The Proposed Model to Increase Security of Sensitive Data in Cloud Computing

Dhuratë Hyseni
Department of Computer Science
University Ukshin Hoti
Prizren, Kosovo

Artan Luma
Department of Computer Science
South East European University
Tetovo, Macedonia

Besnik Selimi
Department of Computer Science
South East European University
Tetovo, Macedonia

Betim Cico
Department of Computer Engineering
Epoka University
Tirana, Albania

***Abstract*—There is a complex problem regarding security of data in cloud, it becomes more critical when the data in question is highly sensitive. One of the main approaches to overcome this problem is the encryption data at rest, which comes with its own difficulties such as efficient key management, access permissions and similar. In this paper, we propose a new approach to security that is controlled by the IT Security Specialist (ITSS) of the company/organization. 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. 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 will present each strategy with the results and comments related to the realized measurements.**

***Keywords*—ITSS-IT security specialist; partitioning; confidentiality; cloud service provider; cloud service client; platform as a service; service as a service; third party auditor**

I. Introduction

Cloud computing has brought impressive advantages to the clients interested to use cloud services such as flexibility in managing the space, automatic software update, easier access to needed information and pay per use services etc. The encryption of data at rest is considered to be one of the main issues related to security in the cloud computing and especially cloud storage [1], [12].

People are becoming more interested in cloud computing due to low cost services that it offers [20], [12]. However, two major concerns lie on the security of data: Data confidentiality and audibility, which seem to be one of the main obstacles to the adoption of cloud computing. In addition, security concerns are preventing some organizations from adopting cloud computing to their businesses, others are considering using combination of a secure internal private cloud with less secured public cloud. Moreover, this is an approach where sensitive data can be deployed in 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 clouds usually operate on an ad-hoc, per-application basis which is not ideal as it lacks rigorosity and audibility.

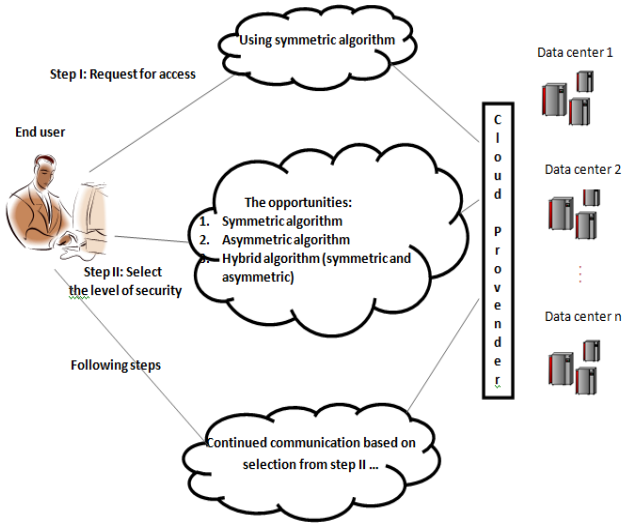

Fig. 1. Scenario of proposed model in the cloud security controlled by the ITSS [2], [3].

To be able to control security from the ITTS of the company/organization, we have proposed a model as an adequate system solution in the cloud computing [2], [3], Fig. 1. In our model, the main actor that manages the security of data in the cloud is the ITSS of the company/ organization. The ITSS selects different security parameters, such as encryption algorithms and keys, as well as partitioning strategies in order to distribute files in the cloud. However, all files transferred to the cloud should follow these company/organization wide rules in the future.

This research starts from our previous works [1], [2] and it continues with proposed scenarios (as new solutions) based on sensitive data.

II. Literature Review

The following research papers claim that there is a large number of researches [12]-[19], even though, the indication is that there is lack of reliability in cloud computing by users.

Based on the literature review, we are going to discuss some security solution in the cloud computing which had great impact in our proposed model.

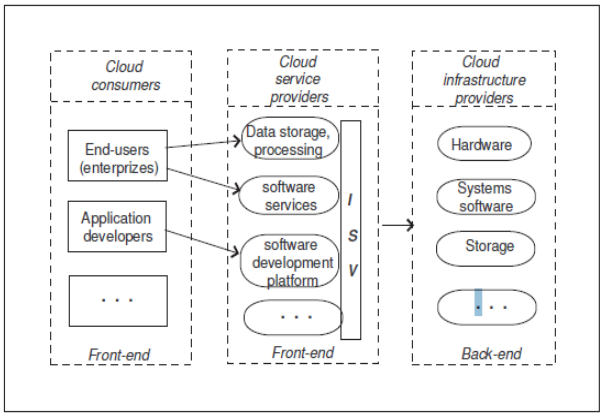

Fig. 2. Levels of abstractions of cloud computing.

The proposed model from [4], consists of three different security scanners with different choices depending on their requests from interested parties for use in the cloud computing, Fig. 2. The researchers began to carry out a thorough analysis of security in the cloud computing modules and then they were focused on the basic requirements to secure a system's cloud protection [4]. Their work orientation is geared towards the Advanced Cloud Protection System (ACPS), which is the result of security for the Linux Kernel Virtual Machine. In this scientific work through the ACPS, it is possible to protect the integrity of virtual machines (VM) and distributed computing middleware, which appear as supporting elements in the cloud computing. Also, different monitoring offered by the VMs in cooperation with the components of the infrastructure is proposed against the various attacks [5].

Authors from [6] have conducted a survey where the main objective is the security on the multi-tenant software platform, offered as part of the PaaS Model. In the PaaS Model, they have discovered the technical weaknesses of the multi-tenancy support platforms, similar to the .Net or Java. In this paper [6], the authors suggested that inside the PaaS, the code isolated by the Cloud Service Client (CSC) and reduces the probability of possible errors in the other applications. Therefore, based on the two weaknesses during the application development, all the rules to ensure this code is developed in the PaaS. As a conclusion, the Cloud Service Provider (CSP) for the PaaS Model should use all the possible mechanisms provided by the security environment, to minimize the potential risks that come to this model. Here the encryption is seen as a choice of the data security during processing and rest of the database, the data has not been tampered with or seen by the other parties in the cloud. Although it has been proposed to encrypt the data for the above mentioned problems, it is not safe for those problems. In the cloud computing, exploited patterns (for management, data processing and storage), security and privacy processes cannot be used with the same encryption techniques as traditional ones [5].

According to [7], authors proposed security for integrity and privacy of the data, based on the efficient audit at low cost. It is also proposed the audit to be carried out by a third party auditor (TPA), which audits the data from time to time and the same data should be available to the client by passing the load and the cost for validation and downloading data at the local level. Practically, this is presented in this way, the data owner has assigned a secret cell used to process the file which is divided into several blocks. Before sending the file and the verification parts to the CSP, one part of the public verification information is already generated and stored in the TPA. Based on the requirements of the data owner, the TPA uses the data retrieval protocol and then enables auditing or controlling data integrity by using public verification information. The perception of this architecture is that it can be implemented in the TPA without including the data owner.

Authors from [8] have requested that the third-party privacy and auditing problems and the data integrity should be resolved by means of the TPA. In this paper, the integrity audit is supported by using the homomorphic encryption. There are solutions in order to increase the efficiency of the TPA which tries to offer both data collection techniques, integrity and the data privacy.

III. Research Methodology

The aim of this study is to propose a model to control data security in the cloud. Recent trends in cloud security have played an important role to attract organizations and companies to deploy sensitive data in cloud. In this context, the proposed model offers different scenarios based on the level of sensitivity of data. In another point of view, it increases reliability of clients in cloud computing. This reliability will be increased by offering controls of data security to the end user- ITSS.

Our model, Fig.1 was proposed in [2], [3], it is the same philosophy for controlling the security in the cloud and it is based on two objectives:

- Control of security depending on the ITSS of a certain organization.
- Possibility to select the security options, based on different algorithms.

The proposed model offers three scenarios based on the data sensitivity:

Scenario I: Security is based on the choice of the ITSS organization, depending on the information proposed by the model.

Scenario II: Based on the features of the file, algorithms which are proposed and the ITSS makes a choice.

Scenario III: Security, based on the file encryption and partition by the ITSS of organization with two possibilities:

A. *The File is Partitioned than Encrypted in Particular Parts (P1, P2,…, Pn)*

It is based on the partitioning of file then encrypts these partitions by algorithm which the ITSS selects, depending on the sensitivity of data in the organization, Fig. 3. This alternative is preferable when it reads 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 uploaded to cloud.

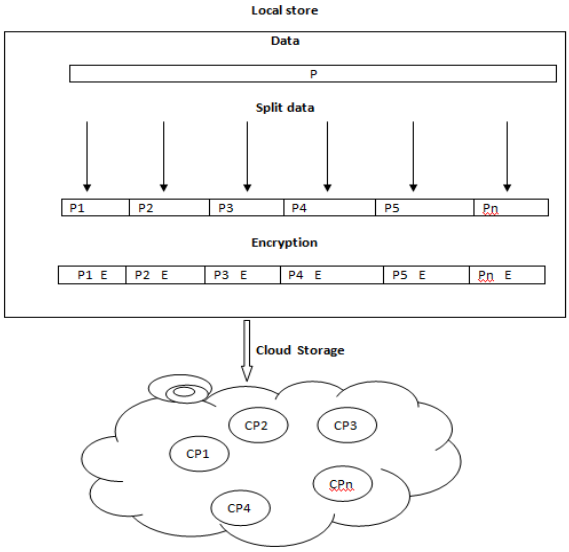

Fig. 3. Partitioned and then encrypted respectively parts of the file - CASE_I.

B. *The File is Encrypted than Partitioned in Particular Parts (P1, P2,…, Pn)*

In the second case of proposed model, we encrypt the file then split it in partitions based on the scenario and algorithm selected. This scenario offers higher security of the data, because we must have all parts of the file in order to be able to read them, Fig. 4.

Each part can be stored in different clouds. A new file *p0*, contains selected algorithms, index and position of the file. File *p0* is significantly smaller, encrypted by DSA algorithm and can be stored anywhere in the cloud or in the local machine.

The steps needed for our proposed model to increase security in the cloud, Fig. 5:

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

Step II: Selection of scenario of security based on the sensitivity data (Scenario I, Scenario II or Scenario III).

Step III: Selection of algorithms of data encryption.

Step IV: Selection of uploading/downloading files to the cloud.

The proposed model is implemented on the .NET Framework 4.5, which is developed by Microsoft that runs primarily on the Microsoft Windows and was developed in the c# programming language.

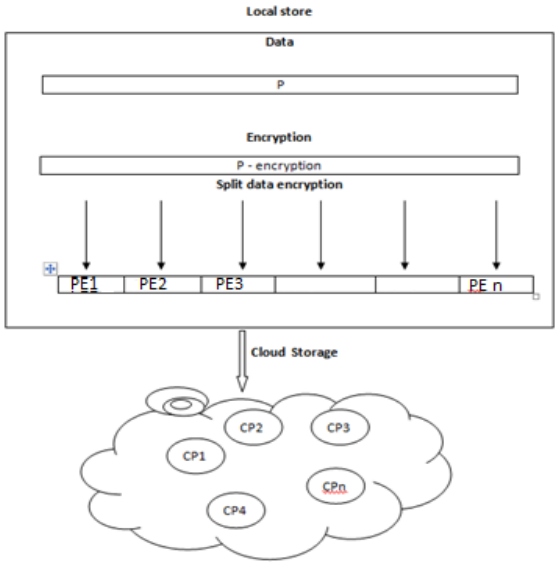

Fig. 4. Encrypted then partitioned file- CASE_II.

IV. Result and Analysis

Considering all measurements, we have 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.

For all measurements we have used measuring unit of time execution in milliseconds. Also, for every case of measurements, there have been two ways of measurements for Upload and Download.

These measurements are realized using three different schemas for every type of algorithms (Symmetric, Asymmetric and Hybrid). Moreover, in this part, the execution time of measurement starts after the file is partitioned and special measurement (i.e. t1,t2…tn) are made for every partition. Also as total time in general is taken T, while in partitions t1,t2…tn, Table I (see Appendix). Also, at Table I (see Appendix), obtained measurements for the type of file, are provided in different colors.

For measurements we have used three symmetric algorithms: AES, DES, TripleDES and three asymmetric algorithms: RSA Diff-Hellman and El Gamal, as well as hybrid algorithms (combination of both symmetric and asymmetric algorithms).

As for the measurements, we have used types of files from Table II:

TABLE II. Files Used For Measurement

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

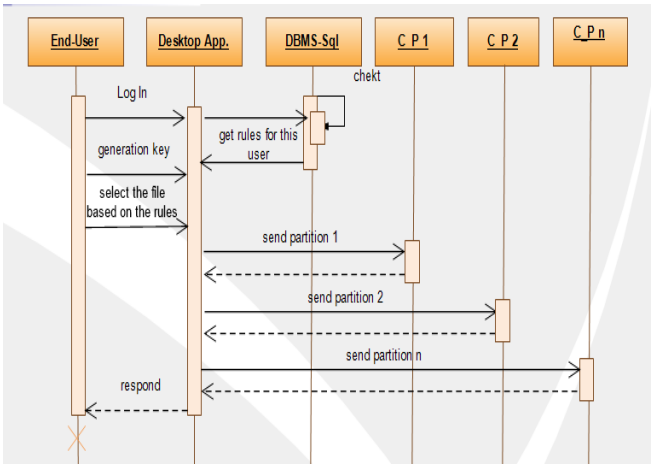

Fig. 5. Communication between user and proposed model.

A. Schema for Symmetric Algorithms

Fig. 6 shows the schema used for symmetric algorithms. It is seen that the file is partitioned then every partition is encrypted with a different symmetric algorithm. 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 Fig. 9. In Table I (see Appendix), this type of measurements is shown in column: "Type of Algorithm: S".

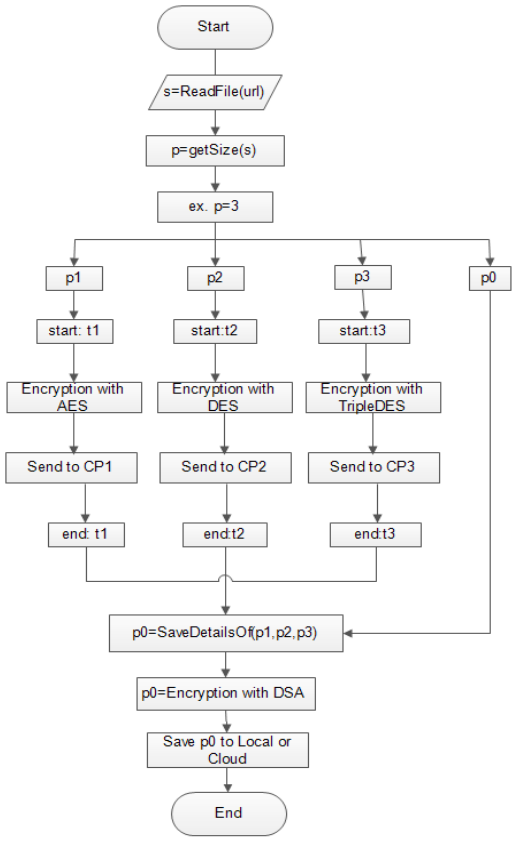

Fig. 6. Schema used of measurements for symmetric algorithms.

B. Schema for Asymmetric Algorithms

Fig. 7 shows the schema used for asymmetric algorithms. It is seen here that the file is partitioned then every partition is encrypted with a different asymmetric algorithm. 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. 9. In Table I (see Appendix), this group of measurements is shown in column: "Type of Algorithm: A".

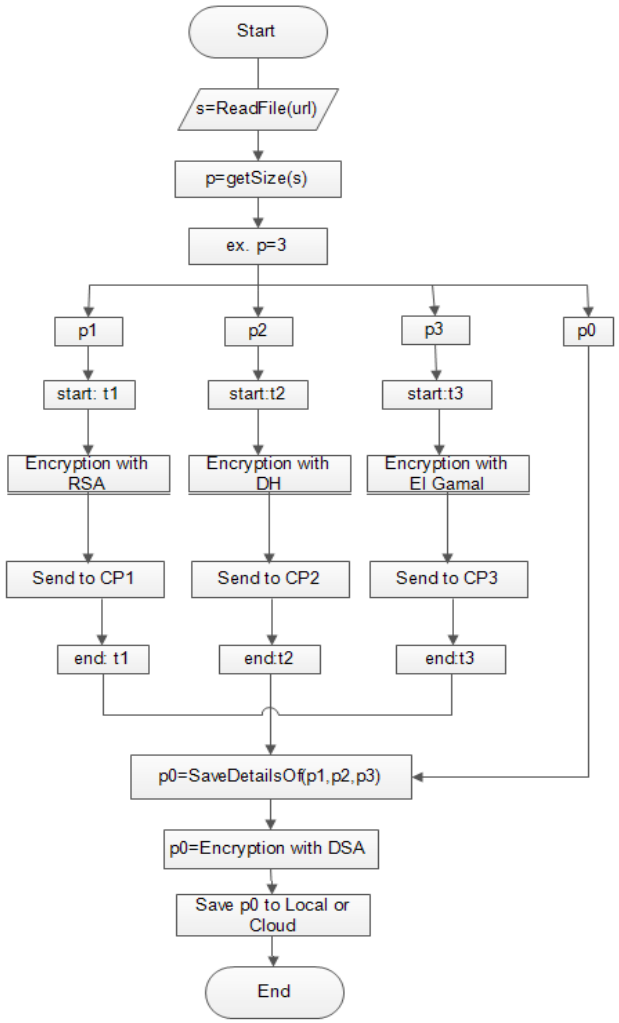

Fig. 7. Schema used of measurements for asymmetric algorithms.

C. Schema for Hybrid Algorithms

Fig. 8 shows the schema used for hybrid algorithms. Here we see that the file is separated in partitions, each partition is encrypted with a different algorithms, symmetric and asymmetric. 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. 9. In Table I (see Appendix), this group of measurements is shown in the column: "Type of Algorithm: H".

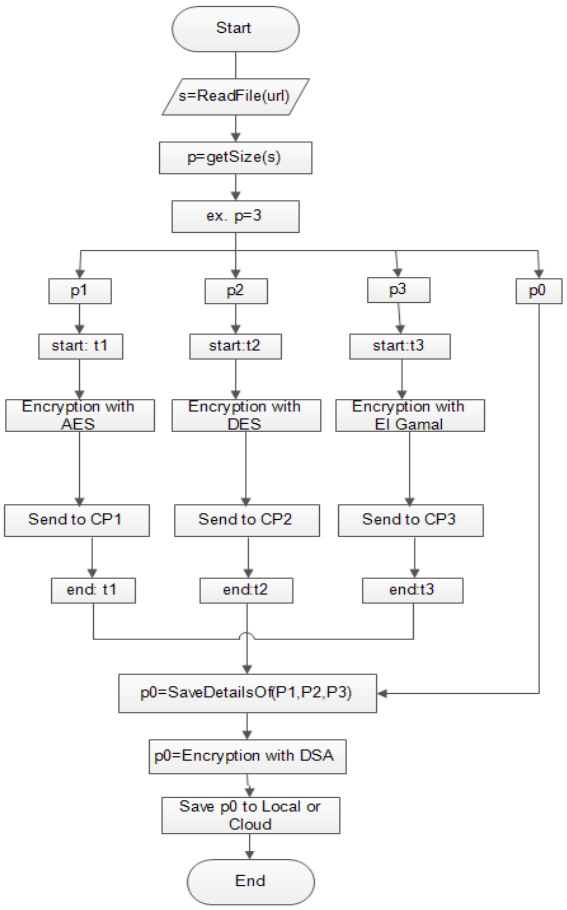

Fig. 8. Schema used of the measurements for hybrid algorithms.

Fig. 8 and Table III (see Appendix), present general results from three types of schemas (Fig. 6, 7 and 8). At this graph we have a better view for every type of file and the execution time.

V. Discussion of the Results

In these measurements we tested types of files from Table II, the focus at this part of measurements were three schemas from Fig. 6, 7 and 8.

The main reason of any measurement was the difference of execution time for three groups of algorithms: symmetric, asymmetric and hybrid. At this point we can conclude that symmetric algorithms are faster than asymmetric algorithms, whereas the hybrid algorithm are in the middle (it is confirmed form Fig. 9 (see Appendix)), therefore the difference of the time of execution for Upload/Download is emphasized when the file is large as in our case with size 2969 KB, Table II. In Fig. 9, we confirm that the type of file does not affect in the time of execution, for both processes (Upload/Download).

The proposed model provides different options for security of data, so 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 security of data from the proposed model uses the method of sending partitions in cloud Fig. 3, CASE_I(file is partitioned then encrypted) and scenario from Fig. 7 (use of asymmetric algorithms) that are safer, referring to [10], [11] and [12].
- Moderate level of security for less sensitive data. For data that the level of security is moderate, we still propose that partitions be sent to cloud as in Fig. 3, CASE_I and scenario in Fig. 8 (use of hybrid algorithms), also hybrid algorithms are proposed by [9] as well, as a better solution for data encryption.
- Lower level of security for data that are least sensitive. For data that is not required a high level of security and big data, then we suggest that partitions should be sent to the cloud as in Fig. 4, CASE_II (the file is encrypted then sent to clouds) referring to the results from Fig. 9, we believe that this method is faster for big and less sensitive data. Also for this case we suggest that symmetric algorithms for the encryption of the partitions (referring to Fig. 6 and Table III (see Appendix), tend to be much faster, also referenced on [10]).

VI. 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 motivation 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 [2], [3], controlling the security in cloud based on different options.

There are offered different schemas for the strategy it uses for the model based on the sensitivity of the data. In addition, another important issue of this research is the measurements realized in two parts:

- First: Using the encryption of partitions by symmetric and asymmetric algorithms (example FileM(p1-RSA, p2-RSA, p3-RSA…pn-RSA)), for methods of sending the partitions in cloud proposed in our model, Fig. 3 and 4.
- Second: The encryption of partitions of the same file with different algorithms. Symmetric and asymmetric (example FileN(p1-RSA, p2-AES, p3-DES…pn-RSA)), for the methods of sending the partitions to the cloud proposed in our model, Fig. 3 and 4.

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

As future work we are going to realize measurements for other types of files, also the possibility of realizing measurements for other scenarios including other algorithms in different working environment. In addition, advance of application in a way that supports users of different professions.

REFERENCES

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

[2] Hyseni, D., Cico, B., & Shabani, I. (2015). 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.

[3] 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).

[4] 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).

[5] 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.

[6] 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

[7] 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

[8] 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

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

[10] 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).

[11] 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.

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

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

[14] 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

[15] 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

[16] 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

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

[18] 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.

[19] 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.

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

APPENDIX

TABLE I. RESULTS OF MEASUREMENTS FROM PROPOSED MODEL

No.	File type	Process	File size	Scenario	Algorithm	Execution Time/ms	Type of Algorithm
t1	.doc	Upload	2969KB	CASE_I	AES	4828	
t1	.doc	Download	2969KB	CASE_I	AES	2230	
t2	.doc	Upload	2969KB	CASE_I	Des	5112	S
t2	.doc	Download	2969KB	CASE_I	Des	4120	
t3	.doc	Upload	2969KB	CASE_I	TripleDES	15575	
t3	.doc	Download	2969KB	CASE_I	TripleDES	11352	
					T=t1+t2+t3	43217	
t1	.doc	Upload	2969KB	CASE_I	RSA	27954	
t1	.doc	Download	2969KB	CASE_I	RSA	21562	
t2	.doc	Upload	2969KB	CASE_I	Diffie-Hellman	28260	
t2	.doc	Download	2969KB	CASE_I	Diffie-Hellman	23323	A
t3	.doc	Upload	2969KB	CASE_I	ElGamal	41837	
t3	.doc	Download	2969KB	CASE_I	ElGamal	32500	
					T=t1+t2+t3	175436	
t1	.doc	Upload	2969KB	CASE_I	RSA	27954	
t1	.doc	Download	2969KB	CASE_I	RSA	21562	
t2	.doc	Upload	2969KB	CASE_I	Des	5112	
t2	.doc	Download	2969KB	CASE_I	Des	4120	H
t3	.doc	Upload	2969KB	CASE_I	ElGamal	41837	
t3	.doc	Download	2969KB	CASE_I	ElGamal	32500	
					T=t1+t2+t3	**133085**	
t1	.doc	Upload	606KB	CASE_I	AES	4476	
t1	.doc	Download	606KB	CASE_I	AES	1203	
t2	.doc	Upload	606KB	CASE_I	Des	6603	S
t2	.doc	Download	606KB	CASE_I	Des	3520	

t3	.doc	Upload	606KB	CASE_I	TripleDES	7,405	
t3	.doc	Download	606KB	CASE_I	TripleDES	3850	
					T=t1+t2+t3	27057	
t1	.doc	Upload	606KB	CASE_I	RSA	7833	A
t1	.doc	Download	606KB	CASE_I	RSA	5422	
t2	.doc	Upload	606KB	CASE_I	Diffie-Hellman	9267	
t2	.doc	Download	606KB	CASE_I	Diffie-Hellman	6055	
t3	.doc	Upload	606KB	CASE_I	ElGamal	8574	
t3	.doc	Download	606KB	CASE_I	ElGamal	5391	
					T=t1+t2+t3	42542	
t1	.doc	Upload	606KB	CASE_I	AES	4476	H
t1	.doc	Download	606KB	CASE_I	AES	1203	
t2	.doc	Upload	606KB	CASE_I	Diffie-Hellman	9267	
t2	.doc	Download	606KB	CASE_I	Diffie-Hellman	6055	
t3	.doc	Upload	606KB	CASE_I	TripleDES	7,405	
t3	.doc	Download	606KB	CASE_I	TripleDES	3850	
					T=t1+t2+t3	32256	
t1	.pdf	Upload	606KB	CASE_I	AES	4922	S
t1	.pdf	Download	606KB	CASE_I	AES	2051	
t2	.pdf	Upload	606KB	CASE_I	Des	5897	
t2	.pdf	Download	606KB	CASE_I	Des	3625	
t3	.pdf	Upload	606KB	CASE_I	TripleDES	6,070	
t3	.pdf	Download	606KB	CASE_I	TripleDES	3986	
					T=t1+t2+t3	26551	
t1	.pdf	Upload	606KB	CASE_I	RSA	6568	A
t1	.pdf	Download	606KB	CASE_I	RSA	4203	
t2	.pdf	Upload	606KB	CASE_I	Diffie-Hellman	10077	
t2	.pdf	Download	606KB	CASE_I	Diffie-Hellman	6950	
t3	.pdf	Upload	606KB	CASE_I	ElGamal	10453	
t3	.pdf	Download	606KB	CASE_I	ElGamal	7106	
					T=t1+t2+t3	45357	
t1	.pdf	Upload	606KB	CASE_I	Des	5897	H
t1	.pdf	Download	606KB	CASE_I	Des	3625	
t2	.pdf	Upload	606KB	CASE_I	TripleDES	6,070	
t2	.pdf	Download	606KB	CASE_I	TripleDES	3986	
t3	.pdf	Upload	606KB	CASE_I	ElGamal	10453	
t3	.pdf	Download	606KB	CASE_I	ElGamal	7106	
					T=t1+t2+t3	37137	
t1	.png	Upload	606KB	CASE_I	AES	4784	S
t1	.png	Download	606KB	CASE_I	AES	2130	
t2	.png	Upload	606KB	CASE_I	Des	5218	
t2	.png	Download	606KB	CASE_I	Des	2962	
t3	.png	Upload	606KB	CASE_I	TripleDES	6,213	
t3	.png	Download	606KB	CASE_I	TripleDES	3908	
					T=t1+t2+t3	25215	
t1	.png	Upload	606KB	CASE_I	RSA	6859	A
t1	.png	Download	606KB	CASE_I	RSA	4799	
t2	.png	Upload	606KB	CASE_I	Diffie-Hellman	8554	
t2	.png	Download	606KB	CASE_I	Diffie-Hellman	5210	
t3	.png	Upload	606KB	CASE_I	ElGamal	9688	
t3	.png	Download	606KB	CASE_I	ElGamal	5865	
					T=t1+t2+t3	40975	
t1	.png	Upload	606KB	CASE_I	RSA	6859	H
t1	.png	Download	606KB	CASE_I	RSA	4799	
t2	.png	Upload	606KB	CASE_I	Diffie-Hellman	8554	
t2	.png	Download	606KB	CASE_I	Diffie-Hellman	5210	
t3	.png	Upload	606KB	CASE_I	TripleDES	6,213	
t3	.png	Download	606KB	CASE_I	TripleDES	3908	
					T=t1+t2+t3	35543	
t1	.mov	Upload	454KB	CASE_I	AES	3601	S
t1	.mov	Download	454KB	CASE_I	AES	1956	
t2	.mov	Upload	454KB	CASE_I	Des	3606	
t2	.mov	Download	454KB	CASE_I	Des	1833	
t3	.mov	Upload	454KB	CASE_I	TripleDES	6359	
t3	.mov	Download	454KB	CASE_I	TripleDES	4662	
					T=t1+t2+t3	15658	
t1	.mov	Upload	454KB	CASE_I	RSA	6923	A
t1	.mov	Download	454KB	CASE_I	RSA	4856	

t2	.mov	Upload	454KB	CASE_I	Diffie-Hellman	7694	
t2	.mov	Download	454KB	CASE_I	Diffie-Hellman	5887	
t3	.mov	Upload	454KB	CASE_I	ElGamal	8711	
t3	.mov	Download	454KB	CASE_I	ElGamal	4985	
					T=t1+t2+t3	39056	
t1	.mov	Upload	454KB	CASE_I	Des	3606	H
t1	.mov	Download	454KB	CASE_I	Des	1833	
t2	.mov	Upload	454KB	CASE_I	Diffie-Hellman	7694	
t2	.mov	Download	454KB	CASE_I	Diffie-Hellman	5887	
t3	.mov	Upload	454KB	CASE_I	ElGamal	8711	
t3	.mov	Download	454KB	CASE_I	ElGamal	4985	
					T=t1+t2+t3	32716	

TABLE III. RESULTS OF MEASUREMENTS PRESENTED IN GENERAL

File type	File size	Algorithm	Execution Time / ms
.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

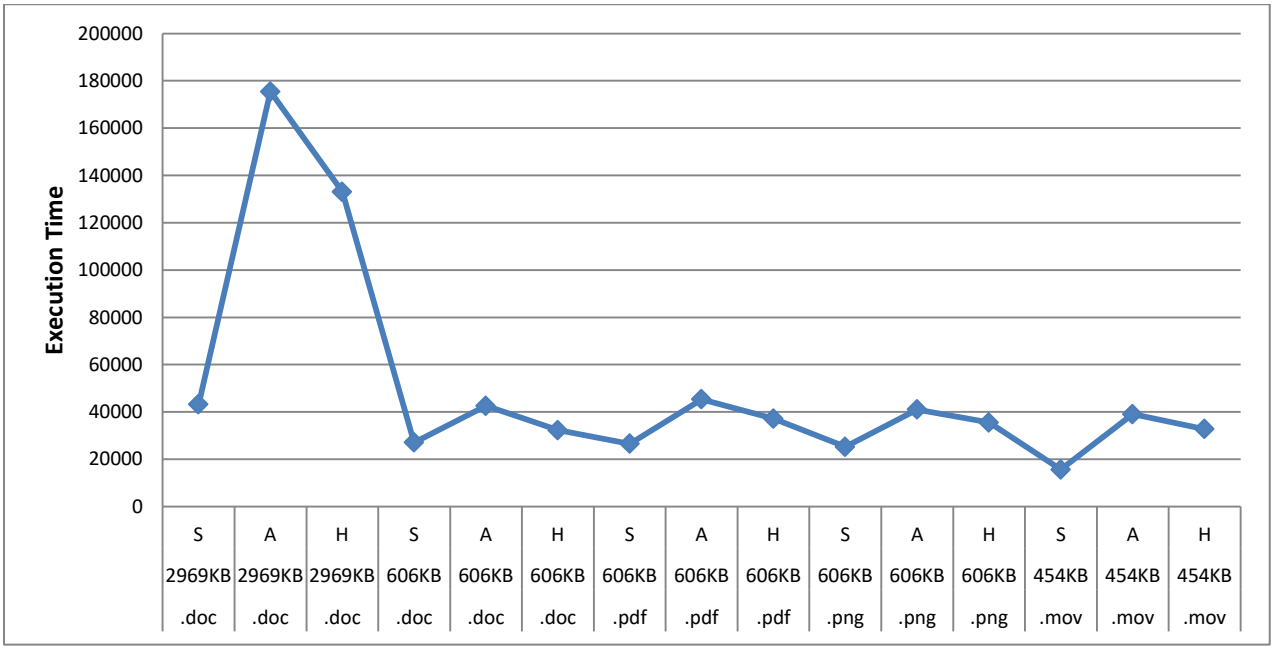

Fig. 9. Graphical presentation of data from the Table III.