tables. Therefore, each part presents the results in graphs bringing a better picture of the obtained measurements.

Finally **Chapter 8** concludes the dissertation and discusses the future work.

Organization of this dissertation:



CHAPTER II

2 FUNDAMENTALS OF CLOUD COMPUTING

2.1 Cloud Computing

Cloud computing brings together the use of different technologies such as virtualization, and clusters. Cloud Computing should be understood as a technology in which it is estimated that in the future we will not have a personal or local computer but one that is managed by a third party and which provides the services required by the client. It should be noted that as regard to this idea in 1961 computer scientist John McCarthy said that "*computation may someday be organized as a public utility*", and he proceeded to project this idea with explanation [*2*].

According to [*3*] Cloud computing, it represents a pool of virtualized resource that includes a variety of different loads, which enable you to overcome these loads faster and with a higher security through virtual or physical machines. It removes the possibility of failure of software and hardware and it can monitor resources all the time and to allow a balance of resources as needed.

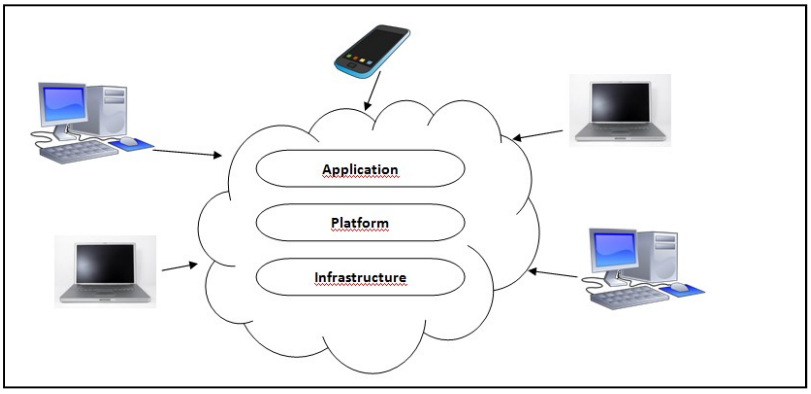


*Figure **1**. Cloud Computing Environment*

This technology started to become really popular because it offers its customers the choice to pay only for the services they use.

Fig 1. Everyone with an Internet connection and browser can simply have a cloud application [*3].*

"*The complexity for minimum costs component has increased at a scale with a factor of two per year ... Surely*, it is expected *that in a short period of time this factor has been increased*" (Moore, 1965). Expressed as Moore's Law, everything in Information Technology is advancing exponentially. The complete cloud computing infrastructure is based on the Infrastructure as a Service (IaaS), software as a service (SaaS) and as a platform or as a service (SaaS). All these services are offered pay-as-you-go, paying rent for as much as we need and the use of hardware and software for our needs. There are many cloud computing advantages and, according to some research, it will replace all the traditional tools which are in every business. But the main concern is how to provide high safety levels and the insulation of services that use different consumers [4].

For those who develop programs, cloud platforms are very interesting, [5]. The diagram we used to organize discussion provided an environment that developers can use to build applications for clients as they requred. It is common to build SaaS applications for new platforms, but this is not necessary. People also use "software leaders" to run traditional SaaS requirements. No matter how they are used, the cloud platforms are an important part of this story.

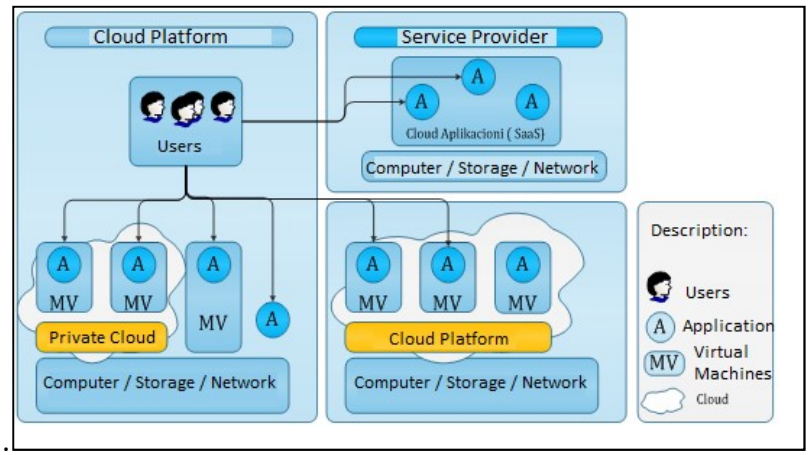


*Figure **2.** Users of Cloud Application Platform*

For fig.2, the Cloud is a platform for developers, which allows developers to create and run applications, databases, etc. This is a platform and not an application. The issue is that we have confused the Cloud Platform and Application of the Cloud. Developers are focused on the platforms of the applied and contemporary market. Such a platform provides a self-service access to resources, such as a virtual machine with a capacity of gigabytes of data storage, which is usually accomplished through a web site. A Cloud platform is very costly. There is no opportunity to seek a physical server for a few months and it has been a tradition to host it. There were requirements for a virtual machine for example the concert (ticket sales) machine for one day. The most important of the four points fig.2, is a Cloud platform which allows payment only for resources using an application. If a customer requires the VM for 6 hours or 30 VM is required for 6 hours, then this service may be paid by the service users. Some of these features, but not all, are very attractive and that is why the Cloud Platform is important [6].

2.2 Feature of Cloud Computing

Cloud computing is a new technology which is developing very fast so it is difficult to find a good definition for a complete accuracy. Because it is a developing technology, its definition is constantly changing with time. The U.S. Government National Institute of Standards and Technology (NIST) seeks to provide much more contemporary definitions of cloud computing. The current version of defining them is dated 15/10/2009 [7], according

to the NIST's a cloud computing application service which provides a cloud with a number of sources in the network. Cloud computing is characterized by five main features that define the main functions. The Cloud is offering three service models which indicate the level of service provided and four development models where the built-cloud is the one you may have access to. The main characteristics of the cloud computing is as follows [8]:

Supermarkets requests: Users can manage the cloud resources by paying only what they consume.

External network access: Resources provided by the cloud can be accessed by as many normal services as possible with laptops, PDAs, phones, etc.

Gathering resources: The Cloud provider enables a set of resources to different clients based on their demand. A client may have accesses to the service without any information on the exact position of the cloud, but may be able to offer a position to a higher level of abstraction, such as region, state, data center etc.

Rapid elasticity: Resources provided by the cloud computing are highly scaleable. Customers may escalate the resources when used, and then turn the system back to the previous state. Scalability of the cloud is in the form of a modular system. They may appear as infinite resources as clients do not need to make plans themselves but require better access.

Measured service: Offered by cloud resources are controlled and optimized depending on their skills. The use of resources can be monitored, controlled and reported in order to provide transparency for parties, client and "server". Due to the different characteristics of the existing software in the cloud compared with hypervisor features, a significant problem appears in the interaction. The organizations of an open source cloud computing system strives to establish a set of principles for operating systems with features that come to help the cloud providers [9].

This statement is supported by over 300 companies including the Novell, VMware, AMD, IBM, etc.

There are six principles declared by the organization of the cloud computing:

1. Cloud providers should cooperate.
2. Cloud providers must use and adopt the existing standards.
3. New standards need to promote innovations.
4. Community support should be guided by the customers' requirements.
5. Organizations responsible for Cloud computing standards should work together.
6. The Cloud providers must not use their popularity to attract customers to their platform.

Another group called the Cloud Computing Use Case also works to bring together the cloud providers and cloud customers. The purpose of this group is to define common cases scenarios of the cloud customers. The groups which try to formalize cloud computing are not adopted by everyone and companies such as Amazon does not want to adopt such standards while Amazon itself takes into account the service users considering the fact that the shift to another cloud is not simple [10].

2.3 Cloud Service Models

The Cloud computing offers three main service models which respond to various user requirements. Three services can be seen in the form of a pyramid mode Fig. 3, with the infrastructure as a Service (IaaS) and with the entire infrastructure at the end managed by the user. In the middle there is the Platform as a Service (PaaS) which provides the infrastructure and client platform, and users do not need to worry about infrastructure, but they can easily manage the platform. And finally at the top is Software as a Service, which offers users software as a platform and infrastructure to manage the server.

Infrastructure as a Service (IaaS) allows the users to take advantage of the cloud resources such as memorization space, processing memory and other resources as a basic calculator operating system and application. The user cannot control the cloud infrastructure layers. However he will be able to maintain control of resources such as

operating system, memory, drives, processing, applications, and a certain number of network components, such as the host firewall, *Figure 3.*

Platform as a Service (PaaS) provides the ability to perform client applications in the cloud infrastructure. The platform can have a different development character. The customer can control applications in the cloud cast and sometimes even in environment configured applications hosting machines. However the client has no control over the infrastructure in which the applications layer.

The PaaS services include application design, testing, and hosting. Other services include group collaboration, integration of databases, security and management of the condition.

The PaaS is found in three different types of systems:

• Add-on development facilities - This includes the SaaS applications which must be regulated

• Stand-alone environments - The environment licenses do not include technical or financial dependence.

• Application delivery-only environments - These environment services support higher levels, for example as security or scalability on-demand. These do not include developing debugger or skills**.**

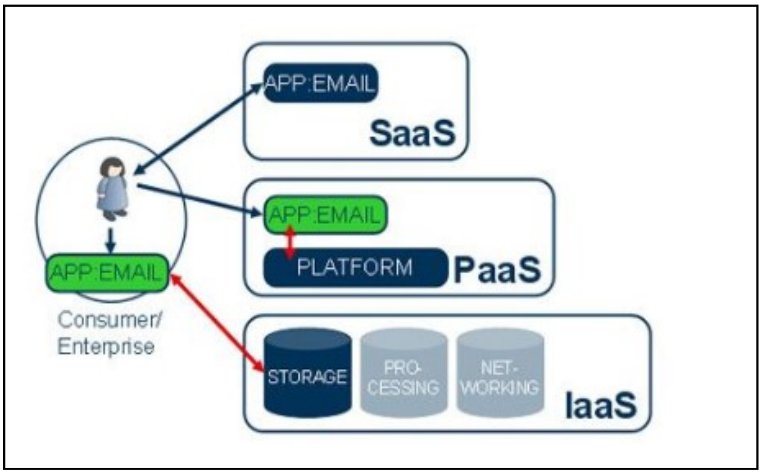


*Figure **3**. Cloud computing architecture with an e-mail aplication example. [11]*

Software as a Service (SaaS) provides customer applications that run in the cloud. Consequently, customers of the cloud-hosted applications need not worry about the

infrastructure or platform. When software is unloaded, the customer cannot maintain it or its supports. On the other hand, it is not in the hand of the customer to decide on the service. Enabled SaaS applications can have access from many devices through a web browser. An example of SaaS can be a web mail client, Figure 3. SaaS is used in many cases to provide a functioning system to a client which is not very expensive and which allows the client to benefit in these commercial licenses, in the system operation without the complexity of installation and management with an initial cost. The SaaS architecture is implemented to trust a large number of customers at the same time and is achieved with the development of multi tenancy. The SaaS exploits the browser used in the Internet but information security officers must consider several different methods of providing the SaaS applications. Web Services Security (WSS), Extended Markup Language (XML) Encryption, Secure Socket Layer (SSL) and other possibilities that are implemented in the institution's data protection during their transmission to the Internet [12]. Consequently, customers of the cloud-hosted applications should not be concerned about the infrastructure or the platform. Enabled applications in the form of the SaaS can be accessed by many devices through a web browser. As mentioned above, cloud computing offers services at various levels, like infrastructure as a service platform (IaaS) or as a service (PaaS) and Software as a service. Infrastructure is the most important part of cloud and there cannot be other layers of the cloud. Performances of all services depend on the performance of the cloud infrastructure. Performances of the cloud computing depends on various parameters such as the CPU speed, amount of memory, network speed and hard disk. The issue of security of Cloud technologies is always an issue that the IT professionals consider and investigative. In most cases public Cloud applications are not as secure as Private Cloud applications. However, we have evaluated the benefits from organizing a Public Cloud. To arrange a Public Cloud concerns should be in three areas, [13]:

Location of records - Many companies faced with the legal side of the country in which they operate their business where certain types of the data are stored in certain

geographical boundaries. There are specific rules that must be followed and the approach should focus on data management and control.

Privacy of data – The Enterprise is responsible for any breach of the data and must be able to guarantee strict data security in the cloud, protecting even the most sensitive information.

Regulation compliance and industry - organizations that provide Cloud services are responsible for the data and the extent of their limitations. Many industries require special regulations and companies must adhere to applicable laws, such as the GLBS, ITAR and PCI DSS, to protect private data such as businesses and so on. One of the solutions of defense and security is an encryption in the gateway Cloud. This serves like the entrance gate "proxy" for applications using sensitive data with those encoded (encrypted) for transmission and storage in the Cloud. This enables organization that provide services to the Cloud to feel comfortable. Information remains under control of the organization at all times. Despite many concerns, organizations of all sizes are ready to protect their data from external attacks and increasingly formalized control processes of potential risk assessment.

2.4 Cloud Deployment Models

The cloud computing is a service request, easily able to allocate network resources and different models exist in more functional ways like [14]:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

The Cloud of various developments can be performed depending on the type of service you want to offer. Depending on the requirements there are four types of development:

Public Cloud: This infrastructure is built for the general public. Resources can be accessed by companies as well as private clients. This means that resources are available to anyone

who is interested in them. To access the resources offered by a public cloud, the client must register with a cloud-distributor of such as Amazon Web Services (AWS).

Private Cloud: The Private Cloud differs from the public because the company cloud is built behind a firewall, and the cloud infrastructure is not manageable by a third party. This solution is applied by companies that want to manage their cloud-in and maintain control of their data. Usually it is more secure than a public cloud because it is usually hosted by the company and the company behind the firewall.

Community Cloud: With this configuration, the Cloud is divided between different organizations, used to support the communities that address the same problems. The Community Cloud infrastructure can be managed by an organization or third a party.

Hybrid Cloud: The Hybrid Cloud infrastructure is made of two or more clouds (public cloud, private and/or community). Each of them consists of unique entities together. This solution allows portability of data and applications. The Hybrid Cloud is based on designing the environment in a way that meets certain requirements to be special for Business and Technology. If some systems have limited privacy of data and level of security requires more than the Hybrid Cloud is recommended. The Hybrid Cloud is used in cases when different organizations have placed their data in the private cloud, but manipulating the data is undertaken in the public cloud.

The following table shows the cloud models in columns, the way of controlling and managing the first part, infrastructure control- second part and the user (third part).

*Table **2**. The way of control and management of models in the cloud computing*

	Public Cloud	**Private Cloud**	**Community Cloud**	**Hybrid**	
Controlled	Provider	Organization	Group of organizations	Provider	Organization
Infrastructure	Provider	Organization	Group of organizations	Provider	Organization
Used	By all	Organization	Group of organizations	By all	Organization

2.5 Cloud Archiceture Description

The main advantage in the architecture of the cloud computing is that it provides flexibility for applications that enable resource sharing with other members participating in that model. This opportunity directly sends flexible architecture as resources increase and will not have complications in configuration [15].

The main difficulty for processing the data at different levels in the work of the earlier representation and it was difficult to get more machines if we needed them during the application, difficulties to make that machine in case someone else needs them, there are difficulties of distribution and cooperation at various levels to machines and managed processes on them and there are difficulties in management dynamic workload and difficulty leaving these machines for management [16].

Cloud computing architecture consists of the following layers [17]:

- *Fabric Layer* – This layer includes part of the hardware resources in which there are parts of the computing, storage and network resources.
- *Unified resource Layer* – At this layer it is obvious that it includes abstract resources which come as part of the implementation of virtualization. With the sole purpose these resources are available to layers with high levels. All these sources and then the final users appear as embedded resources, in this case they can emulate one or more group systems based on signs.
- *Platform Layer* – This layer is intended to add a set of specialized equipment and middleware for services performed by using special resources to enable the development of a platform. In this case, we can take an example of the Web hosting environment, as a separate service.
- *Application Layer*- This layer includes the APOP application system that will appear in the cloud and then the system will be used as service by the customers.

Cloud applications change because the calculations of the cloud in the software applications are based on the cloud infrastructure. The Applications Cloud versions are

not Software as Service (SaaS) and include some things like web applications that are sent to the user between the browsers applications like Microsoft Online Services. These applications dispose the hosting and the IT management in the cloud. The Cloud applications often provide elimination and the need to install and operate applications at the customers' computers. Some applications include cloud like:

- Peer-to-peer connection (like Torrent and Skype)
- Web applications (like My Space or YouTube)
- SaaS (like Google Apps)
- Software plus services (like Microsoft Online Services)

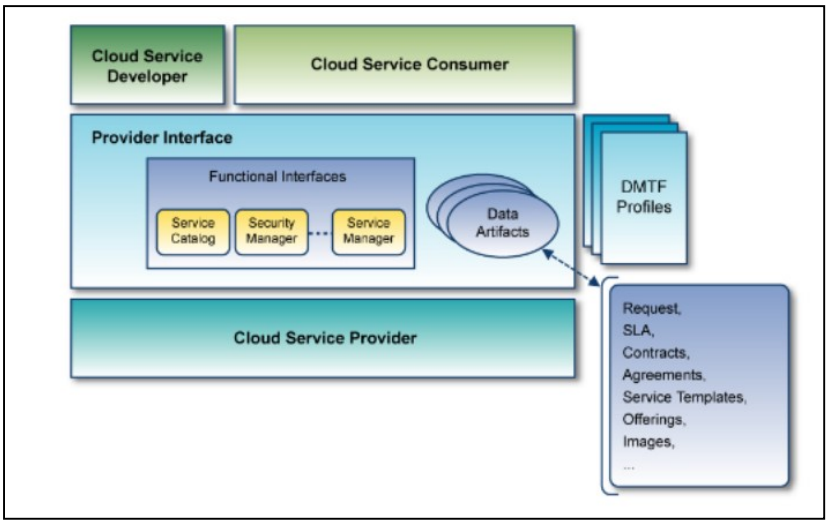


*Figure **4**. Cloud Service Reference Architecture [18]*

In fig. 4, shown below is the reference architecture for the cloud computing environment in which the main elements are presented as actors, interfaces, data objects and their profiles connections between those objects. All these elements of the cloud users must be available. According to this fig. 4 Cloud Services Customers include:

- Approve the financial costs for customer services
- Responsibility for exploiting services
- Other cases require changes in service and in cases that services change
- It also provides access to services for service users

Each user of cloud computing is able to use monitoring services to customers realizing trailers and they have access to billing implemented for the clients. This site enables collaboration services that developers interact with users of services to a trailer in order to create favorable services to the customers. [18]

Just as mentioned above, the cloud computing offers services in three levels as a Service Infrastructure- Platform as a Service and Software as a Service, but the flaw is that standards in these levels are not clearly defined. There is a need for cooperation with the cloud computing and it should also be noted that different incentives for companies for investing in resources are necessary for businesses to implement new technologies. Some parts of Cloud Computing do not have related systems and as services become more complicated they require more resources. They are not able to grow their usage if they do not have a standard which enables the site to have easy access to their data in the cloud computing market [17].

For many businesses the IT strategy of cloud computing is becoming a key strategy and architecture of *cloud* computing is much more in demand. Most businesses have approved or intend to adapt this technology in the future. Cloud computing solutions favor business purposes; access to the Cloud will include a hybrid approach and then access the resources to other types of the cloud. Consumption of cloud computing by large number of businesses is necessary to implement high levels of success in the cloud. The advantage of the main cloud architecture, compared with a traditional architecture layer, is the speed of service delivery, flexibility and automation whereby requirements are implemented by the clients. To have a convenient cloud infrastructure requires deep planning and execution in order for the resources required not to be under or over the need for the proper requirement for that system. It should also be noted that the shift of cloud computing for companies does not cost anything if changing the architecture of the systems is in favor of using cloud technology.

2.6 Security in cloud infrastructure and security risks

2.6.1 Analysis of threats in cloud environments

A part of the threat of security in the cloud is anticipated, the other part is not anticipated by the end user. According to [*19*] these threats are divided into two main groups

- Internal attacks and
- External attacks

Characteristics of internal threats are the attacker is employed by the third party and the provider knows well the infrastructure and the level of security, possibility of authorized access to the consumer's data and their misuse and the use of authorized access to support different attacks from outside.

Characteristics of attacks coming from outside are either he/she is not employed by the outside support service operations, or he/she has authorized access to the services offered by the consumer's data and infrastructure.

Another aspect [20] for the security management is the threat analysis in each phase of the utilization of services in the cloud. This list of threats is presented in Table 3. and is given by the CSA [21][22].

*Table **3**. Overview of cloud related threats as defined by the Cloud Security Alliance [21, 22]*

CSA defined threats	Description
Threat 1: Abuse and nefarious use of cloud computing	Malicious code authors, spammers and other criminals can abuse the relative anonymity behind some of current cloud services.
Threat 2: Insecure interfaces and APIs	A set of software interfaces are utilized by the CSPs for CSC interaction of the services. The security and availability of cloud services depends upon the security of the basic interfaces, such as Application Programming Interfaces (APIs).

Threat 3: Malicious insiders	The threat of a malicious insider is amplified for cloud services due to the convergence of Information Technology (IT) services and customers under a single management domain.
Threat 4: Shared technology issues	The CSPs deliver services in a scalable way. Some underlying component parts of the cloud infrastructure were not originally designed for that environment, and can potentially cause security problems. The main concern is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud
Threat 5:Data loss or leakage	The threat of data compromise increases in the cloud, due to the number of interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.
Threat 6: Account or service hijacking	Phishing, fraud and exploitation of software vulnerabilities can be used for account or even service hijacking.

To understand the essentials of security in cloud computing better, we will explain possible threats and services offered by the cloud. We have shown the transparency for security between CSC and CSP, every possible threat has been analyzed in order to identify precisely factors and negligence coming from CSC. After these factors are identified, then we can work out how to minimize or avoid these concerns.

Threat 1 (Abuse and misuse of CC*),* there are always intentions of misuse or abuse from different groups. One of the most notorious group is "Botnets" that interferes in cloud computing, using every possible chance to use it for their own interest. After interference by such groups there is no chance to identify the authors of such actions. [25] There is the case of "Amazon Zeus botnet" which contains EC2's infrastructure [26], where the cyber hackers of such groups controlled a service placed in Amazon and were able to control and infect the client machines and steal the bank data. This type of threat is dangerous for

the members inside and outside, knowing that the CSP infrastructure is open and enables the use for every CSC.

Threat 2 (Insecure interfaces and APIs): API-s represents the structure and entire map of a service in the cloud. The advantage of publication of the API by the CSP for CSC is because the first expresses its characteristics of the cloud that makes them public by the CSC and second it enables clients to redesign their system of architecture in order to have a mutual profit. Its disadvantage is that the information offered by the CSP can be used by the groups that have no good intentions. The necessity of the CSP to limit the exposure of information related to the infrastructure is important.

Threat 3-5 related to the security of the data in the cloud (confidentiality, integrity and availability-CIA). These threats occur because of the problems that come from the internal actions such as the tenants who use the same sources and have bad intentions. These threats may occur in cases where processing of data is delayed by the CSP offered by the CSC. These are the reasons why the companies do not yet use the cloud. We have advantages at this stage because the IT industry as well as the academic body has offered new encryption strategies to provide confidentiality of the data and security of integrity.

Threat 6 (hacking the account and service), security of services in the cloud cannot easily be provided and this disadvantage can be used by other groups. An example of failing to secure the services can happen even to the big corporations, like Amazon Zeus. To overcome such threats there is the possibility of teaching how to secure the cloud and VM monitoring, which is the only possibility for such threats.

Threat 7 (Unknown profile of security), shows difficulties to determine the level of security in the cloud, especially when we know the level of security is depended on the CSC and the CSP which are participants of this environment. To increase the level of security in the cloud for the CSC and trust the services offered in the cloud, the Service Level Agreement (SLA) is proposed, and monitoring from time to time to audit the security. *Table 4.* shows

information related to a possible solution that exists about the above threats related to the models of the cloud.

*Table **4**.Cloud security threats and some related solutions based on our survey and the CSA documents [21, 22]*

Threats affecting the wider adoption of the cloud	**Some related security solutions**
Threat 1	Customer CSC's network traffic introspection the VM monitoring,
Threat 2	Security Analysis of the API Encryption, Access Control encapsulation, abstraction
Threat 3	The supply chain audit including human resource hiring procedure, Security certification, Audits, Use of Trusted Cloud Computing Platform (TCCP)
Threat 4	The VM monitoring and cloud audit, Access control, the SLA enforcement for patching and vulnerability remediation
Threat 5	The API, Access control, Encryption and key management, the Use of Trusted Cloud Computing Platform (TCCP)
Threat 6	The VM monitoring, Use of Trusted Cloud Computing Platform (TCCP), Access control and authentication
Threat 7	Security certification, Audits, the SLA monitoring

Below there are discussed possible initiatives to provide the CSC transparency and security policies for CSC, [23]. As a part of these initiatives we mention virtual machine monitoring; Use of encryption; Certification, audits and monitoring of the Service Level Agreement (SLA). Based on the threats mentioned in *table 4* above, number 7 it is seen as a kind of threat that cannot offer solutions but only provide technical answers. In this part we have to trust the two parties present in the cloud environment, such as the CSC and the CSP. Cloud security is dependent on the confidence of all participants in this environment. The

complexity of trust can be greater when the service is provided to the CSC and comes as a result of using different CSP resources. So far the CSP security certification approach has been used as a way of satisfying the CSC fears for the flow of the services which they use. This is probably the safest way to use cloud services from CSC. These certifications are realized by the third party as key tools for cloud transparency and play an important role in the lifespan of cloud services, [24].

As an example of these certifications we can obtain ISO / IEC 27001, which has an accurate framework for data security management. These certifications include standards to be achieved by the company in order to be certified. The advantage here is that the client is now familiar with the level of work for that particular company. In addition, the purpose of these standards is to provide companies with a lesser need to address the various security risks that may arise, and also monitor the development and performance of Information Security Management Systems (ISMS) for their businesses. According to the researchers [24], it is proposed that the certification schemes of these standards be at affordable prices even for smaller companies to enable them to rival larger companies. According to the researchers, the CSPs have to be certified by governmental or standardized institutions, which ensure that the provider has an internal security check and that they act in the right manner.

The Cloud Security Alliance has provided clear guidelines for cloud risk management [25]. This specifics that characteristics of the CSP are: Compliance, Governance, Facility, Human Resources, Information Security, Legal Matters, Operations, Risk and Release Management, Resiliency and The security Architecture. Standards specify each field with its own details, then each field is mapped to a particular standard, example the IT Governance (COBIT), cross domain, standard for the management of information security systems (ISO / IEC 27001) etc. According to some researches [21, *25*, 26], the CSA describes the certification process as divided into the security guidance and control objectives. At a primary level it must be a self-evaluation mode, each CSP is obliged to

document the CSA report for the description of the resources. The second level is known as the beginning of certification by the CSA, which is to be a third party controlled by the CSA and its duty is to make an independent evaluation of the participant. The third level is a continuation of the second level. The monitoring and evaluation process continues all the time.

The certification and standards market for cloud services is very specific. The purpose of the standards is that the client, before using the services proved by the CSP, is informed of the security specifications for that service. The large number of standards creates and confuses the company. After that research carried out by the University of Cologne in Germany has proposed a classification of certification, based on the services offered in the cloud. Certification schemes are proposed, depending on the purpose they provide. [27] The use of certificates is seen as a way to adopt security of cloud services and to monitor security for those services acquired by the client. Auditing the third party is accomplished with the sole aim of evaluating of the level of security in different stages. By 2011 the SAS70 standard was used for auditing the company by customers for the use of their services. [49] As a proper proposal for standards it was a necessary and effective assessment of security for the CSP. During this time, the replacement of regional standards with those of the international standards, eg SSAE16 standard (www.ssae16.com), was replaced by the ISAE3402 (http://isae3402.com/), with the sole aim of harmonizing the standards especially those of the USA from where the substitute standard came. The main change for these standards was that the international evaluation company should produce a report on the accuracy of the system and the time taken to realize that valuation. Each standard supports the purpose of the CSP standard audit and then information extracted from audits is used by the clients for its judgment. A very specific requirement is being implemented for Cloud Audit by the CSA (http://cloudaudit.org/CloudAudit/Home.html), which requires it to provide a common API for the CSP, with the specific aim of evaluating internal security resources provided by the CSP. These data are available for each CSC and then, based on the information

received, captures the most appropriate CSP for the assurance of its requirements. It is known that the CSP has greater control over the cloud security but this type of audit is advantageous for the CSC despite the certifications it possesses. Given the recent developments in infrastructure, the realizations of audits at different times and without control of the CSP are necessary and required by the customers.

2.6.2 Security and privacy concerns in cloud services

Since the cloud environment is the result of a combination of early techniques such as virtualization, grid computing, and service-oriented computing, cloud security for the cloud has no major differences from the early techniques, [20].

According to this [28], it is said that there are some unknown security issues in the cloud environments such as downtime, data loss and password weaknesses. And they have taken notice of many proposed cloud security models in their modification. Considering the cloud security, the authors were focused on two main elements that were not in the traditional technology: the complexity of multiparty beliefs and the need for later interception. Both elements have affected security deterioration in the cloud environments.

Since the cloud environments, data and data processing are located in the CSP space. This is one reason for the cloud security to be dependent on the cloud environment provider, and that is why it empowers it: "the cloud computing is about gracefully losing control while maintaining accountability" [29, 30]. The data, depending on the physical location, comply with the country's rules of law. Considering the CSC, where and how the data processing is done is not known, but security and privacy management is challenging for the CSC. For some sensitive data legislation requires to determine their location, and these data should be protected by the legislation rules. The CSC data may be displayed differently depending on their importance. In addition to the CSC data it is important that in any transaction or additional information about the data has the same importance.

Generally, it can be said that the CSC and the CSP security is directly dependent on the security of the model service exploited by them. For example, in the SaaS model, the

security services and the definition of the private sector are defined by a formal agreement between the two parties. In the case of the PaaS and IaaS model, there are separate responsibilities in both parts; the part for the system management mode is the bar of the client system administrator, while the part for providing the main form and infrastructures is the CSP.

After changing from the traditional way to the cloud environment, there is a growing need to provide a higher level of security, and it is also necessary to define various mechanisms that increase security in this environment. If we pass our services to private cloud environments, this makes it much easier for the security, especially if the entire transaction path is controlled by that company; this is because there are no major differences in the security service about these cases. Considering the public and private cloud is the other case where we have concerns about the security, in these environments we have data exposure from the CSCs in different groups which use the same cloud resources. In these spaces we must take into account the confidentiality of the data and the data coming from their processing, [31]. These elements of cloud security linked to the multi-tenancy aspect of the cloud services, reliability and availability, have also been discussed. Multi-tenancy involves the sharing of the same resources where different CSCs are located in the same machine, which have the same or opposite intentions and can utilize the possibility of sequence resources. Considering the use of cloud upgrades we have the Internet connection (the main bridge for the use of the cloud environments), these services can also be accessed by Amazon and Rackspace (CSP) [32].

2.7 Security of Iaas

The task of the provider for the IaaS processing, network and other basic resources is related to the network. The advantage of the IaaS is that the resources that are offered are based on the order received or this service is offered as a self-service.

The model of distribution in the IaaS consists of elements developed at the same time but the combination of these elements to an open cloud is presented with challenges. Security

is the main component that represents it in the cloud computing. If the level of security is not at the expected level at one of the elements presented in the IaaS, the space is used in the whole system, [110].

Providers who offer the IaaS are indifferent in terms of the application or users requirements. Managing user application is seen as a black box by the provider. Client's application of the time is the way it is controlled by the client, whereas execution is realized on the servers offered by the provider for the application security distributed in the cloud computing. Before an application is placed in the cloud, it should be designed in a way that it will not allow any threats coming from the internet. Therefore, we should use standards for security while these applications are designed. Clients are responsible if they do not provide a proper strategy to protect their applications from the potential attack by hackers or malwares, hence not to allow unauthorized access to the data. As for the authentication and authorization ready parts are not a good idea because there is a chance we are not aware of the weaknesses they may have.

Regardless if the cloud is public or private, infrastructure should be secured and the basic services offered in the SaS, IaaS and PaaS should be secured. The infrastructure security is treated in many aspects such: it is evaluated based on the structure level, network level, application host etc.

The advantage layer with the private cloud in respect of possible attacks and vulnerability of security and therefore, authorized people are prepared. But if different requirements for the public cloud are determined then for the security of the network, changes will be needed in the implementation strategy.
Here are some factors of risk that may appear:

- Security of confidentiality and integrity of data in every step of the data processing.
- From every resource that requires access to data, access should be provided for authorized persons only
- Availability of resources is determined for use from particular institutions.

- Security for replacing of the infrastructure model from the before to the new version.

The IaaS-Host Level: when we consider the level of the security of the host we should consider services in the cloud (IaaS, PaaS and SaaS) which are compatible with the private, public, or hybrid systems. The responsibility for host security for PaaS and SaaS rests with the provider of the cloud, whereas for Iaas host security (security of virtualized soft wear security of virtual server etc.) is mainly with clients.

The *IaaS-Application Level:* is the more basic element in soft wear security offered for security in the Cloud. Earlier security programs have been modified for the cloud to reflect requests and standards required of this platform.

The security of applications differs from the application that has small number of users to those with a larger number, all the time needing to be highly secure. Security of infrastructure in the cloud –IaaS, layer in the domain of determining specific security from each participating party in cloud computing [111].

2.8 Security of Paas

There are two main important factors related to security in the PaaS: outsourcing and multi-tenancy. Services for the outsourcing model describe the matter and unknown applications are executed in the infrastructure. Both parties require mutual guarantees to avoid any abuse that may occur. The other factor, multi tenancy, seeks to provide proper isolation of applications that use the same resources. Another important requirement for the PaaS is that the provider should offer a possibility to manage and control accesses and create an interface by standard requirements for communication to the end user. Providers use systems that give the user access to very specific elements about his requests and the entire infrastructure is managed by the provider.

A program deployed in the cloud accepts parameters of configuration from these sources:

The SLA is very important, the client expresses his requirements then the provider, based on these requirements, limits the access if he thinks that they may damage the infrastructure. During this procedure they can make a bilateral agreement. Determining

configuration of certain programs, in some cases it may be necessary to access other services from the program. This type of configuration is done by the user. The paper [112] offers a design for a proposal to secure the PaaS. The first part introduces the supplementary components offered by the provider, and then describes the scenario to be used. However, the other part describes the contents for developing the process. In this proposal [112.], advantages can be seen to be encryption of all fields, but if the client wants to decrypt data this date remains decrypted in the cloud for a short period of time. This space may be misused by others. This problem appears in cases in which the provider of the cloud is not trusted. Although the client is warned about this he still trusts the provider on the terms and conditions he is offered. The only power for the client is to use the scripting structures for data in the cloud. It is proposed that SaaS security is increased by replacing the processes for internet services depending on the power of the computer. This has the advantage that clients have flexibility and complete control of the programs.

2.9 Security of SaaS

Security software as a service is completely depended on the provider of the cloud, who must carry out the work in the best possible way. The client requires the old system to be substituted in the SaaS offered in the cloud, and all attention is on the method of preserving and enhancing the data security and has a safe fast migration of the data.

Just as above, when a third party in cloud computing enables customer data to be settled in various countries with the sole purpose of maintenance and accessibility at all times. Clients should be informed of the manner of data storage in the SaaS. In the figure below is shown a cloud provider and critical aspects which involve all levels with the sole purpose to assure the security of data at all times.

Below are presented some key elements as part of the SaaS security which should be an integral part of the SaaS at all times:

1. Data security,
2. Network security,

3. Data locality,

4. Data integrity,

5. Sharing data,

6. Data access,

7. Authentication and authorization, etc..

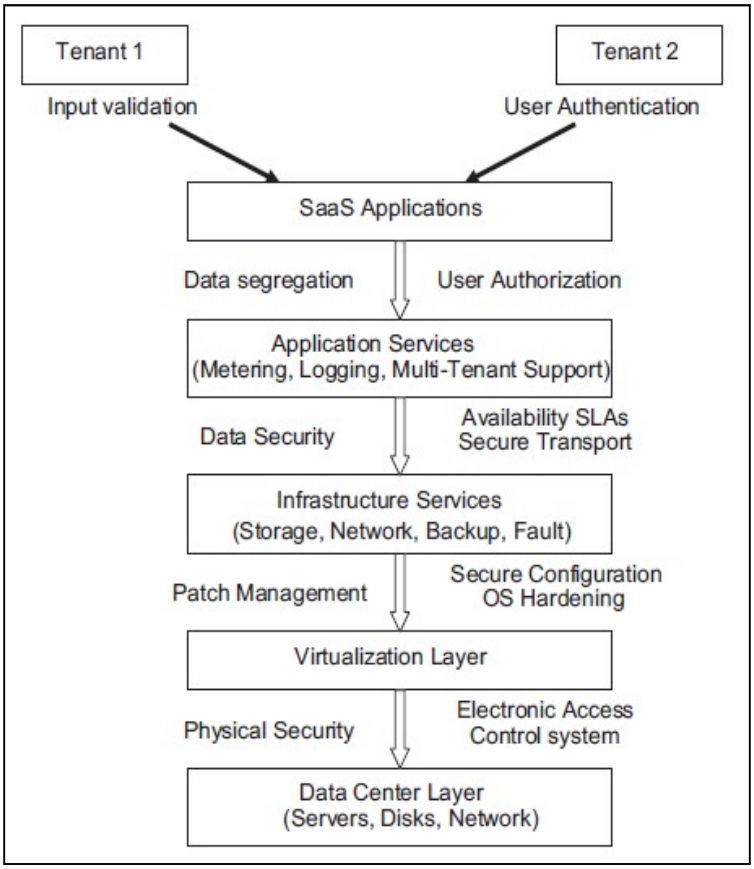


*Figure **5**. Security for the SaaS stack [34]*

In the following, we discuss each element mentioned above:

Data security-In traditional systems of sensitive information within the controls foreseen since the beginning of using systems (here was part of the physical setting, logical and company policies for controlling access to the system). In the SaaS, data will be stored outside the location of the company. This data is under control of the cloud provider. Therefore additional controls are required and data security has the possibility of

unauthorized access to the system. Developers of the cloud and environment system must use encryption techniques to make the level of data security higher. Before implementing the system as a service to customers, it is necessary to test every transaction which is possible in that system in order to move forward with confidence.

Network security -In the SaaS data realized processing is used by the customers for their purposes. All participating networks for all transactions in the cloud environments must be safe in order to remove the possibility of tapping the networks by unauthorized parties. To achieve this, networks are recommended to use Secure Socket Layer (SSL) as well as the Transport Layer Security (TLS) encryption for traffic safety.

Data locality-In the SaaS model, customers use applications in the SaaS, which realizes the processing of their data. Even though the customer is notified that the service used and the data stored in this service is not familiar with the location of the trailer data, they still proceed with it. This represents a theme discussion for some countries, management of personal data is inconsistent with the law, if not found within that country.

As an example is the situation in South America. The law in this country provides that some sensitive data cannot be left to the country because of its content. The SaaS must ensure that customer data is not controlled by unauthorized parties from customers and that data will be accessible only to that client.

Data integrity - This parameter is very important in any application, in the traditional and in the SaaS. Integrity is achieved in many traditional systems with a database and restrictions are maintained for users to have access using the ACID for each limitation. Integrity of the data in the SaaS is under the control of the cloud provider that is why we have to provide the auditing. However, we need to ensure that data integrity is applied throughout the SaaS system.

Sharing data – Multi tenancy plays an important role in cloud computing. As a result of multi-tenancy the clients preserve their information in order to place more SaaS data in the same location. Intervention of a client in another client's data is possible if there is any concession during implementation. Thus there can be release of unauthorized data. For

this reason numerous checks need to be applied in the SaaS in the reception of the data. Restrictions should be applied to the application level. There will be minor concessions used for obtaining data and for this we must be careful with Multi-tenancy. *Data access* - Policy data security is directly related to the access of the data in the system. A company can use different providers for the services used in its businesses. Each employee has a special role; by this we mean that we can have access to the special data groups. Such approaches are defined by the company which must abide by rules on the access of data. The SaaS should be developed in a way that very simple approaches for the division achieved shall have a certain role.

Authentication and authorization - Companies considering access use the secure protocols. The SaaS uses Active Directory (AD) for the management of clients. The data of user authentication is stored in the SaaS using protection methods implemented by systems developers. The SaaS must create new users and remove those requested by the company. Developers must provide the authorization process in order that these parts can be implemented safely and controlled by the company.

Defining demands of safety in the cloud environment is related closely to the user and the level of service being offered. Considering SaaS, PaaS and IaaS, there are special demands in order to offer high security in the cloud environment. Some of the general features defined earlier are part of demand of each level of cloud architecture. Table 5 shows the needs of security for service levels and cloud users.

*Table **5**. Security requirements for different level [33]*

Service level	Users	Security requirements	Threats
Software as a Service (SaaS)	End client applies to a person or organization who subscribes to a service offered by a	Privacy in multitenant Environment Data protection from exposure (remnants) Access control	Interception Modification of data at rest and in transit Data interruption (deletion)

	cloud provider and he /she may have use it	Communication protection Software security Service availability	Privacy breach Impersonation
Platform as a Service (PaaS) **Infrastructure as a Service (IaaS)**	Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure	Access control Application security Data security, (data in transit, data at rest) the Cloud management control	Programming flaws Software modification Software interruption (deletion) Impersonation Session hijacking

2.10 Data security in cloud computing

During cloud computing application adjust system as well as database in provider's responsibility, management and services from our side are not safe. In this environment the security challenge it is important which the access belongs, virtualization, and work control of the third party. Then it includes integration, loss of the data manipulation then identification of various devices which this case totally are spent by the third party. The main goal of the cloud computing is to provide the right utilization of resources and utilizing virtualization not to have charges from the client, but still there are dangers in this new environment presented in Fig 6.:

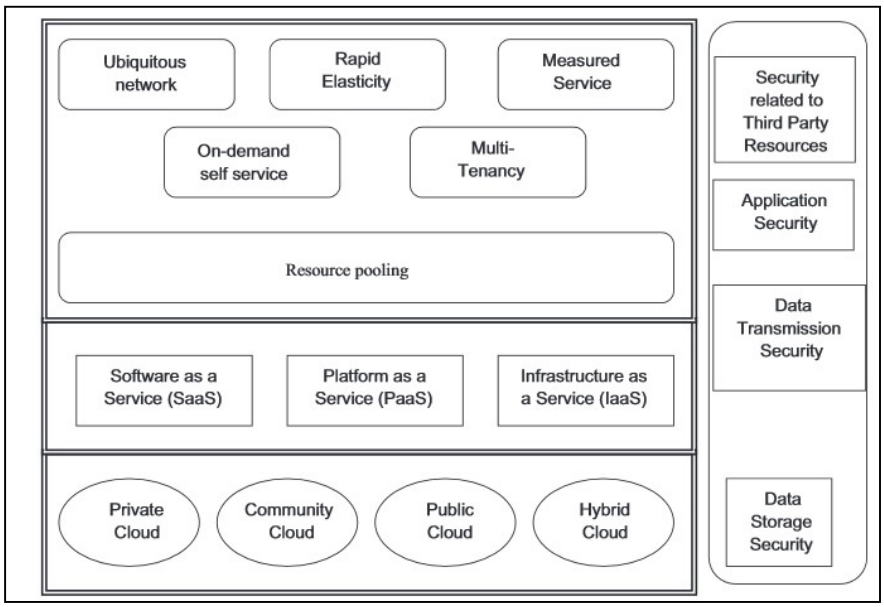


*Figure **6.** Complexity of security in cloud environment [34]*

From this fig. 6 it can be seen that the initial part of the model represents various cloud computing (private, community, public and hybrid cloud). However, different cloud models are located services used in the cloud models such the SaaS, PaaS and the IaaS. These services are essential in cloud computing and offer various services in response to requests, for self service, multi-tenancy. All these elements require security which differs from the cloud computing model already used.

Key risks include the cloud computing data security during storage, transfer of secure data, security in connection with third-party sources etc. [34]. Considering the customers cloud computing models there are three types of services, as discussed above, which enable infrastructure, platform and software as services to the end users. These models are placed in cloud computing at different levels of security. For instance the IaaS is the initial layer for cloud computing services, then PaaS. Safety must exist in each of the layers of the cloud. The third party must notify customers if any security is offered only to certain level. The client must then undertake any appropriate measures to provide security in each level, or at least take responsibility [34].

Although cloud computing [35] offers many benefits for businesses and customers, there is a reluctance to enter this environment of data security. Data security has the following factors: privacy, trust and legacy of the data [36][37]. Data security has been a source of concern in earlier technologies, but the cloud environment has increased this concern. The main problem is that the data is not close to us, it is placed in different machines and is under the control of Cloud Provider. Security in the cloud environments is more difficult to manage than in traditional environments. The growth of cloud users is directly dependent on increased users' confidence in the cloud environment.

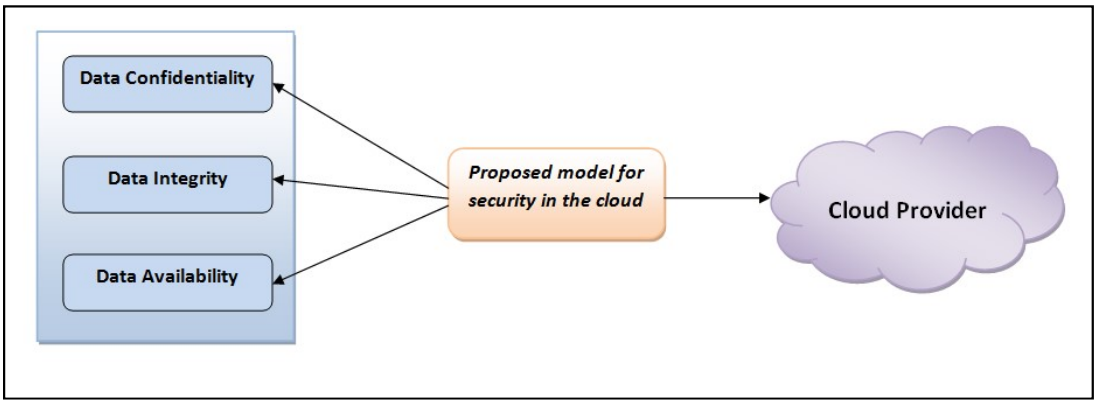


*Figure **7**. Data security for proposel model for cloud security*

According to the type of model offered in the cloud environment [19], there are several ways in which cloud computing is unprotected. We have presented a preview of the latest user tracings such matters as confidentiality, integrity and availability (CIA) and their role in any cloud computing service [35].

2.10.1 Data confidentiality

For the storage of private data for the cloud users we use data confidentiality and part of this is the authentication strategy access control for users. Reliability in the cloud environment is directly related to data confidentiality, authentication, and access control, [38]. However, in cloud computing there is distrust between the sender and the last user because the provider cannot convince us that there will be no possible wadding of our data. The last user should know that it is very dangerous for sensitive data stored in the cloud. The cloud encryption management in the cloud environment has encountered

various problems and there is no way to process different and complex questions of parallel modification etc. Encryption is the startup that is used primarily to ensure data confidentiality. Below we provide some explanation of some of the techniques for using the data confidentiality.

*Homomorphism Encryption, t*his technique was proposed by [39]. The pervasiveness of this technique, which states that the whole process of the data processing is realized in encrypted data, means that we do not have to encrypt the data. The implementation of this technique solves many problems of data confidentiality and operations carried out in the cloud environment. The initial proposal for the use of Homomorphism full encryption came from the authors [40]. It is a very good discovery and provides reliable data processing. The vagueness of this technique means that data processing is complex and the cost of calculation and storage is too high. From this point of view, we can say that the full application of Homomorphic Encryption, in each of the communication clouds in the cloud environments, is far from being a practical use of this technique. Authors [41] proposed to use already known encryption algorithm Diffie Hellman (used in the proposal model), is used for communication in safety and differs in the management of the distribution mechanism. The authors [42], proposed increased security and flexibility, using hybrid algorithms, a combination of the RSA algorithms, 3DES, and random number generation, (which we use in the proposal model). The RSA is used to ensure secure communication by using digital signatures. While the 3DES algorithm is known for encryption of data in the blocks, we proposed other algorithms which can be used in the cloud environment [43].

Encrypted Search and Database- Because of the use of the Homomorphic Encryption algorithm is ineffective according to researchers, we have to consider the limitations that exist in this encryption technique during practical application. Encrypted search is processed as a common cloud process.

Authors [44] have proposed a search mechanism in the database that is known as the transposition, substitution, folding, and shifting (TSFS) algorithm, but even during this

mechanism, with the increased number of cells, processing increases simultaneously. The database encryption technique in the database is proposed for the security of the sensitive data sent to the cloud [45]. Every time there is synchronization between the client and the provider for accessing the data. The first step that is accomplished is the search of the sync by synchronizing the data to be retrieved by the provider. Synchronization is used to store data that is interconnected which keeps the keys used. The issue of this technique is that it causes delays because there is an additional communication with the central synchronization that needs to exist. This part can be reduced if group encryption is used and then communication decreases from sync to sync.

There are also proposed asymmetric algorithms for the cloud database [46], in this encryption the data proposal is realized more than once. However, the public/private encryption/decryption order does not matter much. The encryption mechanism is part of this proposal which shows that this data is being encrypted to increase the security issue in the cloud. These schemes are very favorable in those cases where there is the lack of trust from the cloud computing stakeholders. Private storage proposed [47] a multi-word search model for the cloud-encrypted data which renders data based on results without using the user's privacy.

Distributive Storage – The data storage in distributed locations is part of the cloud environment. According to the researchers [48], they describe security in the cloud-based interconnected data environments, including data integrity, access to data, and the availability of cloud services. In order to preserve the integrity of the data, a solution has been found, if the data is stored in different clouds. To save data from unauthorized persons, a solution is offered by dividing the data into some parts rather than using Shamir's secret algorithm to generate polynomial functions for each single part. By dividing the data in many parts, the cloud security is enhancement as proposed by the researchers [49]. This technology has achieved a security service for securing cloud data. This service is provided by a third party. It seems to be completed and asks the client whether he/she wants his/her parts to be separated or not. The numbers of separate

parts are based on the available bandwidth. Separated segments are encrypted and distributed on various databases which use the concept of the cloud data distribution.

The separating menu is stored in a log file, stored in the master database. To access this database we must have many privileges, and it will be almost impossible for unauthorized persons to gain access. This file serves as an index for the reunion of separate parts.

Because the data is divided into many parts and distributed on different bases it has increased the risk of various attacks which may occur.

The authors [50] are focused on the cloud data distribution; these deliveries are based on the measurements being made. Measurement Techniques are based on network design and traffic paths for entry and exit and change of users based on user requirements. There are different types of distribution networks at the same time, but the system needs to optimize the user's requirements with respect to the resources provided.

Hybrid Technique - This technique is proposed [51] to be used both for coexistence and data integrity. Parts of this technique are two keys-sharing and authentication processes. Relationships between parties are made safer by using these two processes. For safe distribution of cells between the user and the provider it is proposed to use the RSA algorithm. According to the researchers [52], a three-tiered technique is proposed to provide the data: the first layer involves the user authentication process, the second involves the data encryption process securing protection and the third layer involves the process of recovering data by a quick process of deletion. According to the authors [53], a trusted platform called the *Trust Draw,* is proposed as critical for isolating critical or sensitive data in the cloud environment. Parts of this platform are the security transparency that offer and represent a combination of virtual machine introspection (VMI) and trusted computing (TC).

Data Concealment-The data disclosure process is used in the cloud for the data confidentiality. This procedure is accomplished by covering the real data with false data, especially as far as size is concerned. Part of this concept is simply a process of distinguishing fake data from real data by authorized persons. These techniques increase

the overall volume of the data but increase real-time data security. Proper keystrokes are the main factors that have access to the real-world data if the person possessing these keys means they are authorized to access the data. For consumers within the cloud environment [19], the internal search queries for access to the data are bigger, because each model offered to their needs is the SaaS, it is for the customer and the provider in the cloud environment, the PaaS, needed for application developers and the cloud environments testers, the IaaS is the third party responsible, which play an advising role. These trials may come from the cloud computing consumers who have bad keys and the providers who have bad intentions. Challenges coming from the external attacks come from the public clouds, but private clouds are the main target, although every model is said to be endangered by these attacks. Cloud providers possessing large amounts data, as well as robust data personal and government data are the main targets of these attacks and the main purpose is to benefit from this data. There are hardware and software attacks. Outbreaks may be: remote infrastructure attacks, system remotes, hardware overhaul, software overhaul, and hardware targeting cloud environments. A possible search may come from the information flows. Many organizations use the same provider, and because of any possible hardware release during the system implementation, it may be exploited by these groups. Such a trick may occur during data re transfer in the cloud environment or even during the backup. According to [55] the reliability of the cloud security this is based on the Redundant Array of the Independent Net-storages (RAIN). The ability to share data in the multiple segments based on the RAIN and then distribute them to different clouds, segmentation should be private. However, the other users will not be able to access the original data. Although a portion of the data (a segment) can be detected by other users, there is no complete access because there are private data where this menu describes the RAIN's confidentiality.

2.10.2 Data integrity

Data integrity is available in the cloud environment and the traditional environment, which is a very important element that provides data protection from any suspicious

operation that may occur with the data. If part of our system is a data management and integrity entity, then we are aware that our data will not be modified, deleted, or even abused by any unauthorized party. Data integrity can be achieved much more for an isolated system and its part is only the database; there is no dependence on transactions coming from other systems. Doing transaction management by limiting the access to the data coming from the DBMS to use and implement the database, we can say that we have completed the integrity of the data for such a system. Every transaction executed in the system should support the ACID rule (atomicity, consistency, isolation, and durability) in order to ensure the integrity of the data. The mechanism used for this level for others to have access to the system is the authorization of the lifespan used for access control. To allow the use of resources in the system, the user must be authenticated by his or her initials. In the cloud environments, data integrity is known as a mechanism that secures the integrity of the information. The data should not be changed or intercepted by other parties in the cloud environment. The data integrity needs to be provided in each model in the cloud environments (such as the SaaS, PaaS, IaaS). It must be ensured for large data sizes and for smaller ones, and ensure each piece of the data processing in the cloud environment. The RAID stratagem can be part of the integrity of the data similar to the digital signature.

We know that in the cloud environment, the access of different parties is possible at any time and from various points, authorization is a process that ensures that only authorized persons can access and collaborate with the data. Party trust in the cloud environments can be achieved with integrity of the data. Monitoring is a process that directly affects the integrity of the data, monitoring every process realized by the users. Although the cloud provider offers mechanisms to maintain the integrity and accuracy of the data, it is necessary to set up the control or monitoring mechanism besides the cloud provider, even to the last user. The cloud integrity control is primary to utilizing services.

According to the researches [56], a platform known as the trusted platform module (TPM) is proposed, whose task is remote integrity control. According to researchers [57], they

propose a theoretical framework called Proofs of the retrieve ability (POR), which accomplishes data integrity control by combining possible error codes and spot-checking. The work [57] of the researchers [58] is expanded through the HAIL system using the POR mechanism, it is used when storing data in different clouds, removing duplicate data, managing integrity and availability control.

Deletion Confirmation: The deletion confirmation process occurs when we have the user's confirmation of deletion and we know that this data, after deletion, cannot be returned. In the cloud environment there are many data chips to grow into an uncertain one, but if confirmation of deletion is accepted, this process is carried out in all the backup copies available for those data. There are some special techniques in case it is required to retrieve the data on the disks. However, it is the provider's responsibility if the data is deleted by the user. The possibility of reusing the data from the provider itself by an unauthorized party may be used. To ensure the non-use of the data from other parties, the authors [59] have proposed the encryption process without being sent to the cloud. The researchers [59] have proposed a technique, in which the data is encrypted before being sent to the cloud. Part of this system is concerned with deleting the data and overwriting it with new data and no room left for reuse.

*Integrity in the cloud environ*ment of data integrity can be accomplished during the SaaS's complex hosts to share resource access to the latest users. Such a failure may occur during the error-free configuration for secure resource allocation options and the possibility of errors during the configuration of virtual machines [19].

2.10.3 Data availability

Availability is a process including data, if any accident occurs such as: damage to or dislocation of a disk, failure of drives, etc, and the data retrieval depends on the different techniques verified by the user that are the data, but not from the cloud providers. Data storage process is a worrying process for users, the cloud providers are controlled by the country' rules and regulations where the servers are located and users should be familiar with these laws. The cloud provider's task is to ensure the confidentiality and integrity of

the data, as well as any possible disclosure of the data. Security needs to be shared with the client in order to increase trust between these parties. If the place where the data provider keeps the cloud data not only reduces the complexity of clouds but also reduces the user's control of the data spaces this is beneficial. However researchers [60] confirm the successful geographic replicas found in the Amazon cloud.

Reliable Storage Agreement: The usual possibility of abnormal behavior of the cloud provider is non completion of the data modification, which is a problem and should identify the encrypted data. It is necessary to support the simultaneous process of the modifying data from the multiple users. Researchers [61] propose the DEPOT to support Fork-Join-Causal-Consistency. It can withstand possible attacks that occur and support security enforcement in the cloud environment (Amazon 3). The SPORC [62] was proposed, which represents a burden between security, reliability and timely interaction, enabling increased trust in the cloud environment. Meanwhile, we know that many protocols used during data processing are limited, and most of the data processing is carried out by authorized users.

Reliability of Hard-Drive, in the cloud environments a Hard Drive is used. The reliability of a Hard-drive affects the reliability in these environments [63]. They represent potential Hard-Drive errors based on their historical use. In this case the investigator [64] provides the mechanism for detecting errors, realizes a liaison for mistakes and soft sounds which may occur on the disks.

Availability in the cloud environment

Changes in the management part: we mention the impact of recent client testing on the cloud environment where changes affect other customers. As part of the change, we mention the infrastructure for the premises controlled by the tenderer which are directly affected by the last client. In the management role, the responsibility of the cloud providers is increased for all cloud models; this should be seen as positive by the clients [19].

2.11 Virtualization and Multi-Tenancy

Virtualization plays an important role in Multi tenancy in a virtualization environment and every 'Multi Tenancy' is defined as a virtual machine. Both these parts, Virtualization and Multi-Tenancy, are part of cloud computing which has the main task of resource allocation and then isolation of the users, shared resources hardware virtualization system and includes parts of the platforms of Multi tenancy [65].

Multi-Tenancy and virtualization has recently been the subject of much scientific research. This shows that in such networks the money from the customer may reduce the costs of hardware devices and energy consumption, increase efficient use of servers, and reduce the load on client machines. Virtualization is the ability to separate software (the operating system, computer applications, etc.) or hardware systems where they have been installed. Many servers today use less than necessary, and the combination of the cloud computing and virtualization should solve such a phenomenon. This property applied to cloud computing is embodied and the user does not need to worry about concrete implementation of cloud services and take into account the hardware associated with large changes in the installed applications. Moreover, the virtualization allows optimization in terms of using the common resources, allowing applications to be independent in the hardware which is running; more applications can run on a single machine or an application can use several machines at the same time.

The main thing to keep in mind when using virtualized resources and cloud services is to ensure securitization of the information in these environments. Considering this, it is necessary to establish secure controls with adequate access and information management in each computer level virtualized environment which will be shared by many users. In economic terms, both features, virtualization and scalability, increase the elasticity of the system because the costs associated with the use of resources are adapted to the needs of the moment Sensitive data in virtual machines using cloud technology are presented as facilities or a security challenges which provide the main method for protecting the data center. This has an impact on the policy of cloud security. The cloud computing providers

have increased competitive facilities as a result of cost savings and increasing capacity and flexibility. These are just a few reasons to switch to the cloud.

Security in the traditional data center- Data center means a large cluster of servers and they have a direct effect on maintenance which affects data availability. Security in a traditional data center is based on security perimeters which consist of a firewall, divided network, appearance of cases of intervention and prevention systems in these cases (IDS / IPS) and network monitoring. Virtualization in cloud computing enables the provider to have the situation under control even in in the hardware. Traditional data centers are being reduced to minimize the cost of purchase and maintenance of servers. All the cloud computing providers are using virtualization in order to multi-tenant use of these servers.

The lack of physical divisions and attacks completed for the safety of the hardware and virtual machines in the same server give rise to the possibility of communication with the main server or the virtual machine. Creating this connection with the server using virtual machines creates the possibility of sensitive systems with sensitive data present in the modules in the environments of the other cloud models [66].

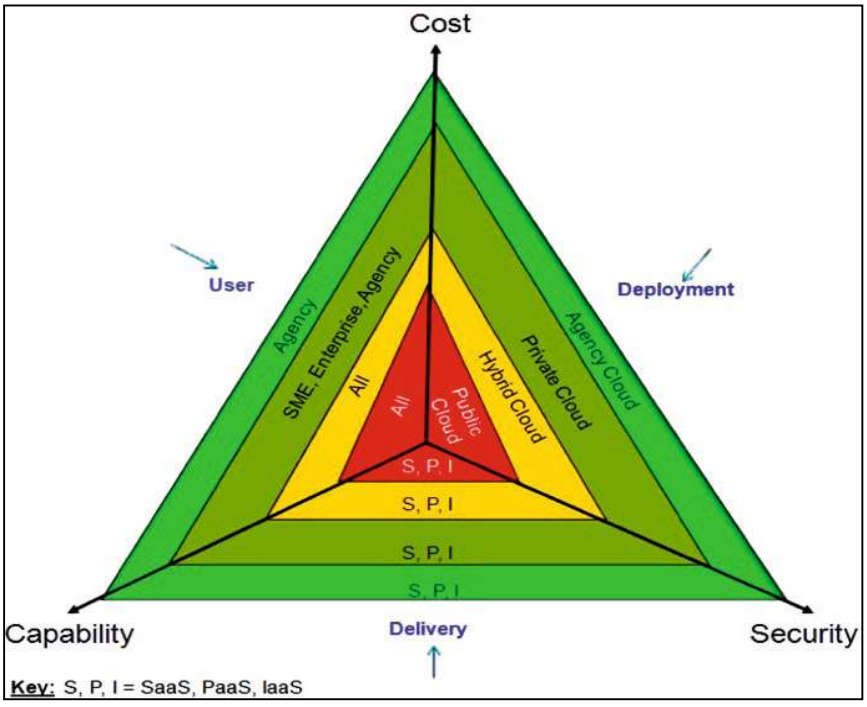


*Figure **8.** Cloud security relationship framework*

In general, the risks in the cloud are approximately the same, depending on the cloud model. However for sensitive data related to data security we should select a more secure model in the cloud. There are many differences about security for the private and public cloud. Privacy of the data in the private cloud is not the same in the public one. It is important to provide risk management modules for cloud computing and present a clear assessment of security of the cloud modules, Fig. 8. A model is proposed which represents the link between cost, security parameters and cloud modules. Based on Figure.8, the security of the data which must be selected for our system can be determined. [67]

2.12 Different types of virtualization

IBM invented the concept of virtual machine (*Creasy, 1981 Goldberg, 1974*). However, IBM was firstly defined as a virtual copy machine entirely isolated and protected with physical hardware [68]. Thus, virtualization refers to virtual simulation processor elements such as hardware, memory, memorizing other units, software, network and so on. Virtualization provides security for the operating system since it allows the execution in a sandbox. Everything happens in the sandbox environment that does not affect the virtual operating system. It improves system management at no additional cost [68]. For example, the hard disk can be divided into different partitions and there will be no need to buy some other discs for the same purpose. The main goals are to maximize the use of virtualization hardware, thus reducing hardware costs by regrouping of several virtualized machines on a single physical machine, reducing energy consumption and simplifying the security management process and the whole system needs to use the Virtual Machine Monitor (VM to perform machine hardware virtualization).

There are three main techniques for virtualization of an operating system [69]:

- Full Virtualization
- Hardware assists virtualization
- Para virtualization

Full Virtualization- This approach, as depicted in Figure 9, translates a kernel code to replace the non-virtualized instructions with new sequences of instructions which have

the intended effect on the virtual hardware. Meanwhile, a user level code is directly executed on the processor for high performance virtualization. Each virtual machine is monitored by providers, including the virtual BIOS, virtual devices and virtualized memory management [69]. This type of operating system is shown in Figure 9.

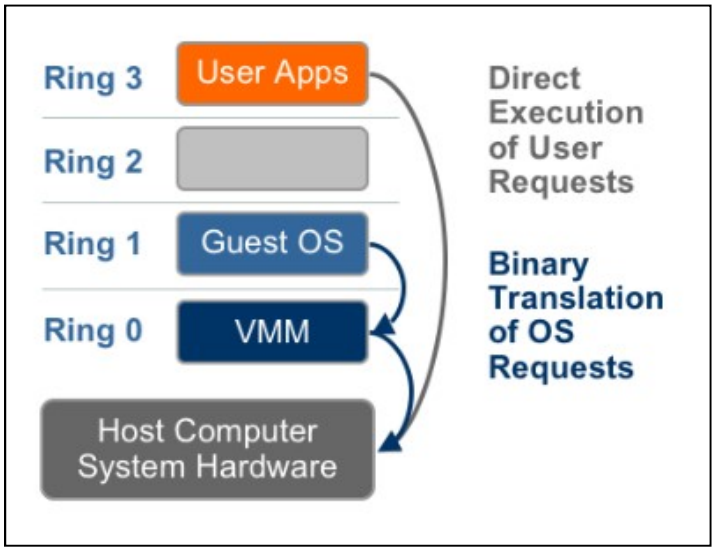


*Figure **9.** Steps to implement full virtualization kernel level [69]*

Para-virtualization- This is a technique used by the SO virtualization client which enables higher performance when using full virtualization or hardware-assisted. By the SO para-virtualization the client is able to communicate through the VMM, and it is necessary to make modifications to the SO client by translating instructions, to enable SO - hypervisor communication (Figure 10).

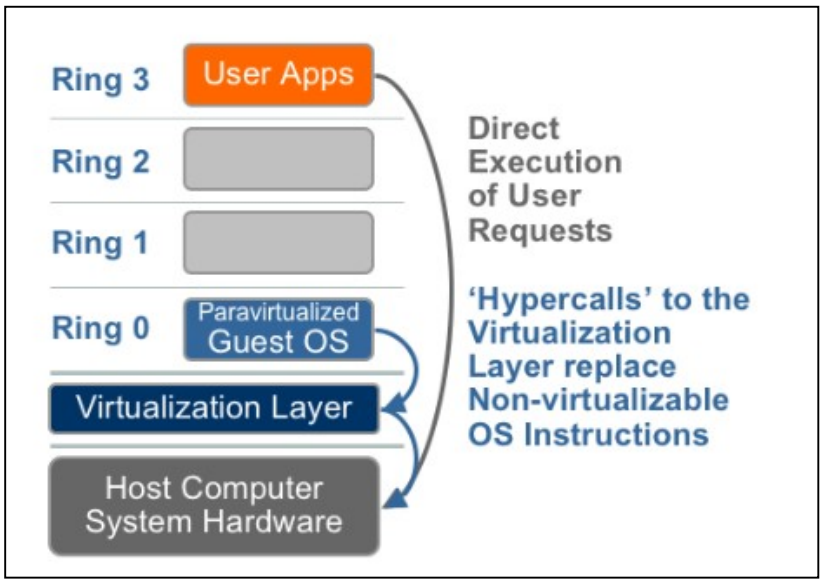


*Figure **10**. Actions taken to implement virtualization the type of paravirtualization kernel leve [69]*

Hyper calls are instructions that enable communication directly with a virtual layer. SO modifications include problems with low adaptability and portability [69].

Hardware assists the virtualization. Hardware, which is developed to overcome the problems of para-virtualization based on hardware modifications, allows the OS client to communicate with the VMM without modification. Hardware supports this kind of virtualization technology which is an Intel virtualization technology (Intel VT) and AMD (AMD-V). These processors have features to capture requirements that come from ring 1 and ring 0, transformed into a virtual ring -1 and ring 1 form, which is a virtual ring 0 where the OS client can operate without modifications (Figure 11) [69].

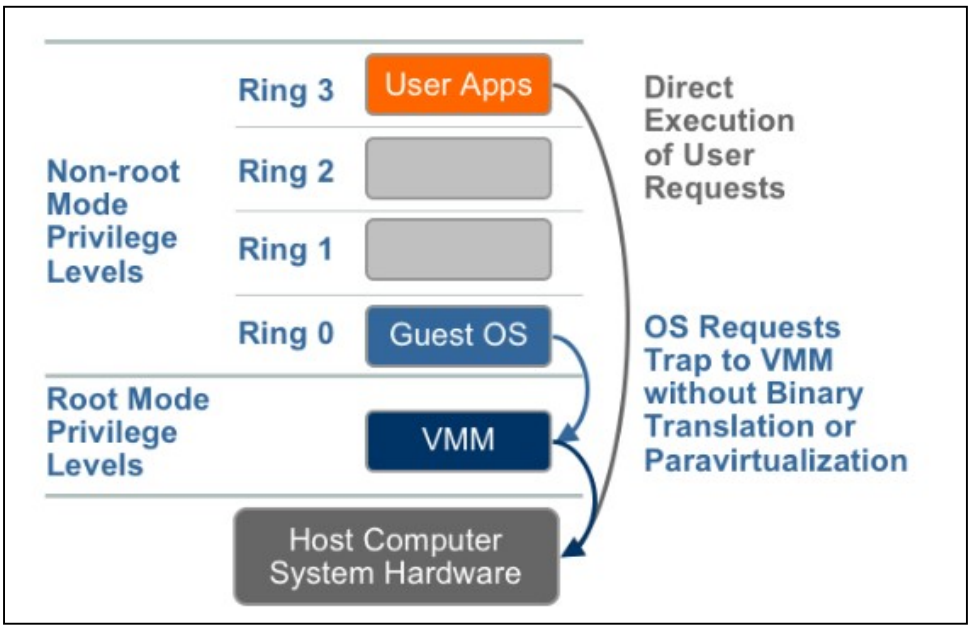


*Figure **11**. Virtualization Hardware-assisted [69]*

2.13 Designing Secure Multi-Tenancy

As an important part of the multi-tenancy cloud is the virtual machine. This kind of model is described as a model where the hierarchy order in each level in the multi-tenancy has different policies and has implemented technology services for customer segmentation. This potential offers customer segmentation and a safe environment. Another advantage is that multi-tenancy customer segmentation allows a better management of resources based on customer demand [70].

Virtualization plays an important role in Multi tenancy, in a virtualization environment every 'Multi-Tenancy' is defined as a virtual machine. Both parts of the Virtualization and Multi-Tenancy are part of cloud computing and have a main task of resource allocation as the isolate users, share resources, hardware virtualization system and includes part of platforms of multi tenancy. [65]

As a key part of the cloud, computing we must mention elasticity, multi-tenancy and scalability. If we have a full cooperation between these technologies then we will have a very comprehensive service for customers in the cloud computing. There are general

definitions for these cloud features, andsome specifications of these features are shown as follows:

- Elasticity relates to the possibilities that the system has the ability to meet all of the requirements coming from the client and has an opportunity and capacity utilization of different resources based on the clients' requirements.
- Horizontal scalability means that a system will be able to contact the sources reduced without any clients who has realized this requirement and while requesting not to have interruptions during the realization of this resource. Simple horizontal scalability can be understood as an ability for the system to increase the additional resources and skills without any interruptions during communication with additional resources.
- Multi-tenancy can be understood as a capability system which allows many users or tenants and each tenant provides services to be isolated and viewed. However, this can enable service by customers who use only the sources of certain facts shared by physical resources. Tenancy can be a company that realizes the organization a request to use a tenancy for the realization of that request, and can be an application which uses resources systems for the realization of a claim.
- Use of the multi-tenancy is completed when resources offered are better managed and accounted to systems which use the same resources. Elasticity of a multi-tenant is realized not in a very high level in those parts that resources are dynamically allocated to certain systems that are used for a particular application, through which transactions should enable improvements in the system. It may be said that none of the flexibility of multi-tenant is a positive factor in the cloud technology. [71]

CHAPTER III

3 RELATED WORKS

3.1 Introduction

Cloud computing is presented as a technology that is derived from cluster computing, grid computing, component-based composition, and lately, service oriented architecture and web services, all described by cloud computing. In the traditional technology the software and the hardware were divided but in cloud computing everything is offered as a service: hardware, software, the CPU power, storage, platform, application software etc. This was one of the main factors that make cloud computing so preferable nowadays. Cloud computing has brought impressive advantages to the clients interested to use cloud services, such as flexibility in managing the space, automatic software updates, easier access to information and payment based on services etc. This was one of the main factors that made it very favorable. Exploiting services as much as you need, in a vase and time set or which is known as "pay as you go".

In this chapter, we have been focused on the initiatives taken for the cloud security and virtual machine monitoring. The latest developments in the data encryption section, is a major initiative expected from the standards to provide transparency in the security and control of all those participating in cloud computing. The work includes several rules that provide a higher level of security transparency for participating parties such as the Cloud Service Provider (CSP) and the Cloud Service Consumer (CSC). Due to the presence of the

third party CSP, many businesses hesitate to support this environment. Work on this point is proposed.

3.2 Solution proposed for cloud security until now

3.2.1 Analysis of the first proposal

Some solutions put forward in cloud security articles have hinted at our proposed model [74]:

This proposed model consists of three different security scanners, with different choices depending on their requests from interested parties for use in the cloud. These scenarios are based on three main abstractions fig.12

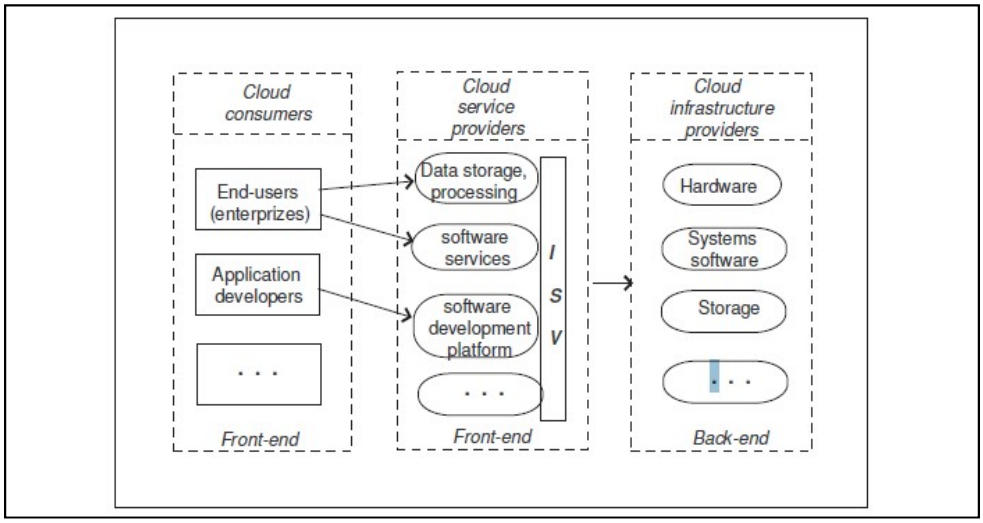


*Figure **12**. Levels of Abstractions of Cloud Computing*

The figure above shows that each part has its own factors.

Based on these main abstractions, three main scenarios are addressed:

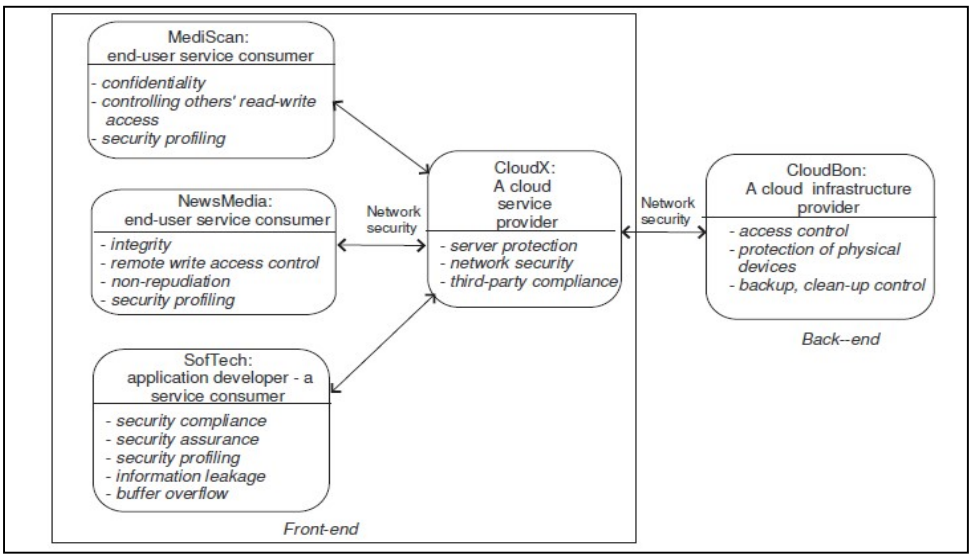


*Figure **13**. Security objectives for different stakeholders*

Based on the requirements for the security of these different scenarios, it can be deduced that the stakeholders have different security requirements in the cloud such as:

Med Scan: In this scenario the main factor for the stockholder is the disclosure, confidentiality and integrity of the data. Although this is not controlled by the end user, it is required. It also manages security for multiple data and, by placing it in different objects, offers a great deal of data. The security requirements for this cloud security scenario are focused on the following:

- How is confidentiality of data stored?
- How is data integrity preserved?
- Controlling access to data being placed and read?

The last use of this scenario is interested in how these requirements are managed in the three abstracts of fig.13

News Media: This scenario uses the same technology but the focus in this scenario is not confidence, because the data is available to everyone. Data integrity is very important and is not controlled by the end user and the CP is responsible for data retention. The security requirements for this scenario are: How is data integrity maintained? How is the

authentication of the CP been maintained? How does communication security take place between stakeholders and CPs?

The main purpose of this scenario is that it is not possible to change or hide from unauthorized persons.

Soft Tech: The key drivers of this scenario are: How are the security requirements of their software combined with the security components which the CP offers? What are the guarantees that the security components and services provided in the CP will be respected at all times? How is security derived from information about the software components?

3.2.2 Analysis of the second proposal

Researchers began by carrying out a common analysis of security in the cc modules, and then focused on elementary requirements to secure the system's cloud protection *[20].* Their work is geared towards the Advanced Cloud Protection System (ACPS), which is the result of security for the Linux Kernel Virtual Machine. In this work through the ACPS it is possible to protect the integrity of virtual machines and distributed computing middleware, which helps elements in the cloud environment. Different monitoring offered by the Vms, in cooperation with the components of the infrastructure, is proposed against the various attacks.

3.2.3 Analysis of the third proposal

The authors of the paper [75] have conducted a survey which has as the main object the assurance offered on the multi-tenant software platform as part of the PaaS model. In the PaaS model, they discovered a technical weakness for multi-tenancy support platforms, similar to the Net or Java. The authors suggested that inside the PaaS they should isolate the code by the CSC to reduce the probability of possible errors in other applications. Based on the two weaknesses during application development, all the rules to ensure that this code is deprecated in the PaaS (above all how it can be manipulated by malaria) and then benefit from the hackers. As a conclusion in this scientific paper [8], the CSP PaaS

model uses all the mechanisms that provide the security environment for minimize the potential risks for to this model.

3.2.4 Analysis of the fourth proposal

The whole work of the authors [76] is geared towards detecting and addressing security risks coming from the IAA model, especially those caused by virtualization and multi-tenancy in the cloud that describes every possible search that comes at all stages of the VR's life cycle from the initial to the final phase. These quirks are identified by the Cloud Security Alliance (CSA), as well as the existing choices for those quests. As a conclusion, the authors recommended that access control and encryption mechanisms are the main techniques we should be mindful of the security concerns that come from virtualization.

For security on cloud services we have discussed [20], the challenges and the choices offered in the work. The model proposed for cloud security needs to be exploited and research undertaken on security transparency and increased confidence in the security issue to trust the unknown party, the CSP. This paper is focused in two directions. First in announcing existing cloud security initiatives to boost the cloud confidence and secondly the review of initiatives both academic and industrial. The second part includes how these initiatives have succeeded in enhancing security transparency between the CSP and the CSC.

3.2.5 Analysis of the fifth proposal

For all customers, who are still struggling to migrate to the cloud environment, the virtual machine monitoring for addressing security and privacy in the cloud is offered as a choice. Authors from the [31] proposed Trusted Cloud Computing Platform (TCCP) allows the calculation of the integrity and confidentiality of data sent by the provider. This platform informs the CSC if the data has been accessed by others or the CSC, then decides whether to interrupt the VM or to continue detecting unauthorized access. The TCCP's main task is to ensure that nothing intervenes between the CSC, CSP, and VM. Finally it is the TCCP approach, based on the plain form the traditional TERRA belief [78], which provides the integrity and confidentiality of the data in respect of multiple hosts. The authors [79] offer

a platform for cloud computing, Private Virtual Infrastructure (PVI). This platform manages, monitoring and combines the Trusted Platform Modules (TPMs) and the Locator Bot (LB) that provide security measurements to the properties they own; it also provides the database and offers continuous monitoring in the cloud. From this point of view, it can be said that the data security falls like the CSC and the CSP. Starting from the SLA, there are no proper roles for security responsibilities for all participants in the cloud environment. Authors [80] argue that cloud service reliability is achieved through the security level of workload to facilitate service quality assurance.

Security Level Determination is based on the following requirements: Workload State Integrity, Guest OS Integrity, Zombie Protection, Denial of Service attacks, malicious resource exhaustion, platform attacks and backdoor protection. In this scientific paper there is no clear way how to determine the level of security, as it is claimed, which is not apparent how these security level information is sent to the CSC and CSP.

3.2.6 Analysis of the sixth proposal

Authors from [81] proposed a private cloud monitoring and management a scheme called the PCMONS. Despite many differences from traditional technologies and the cloud environments, it is argued that it is possible that these resources (inherited network and distributed management methods etc.) have the potential for reuse in the private cloud. The PCMONS is focused on centralized architecture described by these features:

a. A node with accumulated information, which is responsible for collecting local information for the next node,

b. Cluster Data Integrator - a collection of data for the next layer (collected by monitoring)

c. Monitoring Data Integrator which collects information and stores it only for archives in the database, and provides this data to the configuration generator.

d. A Virtual Machine, its task is to transfer data from the VM to the overall monitoring system.

e. A Configuration Generator, its task is to get information from the database.

f. A monitoring Tool Server is used for the sole purpose of gathering information from monitoring of different resources from a database that populates with notes coming from the Configuration Generator and the Monitoring Data Integrator.

The PCMONS projection responds to the private cloud requirements, with the only space to provide a security environment for the CSC and the CSP. The whole architecture of this proposal is based on some interesting features that can be used in similar architectures with the sole purpose of providing a safe environment for all parties. One of the features that can be exploited is the monitoring data integrators, which can be exploited by the CSC as a feature to provide information in the cloud environments. From researche it can be said that researchers have provided some security solutions in the cloud environment, some of which have been implemented. All of the focus has been on the issue of creating a credible environment and monitoring of virtual equipment driven only by the CSP, not by all the participating parties, and the ability to monitor all these parties. The goal is for the entire monopoly to be implemented by the CSP.

3.2.7 Analysis of the seventh proposal

According to [82], mutual trust among the participating parties in the cloud needs to exist in terms of the SLA management. From the mOSAIC project (http://www.mosaic-project.eu/), the cloud-oriented APIs were used, and the authors created a cloud-oriented application from the SLA, which provides authentication security management capabilities and authorization of the IaaS and the CSP. It is true that the client, depending on his/her own requirements, selects the number of models required, all this is accomplished before the node configuration depends on the existing circumstances. As part of the security management by the SLA the client provides a general document for the way the cloud service has been used. From the perspective of the CSP, the SLA is seen as a way for an application to comply with the rules set out. From the research [82], the idea of the SLA for monitoring is presented but there are no tools for monitoring; this figure as a shortage in the research. The research [83] provides a platform for the SLA management, which is part of the EU FP7 project Specs project (http://specs-project.eu/), is seen as a

continuation of the research work [82]. Even the SLA @ SOI project [36] proposed the SLA-oriented architecture of the cloud services. In this research there are more specific features proposed for monitoring the SLA, and the monitoring is carried out in different parts within the cloud environment. The SLA monitoring process is supported by the EVEREST+ [84], which process represents the behavior of distributed systems in each time frame. The aim is to collect information from monitoring and also to review complaints received from the clients. As part of the SLA context cloud computing is also part of many researches related to the problem. These initiatives, which are part of the SLA, come from the sole aim of selecting the right cloud service that meets the maximum SLA requirements [40], using various algorithms [85]. This is the way to go, with the sole purpose of providing billing projects (provided by the A4CLOUD -http: //www.a4cloud.eu), if there is any breach of the SLA or breach of any liability on the Provider side, it can be traced by the various proposed models. The A4 Cloud context is thought to be the concept of accountability. In theory, the purpose and the way of solving security transparency are often expressed, but practically not at the proper level. In this research, several CSPs (in Luxembourg) have been contacted to provide their specifics for the SLAs. Their data was more limited to the allocated bandwidth, storage capacity, and the security section only looked at the availability of the cloud services. In these companies a security argument was the security certificates they possessed. They did not possess any security model for more robust data services that were found to have their bugs.

3.2.8 Analysis of the eighth proposal

All the work is based on this slogan [55] "if the provider does not need to read the information, why should he be allowed to?". The belief in this article was achieved by dividing the information and then controlling the scattered parts. In their work, the author has identified five cloud computing models designed to increase cloud security:

The Separation Model separates storage of data from processing of data at different providers.

The Availability Model ensures that there are at least two providers for each of the data storage and processing tasks, and defines a replication service to ensure that the data stored at the various stage providers remain consistent at all times.

The Migration Model defines a cloud data migration service to migrate data from the stage provider to another.

The Tunnel Model defines a data tunneling servile between a data processing service and a data stage service, introducing a layer of separation where a data processing service is oblivious of the location (or even identity) of a data storage service.

The Cryptography Model extends the tunnel model by encrypting the content to be sent to the stage provider.

By using these models, which allow duplication and task sharing, they reduce their integrity, availability, and confidentiality by encrypting the data storage. According to [86] the EU confidence increases when exposure and access to sensitive data is banned. Considering this, a solution is provided where the client requires that sensitive data to be processed only in the system that their placement is required to know exactly where it is located, to be within the EU. Although this is a dubious point because the cloud service providers have the right to operate all over the world.

A special part is present for the Botnest, a group of computers with a separate hierarchy tied to each other and controlled by a Botmaster. The Command & Control -C & C is world-wide based which uses some of its features.

Approach: a new concept model has been developed where data is subdivided and stored in the RAID-dependent storage, in that a single part does not compromise the confidentiality.

There are two types of the cloud service providers, the first case is when any information, and the way it is segregated and segmented, is located in the C & C node, and this node in the first case is located in a public cloud and has access to each one. This proposal has been offered when we do not have users with bad intentions. The second case is when the

C&C hub is located in the private cloud and the data portions are located in various cloud providers.

There is a protocol scheme [55] used for the RAIN. This scheme called Mix-net, is dependent on independent cloud agendas. Agendas in this scheme have 1 to 1 relationship with the cloud provider and each agent has a unique ID located at the C & C node. From the C & C node, an encryption channel named the IRC is used, which contains the information table for the requirements deriving from the agendas. This node is also intermediate between the C & C node and the data segments located in the cloud. It has been shown that the *mix ()* function is used for data segmentation, this function is part of this scheme. The division into some parts of the data and then the reunification of the parts to form the original data has been shown.

Separating data into segments should be careful because the segments divide into data will be part of the transmission; the segment size is not related to data sensitivity, and it is not allowed that no segment contains the complete set. There are two types of segmentation:

- Sequential Segmentation and
- Random Segmentation is proposed.

To hide data from the provider, two methods are provided, encrypting the data before sending it to the cloud provider or sharing the data in the backup and deciding on different clues. It's been said that everybody wants security, but nobody is willing to pay for it. It has been mentioned that this idea has been developed as a prototype and the next step is to test real-world data in the cloud environment whilst is also noted that, based on experiments, this idea is worth more for small businesses or home users.

3.2.9 Analysis of the nine proposal

This proposes the pi-cloud, personal secure cloud [87], which includes the cloud resource management resources that are interrelated to each other for end users. The pi-cloud objective is the last user to format the IT Infrastructure without losing control over its data. The cloud federation refers to a personal combination of the user, for private and

public cloud sources. Up to this proposal the authors have come up since in the cloud environments are jeopardized three facilities of success availability, integrity and confidentiality. The pi-cloud works by sharing trustworthy and untrustworthy sources. The user adapts the cloud based on his needs, providing data flow and execution of services.

The pi cloud is controlled by the pi box, the task of this gate is to divide sensitive data from the public data. The Pi Box consists of four main components: (1) the Cockpit, (2) the Service Controller, (3) the Data Controller and (4) the Resource Manager.

Cockpit is the component used as the interface for managing resources from the user in the cloud even if he/she is not an expert in this field.

Service Controller is responsible for chasing execution of the service. The execution of servile execution is accomplished by rendering the services as critical and not critical. Critical services are executed in the safe and non-critical resources in public resources.

Data Controller provides secure storage for secure cloud storage. Each file is divided into several parts and then attached to it with a piece of encryption and then the authentication code for various resources is attached.

Resource Manager is responsible for setting up all resources and services available.

The part to discuss for our topic was the description of some of the existing resource management shortcomings. Some of them were:

Availability as an open source to increase integrity and security / reliability, only open source solutions based on open standards are considered safe.

The ability to integrate services from a cloud-based user-based platform, the one that seeks this opportunity.

Opportunity to integrate cloud providers - integration of different services, devices, and servers in the clouds *ie* includes communication in the cloud environments.

Ad hoc migration of management components - needed due to performance, stability and reliability, is anticipated in the cloud pi.

Support for Saas Paas and IaaS: Offered Solution to Support All Platforms for the Saas Paas and IaaS

There is a scenario for component migration by the cloud pi, they must first be registered in the service box or the device then be part of the cloud.

Service Requests to be Part of the Box:

- Extensibility
- Non-functional properties
- Distribution
- Ease of use

3.2.10 Analysis of the ten proposal

People are becoming more and more interested in the cloud computing due to the low cost services it offers, [88]. However, the major concern layer on the security data; “Data confidentiality and auditability” is said to be one of the main obstacles to the adoption of the cloud computing in the influential Berkley report. In addition, security concerns are preventing some organizations from adopting cloud computing at all, others are considering using a combination of a secure internal private cloud with less secured public cloud. In addition, this is an approach where sensitive data can be deployed in the private cloud while less sensitive data can be externally deployed in a public cloud. However, this approach seems to have problems when allocation applications in the clouds usually operate on an ad-hoc, per-application basis which is not ideal as it lacks rigor and audibility.

This proposal [88] describes an alternative to ad-hoc solutions, a method that takes an application consisting of a set of services and data connected to a workflow and determines the valid set deployments over a set of the clouds, ensuring that security requirements are met. The method is based on multilevel security models, specifically Bell-La Padula, this method introduces transformations which need to be performed on the workflow where data is communicated between the clouds, it also identifies the security issues that can be raised as a result, and the extra security checks that need to be performed in order to address this. If the method results in more than one valid

partitioning option there is the issue of how to choose the best. The full method, including the cost model has been implemented in a tool that has been built automate and explore its application.

CHAPTER IV

4 THE ROLE OF CRYPTOGRAPHY FOR CLOUD SECURITY

4.1 Introduction

Cloud Security & Cryptography are based on the early design of cryptography and protocols in order to have a more secure, efficient and usable system for customers. Cryptography must exist in tougher measure than other technologies, enabling safe and appropriate privacy levels. This does not mean you can maintain the data in a cloud, we simply have a need for security. The best way is encryption of data before being sent to the third party.

4.2 Fundamentals on cryptography

People have been fascinated to keep the information as secret from others. History is packed with examples. Kings and generals of armies communicated with their soldiers using simple cryptographic methods to stop opponents from obtaining military information. Thus, for example, Julio Cesar [89] used a simple code named after him. With the development of society there was a need for more sophisticated methods of preserving confidential information. Storage of information today has a special significance. In recent time the network is increasing and the need to maintain confidential information and electronic service is growing. So, with the addition of these services there needs to be add an uncertain electronic system. Already, greater exchange of information is done through the internet.

Cryptography is divided into cryptology and cryptanalysis [90]. First of all it is impossible to do cryptography or cryptanalysis without a good knowledge of the methods of the two fields. Cryptography deals with sending secret messages so that only the recipient can read them. The original message is called plaintext, while the disguised message is called the cipher text. The transformation process of the plaintext into the cipher text is called encryption and the transformation of the plaintext into the cipher text is called decryption. Cryptanalysis deals with the study of mathematical methods and techniques of cryptographic systems [91].

The Coding Theory relates to the presentation of the data symbols called "Symbols of codes". There are three basic types of applications: compression, error correction and concealment. Over the past several decades the word "Coding Theory" has been largely united with codes to correct the errors. The theory of codes is the study of communication channels with noise and guarantees that the message received is exactly a true message. It should be stressed that in any "real time system" error correction codes should be used during encryption. If there are changes, then it is totally destroyed and insufficient to be called a "well designed system".

Confidentiality is the basic technique of creating security, integrity and availability, which are the basic parameters for creating a safe environment. This parameter is used as a cure for those cases in which we need to hide the actual data, especially in open environments such as the cloud, and harsh confidentiality regarding sensitive data must be implemented. Integrity, in many cases is provided by guaranteed methods of privacy and unauthorized access. Availability of the data in which the client understands the opportunity he/she should use the data from the capacity planning [12].

Safety Communication: In the simplest scenario for communication, described in Figure 14, there are two persons named SENDER and RECIPIENT, who want to communicate with each other. The third person is another person, the listener if possible.

When the SENDER sends the message, which will be called plaintext, the RECIPIENT, encrypts the message using a predetermined method known to the RECIPIENT. Usually,

the method of encryption is concerned about whether the other person wants to know the secret contents of the message or not and then it is assumed he must know the key. When the RECIPIENT receives the encrypted message, which will be called the cipher text, then he turns the plaintext message through the decryption key.

Another person may have these purposes (see below):

1. Reads the message.

2. Key finds and reads all messages encrypted with that key.

3. SENDER changing message to another message, the RECIPIENT will think the SENDER has sent a changed message.

4. Fraud can occur with the SENDER communicating with the RECIPIENT, although the RECIPIENT thinks it is communicating with the SENDER

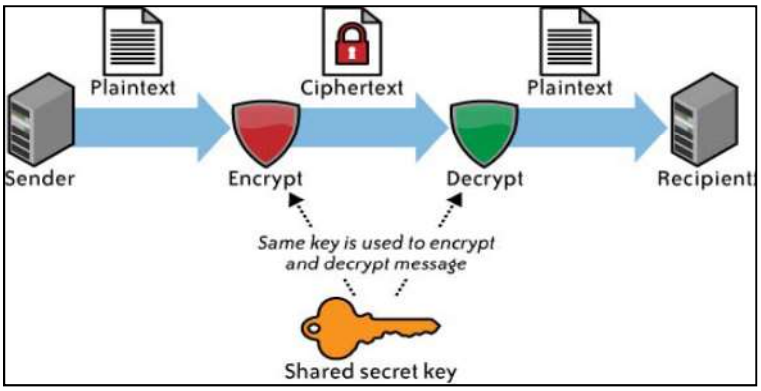


*Figure **14**. Basic scheme for communication*

4.3 Cryptography in cloud security

Like the earlier systems with cloud systems, cryptography plays an important role in the part of data security in cloud computing. We should have computing cloud clear that resources are shared systems and use a multi-tenant virtualization of rest data, and managed to have a perfect approach for the SaaS. The main barrier to this is that the environment at the same time to provide confidence, safety and privacy of statements to the customers. Because of all these barriers the customer will not have full control in this misfortune.

Cryptography is the main factor to enable security techniques to control security in cloud computing and then to enable increased reliability to customers. Space in the cloud services offered includes client, backup etc. In this space it cannot be seen by the client system complexity, which is offered only as a service, and infrastructure that uses this system, headwear management, which enables a connection with the client through a simple browser.

Based on [92] there are some challenges that are part of the cryptography, fig 15:

Proof of irretrievability: possibility of verifying if our data is successfully saved and have access to opportunities at any moment they need customers. Reliability can be achieved if the client use mechanisms at all times familiar to the client who manipulates data and has access to this information. Should we offer integrity and availability of data during the use of the service? You must enable this option for the client to control the whole data. Proof of retrieval enables customers to have an audit data and enable their integration using cryptographic operations. Proof of retrieval model for the first time presented by Ari Juels and Burton S Kaliski Jr [92]. This scheme enables the client to save only part of a key structure and incomplete data encryption. This scheme requires that data encryption is completed if we have a complete system with the sensitive data, or a major part.

Secure Deletion in Cloud: To be sure that after the departure of our data, cloud services will not be available for other systems. The clients in cloud computing submit requests for deletion of data for many reasons, some of them are:

Due to the period between the said services and to limit the exploitation of a particular service client cloud services has selected an economic service and expressed a desire to move on that service. However, we must be careful not to use it as a threat of the trailer data. The CSC wants to wipe data all the time due to changes. Cloud computing client is unable to delete all the data because there is no dual track in all layers of deciding statements. Even though the client deletes data traces remain, the financial statements. Copies of data can be stored without knowledge of the client and then there is a possibility of using this data even if their contract has been accepted. Also there is the

mentality of misuse of these unauthorized copies, but some larger companies have offered the option of deleting the data in general but they are not yet sure.

Storage Security: data storage and management will be possible only by authorized entities and will not have the possibility of unauthorized access entities. Data protection is based on the examination results of security we have applied in that service. The key requirement is the fair security of data storage. Once the data is preserved, then it is needed to apply the security of information on the basis that which the client has set and you need to provide access. Primary mode and favorable for the maintenance of the data is their encryption and these notes will not be accessible to unauthorized entities. The encryption method of transportation, as long as the statements are in the database, is among the safest methods in the cloud environment. For this reason you should go to the financial statements set encryption only if we are dealing with very sensitive alert statements encryption preferably preserved. Control of the log file is a good audit for applications to check the activities due to a safety grow these services. The used data for the processing of data encryption is not carried to them, but the data appear sensitive transactions is mandatory realized to their encryption. Physical location of data is located in different geographical spaces, and at all times they carry copies of statements. These copies should be transferred from one space to another, should provide a safe transportation during transfers of copies, in order to increase reliability and be confidential.

Communication Security: During the communication all the parameters that discussed above must be taken into account, which are very important, if we want to provide a safe environment for the customers. Data communication is realized between the cloud service provider and the client, or cloud communications, conducted within the geographical spread in space. If you do not provide a communication channel in cloud environments, then the transferring data will not be safe.

In order to avoid this risk it is necessary to use a private channel to transfer the financial statements or data during the encryption of communication. If these two methods used in

combination with each other their interaction will be safe for alerts, as well as reduce the risk of eavesdropping by unauthorized persons. We shall use the SSL channels of communication in order schemes client and service provider to be sure, the statements encryption model to highly increase security of the cloud communications environment.

Virtualization Security: allows the client to inform the others the data is successfully stored in the virtual environments, and now they will have access to the data contained in these virtual environments. It is the technology that enables the improvement of using hardware, where is a single physical platform, divided for use by many clients at the same time.

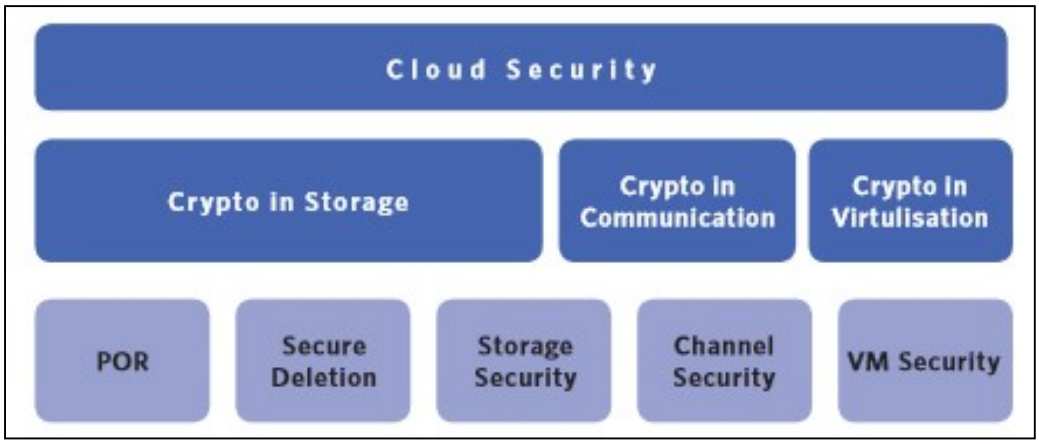


*Figure **15**. Security challenges in major areas of cloud and cryptography role, [92]*

The definition of safety requirements in cloud environment is closely related to the user, the intended usage of the system and the level of service being offered. Nowadays, cloud services are offered at different levels such as the SaaS, the PaaS, the IaaS and each level we have has different requirements in order to offer a highly secure cloud environment. Some of the general features earlier defined, are part of requirements for each level of the cloud architecture [93, 108]. Cryptography is the main factor that enables security techniques to control security in cloud computing, and increase the reliability for the customers. Different providers offer cloud storage services for clients, including complementary services such as backup, redundancy etc. When using such storage services, one cannot see the client system complexity which is offered as a service and

infrastructure which this system uses. In cryptography, based on the used algorithms and the communication model between the parties as said above, two fundamental approaches are known; symmetric and asymmetric encryptions. The main difference occurs in realizing communication between the sender and the receiver of the information [94]. In the Table 6, we give a classification of different symmetric and asymmetric algorithms which will be considered as the basis for our proposed model.

*Table **6**. Classification of cryptographic algorithms*

	Symmetrical cryptography	**Asymmetrical cryptography**
Information Sender	Encryption key	Private key and Public key
Information Receiver	Decryption key	Private key and Public key
Represented	DES (Data Encr. Standard) 3DES AES (Advanced Encryption Standard)	RSA (Rivest Shamir Adleman) Diffie-Hellman El Gamal

4.3.1 The importance and difficulty of encrypting data in the cloud

To ensure integrity and confidentiality as a cloud-based solution, data encryption is seen to be true. Encryption is also seen as a choice of the data security both during processing and database, that data has not been tampered with or seen by other parties in the cloud environments. Although it is proposed to encrypt data for the abovementioned problems, it is not a safe solution to those problems. In the cloud environments, exploited patterns (for management, data processing and storage), security and privacy processes cannot be used with the same encryption techniques as traditional ones, [20].

The primary challenge for using data encryption in the cloud environments is a cryptic management. The first and very important element is the securing of encrypted cells, in order to avoid problems arising after detection of these cells. By providing these cages it means the way and place where the data are stored. Another element is the rule that we should follow for cells to have access. Access to these keys must have personal

authorization and no other cloud computing parties. Another important issue is to ensure the regeneration of these cells in case they are lost or damaged by the members of the cloud, [95].

Some researchers like [96, 97] have shown the difficulties that exist for the use of effective encryption techniques in the cloud environments. According to the author, the main concern when using encryption techniques in the cloud computing cloud-encrypted data and the cost, in case there will be the data leakage on local machines, especially in those cases we are working with large files. Nowadays it can be said that encryption techniques can be applied in cloud computing, but in practice, in case of complex resources the development of the entire encryption process can be seen with some deficiencies [96]. Some of the key initiatives of using the cloud encryption techniques are guided by large companies. One of these companies is IBM's Craig Gentry, based on the homomorphic encryption scheme, part of this scheme deals with the lattices, the perfection of this scheme is being the processing data without having to rely on them [20]. It looks like very important in the cloud, which increases data security in the cloud. By using this homomorphic encryption, the data encoding results are the same as the encoding of the simple texts. The use of this type of encryption holds that data encryption counts as addition and multiplication in simple data making it more powerful. Fully homographic encryption is also proposed by [98], which foresees multiplication calculation or known as the MPC. All of these schemes are based on the multichannel FHE and their perfection, can act with encrypted data using multiple cells which are not connected to each other. If the CSP is a non-trusted part, it is proposed to use the full homographic encryption, but what is likely to be the cost of using this proposed technique, [96]? In the research [99] a combination of primitive encryption techniques is proposed to ensure security of cloud computing. Using virtual private storage services shows that the CSP is not entirely trustworthy. If we are part of the public cloud, then we are obliged to ensure the confidentiality and integrity of the data. The early virtual private storage service proposal consists of three main elements: data processing, data verification and token generation.

Encryption as a process for data processing and data encryption is proposing several types of premium recovery based on the symmetric encryption scheme, where encryption and encoding is the same. If the client submits a request for data retrieval, the token process creates a token labeling and refers to a particular file. Then this field is sent to the provider in order to convert the encrypted file. In these cases, the integrity part is provided by calling the data verifier. During this work on the database, part of it as a tap, seen to be intercommunication between the client and server, it defines an executable protocol that verifies the data requested by the client. From the research [100], proof of Retrieval (POR) protocols have been proposed, which task is for large files to prove that the file was not deleted or modified during the communication process. This encryption technique takes the file and then encrypts and blocks it to randomly encrypt the file. After this step, the cliché requires that its data depends on their sensitivity to determine the manner of their archiving. A similar solution is also proposed for the POR: the Provisional Data Possession (PDP), proposed by the paper [101]. The PDA uses a technique that verifies the possibility of verifying that the data is placed in a secure location and there is the possibility of manipulating your data. Proposes the use of the scheme known as the Homomorphic Linear Authenticator (HLA). The HLA proposes that a certain file should be divided into several blocks and the generated vector verifies the position of the blocks, the server tasks it to homomorphically construct the value of the polynomial that indicates the combination of the vector blocks and their storage on the server. Some researches, like [20], as a basis, have exploited this idea and then have presented additional elements. In recent years cloud computing has been working to explore the cloud data and the cloud integrity techniques.

Authors from the paper [97] propose securing the integrity and privacy of the data, but as part of the proposal of this paper and the efficient audit it is affordable for the client at not very cost. It is proposed that the audit is to be carried out by a third party (TPA), who audits the data from time to time and data which are available to the client by passing the load and the cost for validation and downloading data at the local level to the client.

Practically, the data owner has assigned a secret cell that uses it to process, the file that is divided into several blocks. Before sending the file and the verification parts to the CSP, a part of the public verification information is generated and stored in the TPA. As soon as a data owner requests, the TPA uses a data retrieval protocol and then enables auditing or controlling data integrity by using the public verification information. The perception of this architecture is that it can be implemented in the TPA, without having to include the owner of the data. Authors [102] have requested that third-party privacy, auditing problems and data integrity is resolved by means of the TPA, and the integrity audit in this paper should be supported by using the homomorphic encryption. As a solution both data collection technicians are offered at the same time for the integrity and privacy of the data, in order to influence efficiency of the TPA.

4.4 Encryption and Decryption Techniques

For the security of cloud services, encryption is a technique that for many researches has been the main object used to bring in the cloud data. One way to solve this problem is to provide a homomorphic encryption scheme where we can process the data without having to cite the data, which is a practical solution. Although many customers find it difficult to determine their own data location but Provable Data Possession (PDP) technique, it specifies details of the server specifications that we have changed on the data. The only way to increase the CSC's confidence is an increased security transparency for cloud environments and the transparency of the data processing by the CSP. The cloud service provider remains a major factor in securing services and the CSC with enough information to demonstrate that the CSP is appropriate for its sensitive data [20].

The security transparency of the cloud is seen as an agreement between the CSP and the CSC as the third party in the SLA case. Part of this agreement should be the CSC's and the CSP notification of any incident occurring in their infrastructure. It is necessary that the smallest incidents be reported and the CSC is notified in a timely manner. The CSP should provide a shield from the SLA and also have a certificate issued by specific bodies for that purpose, ensuring that the CSP provides an in-house and efficient security. But there is

also magnesium where this certificate does not guarantee us that this security will exist for a long time. The danger lies in the fact for systems that are offered as cloud services, for various reasons we modify or change the security mechanisms and then go into an ineffective state. We know that many customers, using multi-tenancy, have the opportunity to use the same space and infrastructure in these audit situations that are expected to provide the right level of security, becomes less practical [20], especially if the security audit is accomplished by unreliable parties to the CSC. By exploiting this "gap", the authors of [103], for controlling the security for the SaaS in cloud is based on the multi-agent system (MAS), finally it dynamically executes the virtual machine audit. All this has been achieved by using the Security Service Level Agreements (SSLA) model, which enables the definition of monitoring events and also reviews the business process for the company to proceed.

Based on [20] current proposals such as: encryption, the SLA and virtual monitoring machines to ensure that security activity is completed, this activity includes ongoing investigation and reporting on the accuracy, efficiency of security mechanisms that are established by the CSP, STMA should be respected in the cloud computing. We will list some points and we will discuss each of them:

1. The STMA is based on cloud services:

This will include the creation of an approach that will help evaluate the rankings of the cloud providers based on their security adequacy, security transparency level, and the CSC audit provision.

2. Engineering services provided with the use of the STMA:

This point is related to the top point for elaborating a conceptual model and suitable design for the cloud environments. The main goal is to create engineering methods, which will be part of the software that will take the CSC's requirements in terms of the STMA, in which the CSP will have the design ambiguous space and strategy to meet these requirements.

3. Designing Architecture and Methods to Implement Security Transparency and Mutual Audit:

The two top points can be said to be relevant, and this point is about: differentiating services which are not in the proper security level to use the CSC, at all times collecting information on security support for compliance. The requirements for the services provided by the CSP, as well as the dissemination of security information with the CSC**.**

The Security Committee has provided some solutions which may help prevent some security challenges. As a solution, they include encryption mechanisms, the SLAs, and virtual monitoring mechanisms.

Therefore, as said above, cryptography is a field which deals with plaintext, cyber text and vice versa..

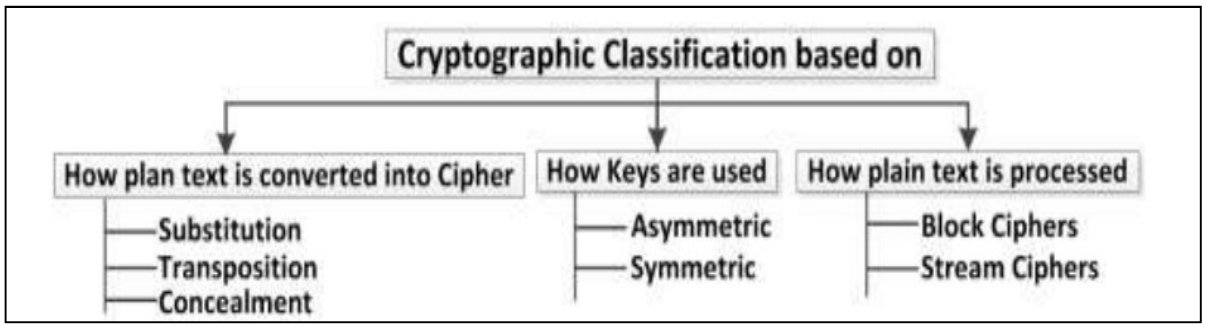


*Figure **16**. Classification of algorithms [113]*

There are different ways of classifying algorithms but the most important one is based on the managing of the keys [114]:

1. Secret Key Cryptography, known as Symmetric Key Cryptography and
2. Public Key Cryptography, known as Asymmetric Key Cryptography.

4.4.1 Symmetric Cryptography

This type of encryption is realized as follows: person A, uses a key for encryption of text known as *Cipher text*, then person B, for decryption of text known as *Plaintext* uses the same key. The main challenge at this type of encryption is the distribution of the key between A and B, because the same key is used for processes encryption and decryption, this type is called the *symmetric encryption*.

In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. The following example describes the scheme of the symmetric encryption and decryption. Thus, it is called one-time-pad encryption schema SE = (K, E, D), for generation of the key it uses algorithm that generates random data and transforms them into random k-bit string K.

The following figure shows steps [115]:

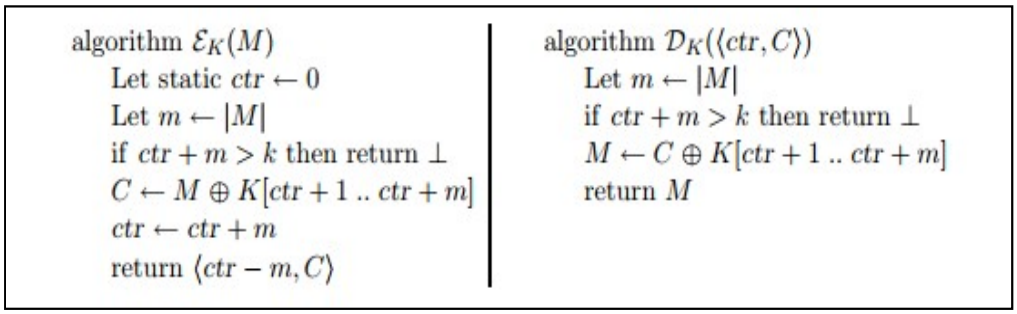


*Figure **17**. The schema of symmetric encryption and deencryption*

According to [*113*], there are some issues in the symmetric cryptography in cloud computing defined as follows:

- *Security key exchange in cloud computing.* At the symmetric encryption receiver and sender use the same key in both main processes. If, for example for any particular reason, third party gains access of the secret key, we are to face a very risky situation. As a solution may be seen the change of the secret key from time to time or the key must be saved to a safer place.

- *Another problem may be the case when the receiver gets the information modified by the other party*. Hackers get to the encryption key and modify the information, which information is sent as modified. It is easy that agreements can be reached between the communicating parties because they use the same key in both cases. As a solution to enforce the process of communication is the Digital Signatures or the Hashing functions.

- *Tools used for the hacking of symmetric encryption.* Hackers use other brutal forces to combine different characters that use different bases of algorithms, so they can reach the encryption key. Then they can easily get the information they need.

For the proposed model [93, 108], we were determined to use some symmetric algorithms as follows:

4.4.2 Data Encryption Standard-DES

Des is an algorithm designed well and very strong. This type of algorithm was proposed in 1977 by the National Institute of Standards and Technology (NIST) and was published as the FIPS-46, [*116*]. It was decided that the standards should be revised every 5 years, if necessary be adopted even though it is required to recertify it, however the DES has always fulfilled the standards for recertification [*115*].

The function of this algorithm will be described in two cases:

- during the process of encryption, it receives a 64 bits plaintext and forms also the 64 bits cipher text, and
- during the process of decryption receives the 64 bits cipher text and creates 64 bits plaintext. Also, in both cases it uses the 56 bits, both for encryption and decryption.

The process of encryption is based on P-boxes or known as permutations. It starts with two P-pox and continues to sixteen rounds festal. For each round a new key is used generated based on a determined algorithm, Fig.18 [116]

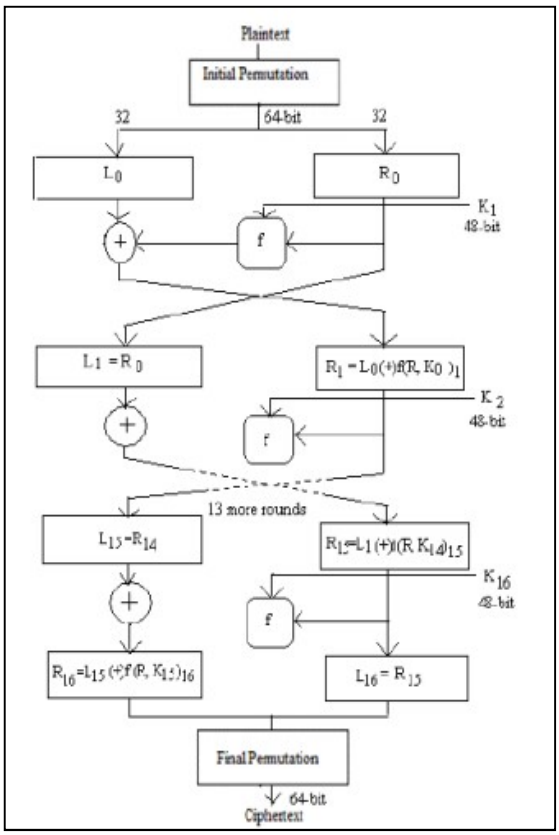


*Figure **18**. Encryption with DES*

During an average process for typical software we use the DES using 80 cycles per byte. This happens since the DES is designed much earlier than the hardware use today. [*115*]

4.4.3 Triple Data Encryption Standard -3DES

The 3DES is an algorithm that is designed to cover the issues emphasized at the DES. The DES uses 56 bits size and is not considered appropriate for sensitive data. The 3DES uses the same work logics as the DES, but it only increases the size of the encryption key, using the application of algorithm three sequential times with different encrypting keys.

The size of the key is 168 bits or 3x56. According to [*115*] for the main processes like Encryption-Decryption three modules of keys are used K1, K2 and K3. We offered a few options which support this algorithm:

- The first option uses independent key from each other (K1≠ K2 ≠ K3).

- The other option uses three keys for manipulation, where two of them are the same (K1 ≠ K2 and K3 = K1). This makes way to create the generation of other keys.
- The last option where the three generated keys are the same ((K1 = K2 = K3)) this option is the same with the DES algorithm.

What makes this algorithm different from the DES is that the encryption is repeated three times, this affects directly increased level of encryption and the average time of execution of the encryption.

4.4.4 Advanced Encryption Standard - AES

This algorithm can be known as Rain Doll, it takes part at symmetric algorithm block cipher that can encrypt blocks of the data using one of the symmetric keys such as 128, 192 or 256 bits, and this is the algorithm which replaces the DES, [117]. These keys are generated by the random rotations that can be done for 10, 12 or 16. The reason why it is known as the replacement of the DES, it is because the DES had a small key length. Therefore, this algorithm was proposed as a standard in the summer of 2001 from National Institute of Standards and Technology (NIST/USA).

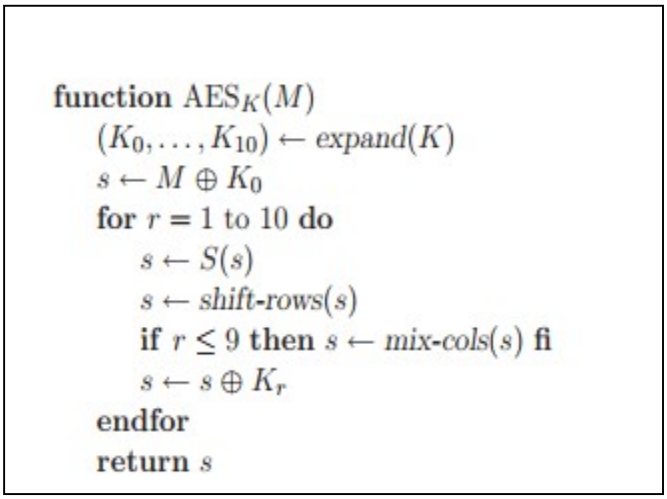


*Figure **19**. The function of AES*

Based on the length of the block of data, this algorithm supports three standards such as the AES128, the AES192 and the AES256. The above figure shows the way of functioning

of the AES, as introducing parameter is variable M and after processing it as an output variable. Every completed roundabout it is known as round. It is seen that this algorithm consists of 10 identical rounds except each round uses special sub key and therefore last round calls on the mix cols method() [115]. Every round realized in the AES, is not connected between them and each step is independent and all this comes as a result of the changing variable S and also matrix's mix-col is inverse.

4.4.5 Asymmetric Cryptography

It is a different concept from the symmetric encryption. The main difference is that now we use different keys for the process of encryption and decryption. Each receiver is given a *private key*. The idea of the key being known from one party only, makes the method of encryption more special. The key used for the encryption process is known as a *public key*. Considering the proposed model [93, 108], we were determined to use the some asymmetric algorithms as follows:

4.4.6 Diffie Hellman - DH

Authors Whitfield Diffe and Martin Hellman in 1976, published a new solution that no one had proposed before, cryptography with two related keys one public and one private, which use the secure sonication protocols, [118]. It is known as algorithm that enables the creation of a joint identity for two systems although these two systems have never had any communication with each other, there should be created a communication line to use it to exchange the encryption keys in a secure way. The DH is usually utilized when you encrypt data on the Web utilizing either the SSL (Secure Socket Layer) or the TLS (Transport Layer Security). The Secure Shell (SSH) protocol also uses the DH, [119]. The DH is known as a strategy to ensure exchanging the data encryption keys. This is functional when making this between two unknown systems up to now as joint "share secret" [118].

This public key framework is created in a way when even it is public one it cannot reach the private key, although both keys are made secretly and are connected to each other. We have used the usual actors for communication: Alice and Bob.

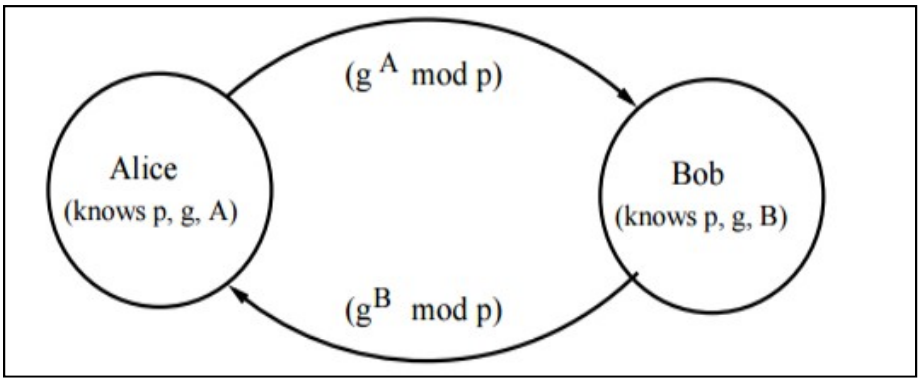


*Figure **20**. The function of Diffie-Hellman*

Steps how this algorithm functions [119]:

i) Alice and Bob agree on a prime number p and a base g.

ii) Alice chooses a secret integer a, then sends Bob

$A = g^a \mod p$

iii) Bob chooses a secret integer b, then sends Alice

$B = g^b \mod p$

iv) Alice computes

$K_1 = B^a \mod p$

v) Bob computes

$K_2 = A^b \mod p$

vi) Alice and Bob now share a secret ie., both Bob and Alice can use this number as their key

Proof for Diffie-Hellman

i) Alice has computed

A = g^a *mod p*

$K_1 = B^a$ mod p

ii) Bob has computed

B = g^b *mod p*

$K_2 = A^b$ mod p

iii) Alice has

$K_1 = B^a$ mod p

$= (g^b)^a$ *mod p*

$= (g^a)^b$ *mod p*

$= A^b$ *mod p*

iv) Bob has

$K_2 = A^b$ mod p

$= (g^a)^b$ *mod p*

$= (g^b)^a$ *mod p*

$= B^a$ *mod p*

v) In the end

$K_1 = K_2$

The advantage of the algorithm Diffie-Hellman, from [119]:

The security factors with respect to the fact that solving the discrete logarithm is very challenging and that the shared key (i.e. the secret) is never transmitted over the channel itself. The disadvantage of the algorithm Diffe-Hellman, from [119]:

The fact that there are expensive exponential operations involved and the algorithm cannot be used to encrypt messages, it can be used for establishing a secret key only, but there is a lack of authentication. There is no identity of the parties involved in the exchange. The computational nature of the algorithm could be used in a denial of service attack very easily etc.

4.4.7 El Gamal

Before the algorithm El Gamal, in the exchange of security the keys were proposed in a secure channel, for Diffe-Hellman algorithms, otherwise this encryption technique was known as the "Di-e-Hellman key exchange". This encryption technique includes the

sender that encrypts with a public key and the receiver that decrypts with a private key. After this algorithm it was proposed the El Gamal algorithm and it is said that the El Gamal algorithm is based on the Diffe Hellman key exchange, [120]. In 1995 Taher Al Gamal proposed the algorithm based on the encryption of public and private keys, the field of security of this algorithm was based on the Discrete Logarithm Problem (DLP).

Therefore El Gamal algorithm is characterized for the way of functioning, where the functioning procedure for encryption and decryption is made in specific ways. For the generation of these keys we should follow these steps, [121]:

1. Prime and Group Generation
2. Private key selection
3. Public key Assembling
4. Public key publishing

To explain the workflow of the El Gamal algorithm we have used these data: A-Sender, B-Receiver and C- bad intentioned party.

Step I:

B, perzgjedh keto informata:

i) Llarge prime $\boldsymbol{p_A}$ (>=three digits),

ii) Primitive element $\boldsymbol{\alpha_A}$ modulo $\boldsymbol{p_A}$,

iii) A (possibly random) integer $\boldsymbol{d_A}$ with $2 \leq \boldsymbol{d_A} \leq \boldsymbol{p_A} - 2$.

Compute:

iv) $\boldsymbol{\beta_A} \equiv \boldsymbol{\alpha_A}^{\boldsymbol{d_A}} \pmod{\boldsymbol{p_A}}$.

Public key is $(\boldsymbol{p_A}, \boldsymbol{\alpha_A}, \boldsymbol{\beta_A})$.

Private key is $\boldsymbol{d_A}$

Step II:

A, encrypts a short message M ($M < \boldsymbol{p_A}$) and sends it to B:

i) Chooses a random integer *k* (which he keeps secret),

ii) Computes $r \equiv \boldsymbol{\alpha_A}, k \pmod{\boldsymbol{p_A}}$ and $t \equiv \boldsymbol{\beta_A}\, M \pmod{\boldsymbol{p_A}}$, and then discards k.

iii) A, sends his encrypted message (r, t) to B

Step III:

B,

i) Receives the encrypted message (r, t),

ii) Decrypts (using private key $\boldsymbol{d_A}$) by computing $\boldsymbol{tr}^{-\boldsymbol{dA}}$

If person C, intercepts the ciphertext(r,t), cannot perform the calculation above because he/she doesn't know $\boldsymbol{d_A}$.

$$\boldsymbol{\beta_A} \equiv \boldsymbol{\alpha_A} (\text{mod } \boldsymbol{p_A}), \text{ so } \boldsymbol{d_A} \equiv \text{L } \boldsymbol{\alpha_A} (\boldsymbol{\beta_A})$$

If C can find $\boldsymbol{d}_A$, than can compute a discrete log in the large prime modulus $\boldsymbol{p_A}$, presumably a computation that is too difficult to be practical, [122].

As an advantage of the El Gamal algorithm is the non-determinism-encrypting, same plaintext is never calculated in the same form of cipher texts, it is depended directly on the parameter k generated randomly. We can also say that as advantage the El Gamal encryption is used in the free GNU privacy Guard Software, recent versions of the PGP, and other cryptosystems, [120].

Based on the same resource [120], as an advantage maybe it depends on the random amount which has a direct impact on the speed and especially in signing. However, as a disadvantage it may be the cipher text, which is twice as long as the plaintext.

4.4.8 Rivest-Shamir-Adleman RSA

Algorithm RSA was designed in 1978, by a group of researchers: Ron Rivest, Adi Shamir, and Leonard Adleman. The cryptosystem for exchanging the public keys made this algorithm known, digital signature and data encryption in blocks. This algorithm uses different size keys. Therefore, this asymmetric algorithm is based in the theory numbers,

[123]. It uses two primary numbers to generate public and private keys, too. The ender uses a public key to encrypt the message then the receiver uses a private key for decryption. The main processes included on this algorithm are: key generation, encryption and decryption. The RSA has some disadvantages during its design, if the two random numbers for key generation are too small then there will be a chance to raise the number of attacks. In the contrary these two numbers generated based on the random theory, they may be greater when the execution time lasts. In order to have better results during the key generation for this algorithm, both numbers should have approximate values to each other, a thing which is often difficult

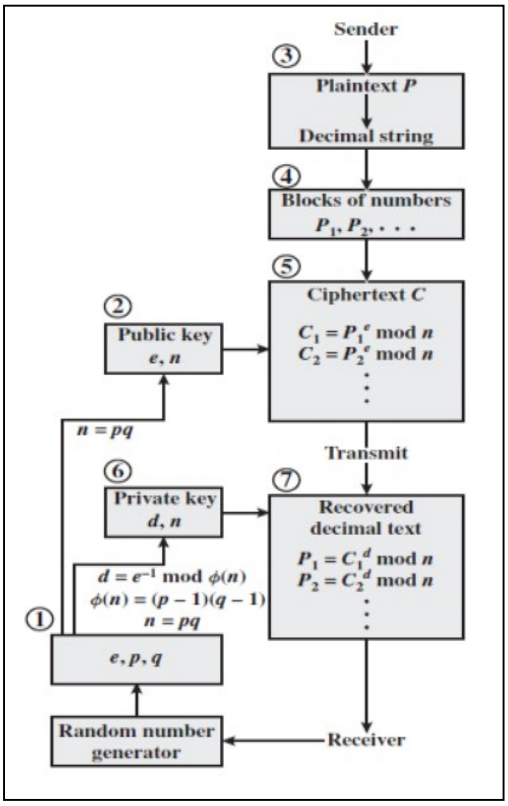


*Figure **21**. RSA processing of Multiple Blocks [123]*

The above figure presents the steps to be executed for RSA algorythm.

Key Generation [123]:

1. Choose two distinct large random numbers p & q , p ≠ q.
2. Compute n= p × q.

3. Calculate: phi (n) = (p-1) (q-1).

4. Choose an integer e such that 1<e< n

Ciphertext: C= Pe mod n.

5. Compute d, d × e = 1 mod phi (n); d is kept as private key exponent.

6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption Plaintext:

P < n Ciphertext: C= Pe mod n

Decryption Ciphertext:

C Plaintext: P=Cd mod n.

4.4.9 Hybrid Cryptography

Refer to [124], one major disadvantage of the traditional crypto system is that if the symmetric encryption/decryption key is revealed during key exchange or by any other means, the whole encryption/decryption process becomes unsafe. Another disadvantage is that if at any stage there is a need for changing the symmetric key, the key transfer process needs to be repeated. In order to address the above-mentioned security problems with the use of the symmetric-key algorithms, the public key algorithms are combined with symmetric-key algorithms to perform the key-exchange.

The design of the proposed hybrid crypto system it will be based on performing encryption and decryption using symmetric key algorithm but it uses public key algorithm to encrypt the symmetric key before performing the key transfer.

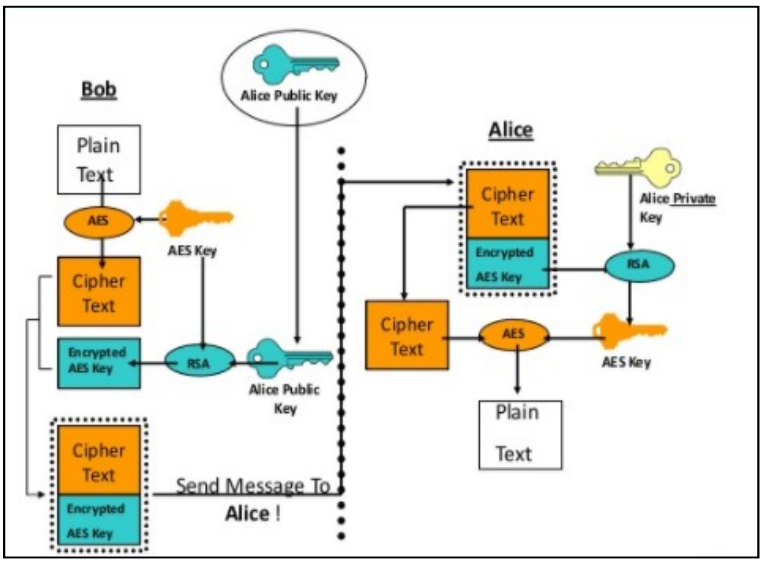


*Figure **22**. Schema for hybrid function [125]*

The fig. 22 shows the block scheme of hybrid encryption function, it also shows that the hybrid cryptography is based on the encryption data using parts of symmetric and asymmetric encryption when combined. Based on the researches [126] [127], symmetric algorithms are much faster than asymmetric algorithms. Hence, asymmetric algorithms, because of using both private and public keys are more secure than symmetric algorithms. Proposition for a hybrid cryptography was a very good solution, because it offered speed and at the same time security for the data. This type of encryption did not require exchange of keys from sender and receiver but used mathematical operations for their calculation, [128].

In the proposed model from Fig. 22, we are going to use the hybrid algorithm Fig.23, how to send partitions in cloud as in Fig 31, Case I. This encryption technique cannot use Fig. 32, because in advance we choose algorithm and continue the encryption of all partitions with the same algorithm.

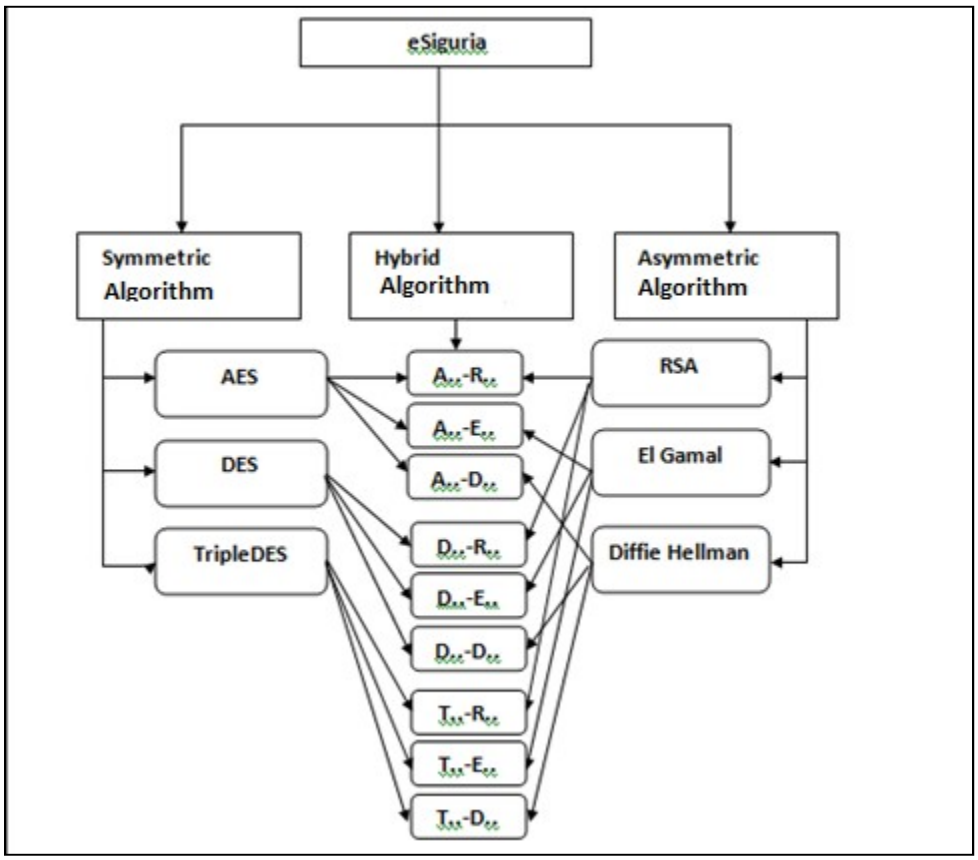


*Figure **23**. Hybrid algorithms used in the app. eSiguria*

CHAPTER V

Part II:

5 PROPOSED MODEL ANALYSIS FOR CLOUD SECURITY CONTROLLED BY END USER-ITSS

In the model proposal we have three following elements as basis to fulfill the security system requirements:

- Confidentiality
- Integrity
- Availability

These are elements that include a set of rules which limit access on the information, offer reliability and accuracy, hence realizing reliable access on the information by the authorized persons only [104]. All these aspects have been initial elements on the basis used in our proposed model. Elements in our model will be supported by the hash functions [104, 105], as a special part in our scheme. We consider evaluation of sensitive reading to be very important, which will be calculated based on the value of availability, confidentiality and integrity [106]. The value of this parameter is assigned by the owner [107].

$$SR[i] = (C[i] +(I[i] + 1/A[i] *10))/4 \quad (1)$$

Where: C[i] = Confidentiality, I[i] = Integrity, A[i] = Availability

The first main task it was to propose safety model in cloud, which we will be based on our model, as shown in Figure 24. Then, an implementation of this proposal model to systems which offer services in cloud was designed and implemented in the following CHAPTER. Formula (1) shows a relation among these parameters which are necessary to provide security in cloud; these elements are components of our proposed model, offering a safe access to the data.

The proposed model is based on two main factors Fig. 24, **Null Hypothesis:**

- Possibility of categorizing the level of security, based on the combination of security algorithms and
- All the control of security depends on the end user – the ITSS of a certain organization.

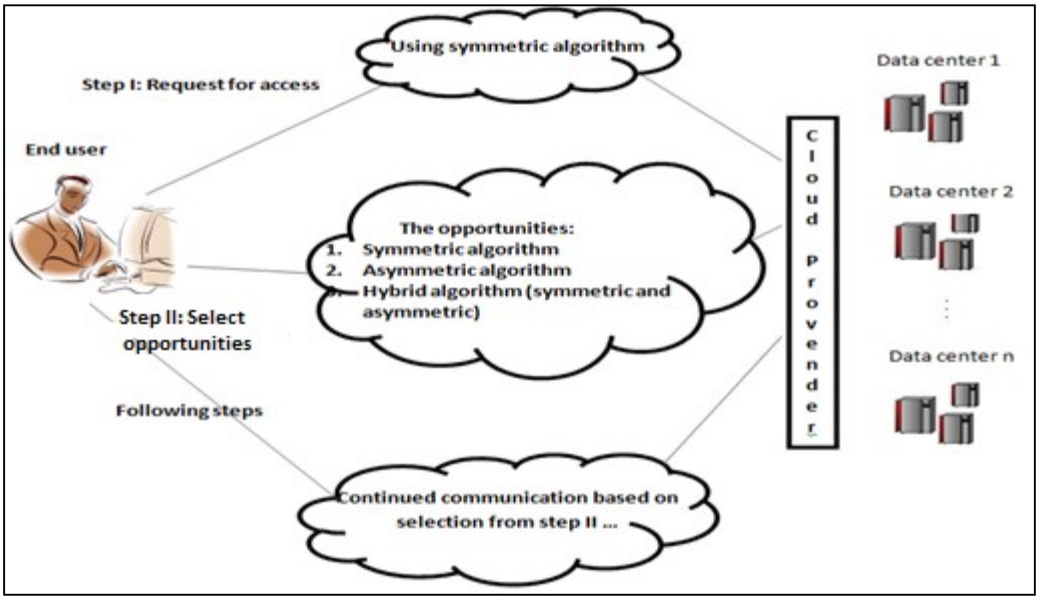


*Figure **24**. Proposed model for security in cloud computing controlled by the ITTS, [93,108]*

Proposed model enables increase of security in cloud Fig. 23, offering three proposals of choices depending on the sort of sensitive data:

Proposal I: Security is based on the choice of the end user the ITSS, depending on the information the proposed model offers.

Proposal II: Based on the features of the file, possible algorithms are proposed and the length of keys to the user, then the user makes a choice.

Proposal III: security is based on the file cryptography by the client, by keys generated locally to the client. Thereafter, the file is partitioned and encrypted in particular parts (P1, P2 ,…, Pn), each part can be stored in different clouds. A new P0 file contains selected algorithm, indexing and the position of the file. The P0 file is significantly smaller, encrypted by a more powerful algorithm and can be stored anywhere in cloud.

During this work it is seen how the client and the server communicate, there is defined an executable protocol which verifies the data requested by the client. From the research [100], Proof of Retrieval (POR) protocols have been proposed, whose task is for large files to prove that the file was not deleted or modified during the communication process. This encryption technique takes the file and then encrypts blocks to randomly encrypt the file. After this step, the cliché requires its data to depend on their sensitivity to determine the manner of their archiving. If the deletion or change of data occurs, the customer will return to the customer. A similar solution is also proposed for the POR, which is the Provisional Data Possession (PDP), proposed by the paper [101]. The PDA uses a technician who verifies the possibility of the data placed in a secure location, and there is the possibility of manipulating your data. There will be proposals the use the scheme known as Homomorphic Linear Authenticator (HLA). The HLA proposes a file to be divided into several blocks, and the generated vector verifies the position of the blocks, the server's task is to homomorphically construct the value of the polynomial which indicates the combination of the vector blocks and their storage on the server. Some research like [20] have exploited this idea and then presented additional elements.

CHAPTER VI

6 IMPLEMENTING PROPOSED MODEL FOR CLOUD SECURITY CONTROLLED BY END USER-ITSS

6.1 Implementation of the proposed model

The proposed model [93, 108] is implemented on the .NET Framework 4.5, which is developed by Microsoft. The program “eSiguria” was developed in the c# programming language.

During the implementation the proposed cloud security model is named as "eSiguria". It is an application that we need to have users and password for accessing, from an administrator of an institution.

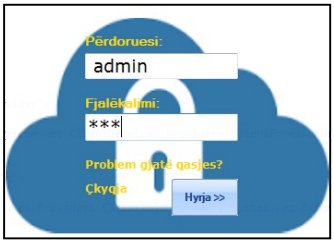


*Figure **25**. Login form for access*

The "eSiguria" application consists of three main modules, Configuration, Document and Administration.

Depending on what role users are playing, they will be active in these modules.

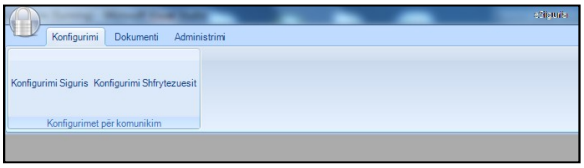


*Figure **26**. Modules in "eSiguria"*

In the Configuration module, only one person may have access to the institution. This person in the proposed cloud security model treated as an IT Specialist. Knowledge about the mode of communication and the opportunities offered by the application is available to this actor.

Part of the *Configuration* module are:

• *Security Configuration*: this form populates with data and details about security configurations. This can be called differently and permanently the communication rule, which is created once and then exploited by the users. First of all, there are different rules of communication within an institution and depending on the sensitivity of the data that the users complete in the institution.

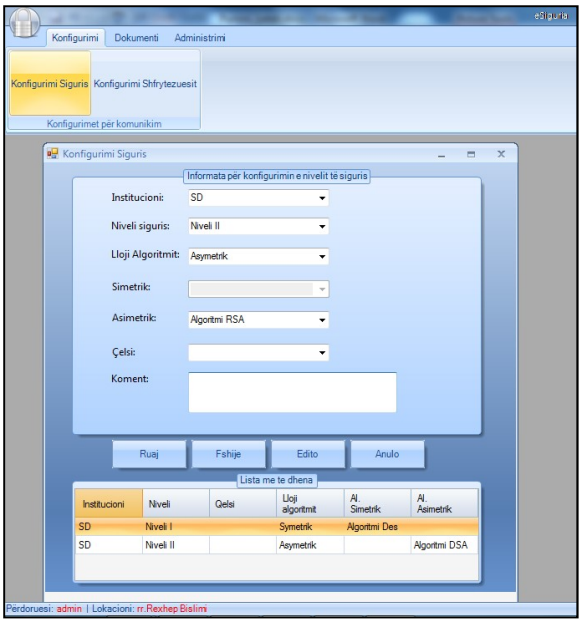


*Figure **27**. The form of configuration of "eSiguria"*

User Configuration: user Configuration Forms makes the connection to the security configuration form to the previously registered user.

Part of this form is: No Configuration to be selected.

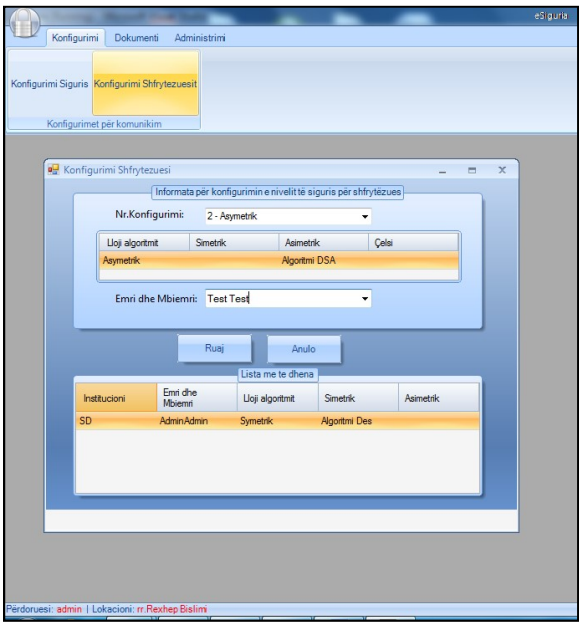


*Figure **28**. The form of user configuration*

The other module is the *Document*, part of this module is form *Send Document*. This module is active for any user who has an account in the institution.

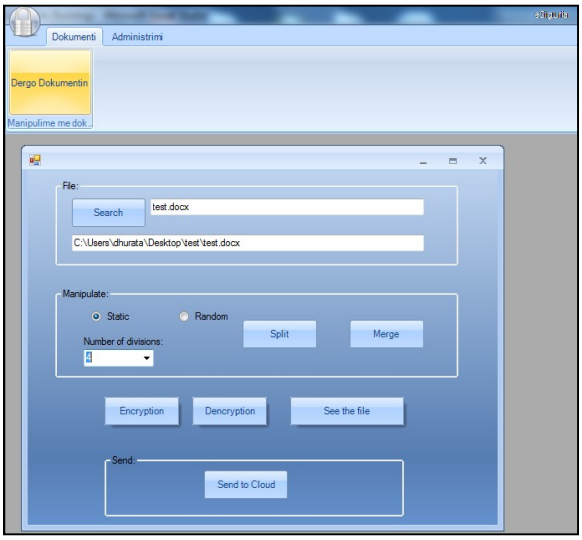


*Figure **29**. The form of sending documents to the cloud*

Based on the security configuration settings that are set for this user, the way how to send the cloud file has been completed. What this user is dependent on this section is the location of the file and the file sharing method.

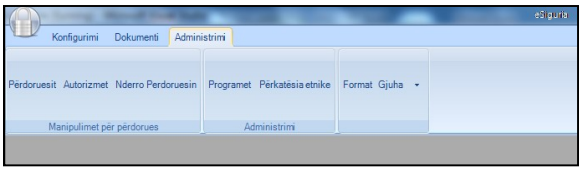


*Figure **30**. Module of Administration*

Part of the *eSiguria* application is also the administration module, which consists of standard forms for administering an application, and has access to all users in this application.

From Fig. 31, it is obvious that the entire workflow depends on this model is end-user is based on. Configuration of this communication rule is accomplished by an IT Specialist of the organization (as explained by the implementation part of the *eSiguria),* then all the communication used for other members is based on this rule.

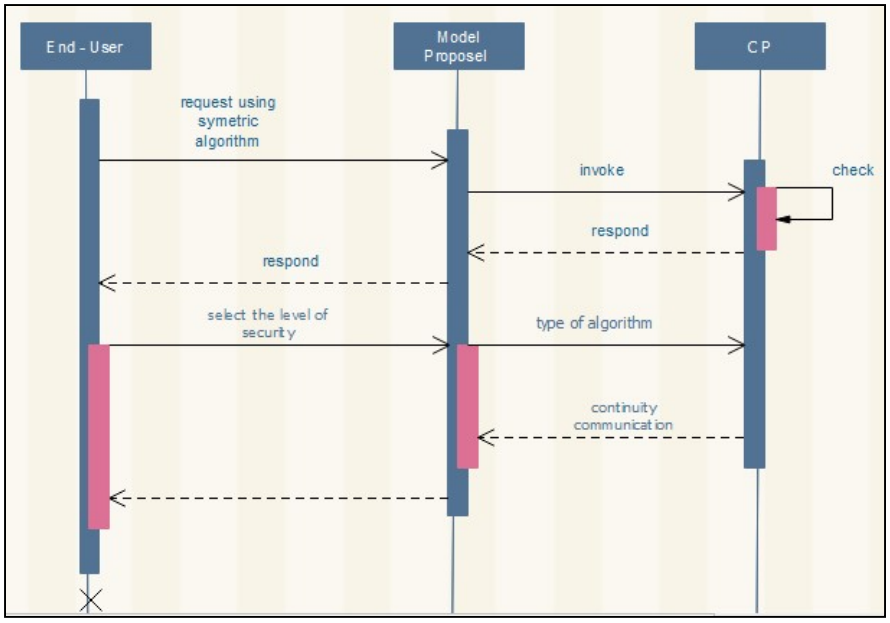


*Figure **31**. Workflow for the proposed cloud security model*

For the database management of eSiguria application, we use SQL Server.

In this figure it is seen that the NoConfiguration field is also recorded with its details in the Configuration table, then those rules placed are transferred to the tblSpreadsheet and tblFile.

In Fig.31, shows the database presenting the tables of the proposed model

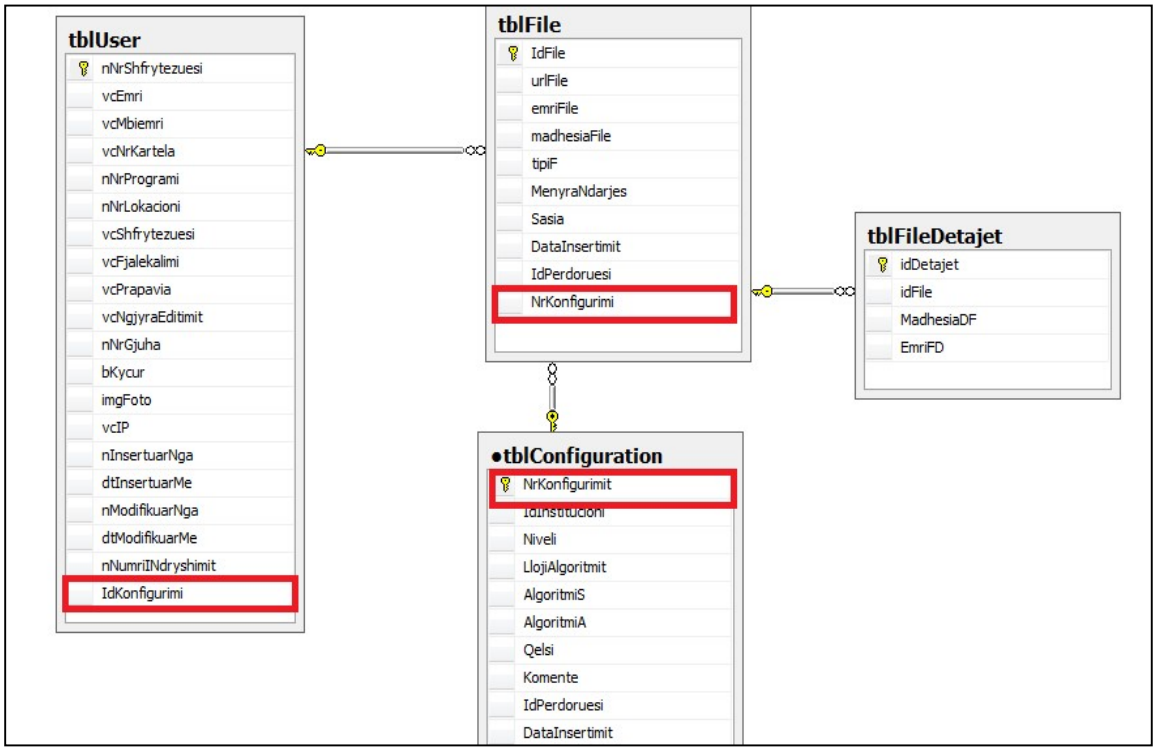


*Figure **32**. Configuration of security for users*

The tblconfiguration, which determines rules of configuration by an ITSS except him or her, no one else, has any right to insert data from this table.

The tbluser (general data for the user and as additional field is number of configuration, which comes from Fig. 32, depending on which type of configuration to choose for the respective user).

The tblFileDetails (General information for managing files and its partitions). The security rules determiner is the ITSS (the person who is aware for the flow of process for every level of security), Fig. 31. Persons within the organization should not be aware of these data. It is sufficient for an ITSS jut to have access on it. According to the above named

scheme, it is obvious that the accesses are minimal because of reduced mistakes by the employees within the organization, even if they have other intentions, they are no right to interfere in the part to secure configuration.

6.2 The strategy of encryption of the proposed model

To provide a secure communication in the communication channels we use the cryptography of data. As technology increases, the need to provide new encrypting strategies increases as well [6] for the only reason that data can be transferred from point A - end user to the point B - to database, to be secured.

For data encryption we are able to use two techniques of cryptography:

Symmetric Algorithm, where the same key is used for encryption, decryption and

Asymmetric Algorithm, however different keys are used for encryption and decryption.

Our proposed model not only uses these two techniques of encryption but uses the combination of both symmetric and asymmetric algorithms as well, known as the hybrid algorithms.

The flow of steps for our proposed model to increase the security in cloud and the steps, we need to follow in the proposed model:

Step I: Access to the program using password and user name.

Step II: Selection level security of the data based on the sensitivity of data (Options I, Options II or Options III)

Step III: Selection of algorithms for data encryption

Step IV: Then selection of the way of sending files in the cloud

Proposed model supports two ways of sending files to the cloud, third hypothesis:

First Case (Case I): Fig. 33 is based on the partitioning of file then encrypting these partitions by algorithms which the IT Specialist selects, depending on the sensitivity of data in the organization. This alternative is preferable in cases where the possibility of starting to read the partitions before retrieving completely all the parts of the file. For example a video starts to play (meaning there won't be delays for the client) before retrieving other parts of the file sent to cloud.

Table 7.Explanation for figure 33 and 34

Abbreviation	Content
p- partition	Part of the file ready for processing.
P1,P2...Pn	Partitions of the file.
P1E,P2E...PnE	Encrypted parts of the file.
CP1, CP2....CPn	Cloud provider that supports the proposed model.

The way of partitioning and cryptography of data in the proposed model

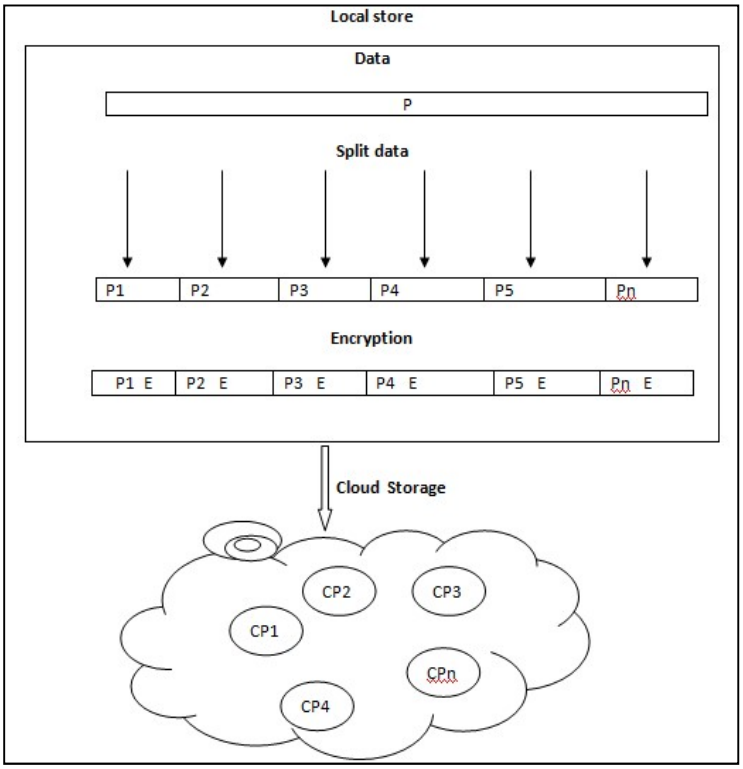


*Figure **33**. Partitioned then encrypted data*

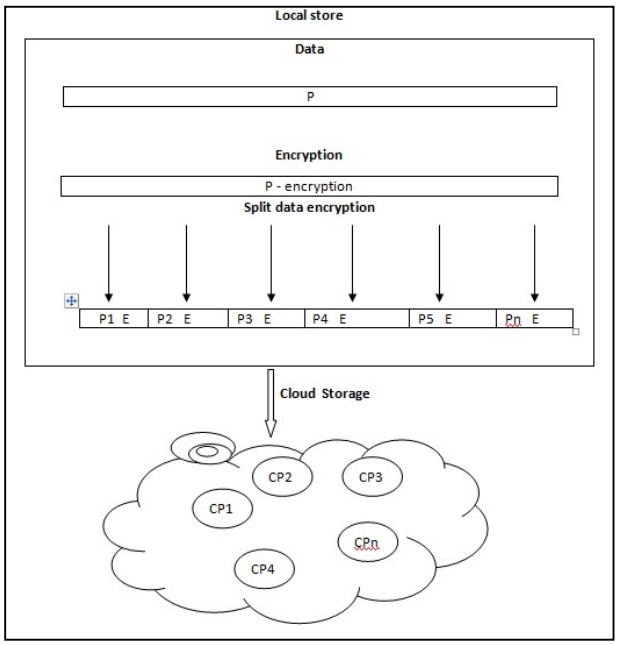


*Figure **34**. Encrypted then partitioned data*

Second Case (Case II): the proposed model, which supports it is in Fig. 34 encrypts the file then it partitions based on the level and algorithm configured by the IT specialist of the organization. The way it is supported by the model it provides higher security because we must have all parts of the file in order to be able to read the data. Usually, this selection is used for data that require a higher level of security because it requires to provide all parts of the file to enable reading the data.

Step V: Distribution of files to the cloud, Fig. 39, shows the scheme of partitioning of files into smaller parts and storing them in the cloud.

Considering the way of partitioning there are three options proposed:

First option: we use the random partition, which is not depended on any parameter. Here it was necessary to determine the minimum of partitions min=1, and the maximum of partitions max=10. These values were determined in the following programming, fig 35.

```
if (RandomStatike == "R")
                {
                    pjesa = GetRandomNumber(1, 10);
                }


private static readonly object syncLock = new object();
        private static readonly Random getrandom = new Random();
        public static int GetRandomNumber(int min, int max)
        {
            lock (syncLock)
            {
                return getrandom.Next(min, max);
            }
        }
```

*Figure **35**. Part of code used to present the implementation of Random partitoning*

Second option – this way of partitioning depends in the number of partitions that is determined by the user. It means that it does not take into consideration any parameter for partitioning, only the value determined by the user, then the same value is used for partitioning. This option was named static option which in programming is easily implemented, fig 36:

```
        if (RandomStatike == "S")
                {
                    pjesa = int.Parse(sasia);
                }
```

*Figure **36**. Part of code used to present the implementation of Static partitoning*

Third option: this way of partitioning is related directly with the size of the file. Based on the file size it is divided in partitions. The comparison is made in the KB and as initial value for 1 partition we have selected from 0 to 500 KB, for 2 partitions, from 500 KB to 1000 KB, continuing up to 10 partitions which applies for files with more than 40000 KB.

The following figure provides block scheme used for this algorithm, Fig 35, as well as the part implemented in programming, Fig. 37.

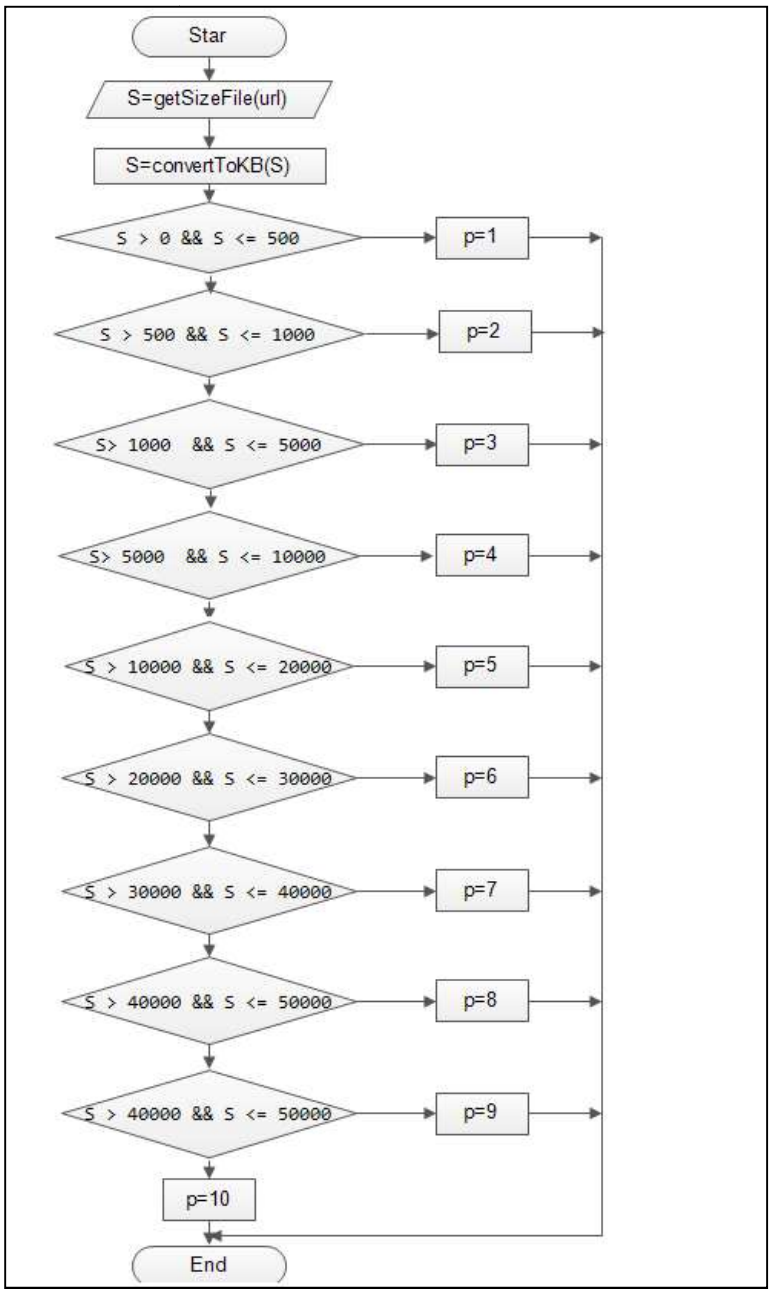


*Figure **37**. Partition Schema based on file size*

```
public int NdarjaNePjese(string path)
        {
            int i = 1;
            int sizeFile = 0;
            String[] sizeArry = new String[] { "KB" };
            int Get_Size_in_KB(ulong sizebytes, int index)
            {
```

```
            if (sizebytes < 1000) return (int)sizebytes;

            else return Get_Size_in_KB(sizebytes / 1024, ++index);

        }
        FileInfo fi = new FileInfo(path);
        sizeFile = Get_Size_in_KB((ulong)fi.Length, 0);

        if (sizeFile > 0 && sizeFile <= 500)
        {
            i = 1;
        }
        else if (sizeFile > 500 && sizeFile <= 1000)
        {
            i = 2;
        }
        else if (sizeFile > 1000 && sizeFile <= 5000)
        {
            i = 3;
        }
        else if (sizeFile > 5000 && sizeFile <= 10000)
        {
            i = 4;
        }
        else if (sizeFile > 10000 && sizeFile <= 20000)
        {
            i = 5;
        }
        else if (sizeFile > 20000 && sizeFile <= 30000)
        {
            i = 6;
        }
        else if (sizeFile > 30000 && sizeFile <= 40000)
        {
            i = 7;
        }
        else if (sizeFile > 40000 && sizeFile <= 50000)
        {
            i = 8;
        }
        else if (sizeFile > 50000 && sizeFile <= 100000)
        {
            i = 9;
        }
        else
        {
            i = 10;
        }
        return i;
    }
```

*Figure **38**. Part of the code providing the implementation of partitions based on the size of file*

To our proposed model distribution of files it has been completed

Based on the number of available Cloud Providers, the space they have and

Random distribution

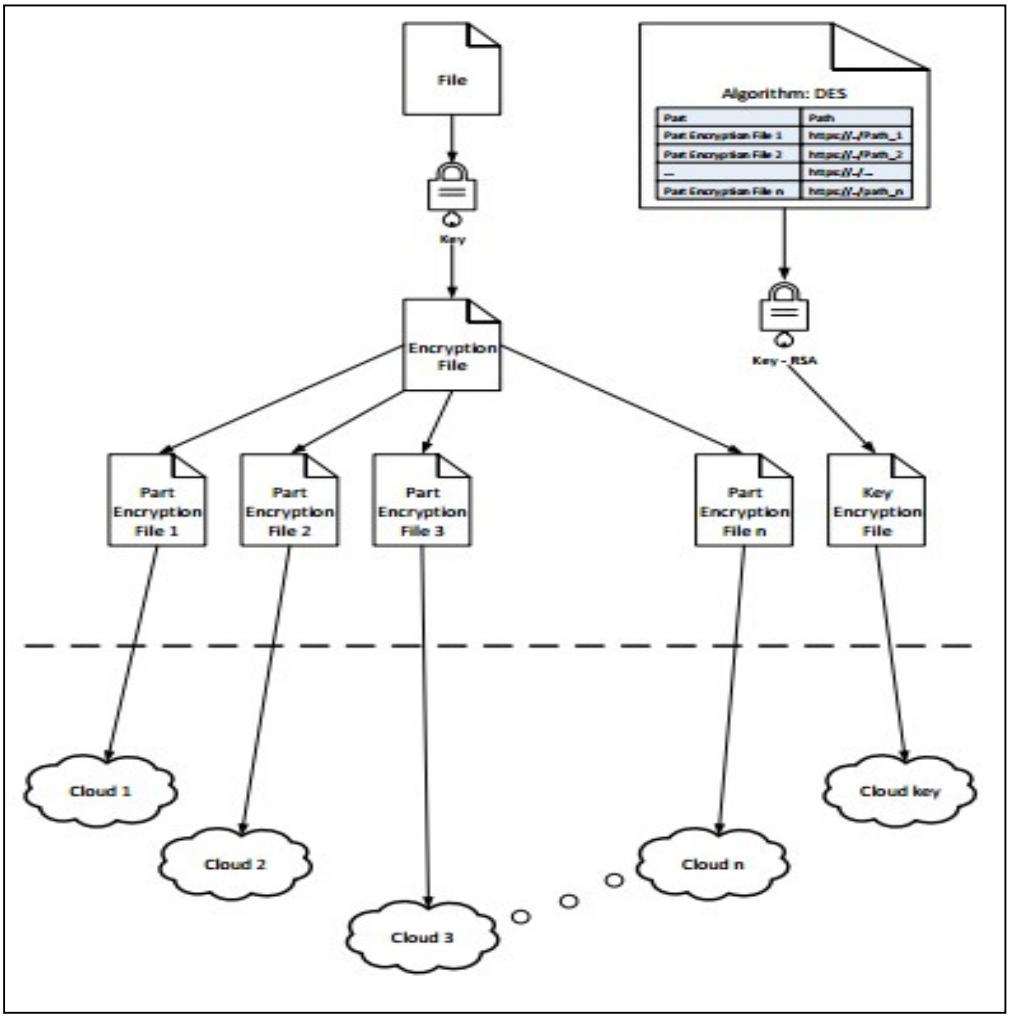


*Figure **39**.Partitioning and distribution of files to the cloud computing*

Despite segments divided depending on the way partitioning we use, another file with *suffix..enc* is generated, which offers general information for the type of algorithm, the way of partitioning, names of the files before and after the encryption (naming of partitioning is random) as well as the keys used for cryptography. In Fig.41 this file is named as the *Key Encryption File*.

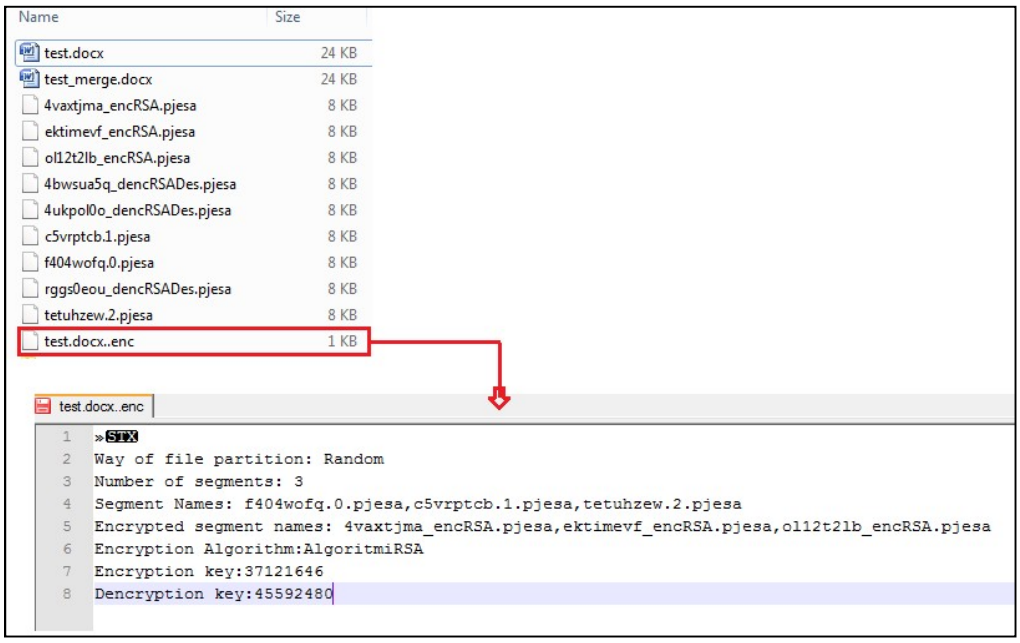


*Figure **40**. Content of the file ..enc*

In Fig. 40 shows a demonstrated case where a test.docx file is used for testing, then we used first level and selected the RSA Algorithm. Partitioning is done randomly, which we selected the option under a), then the partitions are encrypted. The figure shows the case of return, description and the merging and as a result of this option we have the file *test_merge.docx*, which takes us to the first step.

Except classifications we made in algorithms until now, Fig. 16 provides the classification of algorithms based on the ways of processing the plaintext. According to [129], there are two major types of symmetric cryptosystems: Block ciphers (which encrypt a plaintext block into a cipher text, block by mixing it in an invertible way with a fixed key), and the stream ciphers (which uses a finite state machine initialized with the key to produce a long pseudo random bit string, which is the XOR'ed with the plaintext to obtain the cipher text).

Block Cipher- A block cipher is a cipher in which a block of plaintext is treated as a whole and later used to produce a cipher text block of equal length. Typically, a block size of 64 or 128 bits is used. Based on [130], a block cipher algorithm is a basic building block for providing the data security. To apply a block cipher in a variety of applications, four

"modes of operation" have been defined by the NIST. In essence, a mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. The four modes are intended to cover virtually all the possible applications of encryption for which a block cipher could be used.

*Table **8**. Block Cipher Modes of Operation [130]*

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key	Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext	General-purpose block-oriented transmission Authentication
Cipher Feedback (CFB)	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	General-purpose stream-oriented transmission Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	General-purpose block-oriented transmission Useful for high-speed requirements

Stream Cipher- A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. A stream cipher is one that encrypts a digital data stream one bit or one byte at a time [130].

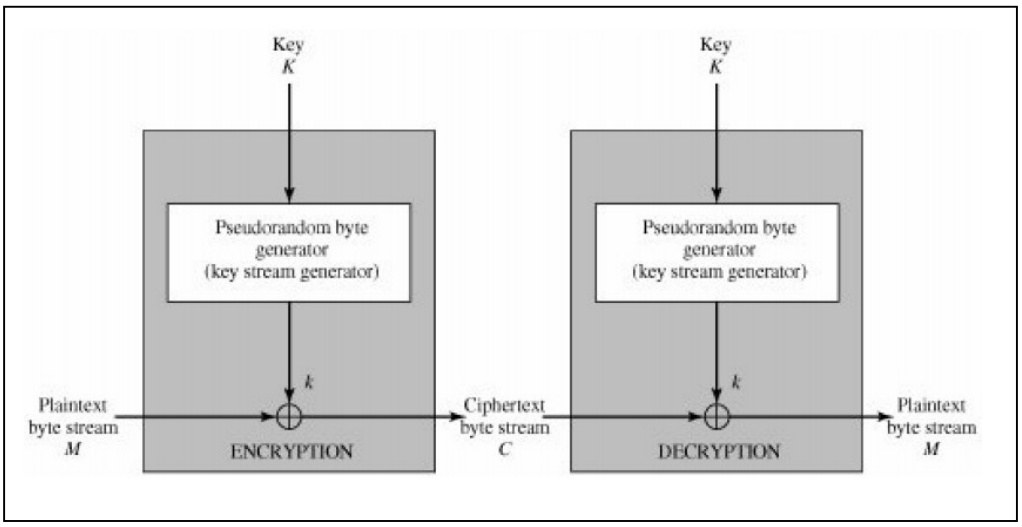


*Figure **41**. Stream Cipher Diagram[130]*

Based on [*131],* the underlying principle behind stream ciphers is as follows:

Let $\boldsymbol{m^{(t)}, t \geq 0}$ be the sequence of message bits. Let$\boldsymbol{z^{(t)}, t \geq 0}$ be a sequence of pseudorandom bits (also called the key sequence). Then$\boldsymbol{c^{(t)} \equiv m^{(t)} \oplus z^{(t)}, t \geq 0}$ **is the sequence of cipher bits. Decryption is done by computing** $\boldsymbol{m^{(t)} \oplus z^{(t)} \equiv c^{(t)}}$ The security of the system depends on the security of the pseudorandom bits$\boldsymbol{z^{(t)}}$.

Stream ciphers are usually classified into two broad categories – synchronous and asynchronous stream ciphers. In the synchronous stream ciphers the key bits do not depend on the message or cipher bits while in asynchronous stream ciphers the key bits depend on the previous cipher and/or message bits. There are two classical models of memory less synchronous stream ciphers – the Nonlinear Filter model and the Nonlinear-Combiner model, *[132][133].*

According to [134] we have shown differences between Stream Cipher and Block Cipher.

Block Cipher	Stream Cipher
Processing or encoding of the plain text is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size here is simply one bit.
The same key is used to encrypt each of the blocks	A different key is used to encrypt each of the bits.
A Pad added to short length blocks	Bits are processed one by one in as in a chain
Uses Symmetric Encryption and is NOT used in asymmetric encryption	High speed and low hardware complexity
Confusion factor: The key to the cipher text relationship could be really very complicated.	Key is often combined with an initialization vector
Diffusion Factor: output depends on the input in a very complex method.	Long period with no repetition
Most block ciphers are based on Feistel cipher in structure	Statistically random
Looks more like an extremely large substitution and Using the idea of a product cipher	Depends on a large key and Large liner complexity
More secure in most cases	Equally secure if properly designed
Usually more complex and slower in operation	Usually very simple and much faster

*Figure **42**. Differences between Stream Cipher and Block Cipher*

In fig. 43. we used Stream Cipher and Block Cipher, Stream Cipher requires smaller infrastructure comparing to Block Cipher. In c#, using `CryptoStream` class, very easily it may encrypt/deencrypt data using Stream Cipher.

```
using (ICryptoTransform cTransform = alg.CreateEncryptor())
                                {
                  using (FileStream fsOutput = new FileStream(output, FileMode.Create))
                {
                      using (CryptoStream cs = new CryptoStream(fsOutput, cTransform,
CryptoStreamMode.Write))
                   {
                       using (FileStream fsInput = new FileStream(Hyrje, FileMode.Open))
                      {
                          int data;
                    while ((data = fsInput.ReadByte()) != -1)
                          {
                           cs.WriteByte((byte)fsInput.ReadByte());
                                                }
                                            }
                                        }
                                    }
                                }
```

```
TripleDESCryptoServiceProvider 3des = new TripleDESCryptoServiceProvider();

    3des.KeySize = madhesia;
    3des.Key = key;
```

```
    3des.Mode = CipherMode.ECB;
    3des.Padding = PaddingMode.None;
    ICryptoTransform ic = 3des.CreateEncryptor();
    byte[] enc = ic.TransformFinalBlock(Hyrja, 0, 8);
```

*Figure **43**. Part of the code from eSiguria, for the use Stream Cipher and Block Cipher*

CHAPTER VII

7 MEASUREMENTS OBTAINED IN THE PROPOSED MODEL

Presenting the results of any scientific research confirms or denies the main idea of that research. This chapter covers different groups of measurements obtained in the application of “eSiguria” in support of hypothesis and our research questions.

For all measurements, we had the following working conditions: Processor: Initial (R) Celeron (R) CPU 1005 M 1.90 GHz, and network details, Ping: 55ms, Download: 15.46 Mbps, Upload: 2.22 Mbps.

All the obtained measurements help to confirm the hypothesis determined in chapter 1. According to scenarios any group presents a scheme used to present the results even the charts and graphics. For more important groups of measurements, we present results through cross tabulations, in order to have a clearer picture of the correlation they have. Throughout all this work, we have used three symmetric algorithms: the AES, the DES, the Triple DES, and three asymmetric algorithms: the RSA Diff-Hellman and El Gamal, as well as hybrid algorithms (combination of both symmetric and asymmetric algorithms), Fig.23. As for the measurements we have used these types of files:

*Table **9**. Files used for measurement*

Type	Size	Comentc
.doc	2969KB	Large
.doc	606KB	Medium
.pdf	606KB	Medium
.png	606KB	Medium
.mov	454KB	Medium

7.1 First part of measurements

For the first part of measurements we have used two types of schema:

- **First schema** – that is connected to *fig. 33* where file is partitioned than encrypted. In this schema, we have used all the above mentioned algorithms both symmetric and asymmetric ones. For example, the following schema, *fig. 44* algorythm AES was taken to devide the file in three partitions ($\boldsymbol{t_1}, \boldsymbol{t_2}$ **and** $\boldsymbol{t_3}$). The time *t* of measurement has started from the reading of the file until the sending of all partitions in different cloud providers, as well as the population with information of partition $\boldsymbol{p_0}$. In *Table 10* this measurement scenario was named "*Scenario: Case_I".*

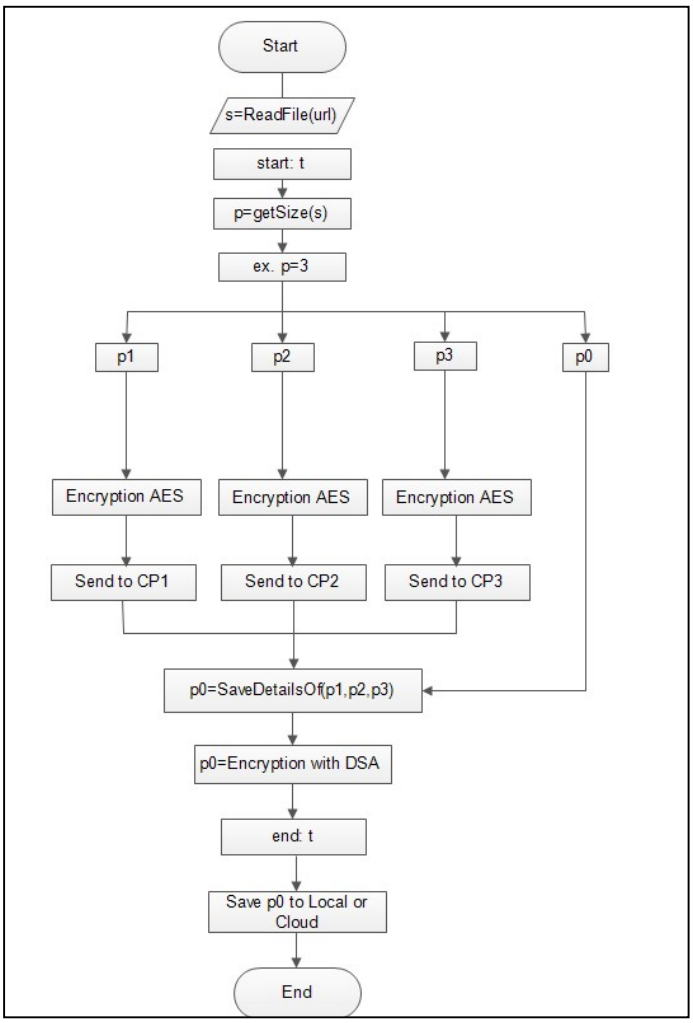


*Figure **44**. Schema of implementation of Case_I, for algorithm AES used at the first group of measurements.*

- **Whereas the second schema** is related to *fig. 34*, the file is encrypted is devided in certain partitions. To start reading this file, we should in advance provide all partitions. Also, for this schema measurements were made for all types of algorithms, asymmetric and symmetric. The time *t* of measurement has started fro the reading of the file until sending it to the cloud in different providers also at this measurement the population of the file $\boldsymbol{p_0}$ with writing is included. In the following schema as an example was used algorithm AES and the number of partitions was 3 ($\boldsymbol{t_1, t_2}$ **and** $\boldsymbol{t_3}$). In *Table 10* this schema was named "*Scenerio: CASE_II*".

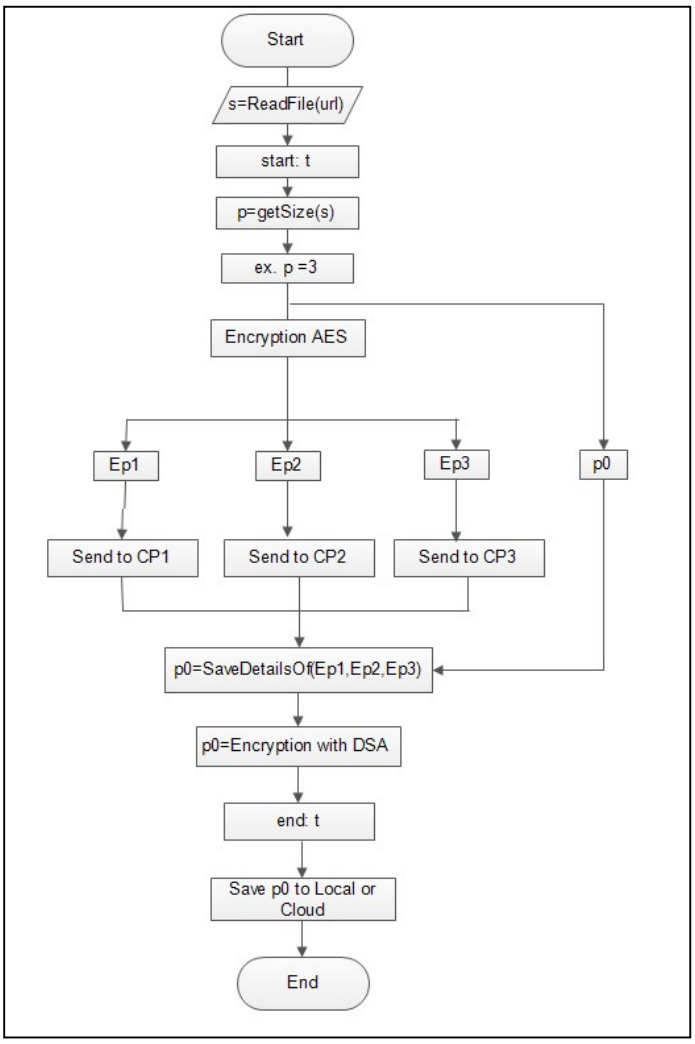


*Figure **45**. Schema for implementation of CASE_II, for algorithm AES used at the first part of measurements.*

Table 10, shows measurements obtained for the scenario from *fig. 33 - Case_I* and *fig. 34- Case_II*, with different features (file size, scenario, process, types of files and different algorithms). All these measurements are obtained for three groups of measurements devided in Group 1, Group 2 (2.1, 2.2, and 2.3) and group 3. Hence, at this table obtained measurements for the groups of measurements are provided in different colors.

*Table **10**. Rezults from the measurements of the first part*

No.	Gr.	File type	Proces	File size	Scenerio	Algorithm		Key length bits	Part/No part	Time/ ms
1	1	.doc	Upload	2969KB	CASE_I	A	RSA	1024	Static/ 3	38009
1	1	.doc	Download	2969KB	CASE_I	A	RSA	1024	Static/ 3	33502
2	1	.doc	Upload	2969KB	CASE_I	S	AES	128	Static/ 3	24896
2	1	.doc	Download	2969KB	CASE_I	S	AES	128	Static/ 3	16644
3	1	.doc	Upload	2969KB	CASE_I	S	Des	128	Static/ 3	28434
3	1	.doc	Download	2969KB	CASE_I	S	Des	128	Static/ 3	21365
4	1	.doc	Upload	2969KB	CASE_I	S	TripleDES	128	Static/ 3	29234
4	1	.doc	Download	2969KB	CASE_I	S	TripleDES	128	Static/ 3	24689
5	1	.doc	Upload	2969KB	CASE_I	A	DH	1024	Static/ 3	40753
5	1	.doc	Download	2969KB	CASE_I	A	DH	1024	Static/ 3	30056
6	1	.doc	Upload	2969KB	CASE_I	A	ElGamal	1024	Static/ 3	40343
6	1	.doc	Download	2969KB	CASE_I	A	ElGamal	1024	Static/ 3	31066
1	1	.doc	Upload	2969KB	CASE_II	A	RSA	1024	Static/ 3	33607
1	1	.doc	Download	2969KB	CASE_II	A	RSA	1024	Static/ 3	30652
2	1	.doc	Upload	2969KB	CASE_II	S	AES	128	Static/ 3	28329
2	1	.doc	Download	2969KB	CASE_II	S	AES	128	Static/ 3	25100
3	1	.doc	Upload	2969KB	CASE_II	S	Des	128	Static/ 3	29452
3	1	.doc	Download	2969KB	CASE_II	S	Des	128	Static/ 3	27573
4	1	.doc	Upload	2969KB	CASE_II	S	TripleDES	128	Static/ 3	36039
4	1	.doc	Download	2969KB	CASE_II	S	TripleDES	128	Static/ 3	32683
5	1	.doc	Upload	2969KB	CASE_II	A	DH	1024	Static/ 3	38928
5	1	.doc	Download	2969KB	CASE_II	A	DH	1024	Static/ 3	35602
6	1	.doc	Upload	2969KB	CASE_II	A	ElGamal	1024	Static/ 3	39068
6	1	.doc	Download	2969KB	CASE_II	A	ElGamal	1024	Static/ 3	35998
1	2.1	.doc	Upload	606KB	CASE_I	A	RSA	1024	Static/ 3	12432
1	2.1	.doc	Download	606KB	CASE_I	A	RSA	1024	Static/ 3	11652
2	2.1	.doc	Upload	606KB	CASE_I	S	AES	128	Static/ 3	10985
2	2.1	.doc	Download	606KB	CASE_I	S	AES	128	Static/ 3	9638
3	2.1	.doc	Upload	606KB	CASE_I	S	Des	128	Static/ 3	10972
3	2.1	.doc	Download	606KB	CASE_I	S	Des	128	Static/ 3	10205
4	2.1	.doc	Upload	606KB	CASE_I	S	TripleDES	128	Static/ 3	11721
4	2.1	.doc	Download	606KB	CASE_I	S	TripleDES	128	Static/ 3	10080
5	2.1	.doc	Upload	606KB	CASE_I	A	DH	1024	Static/ 3	13990
5	2.1	.doc	Download	606KB	CASE_I	A	DH	1024	Static/ 3	12060
6	2.1	.doc	Upload	606KB	CASE_I	A	ElGamal	1024	Static/ 3	12979

6	2.1	.doc	Download	606KB	CASE_I	A	ElGamal	1024	Static/ 3	11520
1	2.1	.doc	Upload	606KB	CASE_II	A	RSA	1024	Static/ 3	14438
1	2.1	.doc	`Download	606KB	CASE_II	A	RSA	1024	Static/ 3	11568
2	2.1	.doc	Upload	606KB	CASE_II	S	AES	128	Static/ 3	11938
2	2.1	.doc	Download	606KB	CASE_II	S	AES	128	Static/ 3	8269
3	2.1	.doc	Upload	606KB	CASE_II	S	Des	128	Static/ 3	13726
3	2.1	.doc	Download	606KB	CASE_II	S	Des	128	Static/ 3	9119
4	2.1	.doc	Upload	606KB	CASE_II	S	TripleDES	128	Static/ 3	13865
4	2.1	.doc	Download	606KB	CASE_II	S	TripleDES	128	Static/ 3	8584
5	2.1	.doc	Upload	606KB	CASE_II	A	DH	1024	Static/ 3	14814
5	2.1	.doc	Download	606KB	CASE_II	A	DH	1024	Static/ 3	12562
6	2.1	.doc	Upload	606KB	CASE_II	A	ElGamal	1024	Static/ 3	13501
6	2.1	.doc	Download	606KB	CASE_II	A	ElGamal	1024	Static/ 3	12150
1	2.2	pdf	Upload	604KB	CASE_I	A	RSA	1024	Static/ 3	17108
1	2.2	pdf	Download	604KB	CASE_I	A	RSA	1024	Static/ 3	15986
2	2.2	pdf	Upload	604KB	CASE_I	S	AES	128	Static/ 3	10855
2	2.2	pdf	Download	604KB	CASE_I	S	AES	128	Static/ 3	9678
3	2.2	pdf	Upload	604KB	CASE_I	S	Des	128	Static/ 3	10181
3	2.2	pdf	Download	604KB	CASE_I	S	Des	128	Static/ 3	8734
4	2.2	pdf	Upload	604KB	CASE_I	S	TripleDES	128	Static/ 3	12431
4	2.2	pdf	Download	604KB	CASE_I	S	TripleDES	128	Static/ 3	9837
5	2.2	pdf	Upload	604KB	CASE_I	A	DH	1024	Static/ 3	15657
5	2.2	pdf	Download	604KB	CASE_I	A	DH	1024	Static/ 3	13250
6	2.2	pdf	Upload	604KB	CASE_I	A	ElGamal	1024	Static/ 3	16799
6	2.2	pdf	Download	604KB	CASE_I	A	ElGamal	1024	Static/ 3	14550
1	2.2	pdf	Upload	604KB	CASE_II	A	RSA	1024	Static/ 3	20724
1	2.2	pdf	Download	604KB	CASE_II	A	RSA	1024	Static/ 3	18503
2	2.2	pdf	Upload	604KB	CASE_II	S	AES	128	Static/ 3	13155
2	2.2	pdf	Download	604KB	CASE_II	S	AES	128	Static/ 3	11074
3	2.2	pdf	Upload	604KB	CASE_II	S	Des	128	Static/ 3	9010
3	2.2	pdf	Download	604KB	CASE_II	S	Des	128	Static/ 3	8583
4	2.2	pdf	Upload	604KB	CASE_II	S	TripleDES	128	Static/ 3	13431
4	2.2	pdf	Download	604KB	CASE_II	S	TripleDES	128	Static/ 3	9330
5	2.2	pdf	Upload	604KB	CASE_II	A	DH	1024	Static/ 3	14351
5	2.2	pdf	Download	604KB	CASE_II	A	DH	1024	Static/ 3	12650
6	2.2	pdf	Upload	604KB	CASE_II	A	ElGamal	1024	Static/ 3	15627
6	2.2	pdf	Download	604KB	CASE_II	A	ElGamal	1024	Static/ 3	12982
1	2.3	png	Upload	606KB	CASE_I	A	RSA	1024	Static/ 3	17187
1	2.3	png	Download	606KB	CASE_I	A	RSA	1024	Static/ 3	15300
2	2.3	png	Upload	606KB	CASE_I	S	AES	128	Static/ 3	10551

2	2.3	png	Download	606KB	CASE_I	S	AES	128	Static/ 3	9147
3	2.3	png	Upload	606KB	CASE_I	S	Des	128	Static/ 3	9732
3	2.3	png	Download	606KB	CASE_I	S	Des	128	Static/ 3	8446
4	2.3	png	Upload	606KB	CASE_I	S	TripleDES	128	Static/ 3	11389
4	2.3	png	Download	606KB	CASE_I	S	TripleDES	128	Static/ 3	10321
5	2.3	png	Upload	604KB	CASE_I	A	DH	1024	Static/ 3	13212
5	2.3	png	Download	604KB	CASE_I	A	DH	1024	Static/ 3	11520
6	2.3	png	Upload	604KB	CASE_I	A	ElGamal	1024	Static/ 3	13087
6	2.3	png	Download	604KB	CASE_I	A	ElGamal	1024	Static/ 3	11985
1	2.3	png	Upload	606KB	CASE_II	A	RSA	1024	Static/ 3	14979
1	2.3	png	Download	606KB	CASE_II	A	RSA	1024	Static/ 3	12620
2	2.3	png	Upload	606KB	CASE_II	S	AES	128	Static/ 3	10802
2	2.3	png	Download	606KB	CASE_II	S	AES	128	Static/ 3	9602
3	2.3	png	Upload	606KB	CASE_II	S	Des	128	Static/ 3	9796
3	2.3	png	Download	606KB	CASE_II	S	Des	128	Static/ 3	8217
3	2.3	png	Upload	606KB	CASE_II	S	TripleDES	128	Static/ 3	12093
3	2.3	png	Download	606KB	CASE_II	S	TripleDES	128	Static/ 3	8728
5	2.3	png	Upload	604KB	CASE_II	A	DH	1024	Static/ 3	13270
5	2.3	png	Download	604KB	CASE_II	A	DH	1024	Static/ 3	11595
6	2.3	png	Upload	604KB	CASE_II	A	ElGamal	1024	Static/ 3	13619
6	2.3	png	Download	604KB	CASE_II	A	ElGamal	1024	Static/ 3	12030
1	3	.doc	Upload	606KB	CASE_I	A	RSA	1024	Random/3	16229
1	3	.doc	Download	606KB	CASE_I	A	RSA	1024	Random/3	11350
2	3	.doc	Upload	606KB	CASE_I	S	AES	128	Random/7	18435
2	3	.doc	Download	606KB	CASE_I	S	AES	128	Random/7	12547
3	3	.doc	Upload	606KB	CASE_I	S	Des	128	Random/4	17901
3	3	.doc	Download	606KB	CASE_I	S	Des	128	Random/4	10271
4	3	.doc	Upload	606KB	CASE_I	S	TripleDES	128	Random/2	13545
4	3	.doc	Download	606KB	CASE_I	S	TripleDES	128	Random/2	9038
5	3	.doc	Upload	606KB	CASE_I	A	DH	1024	Random/3	14353
5	3	.doc	Download	606KB	CASE_I	A	DH	1024	Random/3	12566
6	3	.doc	Upload	606KB	CASE_I	A	ElGamal	1024	Random/2	13959
6	3	.doc	Download	606KB	CASE_I	A	ElGamal	1024	Random/2	12005
1	3	.doc	Upload	606KB	CASE_II	A	RSA	1024	Random/1	12884
1	3	.doc	`Download	606KB	CASE_II	A	RSA	1024	Random/1	11520
2	3	.doc	Upload	606KB	CASE_II	S	AES	128	Random/8	20967
2	3	.doc	Download	606KB	CASE_II	S	AES	128	Random/8	15350
3	3	.doc	Upload	606KB	CASE_II	S	Des	128	Random/5	15812
3	3	.doc	Download	606KB	CASE_II	S	Des	128	Random/5	14351
4	3	.doc	Upload	606KB	CASE_II	S	TripleDES	128	Random/3	13039

4	3	.doc	Download	606KB	CASE_II	S	TripleDES	128	Random/3	9718
5	3	.doc	Upload	606KB	CASE_II	A	DH	1024	Random/4	17538
5	3	.doc	Download	606KB	CASE_II	A	DH	1024	Random/4	14522
6	3	.doc	Upload	606KB	CASE_II	A	ElGamal	1024	Random/5	16058
6	3	.doc	Download	606KB	CASE_II	A	ElGamal	1024	Random/5	13205

In this part measurements are divided in three main groups:

Group 1-Large size files, differ on these characteristics: type of file: .doc, size of file: 2969KB, and the way of file partition: static way (three parts) and Uploading/Downloading them to three different providers. These were taken into consideration for two types of scenarios, *Fig. 33- Case I* and *Fig. 34- Case II.*

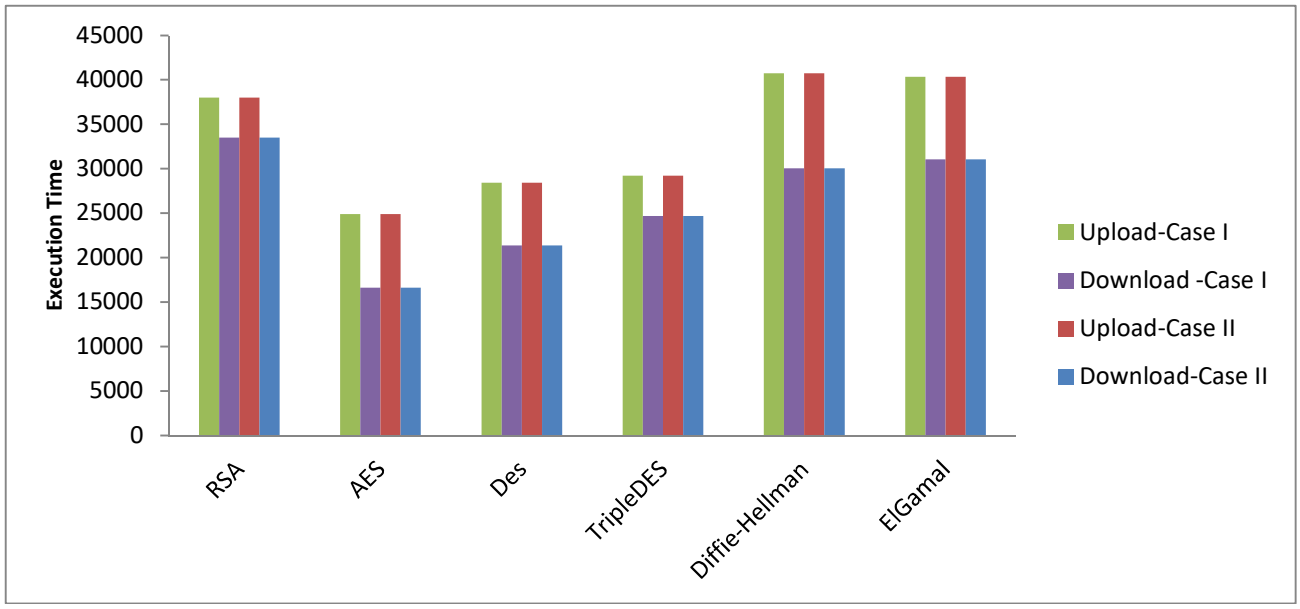


*Figure **46**. Graph of the group 1*

Group 2: Different types of files: .pdf, .doc, .png with same size 606KB, using static way of partitioning (three parts) and Uploading/Downloading them to the cloud in three different providers. As in the above table these characteristics taken into consideration for two types of measurements, *Fig. 33- Case I* and *Fig. 34- Case II.*

2.1 The following table shows measurements for the .doc file.

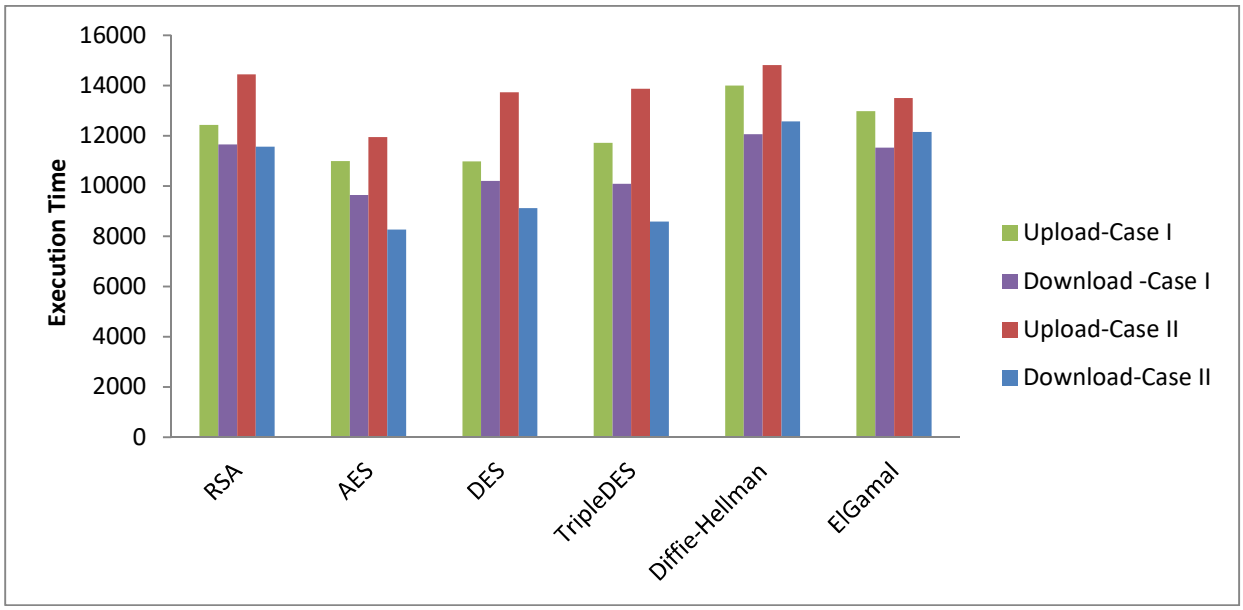


*Figure **47**. Graph of the group 2.1*

2.2 The following table shows obtained measurements for .pdf file.

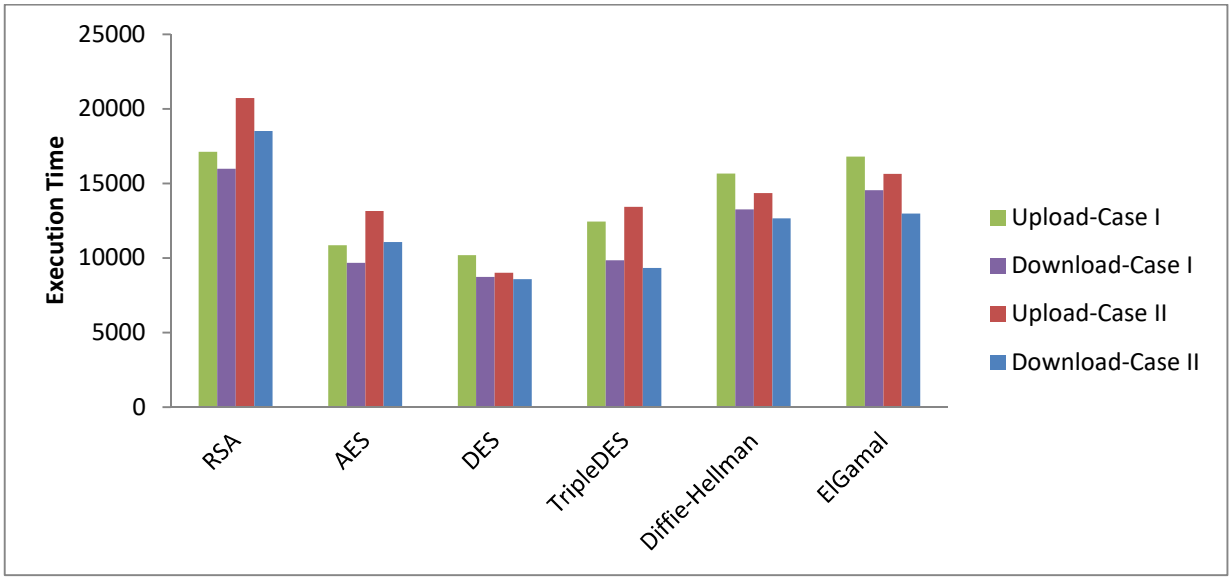


Figure 48. Graph of the group 2.2

2.3 The following table shows obtained measurements for the .png file.

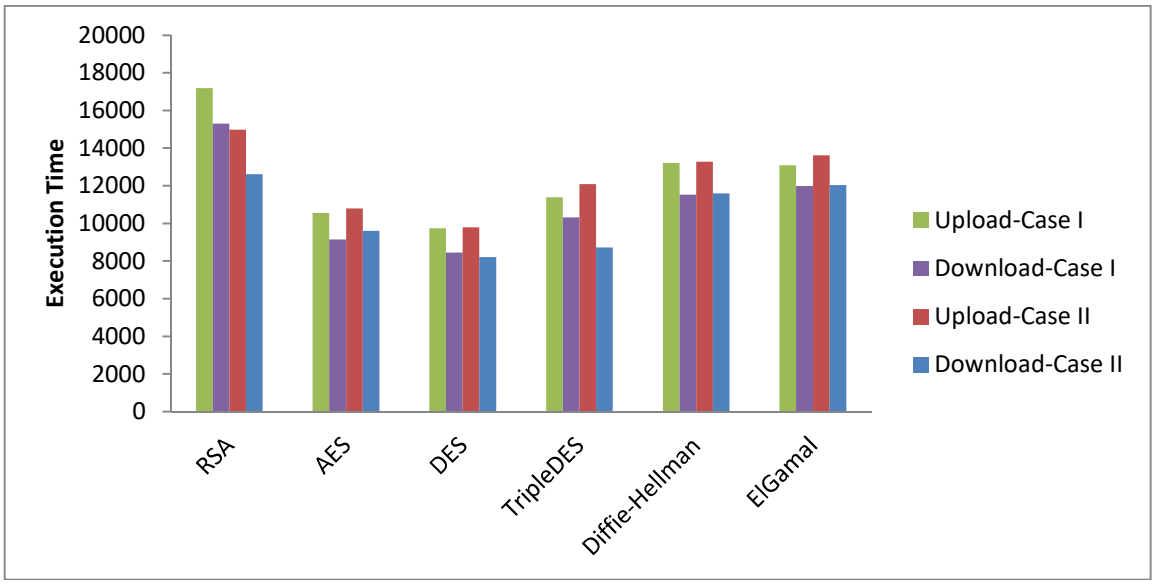


*Figure **49**. Graph of the group 2.3*

Group 3: The measurements are based on the way of partitioning (random way) and Uploading/Downloading them to the cloud, in the programming we set the minimum partitioning 1 part and the maximum up to 10. Characteristics of the file: the type of file .doc was used with size 606KB. These measurements were obtained for two scenarios, *Fig. 33- Case I* and *Fig. 34- Case II.*

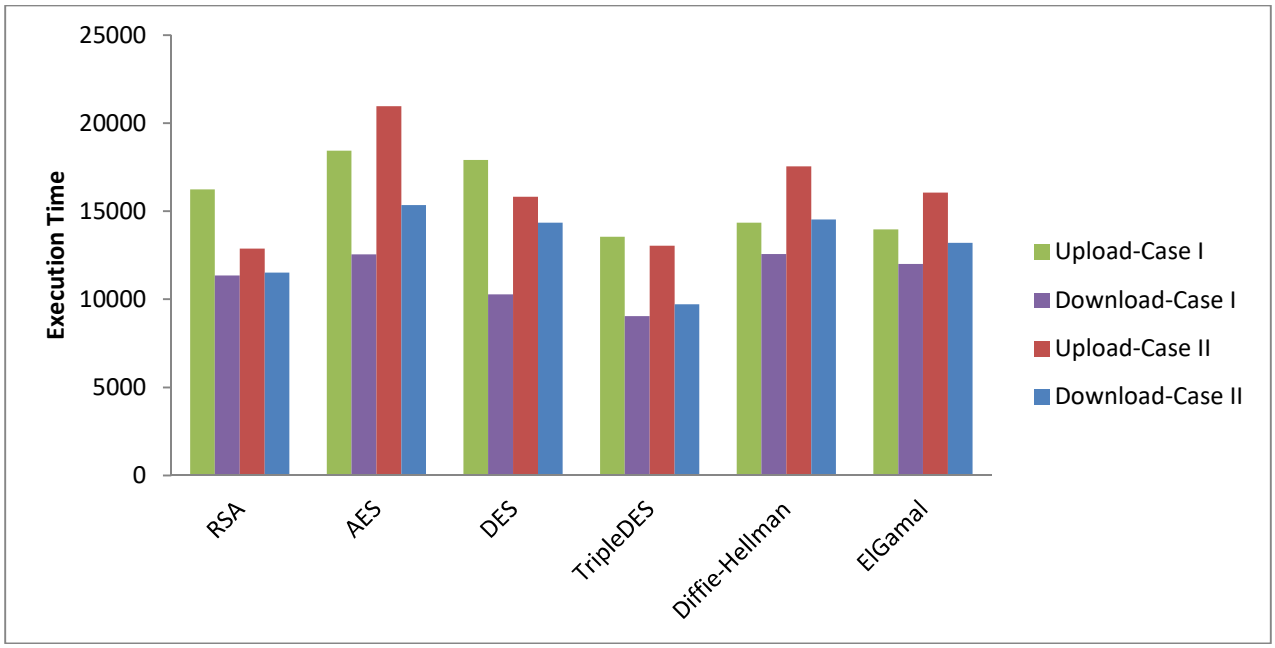


*Figure **50**. Graph of the group 3*

7.1.1 Discussions on obtained measurements, based on our model for first part

- **Group 1** (large file 2969KB): From the achieved results it is seen that, for larger size files asymmetric algorithms are not supported because they need much more time to be executed than symmetric algorithms. At the groups of faster algorithms results to be the symmetric algorithm AES, in the meantime this algorithm is faster for case I and the download mode.
- **Group 2** (different type of files: .doc, .pdf, .png): From the achieved results it is seen that the types of files do not have any effect on the results, almost at the three measurements we have achieved similar results, as in group 1. Therefore, symmetric algorithms are faster comparing to asymmetric algorithms and the AES is the fastest one.
- **Group 3:** At this group of measurements we used general characteristics of measurements such as group 1 and 2, but the focus was the random way of partitioning (Case I and II). Based on the results it is also seen that there is no exact classification which from options could be the best because we are completely depended on the number of segments.
- As a key point here seems to be symmetric and asymmetric algorithm, the work flow for the both proposed methods in our model as in *fig. 32* and *fig 33*. This analysis of data is shown in fig 46. This data was taken from *table 10*, first we grouped them based on the type and size of file then based on the algorithm S-symmetric and A-asymmetric and finaly based on the method used for partition and encryption from our model (Case_I dhe Case_II).

  According to this graph, *fig. 51* we can conclude that the difference between Case_I and Case_II proposed in *fig. 33* and *fig*. *34* is only at large size files, so there is no difference at small size files.

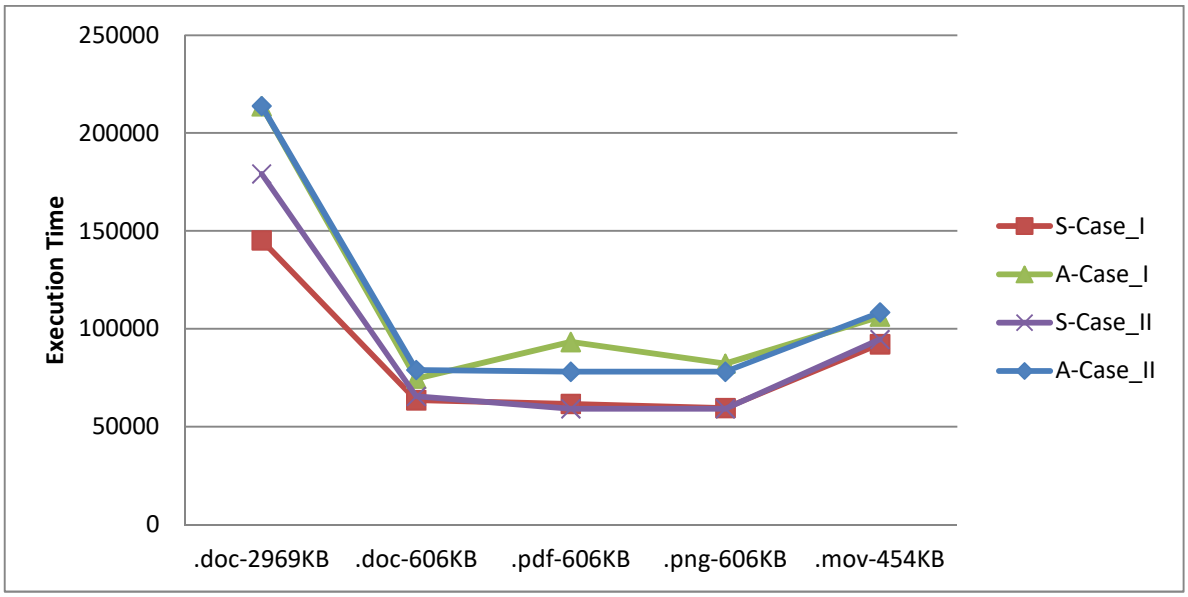


Figure 51. Graphic presentation of Case_I and Case_II for symmetric and asymmetric algorithms

7.2 Second part of measurements

The second part of measurements is realized using three different schemas, for every type of algorithms (Symmetric, Asymmetric and Hybrid), **Hypothesis II**. Moreover, in this part the time of measurement starts after the file is partitioned and special measurement are made for every partition. As total time in general is taken *T,* while in partitions $t_1, t_2, t_3 \ldots . t_n$. Second part of the measurements is completed only for *fig. 33* since this scenario includes the partition and then the encryption of partitions. In addition, this part of encryption is made in different algorithms. We were not able to do these measurements for *fig. 34* (in this scenario the file is encrypted then partitioned, consequently is the same as in measurements of the first part).

- **Symmetric algorithms:**

  Fig. 52 shows the schema used for symmetric algorithms, it is seen that the file is partitioned then every partition is encrypted with a different algorithm: Symmetric (AES, DES and TripleDES). The time of measurement for upload starts from partitioning and continues with encryption then sending the file to the cloud and vice versa for

download. Measurements are obtained separately for every partition: as in schema fig. 52, *table 11*, this type of measurements is shown in column "*Type of Algorithm: S*".

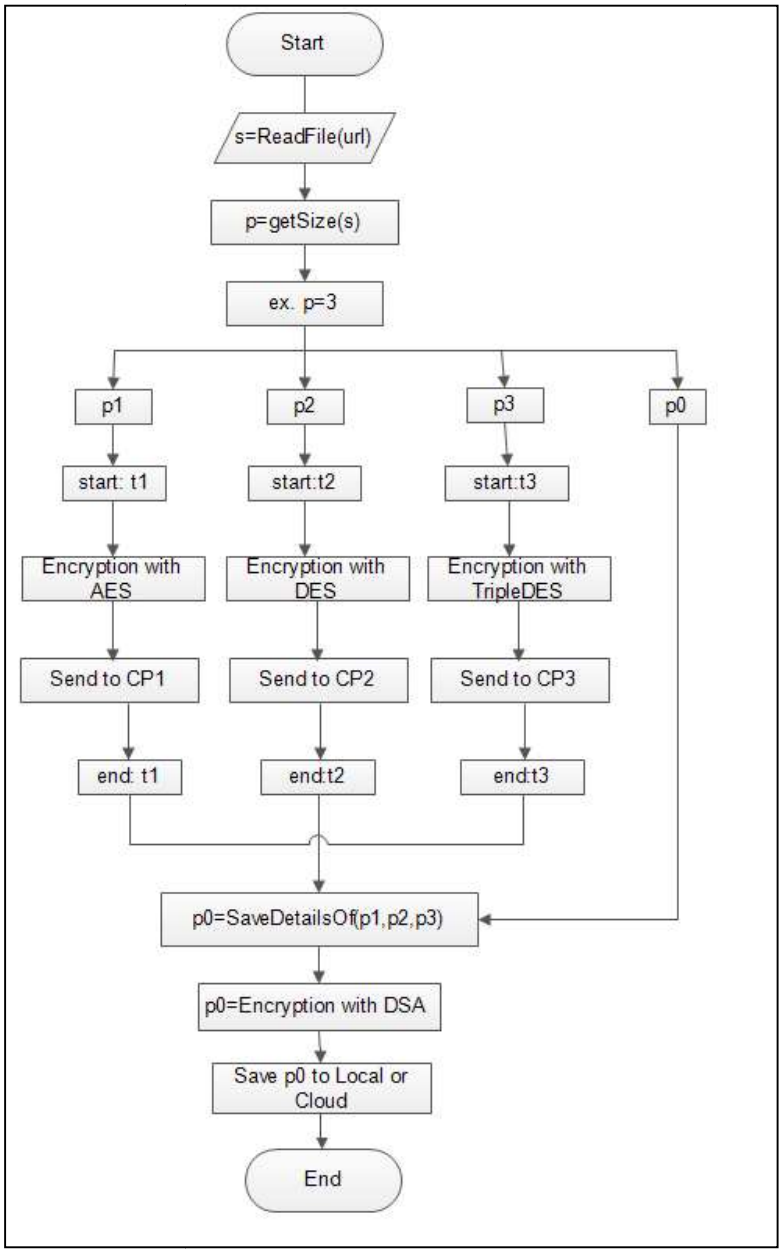


*Figure **52**. Used schema in the second part of measurements for symmetric algorithms*

- **Asymmetric Algorithms:**

Fig. 53 shows the schema used for asymmetric algorithms. It is seen here that the file is partitioned then every partition is encrypted with a different symmetric algorithm (RSA,

DH dhe El Gamal). The time of measurement begins from the separation of the file then it is encrypted and sent to the cloud providers and vice versa for download. Measurements are done separately for each partition as in *fig. 53*. In *table 11*. this group of measurements is shown in column "*Type of Algorithm: A".*

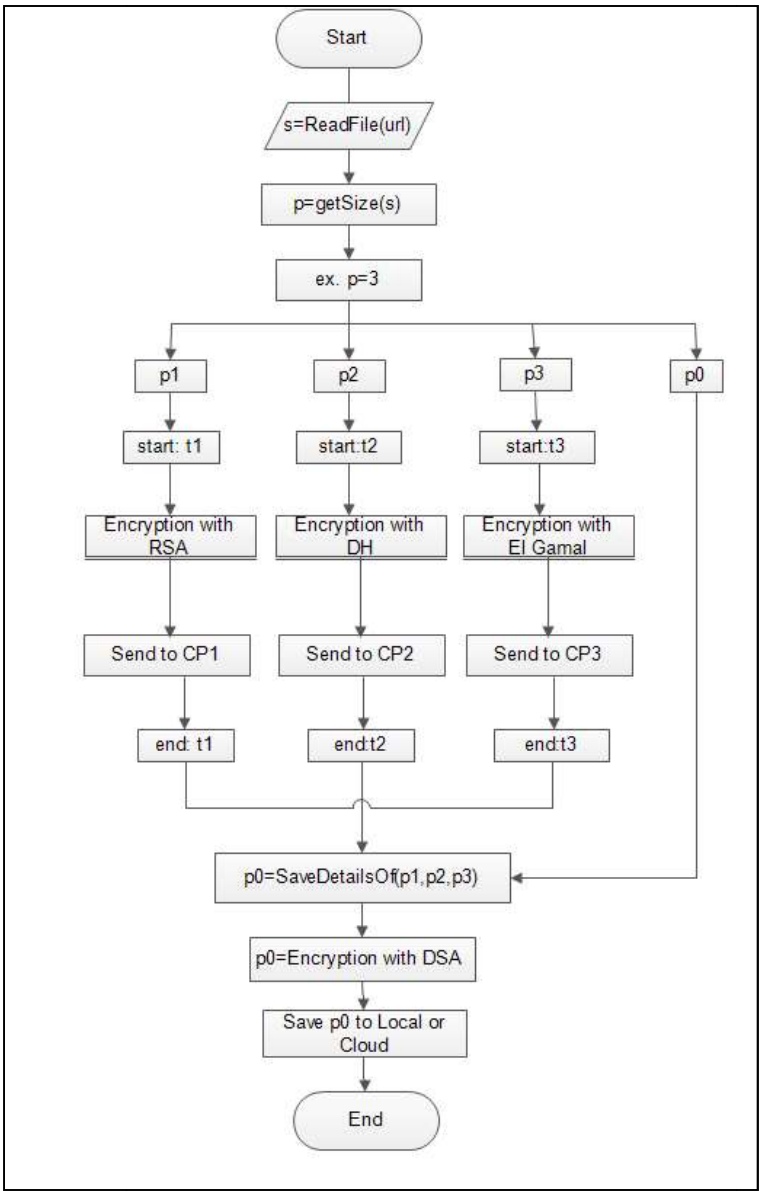


*Figure **53**. Schema used in the second part of measurements for asymmetric algorithms*

- **Hybrid algorithms:**

  Fig. 54 shows the schema used for hybrid algorithms. We see here that the file is separated in partitions, each partition is encrypted with a different algorithm, symmetric and asymmetric (AES, DES, TripleDES and RSA, DH, El Gamal). The time of measurement for upload begins from partitioning, continues with encryption then sending the file to different cloud providers and vice versa for download. Measurements were made separately for every partition, as in schema fig. 54. In *table 11*, this group of measurements is shown in the column "*Type of Algorithm: H"*

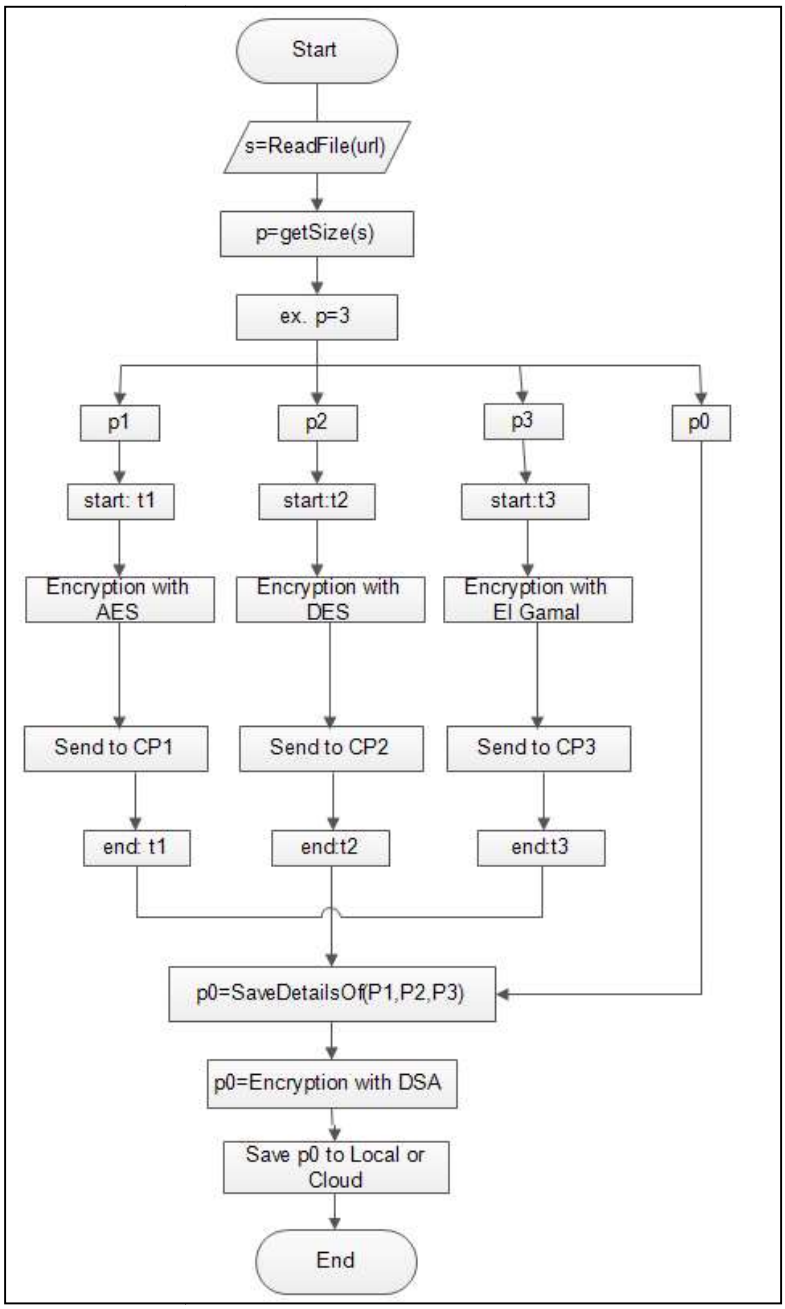


*Figure **54**. Schema used in the second part of the measurements for hybrid algorithms*

In table 11. shows the measurements realized for three schemas in *fig. 52, fig. 53* and *fig. 54*. These measurements are realized for different characteristics (type of file, size of file and different algorithms). Moreover, *table 11*, *T* shows the general time of measurements

for the type of algorithm ($\boldsymbol{T = t_1 + t_2 + t_3}$). Also, the rows that belong to the same type of file with same size are grouped in a same color.

*Table **11**. Results of measurements for the second part*

No.	File type	Proces	File size	Scenerio	Algorithm	Key length bits	Part/No part	Time/ms	Type of Algorithm
t1	.doc	Upload	2969KB	CASE_I	AES	128	1	4828	
t1	.doc	Download	2969KB	CASE_I	AES	128	1	2230	
t2	.doc	Upload	2969KB	CASE_I	Des	128	1	5112	S
t2	.doc	Download	2969KB	CASE_I	Des	128	1	4120	
t3	.doc	Upload	2969KB	CASE_I	TripleDES	128	1	15575	
t3	.doc	Download	2969KB	CASE_I	TripleDES	128	1	11352	
						T=t1+t2+t3		43217	
t1	.doc	Upload	2969KB	CASE_I	RSA	1024	1	27954	
t1	.doc	Download	2969KB	CASE_I	RSA	1024	1	21562	
t2	.doc	Upload	2969KB	CASE_I	Diffie-Hellman	1024	1	28260	A
t2	.doc	Download	2969KB	CASE_I	Diffie-Hellman	1024	1	23323	
t3	.doc	Upload	2969KB	CASE_I	ElGamal	1024	1	41837	
t3	.doc	Download	2969KB	CASE_I	ElGamal	1024	1	32500	
						T=t1+t2+t3		175436	
t1	.doc	Upload	2969KB	CASE_I	RSA	1024	1	27954	
t1	.doc	Download	2969KB	CASE_I	RSA	1024	1	21562	
t2	.doc	Upload	2969KB	CASE_I	Des	128	1	5112	H
t2	.doc	Download	2969KB	CASE_I	Des	128	1	4120	
t3	.doc	Upload	2969KB	CASE_I	ElGamal	1024	1	41837	
t3	.doc	Download	2969KB	CASE_I	ElGamal	1024	1	32500	
						T=t1+t2+t3		133085	
t1	.doc	Upload	606KB	CASE_I	AES	128	1	4476	
t1	.doc	Download	606KB	CASE_I	AES	128	1	1203	
t2	.doc	Upload	606KB	CASE_I	Des	128	1	6603	S
t2	.doc	Download	606KB	CASE_I	Des	128	1	3520	
t3	.doc	Upload	606KB	CASE_I	TripleDES	128	1	7,405	
t3	.doc	Download	606KB	CASE_I	TripleDES	128	1	3850	
						T=t1+t2+t3		27057	
t1	.doc	Upload	606KB	CASE_I	RSA	1024	1	7833	
t1	.doc	Download	606KB	CASE_I	RSA	1024	1	5422	A
t2	.doc	Upload	606KB	CASE_I	Diffie-Hellman	1024	1	9267	

t2	.doc	Download	606KB	CASE_I	Diffie-Hellman	1024	1	6055	
t3	.doc	Upload	606KB	CASE_I	ElGamal	1024	1	8574	
t3	.doc	Download	606KB	CASE_I	ElGamal	1024	1	5391	
						T=t1+t2+t3		42542	
t1	.doc	Upload	606KB	CASE_I	AES	128	1	4476	
t1	.doc	Download	606KB	CASE_I	AES	128	1	1203	
t2	.doc	Upload	606KB	CASE_I	Diffie-Hellman	1024	1	9267	H
t2	.doc	Download	606KB	CASE_I	Diffie-Hellman	1024	1	6055	
t3	.doc	Upload	606KB	CASE_I	TripleDES	128	1	7,405	
t3	.doc	Download	606KB	CASE_I	TripleDES	128	1	3850	
						T=t1+t2+t3		32256	
t1	.pdf	Upload	606KB	CASE_I	AES	128	1	4922	
t1	.pdf	Download	606KB	CASE_I	AES	128	1	2051	
t2	.pdf	Upload	606KB	CASE_I	Des	128	1	5897	S
t2	.pdf	Download	606KB	CASE_I	Des	128	1	3625	
t3	.pdf	Upload	606KB	CASE_I	TripleDES	128	1	6,070	
t3	.pdf	Download	606KB	CASE_I	TripleDES	128	1	3986	
						T=t1+t2+t3		26551	
t1	.pdf	Upload	606KB	CASE_I	RSA	1024	1	6568	
t1	.pdf	Download	606KB	CASE_I	RSA	1024	1	4203	
t2	.pdf	Upload	606KB	CASE_I	Diffie-Hellman	1024	1	10077	A
t2	.pdf	Download	606KB	CASE_I	Diffie-Hellman	1024	1	6950	
t3	.pdf	Upload	606KB	CASE_I	ElGamal	1024	1	10453	
t3	.pdf	Download	606KB	CASE_I	ElGamal	1024	1	7106	
						T=t1+t2+t3		45357	
t1	.pdf	Upload	606KB	CASE_I	Des	128	1	5897	
t1	.pdf	Download	606KB	CASE_I	Des	128	1	3625	
t2	.pdf	Upload	606KB	CASE_I	TripleDES	128	1	6,070	H
t2	.pdf	Download	606KB	CASE_I	TripleDES	128	1	3986	
t3	.pdf	Upload	606KB	CASE_I	ElGamal	1024	1	10453	
t3	.pdf	Download	606KB	CASE_I	ElGamal	1024	1	7106	
						T=t1+t2+t3		37137	
t1	.png	Upload	606KB	CASE_I	AES	128	1	4784	
t1	.png	Download	606KB	CASE_I	AES	128	1	2130	
t2	.png	Upload	606KB	CASE_I	Des	128	1	5218	S
t2	.png	Download	606KB	CASE_I	Des	128	1	2962	
t3	.png	Upload	606KB	CASE_I	TripleDES	128	1	6,213	
t3	.png	Download	606KB	CASE_I	TripleDES	128	1	3908	
						T=t1+t2+t3		25215	
t1	.png	Upload	606KB	CASE_I	RSA	1024	1	6859	A

t1	.png	Download	606KB	CASE_I	RSA	1024	1	4799	
t2	.png	Upload	606KB	CASE_I	Diffie-Hellman	1024	1	8554	
t2	.png	Download	606KB	CASE_I	Diffie-Hellman	1024	1	5210	
t3	.png	Upload	606KB	CASE_I	ElGamal	1024	1	9688	
t3	.png	Download	606KB	CASE_I	ElGamal	1024	1	5865	
						T=t1+t2+t3		40975	
t1	.png	Upload	606KB	CASE_I	RSA	1024	1	6859	H
t1	.png	Download	606KB	CASE_I	RSA	1024	1	4799	
t2	.png	Upload	606KB	CASE_I	Diffie-Hellman	1024	1	8554	
t2	.png	Download	606KB	CASE_I	Diffie-Hellman	1024	1	5210	
t3	.png	Upload	606KB	CASE_I	TripleDES	128	1	6,213	
t3	.png	Download	606KB	CASE_I	TripleDES	128	1	3908	
						T=t1+t2+t3		35543	
t1	.mov	Upload	454KB	CASE_I	AES	128	1	3601	S
t1	.mov	Download	454KB	CASE_I	AES	128	1	1956	
t2	.mov	Upload	454KB	CASE_I	Des	128	1	3606	
t2	.mov	Download	454KB	CASE_I	Des	128	1	1833	
t3	.mov	Upload	454KB	CASE_I	TripleDES	128	1	6359	
t3	.mov	Download	454KB	CASE_I	TripleDES	128	1	4662	
						T=t1+t2+t3		15658	
t1	.mov	Upload	454KB	CASE_I	RSA	1024	1	6923	A
t1	.mov	Download	454KB	CASE_I	RSA	1024	1	4856	
t2	.mov	Upload	454KB	CASE_I	Diffie-Hellman	1024	1	7694	
t2	.mov	Download	454KB	CASE_I	Diffie-Hellman	1024	1	5887	
t3	.mov	Upload	454KB	CASE_I	ElGamal	1024	1	8711	
t3	.mov	Download	454KB	CASE_I	ElGamal	1024	1	4985	
						T=t1+t2+t3		39056	
t1	.mov	Upload	454KB	CASE_I	Des	128	1	3606	H
t1	.mov	Download	454KB	CASE_I	Des	128	1	1833	
t2	.mov	Upload	454KB	CASE_I	Diffie-Hellman	1024	1	7694	
t2	.mov	Download	454KB	CASE_I	Diffie-Hellman	1024	1	5887	
t3	.mov	Upload	454KB	CASE_I	ElGamal	1024	1	8711	
t3	.mov	Download	454KB	CASE_I	ElGamal	1024	1	4985	
						T=t1+t2+t3		32716	

Based on the results from *table 11*, the time of execution is shown in graphs for the type of file .doc with size 2969 KB. Measurements are grouped for three types of algorithms symmetric, asymmetric and hybrid.

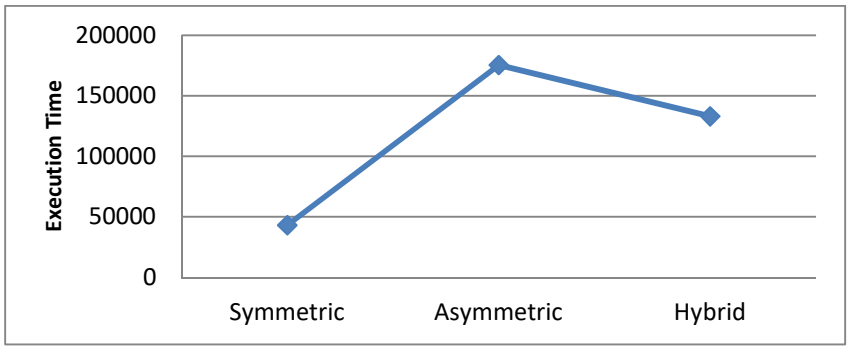


*Figure **55**. Graphical presentation of measurements for the type of file .doc with size 2969*

Based on the results from *table 11,* the time of execution for the type of file .doc with size 606 KB is shown in the graph. Measurements are grouped for three types of algorithms symmetric, asymmetric and hybrid.

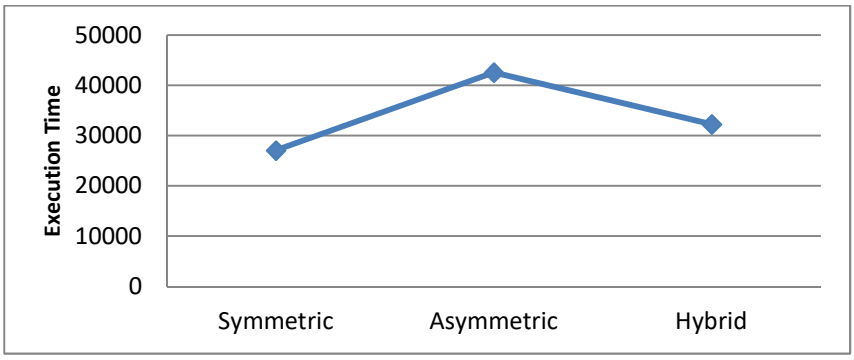


*Figure **56**. Graphical presentation of measurements for the type of file .doc with size 606 KB*

Based on the results from *table 11,* the graphical presentation shows the tie of execution for the type of file .pdf with size 606KB. Measurements are grouped for three types of algorithms: symmetric, asymmetric and hybrid.

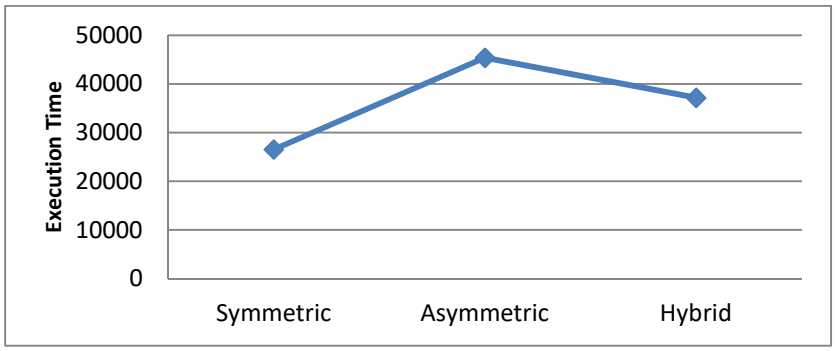


*Figure **57**. Graphical presentation of measurements for the type of file .pdf with size 606 KB*

Based on the results from table *11,* the graphical presentation shows the time of execution for the type of file .png with size 606KB. Measurements are grouped for three types of algorithms: symmetric, asymmetric and hybrid.

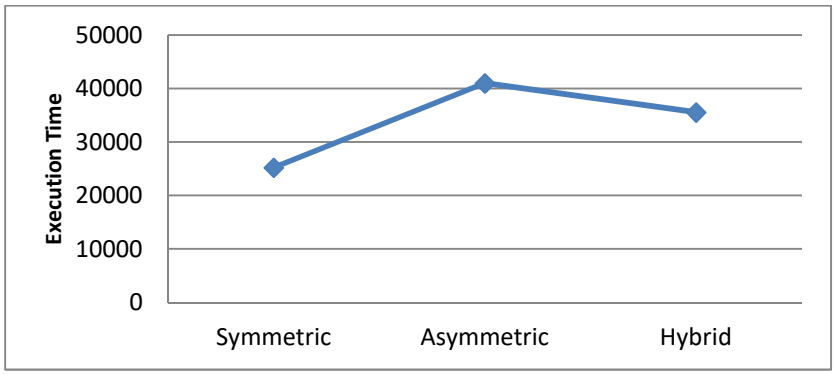


*Figure **58**. Graphical presentation of measurements for the type of file .png with size 606 KB*

Based on the results from *table 11,* the graphical presentation shows the time of execution for the type of file .mov with size 606KB. Measurements are grouped for three types of algorithms: symmetric, asymmetric and hybrid.

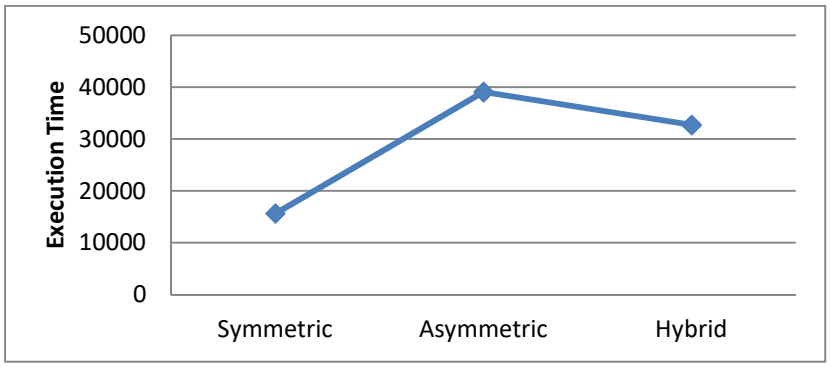


*Figure **59**. Graphical presentation of measurements for the type of file .mov with size 606 KB*

Fig. 60 shows the time of execution for all files taken as samples for testing, *table 9.* It is seen that in the proposed model for the processing time does not have any impact the tipe of file only the size.

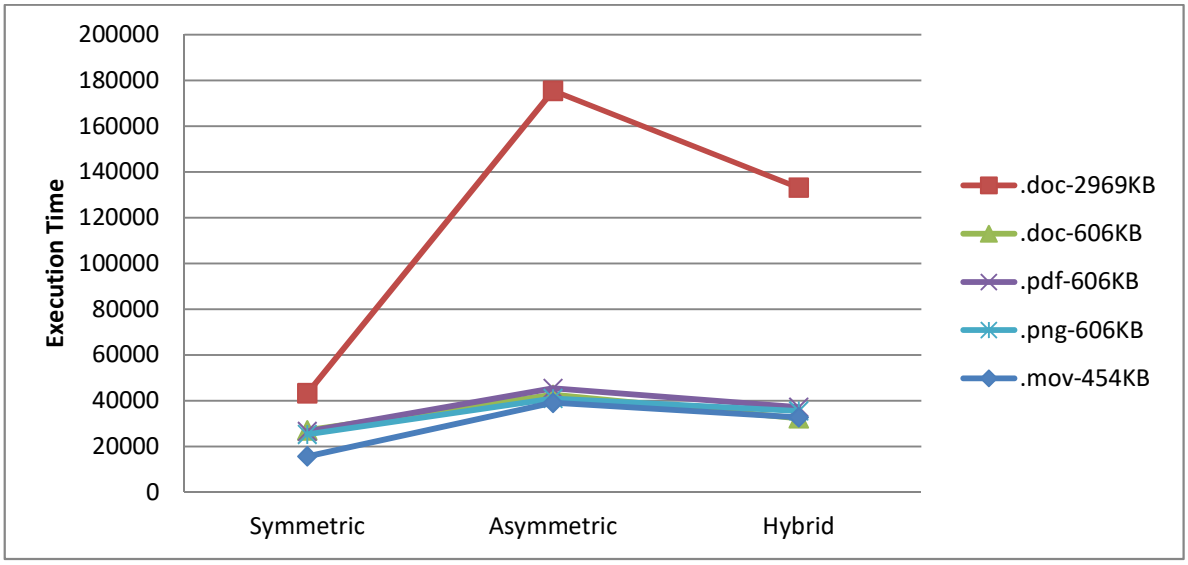


*Figure **60**. Graphical presentation of measurements for the different type of files*

Table 12, is derived from *table 10,* measurements for the types of algorithms are presented in general time for type of file and size of file.

*Table **12**. Rezults of measurements for the second part presented in general*

File type	File size	Algorithm	Time
.doc	2969KB	S	43217
.doc	2969KB	A	175436
.doc	2969KB	H	133085
.doc	606KB	S	27057
.doc	606KB	A	42542
.doc	606KB	H	32256
.pdf	606KB	S	26551
.pdf	606KB	A	45357
.pdf	606KB	H	37137
.png	606KB	S	25215
.png	606KB	A	40975
.png	606KB	H	35543
.mov	454KB	S	15658
.mov	454KB	A	39056
.mov	454KB	H	32716

*Fig.**61*** presents graphical results from table 11, at this graph we have a better picture for every file and the needed time.

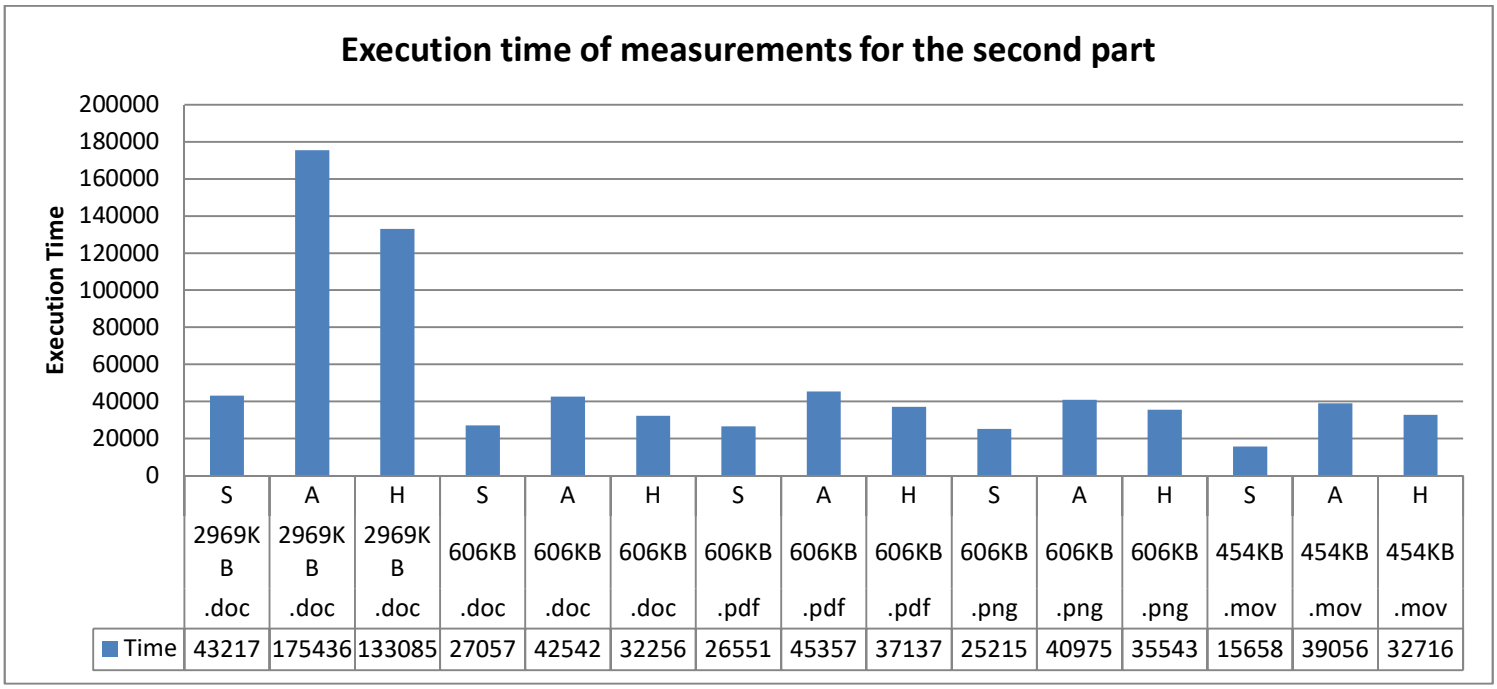


*Figure **61**. Graphical presentation of data from the table **12***

7.2.1 Discussions on obtained measurements, based on our model for second part

Considering the second part of measurements we tested files in details from *table 9*. The main focuses at this part of measurements were the three schemes from *Fig. 52, 53 and 54*. All measurements are presented in *table 11* with all the details placed in the columns of this table.

The main reason of every measurement was the difference of the time of execution for three groups of algorithms: symmetric, asymmetric and hybrid. From this part of measurements we can conclude that symmetric algorithms are faster than asymmetric ones, whereas the hybrid algorithms are somewhere in the middle (it is confirmed in every graph presented for the second part) therefore the difference of the time of execution for Upload/Download is emphasized when the file is as large as in our case with the size of 2969 KB. In Fig. 61, we reconfirm again that the type of file does not affect the time of execution, for both processes.

Proposed model of the “eSiguria” provides different options for security of data, so the ITSS of the organization/company decides on the options:

- *High level of security, for very sensitive data:*

  In this part of measurements we can conclude that high level for the security of data from the proposed model uses the method of sending partitions to cloud fig.32, CASE II and scenario from fig. 53 (use of asymmetric algorithms), that are safer, referring to [126], [127] and [116].

- *Moderate level of security for less sensitive data:*

  Considering the data level the security is moderate. However, still we propose partitions to be sent to the cloud as in fig. 32, CASE II, and scenario in Fig. 54 (use of hybrid algorithms), also hybrid algorithms are proposed by [128] as well, as a better solution for data encryption.

- *Lower level of security for data that are less sensitive:*

  Considering the data where no high level of security is required, we suggest that partitions should be sent to the cloud as in fig. 33, CASE I, referring to the results from fig.51 , we say that this method is faster for big and less sensitive data. Considering this case we suggest that symmetric algorithms for the encryption of the partitions (referring to fig. 51), tend to be much faster, referenced on [126]).

8 CONCLUSION

Based on the recent trends of cloud computing, security practices in current researches have often overlooked the importance of mutual trust. Therefore, the growth of this trust has been the main motive for our research.

Despite the fact that different ideas exist for security in cloud, our proposed model offers the possibility of controlling security by the ITSS, (Hyseni et.al, 2015 & Hyseni et. al 2016), controlling the security in cloud based on different options.

The proposed model of "eSiguria" enables the separation of the file in many partitions (supporting two scenarios fig. 32 and fig. 33) sending these partitions to different cloud providers. Furthermore, this model emphasizes the encryption of partitions then sending them to the cloud. This encryption is realized with different algorithms (symmetric, asymmetric and hybrid) chosen by the ITSS.

The second part of our study presents the implementation and function of the proposed model. There have been offered different schemes for the strategy used for this model based on the sensitivity of the data. In addition, another important issue of this research is the measurements completed in two parts:

- First: using the encryption of partitions by symmetric and asymmetric algorithms (e.g. F1($\mathbf{p_1 - RSA}, \mathbf{p_2 - RSA}, \mathbf{p_3 - RSA} \ldots . \mathbf{p_n RSA}$)), for methods of sending the partitions in cloud proposed in our model, Fig. 32 and 33.
- Second: the encryption of partitions of the same file with different algorithms, symmetric and asymmetric (e.g. F1($\mathbf{p_1 - AES}, \mathbf{p_2 - RSA}, \mathbf{p_3 - DH} \ldots . \mathbf{p_n DES}$)), for the methods of sending the partitions to the cloud proposed in our model *fig. 32* and *fig. 33.*

The proposed model for security in cloud enables the application in different working environments, especially for those environments that work is based on sensitive data and still hesitates to deploy in cloud.

As future work we are going to complete other measurements for other types of files, as well as the possibility of realizing measurements for other scenarios including other algorithms and different working environments. In addition, the advance of the *app. "eSiguria"* in a way it supports users of different professions. However, we hope there will be more researches in the field of cloud security, in the lack of security transparency, and mutual audit in the cloud environments.

9 References

[1] Thales e-Security, (April 2017). Global encryption trends study, https://gets.thalesesecurity.com/ *date of visit:* 10/10/2017

[2] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In Grid Computing Environments Workshop, 2008. GCE'08 (pp. 1-10). Ieee.

[3] Lawal, B. O., Ogude, C., & Abdullah, K. K. A. (2013). Security management of infrastructure as a service in cloud computing. African Journal of Computing & ICT, 6(5).

[4] Leandro, M. A., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth. In Proceedings of the Eleventh International Conference on Networks (pp. 88-93).

[5] Erickson, J., Rhodes, M., Spence, S., Banks, D., Rutherford, J., Simpson, E., ... & Perry, R. (2009). Content-centered collaboration spaces in the cloud. IEEE Internet Computing, 13(5), 34-42.

[6] Marks, E. A., & Lozano, B. (2010). Executive's guide to cloud computing. John Wiley and Sons.

[7] Morgan, L., & Conboy, K. (2012). Assimilation of the Cloud: Report on the Benefits and Challenges of Adopting Cloud Technology.

[8] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing (Vol. 17). Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

[9] Open Cloud Manifesto, Creative Commons Attribution-Share Alike 3.0 Unported License, 2009

[10] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616.

[11] Theron, P. (2013). *Criteria for the evaluation of private cloud computing*(Doctoral dissertation, Stellenbosch: Stellenbosch University).

[12] Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In *MIPRO, 2010 proceedings of the 33rd international convention* (pp. 344-349). IEEE.

[13] http://translate.google.com/translate?sl=auto&tl=sq&js=n&prev=_t&hl=en&ie=UTF-8&eotf=1&u=http%3A%2F%2Fwww.perspecsys.com%2Fresources%2Fcloudsecurity%2F&act=url 17-03-2013; *date of visit:* 14/01/2014 *22:00*

[14] Shimba, F. (2010). Cloud computing: Strategies for cloud computing adoption.
[15] Cloud Computing for Beginners, http://www.techno-pulse.com/, *date of visit:* 01/02/2014 *23:30*

[16] Varia, J. (2008). Cloud architectures. White Paper of Amazon, jineshvaria. s3. amazonaws. com/public/cloudarchitectures-varia. pdf, 16.

[17] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). Ieee.

[18] Pelletingeas, C. (2010). *Performance evaluation of virtualization with cloud computing* (Doctoral dissertation, Edinburgh Napier University).

[19] Sen, J. (2013). Security and privacy issues in cloud computing. Architectures and Protocols for Secure Information Technology Infrastructures, 1-45.

[20] Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., & Dubois, E. (2015). Security transparency: the next frontier for security research in the cloud. *Journal of Cloud Computing*, *4*(1), 12.

[21] Cloud Security Alliance (2010) Top Threats to Cloud Computing. Accessed 21 March 2014 from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[22] Cloud Security Alliance. (2013) The Notorious Nine Cloud Computing Top Threats in 2013. Accessed 20 October 2014 from https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[23] Winkler V. (2011) Securing the cloud- cloud computer security techniques and tactics.

[24] Sunyaev A, Schneider S (2013) Cloud services certification. Communication of the ACM 56(2):33–36, ACM digital Library, New York

[25] Cloud Security Alliance –CSA (2011). Cloud Controls Matrix v.1.3, Accessed 23rd March 2014 from:
https://cloudsecurityalliance.org/

[26] Cloud Security Alliance –CSA. (2012). Consensus Assessments Initiative Questionnaire 1.1. Available at: https://cloudsecurityalliance.org

[27] Schneider S, Lansing J, Gao F, Sunyaev A (2014) A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. In: Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS 2014). IEEE, Waikoloa

[28] Chen Y, Paxson V, Katz RH (2010). What's New About Cloud Computing Security? Report EECS Department, University of California, Berkeley. Accessed September 13, 2012 from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

[29] Cloud Security Alliance (2011) Security guidance for critical areas of focus in cloud computing V3.0, Accessed 20rd October, 2014 from http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[30] Cloud Security Alliance. (2009) Security guidance for critical areas of focus in cloud computing V2.1.0, Accessed 18rd March, 2014 from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[31] Santos N, Gummadi KP, Rodrigues R (2009) Towards Trusted Cloud Computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing (HOTCLOUD). USENIX, San Diego

[32] Brodkin J. (2009) Cloud computing outages: Amazon customers the latest to suffer downtime. Accessed 12th March 2014 from: http://www.networkworld.com/community/node/48961

[33] Chandra, J. V., Challa, N., & Hussain, M. A. (2014). Data and information storage security from advanced persistent attack in cloud computing. International Journal of Applied Engineering Research, 9(20), 7755-7768.

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

[35] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903.

[36] Shah M. A., Swaminathan R., Baker M. Privacy-preserving audit and extraction of digital contents IACR Cryptology EPrint Archive 2008 186

[37] Shah, M. A., Swaminathan, R., & Baker, M. (2008). Privacy-Preserving Audit and Extraction of Digital Contents. *IACR Cryptology EPrint Archive*, *2008*, 186.

[38] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no. 5, pp. 11–14, 2012.
[39] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978

[40] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009.

[41] D. Boneh, "The decision Diffie-Hellman problem," in Algorithmic Number Theory, vol. 1423, pp. 48–63, Springer, 1998.

[42] A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security," Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012

[43] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013

[44] D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm," in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 1–7, IEEE, 2010.

[45] F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC '11), pp. 30–37, September 2011

[46] K. Huang and R. Tso, "A commutative encryption scheme based on ElGamal encryption," in Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC '12), pp. 156–159, IEEE, August 2012.

[47] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[48] M. A. AlZain, B. Soh, and E. Pardede, “Mcdb: using multiclouds to ensure security in cloud computing,” in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC ’11), pp. 784–791, 2011

[49] C. P. Ram and G. Sreenivaasan, “Security as a service (sass): securing user data by coprocessor and distributing the data,” in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010

[50] M. Asad Arfeen, K. Pawlikowski, and A. Willig, “A framework for resource allocation strategies in cloud computing environment,” in Proceedings of the 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW ’11), pp. 261–266, July 2011.

[51] A. Rao, “Centralized database security in cloud,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544–549, 2012.

[52] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12), pp. CC-12–CC-17, IEEE, 2012

[53] S. Biedermann and S. Katzenbeisser, “POSTER: event-based isolation of critical data in the cloud,” in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 1383–1386, ACM, 2013.

[54] C. Delettre, K. Boudaoud, and M. Riveill, “Cloud computing, security and data concealment,” in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC ’11), pp. 424–431, Kerkyra, Greece, July 2011.

[55] Jaatun, M. G., Zhao, G., Vasilakos, A. V., Nyre, Å. A., Alapnes, S., & Tang, Y. (2012). The design of a redundant array of independent net-storages for improved confidentiality in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 13.

[56] Schiffman J., Moyer T., Vijayakumar H., Jaeger T., McDaniel P. Seeding clouds with trust anchorsProceedings of the ACM workshop on Cloud computing security workshop (CCSW '10) October 2010ACM 43 46 10.1145/1866835.1866843 2-s2.0-78650083239

[57] Bowers K. D., Juels A., Oprea A. Proofs of retrievability: theory and implementation Proceedings of the ACM Workshop on Cloud Computing Security (CCSW '09) November 2009 43 5310.1145/1655008.1655015 2-s2.0-74049136395

[58] Bowers K. D., Juels A., Oprea A. HAIL: a high-availability and integrity layer for cloud storage Proceedings of the 16th ACM conference on Computer and Communications Security November 2009 Chicago, Ill, USA ACM 187 198 10.1145/1653662.1653686 2-s2.0-74049144464

[59] Tang Y., Lee P. P. C., Lui J. C. S., Perlman R. Fade: secure overlay cloud storage with file assured deletionSecurity and Privacy in Communication Networks 2010 New York, NY, USA Springer 380 397

[60] Benson K., Dowsley R., Shacham H. Do you know where your cloud files are? Proceedings of the 3rd ACM workshop on Cloud computing security workshop October 2011 ACM 73 8210.1145/2046660.2046677 2-s2.0-80955142131

[61] Mahajan P., Setty S., Lee S., Clement A., Alvisi L., Dahlin M., Walfish M. Depot: cloud storage with minimal trust ACM Transactions on Computer Systems 2011 29 4, article 12 10.1145/2063509.2063512 2-s2.0-84863181209

[62] Feldman A. J., Zeller W. P., Freedman M. J., Felten E. W. SPORC: group collaboration using untrusted cloud resources 10 Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI '10) 2010 337 350

[63] Pinheiro E., Weber W.-D., Barroso L. A. Failure trends in a large disk drive population 7 Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07) 17 23

[64] Tsai T., Theera-Ampornpunt N., Bagchi S. A study of soft error consequences in hard disk drivesProceeding of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '12) June 2012 Boston, Mass, USA 1 8 10.1109/DSN.2012.6263936 2-s2.0-84866668816

[65] Shroff, G. (2010). Enterprise cloud computing: technology, architecture, applications. Cambridge university press.

[66] Micro, T. (2010). Cloud Computing Security--Making Virtual Machines Cloud-Ready. In *Trend Micro White Paper*.

[67] Onwubiko, C. (2010). Security issues to cloud computing. In *Cloud Computing* (pp. 271-288). Springer London.

[68] Virtualizing I/O Devices on VMware Workstation’s Hosted Virtual Machine Monitor, Jeremy Sugerman, Ganesh Venkitachalam and Beng-Hong Lim, 2001

[69] Marshall, D. (2007). Understanding Full Virtualization, Paravirtualization, and Hardware Assist. *VMWare White Paper*.

[70] Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010, October). Security in multi-tenancy cloud. In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on* (pp. 35-41). IEEE.

[71] http://blogs.gartner.com/yefim_natis/2010/03/24/on-multi-tenant-elasticity/; date of visit: 01/02/2014 20:30

[72] http://blogs.idc.com/ie/?p=730, date of visit : 05/02/2014 20:30

[73] http://searchcloudcomputing.techtarget.com/opinion/Clouds-are-more-secure-than-traditional-IT-systems-and-heres-why, date of visit: 02/02/2014 22:00

[74] Khan, K. M. (2009). Security dynamics of cloud computing.

[75] Rodero-Merino L, Vaquero LM, Caron E, Muresan A, Desprez F (2012) Building safe PaaS clouds: a survey on security in multitenant software platforms. Computers & Security 31(1):96–108

[76] Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the sky: a survey on IaaS cloud security. Computing 91(1):93–118, Springer, Vienna

[78] Garfinkel T., Pfaff B, Chow J, Rosenblum M, Boneh D. (2003) Terra: a virtual machine-based platform for trusted computing. In: Proceedings of SOSP 2003, ACM

[79] Krautheim FJ (2009) Private Virtual Infrastructure for Cloud Computing. In: Proceedings of the HOTCLOUD conference 2009. ACM, New York

[80] Arshad J, Townend P, Jie X (2009) Quantification of Security for Compute Intensive Workloads in Clouds. In: Proceedings of the 15th International Conference on Parallel and Distributed Systems. IEEE, Shenzhen

[81] De Chaves SA, Uriarte RB, Westphall CB (2011) Towards an architecture for monitoring private clouds. IEEE Commun Mag 49(12):130–7, IEEE

[82] Rak M, Liccardo L, Aversa R (2011) A SLA-based interface for security management in cloud and GRID integrations. In: Proceedings of the 7th International Conference on Information Assurance and Security (IAS). IEEE, Melaka, pp 378–383

[83] Rak M, Luna J, Petcu D, Casola V, Suri N, Villano U. (2013) Security as a Service Using an SLA-based Approach via SPECS. In:Proceedings of IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), pp, 1 – 6, IEEE

[84] Lorenzoli D, Spanoudakis G (2010) EVEREST+: Runtime SLA Violations Prediction. In: Proceedings of the 5th Middleware for Service-oriented Computing Workshop. ACM, New York

[85] Maity S, Chaudhuri A (2014) Optimal negotiation of SLA in federated cloud using multiobjective genetic algorithms. In: Proceedings of CLOUDNET 2014. IEEExplore, New York, pp 269–271

[86] European Parliament: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.1995.

[87] Mosch, M., Groß, S., & Schill, A. (2014). User-controlled resource management in federated clouds. *Journal of Cloud Computing*, *3*(1), 10.

[88] Watson, P. (2012). A multi-level security model for partitioning workflows over federated clouds. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 15.

[89] Anshel, M., & Boklan, K. D. (2007). Introduction to cryptography with coding theory. *The Mathematical Intelligencer*, *29*(3), 66-69.

[90] Goldreich, O. (2009). Foundations of cryptography: volume 2, basic applications. Cambridge university press.

[91] Colbourn, C. J., & Dinitz, J. H. (Eds.). (2006). *Handbook of combinatorial designs*. CRC press.

[92] Chauhan, N. S., & Saxena, A. (2013). Cryptography and Cloud Security Challenges. CSI Communications.

[93] Hyseni, D., Cico, B., & Shabani, I. (2015, June). The proposed model for security in the cloud, controlled by the end user. In Embedded Computing (MECO), 2015 4th Mediterranean Conference on (pp. 81-84). IEEE

[94] Li, H., Dai, Y., & Yang, B. (2011). Identity-Based Cryptography for Cloud Security. *IACR Cryptology ePrint Archive*, *2011*, 169.

[95] Kerschbaum F.(2013) Searching over encrypted data in cloud systems, in: Proceedings of SACMAT 2013, pp.87-88, ACM ditigal library

[96] Anthes G (2010) Security in the cloud. Communication of the ACM 53(11):16–18, ACM digital library, New York

[97] Zhu Y, Hu H, Ahn GJ, Yau SS (2012) Efficient audit service outsourcing for data integrity in clouds. J Syst Softw 85(5):108–1095, Elsevier

[98] López-Alt A, Tromer E, Vaikuntanathan V (2012) On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of STOC 2012. ACM, New York, pp 1219–1234

[99] Kamara S, Lauter K (2010) Cryptographic cloud storage. In: Proceedings of Financial Cryptography. Workshop on Real-Life Cryptographic, Protocols and Standardization, Springer, Heidelberg

[100] Juels A, Kaliski BS Jr (2007) Pors: proofs of retrievability for large files. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security (CCS 2007). ACM Digital library, New York, pp 584–597

[101] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson NJZ, Song D (2007) Provable Data Possession at Untrusted Stores. In: Proceedings of CCS'07, Alexandria, VA. ACM, New York, pp 598–609

[102] Wang C, Wang Q, Ren K, Lou W (2010) Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In: Proceedings of the 29th conference on Information Communications (INFOCOM 2010). IEEE, San Diego, pp 525–533

[103] Doelitzscher F, Reich C, Knahl M, Clarke N (2012) An agent based business aware incident detection system for cloud environments. Journal of Cloud Computing:Advances, Systems and Applications 1(9):1–19, Springer-Verlag, Berlin

[104] Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. " O'Reilly Media, Inc.".

[105] Cruz, Z. B., Fernández-Alemán, J. L., & Toval, A. (2015). Security in cloud computing: A mapping study. *Computer Science and Information Systems*, *12*(1), 161-184.

[106] Chandra, J. V., Challa, N., & Hussain, M. A. (2014). Data and information storage security from advanced persistent attack in cloud computing. *International Journal of Applied Engineering Research*, *9*(20), 7755-7768.

[107] White Paper, Carestream Health, “How to Evaluate the Data Security Capabilities of Cloud-Based Services”, 2011

[108] Hyseni, D., Çiço, B., & Selimi, B. (2016). CONCEPTION, DESIGN AND IMPLEMENTATION OF AN INTERFACE FOR SECURITY IN CLOUD CONTROLLED BY THE END USER. International Journal on Information Technologies & Security, 8(2).

[109] Fedorova, A., Blagodurov, S., & Zhuravlev, S. (2010). Managing contention for shared resources on multicore processors. Communications of the ACM, 53(2), 49-57.

[110] Lawal, B. O., Ogude, C., & Abdullah, K. K. A. (2013). Security Management of Infrastructure as A Service in Cloud Computing. African Journal of Computing & ICT, 6(5).

[111] Velev, D., & Zlateva, P. (2011). Cloud infrastructure security. In Open Research Problems in Network Security (pp. 140-148). Springer Berlin Heidelberg.

[112] Sandikkaya, M. T., & Harmanci, A. E. (2015). A SECURITY PARADIGM FOR PAAS CLOUDS. PROCEEDINGS OF THE ROMANIAN ACADEMY SERIES A-MATHEMATICS PHYSICS TECHNICAL SCIENCES INFORMATION SCIENCE, 16, 345-355

[113] Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security Algorithms for Cloud Computing. Procedia Computer Science, 85, 535-542.

[114] Ayushi, A. (2010). Symmetric key cryptographic algorithm. International Journal of Computer Applications, 1(15), 1-2.

[115] Bellare, M., & Rogaway, P. (2005). Introduction to modern cryptography. Ucsd Cse, 207, 207.

[116] Khan, M. S. S., & Tuteja, R. R. (2014). Security in cloud computing using cryptographic algorithms. IJCA.

[117] Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International journal of emerging technology and advanced engineering, 1(2), 6-12.

[118] Revuelto, K. V., & SOCHA, K. (2016). Weaknesses in diffie-hellman key exchange protocol. Computer Emergency Response for the EU institution, Tech. Rep

[119] Diffie-Hellman:Key Exchange and Public Key Cryptosystems Sivanagaswathi Kallam, from: http://cs.indstate.edu/~skallam/doc.pdf

[120] ElGamal: Public-Key Cryptosystem Jaspreet Kaur Grewal, from: http://cs.indstate.edu/~jgrewal/steps.pdf

[121] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[122] Desmedt, Y. (2011). Elgamal public key encryption. In Encyclopedia of Cryptography and Security (pp. 396-396). Springer US.

[123] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[124] Gutub, A. A. A., & Khan, F. A. A. (2012, November). Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on(pp. 116-121). IEEE.

[125] https://www.slideshare.net/infosecedu/cissp-d5cryptography-v2012mini-coursev2**,** *date of visit:* 01/12/2016

[126] Janakiraman, V. S., Ganesan, R., & Gobi, M. (2007, July). Hybrid Cryptographic Algorithm for Robust Network Security. In The International Congress for global Science and Technology (Vol. 17, No. 24, p. 33).

[127] Arockiam, L., & Monikandan, S. (2013). Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Research in Computer and Communication Engineering, 2(8), 3064-70.

[128] Hofheinz, D., & Kiltz, E. (2007). Secure hybrid encryption from weakened key encapsulation. Advances in Cryptology-CRYPTO 2007, 553-571.

[129] Biryukov, A., & Shamir, A. (2000, December). Cryptanalytic time/memory/data tradeoffs for stream ciphers. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 1-13). Springer, Berlin, Heidelberg.

[130] Stallings, W., & Tahiliani, M. P. (2014). Cryptography and network security: principles and practice (Vol. 6). London: Pearson.

[131] Sarkar, P. (2002, August). The filter-combiner model for memoryless synchronous stream ciphers. In Crypto (Vol. 2442, pp. 533-548).

[132] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[133] R. A. Rueppel. Analysis and Design of Stream Ciphers Springer-Verlag, 1986

[134] https://www.securityconsulting.net.au/block-cipher-stream-cipher-comparison/, *date of visit:* 01/10/2017

[135] Pagano, F. (2015). A Distributed Approach to Privacy on the Cloud. arXiv preprint arXiv:1503.08115.

Curriculum Vitae

NAME AND SURNAME: DHURATË HYSENI
PHONE: +(377)44 202 109
E-MAIL: dhurate.hyseni@gmail.com
DATE OF BIRTH: February 15th 1988

Education/Professional training

2006-2009	South Eastern European University – Tetovo, Macedoni Faculty of Communication Sciences and Technologies Department of Computer Sciences, Computer Sciences - [graduated]
2010-2012	South Eastern European University – Tetovo Macedonia, Faculty of Communication Sciences and Technologies Department of Computer Sciences, Master of Data Base Management - [graduated]
2014-	South Eastern European University – Tetovo Macedonia, Faculty of Communication Sciences and Technologies, E-Technologies, PhD-Candidate

Professional experience

October 2015 -	University “Ukshin Hoti”, Lecturer and Assistant - Full time
October 2014 -	University “Kadri Zeka”, Assistant – Part time
October 2012-2016	University “AAB”, Lecturer and Assistant – Part time
January 2008 –October 2015	DataProgNet, Programmer – Full time

Research activities:

- Research and development in the areas of Programming Languages, Cloud Computing Security, Database Management Systems.
- Participation in some of the main projects in Kosovo: Asset Management System, Digitalization of municipal administration, Application for registration of vehicles and driving license etc.