International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:8, 2013

Cloud Computing Cryptography "State-of-the-Art"

Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem

Abstract**—**Cloud computing technology is very useful in present day to day life, it uses the internet and the central remote servers to provide and maintain data as well as applications. Such applications in turn can be used by the end users via the cloud communications without any installation. Moreover, the end users' data files can be accessed and manipulated from any other computer using the internet services. Despite the flexibility of data and application accessing and usage that cloud computing environments provide, there are many questions still coming up on how to gain a trusted environment that protect data and applications in clouds from hackers and intruders. This paper surveys the "keys generation and management" mechanism and encryption/decryption algorithms used in cloud computing environments, We proposed new security architecture for cloud computing environment that considers the various security gaps as much as possible. A new cryptographic environment that implements quantum mechanics in order to gain more trusted with less computation cloud communications is given.

Keywords**—**Cloud Computing, Cloud Encryption Model, Quantum Key Distribution.

I. Introduction

WITH the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and released by users through the Internet on-demand fashion [1, 2]. Generally, cloud users use the resource allocation and scheduling that is offered by the cloud service provider. Therefore, security in cloud computing platforms is necessary to provide secured transmitting channels through the internet in order to protect transferred data and files [3], [4]. Otherwise, any cloud client can manipulate any files transferred through these cloud communication and transferred data or files can easily be corrupted or damaged as a result of the misuse of the intruders or hackers.

Accordingly, many companies have researched such critical security issue in cloud computing environment in order to produce commercial models that guarantee more trusted communication [9], [10], [11], [12], and [13]. Some of these models depend basically on implementing the concept of hardware encryption for gaining more secured communication channels [29]. However, such hardware implantations was so helpful for databases only it cannot be used for providing a trusted environment for the types of files without using a new encryption model exploit to key generation, distributed, and management.

CSA [5], as another example for the developed commercial models, delivers a set of practices as cloud provider for consumers and vendors to follow in each domain. However these practices did not consider the misuse of the original files or data issue, which led to more vulnerable communication that can be easily attacked and interrupted.

Later on, Meiko et al [6] consider the communication security issues that arising from adopting the cloud computing model such as side channel-attacks, Browsers attacks, Browsers' related attacks and authentication attacks. However, their solutions taking into account the provider services side only, which considered as a weak point that can be exploited by intruders and hackers to distort and intrudes on the communication contents.

After then, Bernd et al [7], [8] discuss the security vulnerabilities existing in the cloud platform. They grouped the possible vulnerabilities into technology-related, cloud characteristics-related and security controls- related. This set of groups provide a central management for monitoring all events (upload, download) done in the cloud and classify them. Whereas a low performance accomplished with high delaying in the data transmission was clearly noticed through the implementation and verification process.

In his paper, we proposed new security architecture for cloud computing environment that considers the various security gaps as much as possible. The new environment offers a new hybrid technique that combines both the Advanced Encryption Standard (AES) algorithm and the QKD as the main security algorithm used for encryption and decryption process by randomly keys generation mechanisms. The random key generation based QKD process provides more flexibility for the communication parties through attack detection. It is considered as the first hybrid technique in the field of cloud computing, which mainly concerns both the short distance associated with QKD and the Key availability associated with AES problems.

The rest of this paper is organized as follows: Section II contains the related work of the cloud computing environments. In Section III, our proposed architecture and its

Omer K.Jasim, Safia Abbas, El-Sayed M. El-Horbaty. and Abdel-Badeeh M. Salem are with the Faculty of Computer and Information Science, Ain Shams University, Egypt (omarkj@auc-edu.org, safia_abbas@cis.asu.edu.eg, Shorbaty@cis.asu.edu, absalem@cis.shams.edu.eg).

main building block is given. Finally, the conclusion and the future work are given in Section IV.

II. Related Work

Cloud computing is an internet base environment where users can store the data remotely in the cloud**.** Any cloud computing environment architecture can be divided basically into three layers, the characteristics layer, the models layer (infrastructure as a services, platform as a services, and software as a services), and the deployment layer [14]. These layers aim to (i) develop and adopt the rapidly evolving of cloud technology, (ii) abstract the details of inner implementations, and, (iii) facilitate the information retrieving service anywhere, anytime[15,16]. The following subsections explain the Cloud Data Encryption Based Quantum (CDEQ) model and the Cloud Encryption Model (CEM) in details as they are the most popular models used in the encryption process based clouds.

A.Cloud Data Encryption Based Quantum (CDEQ)

Cloud data encryption based quantum technology platform dispels all security fears through cloud data transmission [17], [18], and [19]. This technology offers: simple low-cost data protection, tools and security services integration, and an efficient disasters recovery.

Quantum technology solves one of the key challenges in distributed computing. It can preserve data privacy when users interact with remote computing centers [18]. Its power came from the deployment of the Quantum Cryptography or Quantum Key Distribution (QKD) mechanisms, which are considered as the art of the encryption/ decryption process [20], [21], see fig.1. Through quantum channels, data is encoded based on prepared states known as photons. These photons are then sent as "keys" for encryption/ decryption secured messages [22]. The advantage of using such photons in data transmission lays in the no-cloning theorem (the quantum state of a single photon cannot be copied).

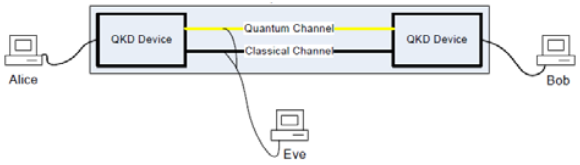

Fig. 1 Schematic of QKD

Bowfins looking for the perfect alliance between cloud computing and the quantum computing, which guarantees data protection for hosted files on remote computers or servers. He encrypted heavy duty of data by using the data processing servers as quantum computer, which succeeds in hiding input, processing and output data from malicious and attacks [22], [23], [24], and [25].

B.Cloud Encryption Models(CEM)

The two most important fields of information security in cloud environment are encryption and authentication. Generally, the encryption mechanism has become one of the basic priorities in maintaining the data security in the cloud, two popularity models based on data encryption technique are going to be explained briefly.

1. Cipher Cloud

Cipher Cloud provides a unified cloud encryption gateway with award-winning technology to encrypt sensitive data in real time before it's sent to the cloud. It also protects enterprise data by using operations-preserving encryption and tokenization in both private and public cloud communication without affecting functionality, usability, or performance [28], [29]. Cipher cloud provides ability to create a unified data protection policy across all clouds that users probably used to store data, such as Google, Amazon, Azure and others. [30].

One the cipher cloud advantages are the offering of multiple AES-compatible encryption and tokenization options, including format and function-preserving encryption algorithms. Users see the real data when accessing an application through the Cipher Cloud security gateway, whereas the data stored in a cloud application is encrypted [30], [31].

By applying encryption in a cloud security gateway, Cipher Cloud eliminates the inherent security, privacy, and regulatory compliance risks of cloud computing [31].

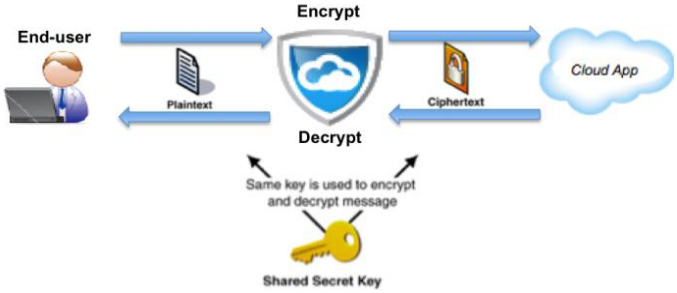

Fig. 2 Cipher Cloud Model

Cipher Cloud's highly secured encryption preserves both the format and function of the data, so that cloud applications remain operational, but their real content remains locked within the enterprise [31]. After then, the process is reversed when employees access cloud applications through the appliance decrypting data in real time so that users see the actual data rather than the encrypted version that resides within the cloud.

2.Cryptographic Cloud Storage

Kamara and Lauter et al [32] proposed a virtual private storage services that would satisfy the standard demands (Confidentiality, integrity, Authentication .etc.). Most of the demands are done by encrypting the documents stored in the cloud. However, such encryption leads to hardness in both the search processes through documents and the collaboration process in real time editing.

Fig. 3 shows the architecture of the cryptographic storage service that are used in solving the security problems of

"back-ups, archival, health record systems, secure data exchange and e-discovery" [33]. It contains three main components: Data Processor (DP) that processes data before sending it to the cloud, Data Verifier (DV) which verifies data's integrity and finally, Token Generator (TG) that generates tokens allowing the service provider to retrieve documents.

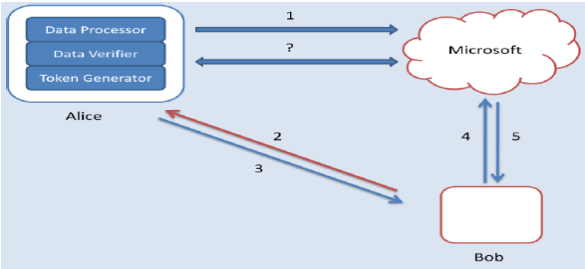

Fig. 3 Cryptographic Cloud Storage Architecture

Before uploading data to the cloud, *Alice* uses the data processor to encrypt and encode the documents along with their metadata (tags, time, size, etc.), then she sends them into the cloud. When she wants to download some documents, *Alice* uses the TG to generate a token and a decryption key. The token is sent to the storage provider to select the encrypted files to be downloaded. After that, the DV is invoked to verify the integrity of the data using a master key. The document is decrypted using the decryption key [33].

C. Proposed Model Main Building Block

This model combines cipher cloud model and cloud data encryption based quantum cryptography, in order to: (i) Deploy the key generation and key management techniques based on QKD to improve the availability and the reliability of the cloud computing encryption and decryption mechanisms, (ii) Manipulate heavy computing processes that cannot be executed using personal computers.

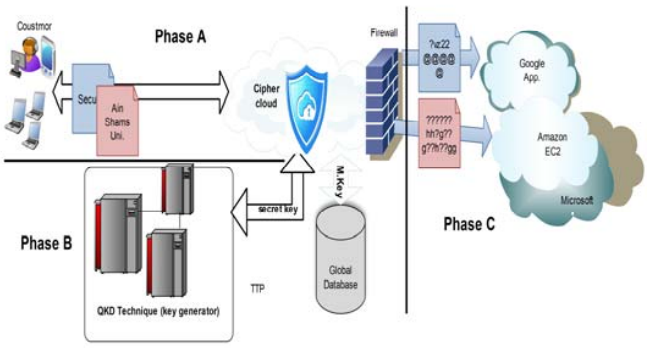

Fig. 4 Proposed Architecture

Numbers of computations are done in the proposed model before the data flying to the cloud environment, these computations can be summarized in three basic phases, enterprise, QKD, and open cloud phase as shown in fig. 4:

- **Enterprise Control (EC):** - in this phase, clients perform some pre-processing operations on of the input data before sending to the cloud environment using the following steps consequently:

1. Customer side: ambit of end user, enterprise, and remote mobile.
2. Cipher Cloud: embracing the encryption/decryption issues for the data or attachment files. This is bolstered by using one type of encryption algorithms such as AES, DES, and RSA.

- **QKD:** QKD is a powerful secure technique in which all tasks are computed by quantum physics and computing theory. It is not pure mathematical evolution but it is a combination of conventional cryptography, information theory and quantum mechanics [26], [27]. QKD is the most important phase in the proposed model that is annotated as the third trusted phase (TTP), it is responsible of key generation, key management and distribution. These keys used to encrypt the documents or files uploaded from client side based on symmetric encryption algorithm (AES). Moreover, it is considered as the core of the proposed model because it is hard to be traced or hacked. However, it is easy to be used, simple to be maintained and solves the complexity of the computational design that is associated with the conventional cryptography.

- **Open Cloud Phase**: this is the beefiest phase used to absorb and share the documents, the applications or the attachment files over the internet, such as Google Apps., Amazon EC2.

III. Conclusion and Future Work

This paper introduced a new cloud computing environment, which suggested integrates and deploys both the AES based cipher cloud and QKD as a new hybrid technique. Since any existing cloud computing environment depends on either QKD or AES algorithms for encryption/ decryption process which protect users' data from hacking as much as possible. Our attempt proposes a hybrid technique that combines both the AES and the QKD to build more secured channels for data transmission. The encryption/ decryption process based the hybrid technique will be done before the storage and retrieval phases and after the user authentication phase.

Our attempt enjoys certain advantages when compared with the others, especially with respect to the secret key generation used in the encryption/ decryption process, such that it (i) provides a more flexible and secured communication environment, (ii) improves the performance of the encryption/decryption process, and (iii) supports more secured data transmission process using less computational time. It can be considered as the first cloud environment that integrates both the cipher cloud gateway and the QKD mechanisms. In the future analytical and empirical evaluations will be done in order to verify the expected results from the proposed environment.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, Accessed April 2011.
[2] Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010).
[3] IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July 2011.
[4] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.
[5] Cloud Security Alliance (CSA). (2010). Available: http://www.cloudsecurityalliance.org/
[6] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.
[7] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
[8] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.
[9] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
[10] S. Subashini, Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.
[11] Lohr, Steve. "Cloud Computing and EMC Deal." New York Times. Feb. 25, 2009. pg. C 6.
[12] McAllister, Neil. "Server virtualization." InfoWorld. Feb. 12, 2008. Retrieved March 12, 2008. http://www.infoworld.com/article/07/02/12/07FEvirtualserv_1.html
[13] Markoff, John. "An Internet Critic Who Is Not Shy About Ruffling the Big Names in High Technology." New York Times. Apr. 9, 2001. pg. C6
[14] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, http://www.theregister.co.uk/2009/03/16/azure_cloud_crash/
[15] P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf
[16] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal,March 26, 2010
[17] L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, held with SC08, November 2008. http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf
[18] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik. Scalable and e_cient provable datapossession. In Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08), pages 1{10, New York, NY, USA, 2008. ACM.
[19] Hodges, A. (2005), 'Can quantum computing solve classically unsolvable problems"
[20] H.K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrary long distances. Science 1999; 283(5410): 2050-2056.
[21] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
[22] L. Lydersen, Wiechers, C., Wittman, C., Elser, D., Skaar, J. and Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics 4, 686, 2010.
[23] K. Inoue, Quantum Key Distribution Technologies. IEEE Journal of Selected Topics in Quantum Electronics, vol. 12, no.4, July/August 2006.
[24] http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm
[25] http://www.bbc.co.uk/news/scienceenvironment-16636580
[26] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm
[27] G. Brassard, T. Mor and B. C. Sanders, \Quantum cryptography via parametric downconversion", in Quantum Communication, Computing, and Measurement 2,P. Kumar, G. Mauro D'Ariano and O. Hirota (editors), Kluwer Academic/Plenum Publishers, New York, 2000, pp. 381.
[28] P. D. Townsend, \Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems", IEEE Photonics Technology Letters, Vol. 10, 1998, pp. 1048.
[29] J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartnerseven- cloud-computing-security-risks-853, 2008.
[30] C.C.A : CipherCloud Gateway Architecture, www.ciphercloud.net.
[31] M. v. Dijk and A. Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In Hot topics in Security (HotSec'10), pages 1{8. USENIX Association, 2010.
[32] Kamara and Lauter . CS2: A Searchable Cryptographic Cloud Storage System,IJSIR,2012.
[33] G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identi_cation protocols. In Advances in Cryptology - ASIACRYPT '09, volume 5912 of Lecture Notes in Computer Science, pages 319{333. Springer, 2012}.