Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm

Sana Belguith
Laboratory of Electronic Systems and Communication Network, Tunisia Polytechnic School
Telnet Innovation Labs, Telnet Holding
E-mail: sana.belguith@telnet-consulting.com

Abderrazak Jemai
Laboratoire LIP2, Faculté des Sciences de Tunis, Tunisie
E-mail: Abderrazak.Jemai@insat.rnu.tn

Rabah Attia
Laboratory of Electronic Systems and Communication Network, Tunisia Polytechnic School
E-mail: Rabah.attia@enit.rnu.tn

Abstract— **Cloud computing is a new architecture that has released users from hardware requirements and complexity. The rapid transition toward clouds has advanced many concerns related to security issues which can hold back its widespread adoption. In fact, cloud computing's special architecture has introduced many challenges especially in maintaining the security of outsourced data. Thus, to address this issue, we propose in this article, a new lightweight encryption algorithm which consists of combining symmetric algorithm to encrypt data and asymmetric one to distribute keys. This combination helps to benefit from the efficient security of asymmetric encryption and the rapid performance of symmetric encryption while conserving the rights of users to access data by a secured and authorized way. Evaluation results prove that the processing time of our lightweight algorithm is faster than state-of-the-art cryptographic algorithms.**

Keywords-Cloud computing; Security; Privacy; Data security; Cryptography.

I. INTRODUCTION

In recent years, there has been a huge proliferation of the distributed computing systems use and advancement. This increase has produced a large amount of network distributed paradigms, infrastructures and architectures such as Grid, Pervasive, Autonomic, Cloud, etc.

Cloud computing refers to a network of computers, usually connected through internet, sharing an amount of resources scalable to reach the user's needs and offered by a service provider [1].

The US National Institute of Standards and Technology (NIST) [2] defines cloud computing as follows: '*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*'.

Cloud computing allows users to access software applications and computing capabilities, while using different service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [3]. These three service models are described below:

- Infrastructure as a Service (IaaS) enables the consumer to provide fundamental computing resources (such as processing, storage, networks, etc.). The consumer can deploy and run different kinds of software including operating systems.
- Platform as a Service (PaaS): This model enables the consumer to deploy onto the cloud infrastructure applications created or acquired by the consumer.
- Software as a Service (SaaS): In this model, the user can benefit of the capability of using applications already deployed on the cloud environment by a provider.

Four deployment models are used to deploy cloud computing solutions. The first model is the private cloud which is a cloud infrastructure available only for an exclusive use by a single organization. It is managed by the organization itself or by a third party. The second model is the public cloud providing the cloud infrastructure to the use of the general public. It is owned and managed by a third party who is the cloud provider. The third cloud deployment model is the community cloud which consists of several organizations, having the same interests such as security requirements, share the cloud infrastructure. The last model is the hybrid cloud composed of two or more cloud infrastructures (private, community, or public), which are independent but associated, by standardized or proprietary technology, in order to reach information portability.

On the other hand, there are currently several challenges facing cloud computing mainly related to scalability, interoperability and multi-tenancy. But, the most important issues are related to the security since cloud computing as a system using internet network (such as grid computing, embedded systems, etc.) is exposed to a number of attacks [4]. The cloud computing security issues can hold back its widespread adoption. In fact, sharing resources in cloud computing causes the problem of maintaining these resources secured and protected from malicious access or

 ISBN: 978-1-61208-405-3

use. This problem is particularly faced on the data outsourced to the cloud.

In order to provide a novel mechanism that enhances data security in the cloud computing environment, this paper introduces a new lightweight cryptographic algorithm useful to encrypt data outsourced to cloud storage. This proposed solution is based on the combination of symmetric and asymmetric cryptography to encrypt data. This combination helps to benefit from the efficient security of asymmetric encryption and the rapid performance of symmetric encryption while conserving the rights of users to access data by a secured and authorized way. The paper introduces a comparison of the two categories of encryption algorithms (Asymmetric and symmetric) using various input files. Then, it offers an evaluation of the proposed algorithm.

The rest of the paper deals with the following points. First, Section II surveys the security problems addressed by cloud computing. After a literature review and a description of existent solutions in Section III, we provide a logical description of the proposed algorithm in Section IV. Then, in Section V, we present a comparative study of a variety of cryptographic algorithm and we implement the new algorithm. Finally, Section VI proposes some final remarks and future works.

II. CLOUD COMPUTING SECURITY

A. Trust

Trust is defined as "*the act of having confidence and reliance on someone or something to behave as promised*" [5]. In computer science, trust goes through many areas, such as security and access control in computer networks, reliability in distributed systems, etc. [6].

The fact of outsourcing data and applications, in a cloud environment, delegates their control out of the owner's strict control to the cloud provider. As a consequence, Trust depends on the deployment model and on the cloud provider.

B. Cloud security issues

Due to the novel architecture of cloud computing, many traditional security issues are countered effectively. Although, its infrastructure's singular characteristics have introduced a number of distinctive security challenges.

Security in general is related to the AIC triad, namely, Availability, Integrity and Confidentiality. These three properties have become the key aspects used in designing secure systems, especially, in the case of cloud computing architecture.

1) Confidentiality: it refers only to authorized parties or systems having the ability to access protected data [6]. Outsourcing data, delegating its control to a cloud provider and making it accessible to different parties increase the risk of data breach. A number of concerns emerge regarding the issues of multi-tenancy, data remanence, application security and privacy [7]. Multi-tenancy refers to the cloud characteristic of resource sharing [6]. The cloud computing architecture consists of sharing different kinds of resources to enable multiple clients to use the same resource at the same time which presents a number of privacy and confidentiality threats.

2) Integrity: It means that only authorized parties can modify assets in authorized ways and it refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication [6]. Authorization is the mechanism used by the system to determine what level of access a particular authenticated user should have to secure resources [6]. Due to the rise of the number of parties involved in a cloud environment, authorization is important to ensure data integrity.

3) Availability: It refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a system's ability to carry on operations even when some authorities misbehave [6]. To ensure availability, the system has to be able to operate even if there is a security threat. The user of a cloud environment, who is discharged of hardware infrastructure requirements, relies on the availability of the ubiquitous network.

III. LITERATURE REVIEW

Information security is defined by IEEE as "*the degree to which a collection of data is protected from exposure to accidental or malicious alteration or destruction*" [8].

The International Standard Organization in 2005 defines information security by the ISO/I EC 27002 standard. It is specified by the standard as "*the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safe guarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)*" [9].

To achieve data security, many techniques are used. These techniques can be categorized into four categories: masking, erasure, backup, and encryption. In an unreliable environment, like cloud computing, where there is not a physical control over our data, cryptography seems to be the best way to secure outsourced data. In fact, multi-tenancy characteristics and easy provider access to data force us to ensure confidentiality through innovative techniques based essentially on encryption techniques and access control.

Data encryption refers to the technique that uses cryptography theory to encrypt data on storage devices. Cryptography is the study of mathematical techniques

 ISBN: 978-1-61208-405-3

related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [10]. Cryptography systems are classified into two basic types: Symmetric techniques (also known as conventional or secret key) and asymmetric techniques (public key).

Symmetric encryption consists of using the same key by the sender and the receiver parties. This key is used once to encrypt the data by the sender, and then, time it is used by the recipient to decrypt the data. The asymmetric encryption is based on the use of a pair of keys: a Public key and a private key. The data are encrypted by the public key which can be published. Then, the data are decrypted by the private key which must be kept secret.

In 2012, Dimitrios et al. [6] studied in depth cloud security while identifying security requirements. The authors proposed the use of a trusted third party as a security solution. The solution consists of using cryptography, specifically public key infrastructure with Single-Sign-On (SSO) mechanisms [11] and the lightweight directory access protocol (LDAP) [11], to ensure access control, data integrity and confidentiality and secured communications. This proposed solution consists of using cryptography to ensure confidentiality and integrity of involved data. However, it does not identify encryption algorithms to be used.

In 2009, Cunsolo et al. [12] proposed a mechanism to protect data in distributed systems (grid, cloud, autonomic, etc.). This technique consists of the use of a combination of symmetric and asymmetric cryptographic algorithms. Although in this scheme, only the data owner can access the data which contradicts the concept of sharing resources in the cloud environment.

Hashizume et al. [13] presented a classification of security issues in different service models (SaaS, PaaS and IaaS). This paper offers an identification of the main vulnerabilities in cloud computing while presenting the common threats and its relations to cloud layers. In spite of proposing some available countermeasures, this study does not provide technical implementation of these solutions.

In 2013, Rahmani et al. [14] proposed Encryption as a Service (EaaS) as a solution for cryptography in cloud computing based on XaaS concept. This solution presents a response to prevent the security risks of cloud provider's encryption and the inefficiency of client-side encryption. However, there is not a comparative study of cryptographic algorithms which can be integrated in this solution.

Bugiel et al. [15] proposed a secured cloud architecture which consists of using two clouds (twins) to perform computations. This model differentiates between computations based on their security and performance aspects; trusted cloud performs security-critical operations and the commodity cloud performs performance-critical operations.

In [16], Mohammad et al. evaluated the performances of cryptographic algorithms (symmetric and asymmetric algorithms) in a cloud platform. Based on key size, the performance and the size of the output file, the paper offers a study of different encryption techniques in a cloud environment. Finally, it proposes to use AES algorithm to encrypt data but it does not propose a secure way to distribute encryption keys.

Dimitrios et al. was the first proposing the use of cryptography to secure cloud architecture [6]. Ever since, many authors proposed to use cryptographic algorithms in the cloud storage [14][16]. But, these solutions remain incomplete because they do not specify which algorithm is recommended to encrypt data and how to distribute cryptographic keys while maintaining adequacy with cloud characteristics.

IV. METHODOLOGY

In this section, we provide a logical description of the approach proposed to countermeasure data security issues in cloud computing.

A. Proposed Solution for enhancing data security in the cloud

While using cloud storage, sharing resources, especially sharing data between data owner and authorized clients, can pose the risk of data breach or leakage. In fact, securing data in the cloud is difficult to fulfill if the client does not trust the service provider. The client is obliged to blindly trust the provider's mechanisms but this can be hold back by the threats of malicious insiders among them cloud administrators who can access data simply.

To ensure data security, many techniques and technologies were proposed among them the most efficient one is cryptography. The most successful approach adopted to secure data is symmetric cryptographic techniques. But, this technique alone is not efficient in a multi-tenant scenario; many authorized clients have the right to access data so the key has to be distributed to each client. The key management is too difficult to perform since there are risks in sending keys to different clients at the same time.

The asymmetric cryptographic techniques could be a suitable way to ensure data security. Although, this solution restricts data access to the data owner which contradicts the multi-users aspect of cloud computing. Besides, the asymmetric cryptography algorithm presents a heavy impact on data access. This usually does not allow the encryption of large amounts of data in acceptable time for users. Thus, it is necessary to propose a new solution that can offer a trade-off between security requirements and system performance

 ISBN: 978-1-61208-405-3

and which preserves the multi-tenancy aspect of cloud computing.

The solution we propose combines the efficient security of asymmetric encryption and the rapid performance of symmetric encryption while conserving the rights of users to access data by a secured and authorized way. In our model, the data will be encrypted by a symmetric algorithm. Then, the symmetric key distribution between cloud provider and authorized users will be performed using asymmetric algorithm. Our new solution is basically proposed to protect data confidentiality and integrity using encryption. Moreover, the cryptographic keys are stored at cloud provider side, to decrypt/encrypt data and share it with other clients. The data stored in the cloud remain available on demand by authorized clients and can be accessed rapidly.

B. *Enhancing data security's algorithm*

The data in the cloud storage are encrypted by a symmetric key cryptographic algorithm.

1) *Key exchange*

The first step of the algorithm is the key exchange. This step is composed of two phases: key generation and key exchange.

The data owner generates the symmetric key used to encrypt data, and then, asymmetric two keys used to encrypt the symmetric key. He sends his public key to the cloud storage, which, in turn, generates his two asymmetric keys. Then, the cloud storage saves the cloud public key *Cpub* and the owner's public key *Upub*. In the second phase, the data owner requests the public key of the cloud provider and he encrypts the symmetric key *ksym* with the public key of the cloud provider. Finally, he sends K_E to the cloud storage to be stored.

The step by step algorithm describing the key exchange phase is reported by the diagram of Figure 1.

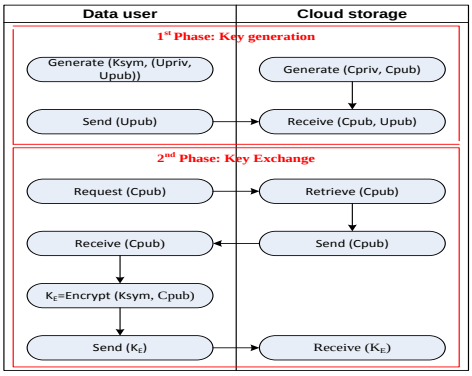

Figure 1. Key generation phase.

2) *Data storage*

The second step of the algorithm is the storage of the encrypted data in the cloud storage. In this step, the data owner encrypts his data by the symmetric key *ksym* and he sends it to the cloud storage in encrypted form. This phase is described in Figure 2.

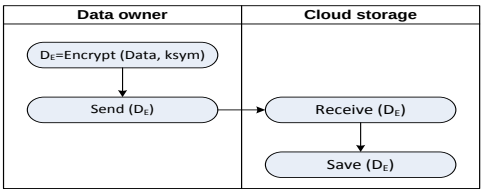

Figure 2. Data storage phase.

3) *Data access*

To access the data stored in the cloud storage, the user requests the data from the cloud storage as shown in Figure 3.

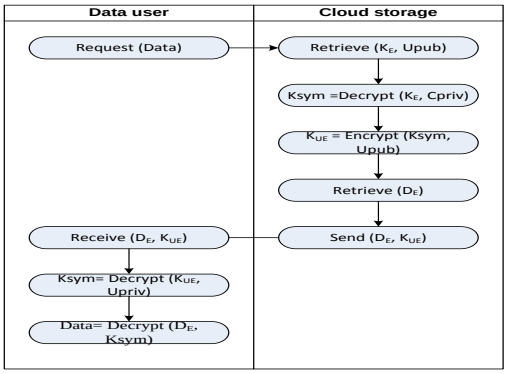

Figure 3. Data access phase.

The cloud storage finds the encrypted symmetric key K_E and the user public key. Then, the cloud storage decrypts the symmetric key K_E with his own private key *Cpriv* and re-encrypt it with the user public key *Upub*. Next, he finds the encrypted data and he sends it with the encrypted key to the user. The user, in turn, decrypts the symmetric key with his private key *Upriv* and he decrypts the data with the symmetric key.

V. IMPLEMENTATION OF THE SOLUTION IN THE CLOUD ENVIRONMENT: RESULTS AND DISCUSSION

A. *Experimental environment*

In order to study the performance of the solution theoretically proposed in the previous section, we have implemented different kinds of symmetric and asymmetric cryptographic algorithms in the cloud environment. Then, we have implemented the hybrid algorithm proposed.

The experimental environment consists of the cloud network composed by the hypervisor Xen Server (6.1), the middleware Openstack and the client that uses Citrix Desktop [17] to access to the virtual machine hosted by XenServer. The cloud server uses the Core I5 (4.8 GHz)

 ISBN: 978-1-61208-405-3

with 4 GB of RAM and the client machine utilizes the Core I3 with 4 GB of RAM.

B. *Experimental results and discussion*

In this section, the study distinguishes between symmetric and asymmetric algorithms by implementing them in the same cloud environment [18].

In Table I, all the symmetric algorithms such as AES [10][19], DES [10], 3DES [10] and Blowfish [10], and asymmetric techniques like RSA [10] and ElGamal [10], have been implemented and tested using different input text file sizes: 1 MB, 10 MB, 50 MB and 100MB. The results mentioned in the table I, are the average of the encryption time calculated after doing the experiments three times.

TABLE I. PROCESSING TIME AND KEY SIZE

		AES	DES	3 DES	Blowfish	RSA	ElGamal
Key size		256	64	192	256	2048	1024
File size (MB)	1	0,03	0,03	0,09	0,03	332.29	2935.90
	10	0,32	0,32	0,77	0,24	-	-
	50	1,61	1,89	4,49	2,13	-	-
	100	4,27	5,50	7,96	5,64	-	-

From this analysis, we can conclude that the symmetric algorithms are faster than the asymmetric algorithms. However, the asymmetric algorithms are the most robust against the code breaking thanks to the lengthy keys used. Among the symmetric algorithms, AES has the lowest data processing time. Moreover, RSA is the asymmetric algorithm having the longest key size as shown in Figure 4.

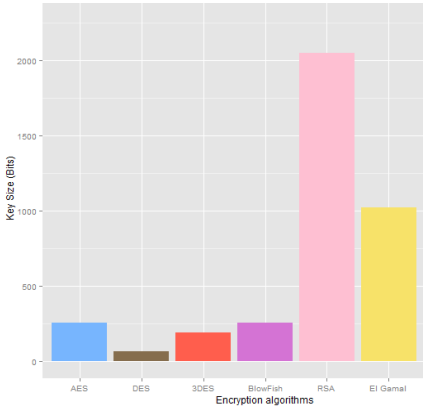

Figure 4. Key size of different cryptographic algorithms.

Obviously, Figure 5 represents the processing time of the implemented symmetric and asymmetric algorithms in the cloud environment.

Finally, using the analysis above, we choose to evaluate the new algorithm proposed by combining the AES algorithm as the symmetric technique and the RSA algorithm as the asymmetric technique.

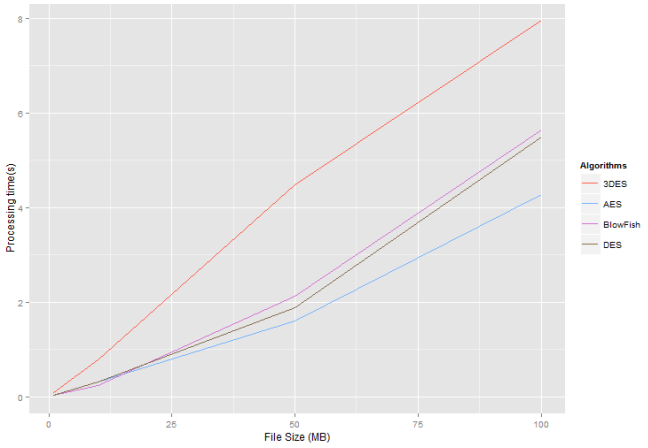

Figure 5. Processing time of different cryptographic algorithms.

TABLE II. PROCESSING TIME OF THE NEW HYBRID TECHNIQUE

File size (MB)	1	10	50	100
Time (s)	0,06	0,30	1,93	4,02
	0,02	0,22	1,54	2,89
	0,03	0,19	1,08	2,83
Average time (s)	0.04	0.24	1.52	3.25

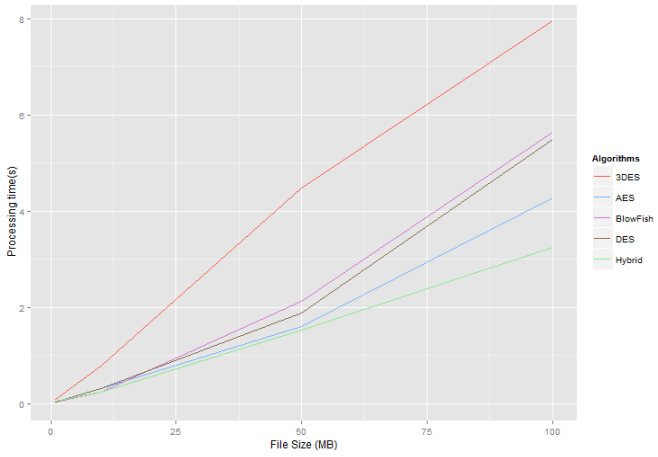

Figure 6. Processing time of the new hybrid technique.

The data processing time composed by the encryption and key distribution time of the new algorithm is faster than the other algorithms while having the secure key distribution as shown in Table II and Figure 6. By this hybrid technique, we can achieve a rapid performance of data processing and an efficient security level using the key distribution mechanism. This new technique enhances confidentiality and integrity of data stored in the cloud while maintaining it available on-demand.

 ISBN: 978-1-61208-405-3

VI. CONCLUSION AND FUTURE WORK

Data security is an open problem in cloud computing environment. To ensure data security, many techniques and technologies were proposed among them the most efficient one is cryptography.

In this work, we propose a hybrid encryption technique consisting of using asymmetric and symmetric cryptographic algorithms. In our model, the data is encrypted by a symmetric algorithm. Then, the symmetric key distribution between cloud provider and authorized users is performed using an asymmetric algorithm.

This paper offers a comparison of the two categories of encryption algorithms (Asymmetric and symmetric) using various input files. Based on the output analysis, we can conclude that the symmetric algorithms are the more efficient in cloud environment thanks to the rapidity of processing data, among them the AES is the faster one. Moreover, the analysis proves that the asymmetric algorithms are more robust thanks to the key length used especially the RSA algorithm. Finally, we evaluated the hybrid technique using the combination of the AES algorithm and the RSA algorithm. This analysis proves that the novel technique enjoys the advantages of symmetric algorithm in the processing time and the robustness of asymmetric algorithm in key length. In fact, this new lightweight algorithm is faster than other cryptographic techniques in processing data. Moreover, it is robust and secured thanks to its key distribution mechanism.

This work can be enhanced by proposing a new key distribution scheme which aims to give every authorized user the encryption key without the cloud provider interaction.

ACKNOWLEDGMENT

This work is a part of the MOBIDOC project achieved under the PASRI program, funded by the European Union and administered by the ANPR [20].

REFERENCES

[1] M. Koehler and S. Benkner, "VCE-A Versatile Cloud Environment for Scientific Applications." The Seventh International Conference on Autonomic and Autonomous Systems (ICAS'11) IARIA, 2011, pp. 81-87

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Information Technology Laboratory, 2011.

[3] A. Tchana, L. Broto, and D. Hagimont, "Fault Tolerant Approaches in Cloud Computing Infrastructures", The Eighth International Conference on Autonomic and Autonomous Systems ICAS'12), 2012, pp. 42-48.

[4] A. Jemai, A. Mastouri, and H. Elleuch, "Study of key pre-distribution schemes in wireless sensor networks: case of BROSK (use of WSNet)", International Journal of Applied Mathematics & Information Sciences (AMIS'12). 2012, pp. 655-667.

[5] P. I. Bhosle and S. A. Kasurkar "Trust in Cloud Computing". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). Volume 2, Issue 4, 2013, pp. 1541-1548.

[6] D. Zissis and D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems, 28(3), 2012, pp. 583-592

[7] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[8] The Authoritative Dictionary of IEEE Standards Terms, 7th ed., Institute of Electrical and Electronics Engineers, Los Alamitos, CA, USA, 2000.

[9] ISO/IEC 27002:2005 Standard: Information technology – Security techniques – Code of practice for information security management, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Geneve, Switzerland, 2005.

[10] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, "Handbook of Applied Cryptography", Boca Raton, FL, USA:CRC Press, Inc., 1996.

[11] "Directories and Public –Key Infrastructure (PKI)", VeriSign, 2004.
https://www.verisign.com.br/static/Directories_PKI.pdf

[12] V. D. Cunsolo, S. Distefano, A. Puliafito, and M. Scarpa, "Achieving information security in network computing systems", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'09.), 2009, pp. 71-77.

[13] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing". Journal of Internet Services and Applications, vol. 4, 2013, pp. 1-13.

[14] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud". Procedia Technology, vol. 11, 2013, pp. 1202-1210.

[15] S. Bugiel, S. Nürnberger, A. R. Sadeghi, and T. Schneider, "Twin clouds: Secure cloud computing with low latency". Communications and Multimedia Security. Springer Berlin Heidelberg, 2011, pp. 32-44.

[16] J. Mohammad, K. Omer, S. Abbas, E. S. M. El-Horbaty, and A. B. M Salem, "A comparative study between modern encryption algorithms based on cloud computing environment". 8th International Conference for Internet Technology and Secured Transactions (ICITST'13), IEEE, 2013, pp. 531-535.

[17] mc software company, "Cloud Lifecycle Management with CitrixXenServer Virtualization", manual guide, network partner, 2013.

[18] «PyCrypto - The Python Cryptography Toolkit». Available from: https://www.dlitz.net/software/pycrypto/
retrieved: 2015.03.10.

[19] A. Sachdev and M. Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications, vol. 67, No. 9, 2013, pp. 19-23.

[20] http://www.pasri.tn/pr%C3%A9sentation
retrieved:2015.04.06.

 ISBN: 978-1-61208-405-3