IJIAM
International Journal of Informatics
and Applied Mathematics

International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 2, No. 2, 15-27

State of the Art in Some Cloud Security Through Data Tracking

Mebarka Aya DEY, Ahmed Chaouki LOKBANI, Reda Mohamed HAMOU,
Mohamed Amine BOUDIA, and Abdelmalek AMINE

GeCode Laboratory, Department of Computer Science, Tahar Moulay University of Saida, Algeria
deymebarkaaya@gmail.com

Abstract. Today cloud computing helps small businesses and users who miss them powerful resources, a shared information system or data security, etc.Let's introduce through this article: cloud service models, cloud deployment models and essential features, computer security in general. The different solutions proposed in the field of cloud security.We finish with a conclusion and our proposal in this domain to strengthen the security of this new paradigm.

Keywords: cloud computing · computer science security · cloud security · data tracking · traceability.

1 Introduction

Cloud computing is a new paradigm, a set of technologies information and computer components (hardware,software,networks and services)to provide the delivery of computer services via the Internet or a particular network.It is composed to models of services,deployment models and essential features. Cloud computing is radically different from the traditional approach that companies take in computing resources here are some common reasons why organizations opt for cloud computing services:

- Cost: It allows them to replace capital costs with variable costs [1]
- Speed: The resources of huge calculations can be implemented in minutes and with a few clicks, offering businesses a high level of flexibility and storage [2]
- Global Scaling: This means that it is possible to implement the necessary amount IT resources when they are needed [2]
- Performance: Cloud services run on a network of secure data centers,whose hardware is regularly upgraded to ensure fast performance and effective [2]

Despite these advantages, the question of data security remains an obstacle to business confidence and users.This document is organized as follows: Section 2 shows a view of the clouds. Section 3 gives an overview of IT security in general. Section 4 deals with cloud security. Section 5 presents some related work on cloud security. Section 6 discusses the layered methodology, and sections 7 and 8 present a review of some technical solutions to enhance data security, and we finish with a conclusion.

2 Cloud View

2.1 The Service Models

1. Iaas: (Infrastructure As A Service) provides a virtual infrastructure (server, virtualization layers) storage, networks). The user can - for example - rent servers Linux, Windows ... etc. These systems actually run in a virtual machine like: Amazon Web Services.
2. Paas: (As A Service Platform) is a platform for running software and applications, on the which user will be able to install, configure and use the desired applications like: Microsoft Azure, Force.com and Google App Engine.
3. Saas: (Software As A Service) This is to make an application accessible to end users in services like: Google Gmail or Yahoo Mail.
4. Xaas: (Anything As A Service) largely encompasses a software component activation process reusable on the network. [1]

2.2 Cloud Deployment Models

The main cloud deployment models are as follows:

1. Private Cloud: It is hosted internally and is used by a single organization. Infrastructure can placed on the premises of the organization or outside.
2. Community cloud: it is shared by several organizations for the needs of a community who wants to pool means (security, compliance, etc.).
3. Public Cloud: It is hosted externally, open to the public or to large industrial groups. This infrastructure is owned by an organization that sells cloud services.
4. Hybrid cloud: it is composed of one or more models above which remain separate entities. These infrastructures are linked together by the same technology that allows the portability of applications and data.

2.3 The Essential Characteristics

The essential characteristics are given below:

1. On-demand self-service: provides the customer with computing capabilities and resources at the time of need and demand;
2. Broad network access: Access and capabilities are available over the network through devices standards;
3. Pooling: Many customers consume the same services and same resources;
4. Fast elasticity: scalable service and flexibility in its modification and deployment;
5. Measured Service and Usage Billing: The customer will pay just what has consumed.

3 Computer Science Security in General

Computer security is all the means implemented to reduce the vulnerability of a system against accidental or intentional threats.

3.1 Objectives of Computer Security

The notion of security refers to the ownership of a system, service or entity.She speaks most often by the following security objectives:

1. Integrity:That is to say,to guarantee that the data are the ones we believe to be;
2. Confidentiality:Ensuring that only authorized persons have access to resources exchanged;
3. Availability:Let the information system running good;
4. Non-repudiation:Ensures that a transaction can not be denied;
5. Authentication:Ensures that only authorized people have access to resources.

3.2 Fields of Application of Computer Security

These objectives apply in different fields or fields of application,each one involves different techniques to achieve the same objective(s);these fields are:

- Physical security;
- Personal security;
- Procedural security;
- The security of physical emissions (screens, power cables, power consumption curves current ...);
- The security of the operating systems;
- Security of communications;
- Cloud security.

4 Security in the Cloud

Cloud computing based on multi-lease technologies(see figure below)and virtualization This introduces new risks and security vulnerabilities specific to cloud computing.In addition to the risks of traditional environments [13].Security risks in the cloud may differ from the risks of traditional IT infrastructure,either in nature or tensity or both [14].

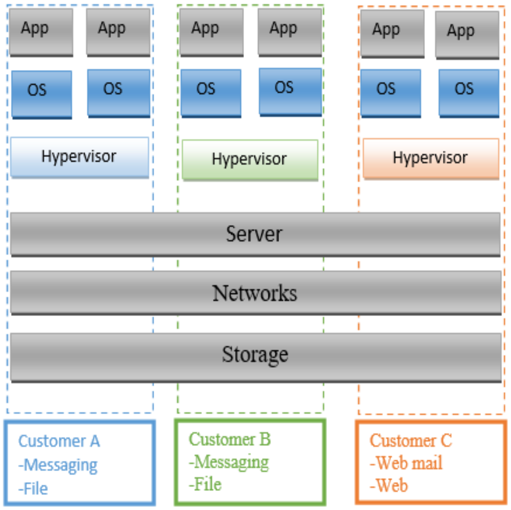


Fig. 1. Secure multi-tenancy

The pooling of resources allows a saving on materials and therefore indirectly a decrease in power consumption through virtualization technologies and multi-locations,but these technologies introduce some risks into the system.Sharing the infrastructure structure between multiple clients leads to the risks of data visibility by other users.Of more,cloud users want to ensure that critical data is not accessible and used illegally,even by cloud providers.On-demand service is provided to customers through web-based management interfaces that causes the probability of unauthorized access to the interface of higher management than traditional systems.

According to [14], there are two types of communication:

1. External communication(between clients and cloud).
2. Internal communication(between the cloud infrastructure).

For the first,cloud services are accessible via the internet using and standard internet protocols to transmit data or applications between clients and the cloud.This type of communication is similar to any other communication on the Internet.Indeed,data in transit can be the target of several malicious attacks [13] [14].Among these attacks,we can deny denial of service(Dos),listening,identity theft,home environment,etc. Regarding the second,that is to say the communication between the MVs.This communication is targeted awakening attacks because of the following factors,the shared communication infrastructure,virtual network and the bad configuration of security.According to [15],cloud security must be everyone's business, namely,providers,providers and users.Cloud security requires deep questioning corporate security policies.They must go beyond the narrow management of passwords connection privileges.It is necessary to go over to the next step and to think about security of use and types of data.The more sensitive they are,the higher the security must be and the more the choice of Cloud type is critical and crucial.Public Cloud security level is not optimized for use professional,but the flexibility of use and its quality-price can make it attractive in the eyes of many small structures.

The Private Cloud meanwhile rests on the same principle as the public cloud, but it is well owned by a business and to a smaller number of users, customers or partners of the company owner.Finally Cloudhybride is a mix of private and public Cloud.It is composed of several partners internal and external.His interest lies in his ability to navigate data between the public part and private according to their sensitivity in order to optimize costs.Whatever its type, suppliers cloud solutions rely on a mix of proprietary code and open source to ensure security and the integrity of the data they host and protect.According to [16], Whatever the form of the contract of Cloud Computing,this contract must absolutely include these five key points,namely,data localization,Law and Jurisdiction,service levels provided by the cloud provider,reversibility and access to data and data security.In addition,the order of importance of these five key points will vary according to the service used (IaaS, PaaS, SaaS) and its purpose (storage space, development environment, billing).According to [17],Cloud security challenges are the dispersion of data and international laws respect for privacy, need for isolation management,multi location,logging challenges,data ownership issues and service quality guarantees,dependency on secure hypervisors,attraction of hackers (interesting target),security of virtual OS in the Cloud, possibility of interruptions Massive Service, Encryption Requirements for Cloud

Security,Public vs.Cloud Security private cloud security and lack of public version control device of SaaS versions.And among the main threats according to CSA / HP are among others,abuse and misuse Cloud Computing,Insecure APIs and APIs,Internal Malware, Sharing Problems of technology,loss or leakage of data,misappropriation of account or service and finally risk profile unknown.In addition,ENISA identified thirty-five security risks,these risks are related to political risks and organizational,technical,legal and non-cloud risks.And among the highest risks according to ENISA we find,locked in a solution,loss of governance and control,compliance challenges,insulation failure (multi-lease),court order,quote,search warrant seized by local government,change of jurisdiction,data protection and finally network (congestion, non-optimal use ...).Secure colocation consists of hosting on cloud applications and data from multiple customers (companies,organizations,business entities ...) to within a single physical infrastructure,pooled,while respecting security,particularly sense of confidentiality.According to [18], there are nine main risks,namely,loss of control and / or governance,deficiencies in interfaces and APIs,compliance and maintenance of compliance, data localization,segregation or isolation of environment and data, loss and destruction mastered data,data recovery,malice in the use and finally usurpation.From legal responsibilities for data security and privacy in the Cloud according to [18],there is Customer is legally responsible for its data and usage,including any their compliance with legal obligations.While, the Service Provider is subject to obligations technical and organizational.It is committed to preserving the integrity and confidentiality of the data,to protect and retrieve data,encrypt data,etc.

5 Related Work on Cloud Security

Privacy and data security are paramount in the use of services cloud. There are several works in this field [3][4][5].Models,approaches and techniques are proposed to protect the data.

- Mr.Singh and S.Singh [6] proposed a multi-level authentication system aimed at strengthen security in financial transactions.
- Satish and Anita [7] proposed a fake screen method to provide two-way authentication levels in the cloud computing.
- While, Arasu et al. [8], proposed a method using the message authentication code in which the cryptographic key, the message and the hash function are concatenated together to provide authentication.
- Parsi and Sudha [9] proposed a method using the RSA algorithm for authentication and secure transfer of data. This method involves a key generation phase, encryption and decryption. In [3] He proposed a data security technique in the cloud by the combination of different mechanisms, namely: multi factor authentication with a password single-use and the authentication code of a message cryptographic fingerprint with a key. In [10], the concept of digital signature with the RSA algorithm has been proposed, to encrypt the data

before transmitting it over the network. This technique solves the problem authentication and security using privacy techniques.

- Balasaraswathi and Manikandan [11] proposed a multiple cloud architecture based on the partitioning of encrypted data with a dynamic approach to secure information in transit or remainder.

According to the analysis of several approaches to secure data transfer, these approaches focus on mainly on authentication settings.Indeed,data in transit to the cloud can be attacked by various unauthorized interceptors.A particular method could not be processed all questions of data security and condency.Therefore,different techniques and integrated mechanisms should be used[12].

6 Layered Methodology

6.1 Data Security Model Proposed in the Cloud

The layered approach has been given in Figure 2,where the first layer is responsible for user authentication .The second layer is responsible for anonymizing data and protection of users' privacy and the third layer is responsible for data recovery and tearing[19][20].

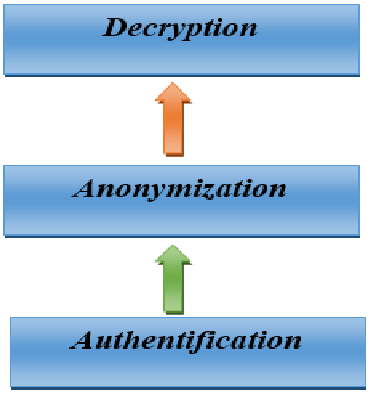


Fig. 2. Cloud data security model

6.2 OTP Mechanism

One time password (OTP) mechanism where the single-use password is a password that is not valid only for one session or one transaction. The use of multifactor authentication with OTP reduces the risks associated with connecting to the system from an unsecured workstation[21]. OTP is as a validation system that provides an additional layer of security for data and sensitive information by requesting a password that is only valid for one connection. In addition, this password is no longer chosen by the user, but is automatically generated by a method pre-calculated, which will eliminate some gaps associated with static passwords such as gaps password longevity, password simplicity and brute force attack. OTPs are generated on the server side and sent to the user using a telecommunication channel. They are not susceptible to malicious users to find the username and password to access the resource. There is nothing you can do to get in the cloud without the right combination of usernames, the password and the one-time password. An to secure the system in a more secure way,the generated OTP must be difficult to estimate, find, or trace by hackers. Therefore, it is very important to develop algorithms for secure OTP generation[22]. Several elements can be used to generate a one-time password that is difficult to guess[23], namely, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), user name, PIN, minute, hour, etc.

7 Technical Solutions to Reinforce Data Security

It can be said that data protection in cloud computing can be similar to data protection in a traditional data center. Authentication and identity, access control, encryption, integrity and traceability are data protection methods applicable in cloud computing. This section will briefly review these methods.

1. Authentication and identity: Authentication of users and even of communicating systems is carried out by various means, but each of them is underlying cryptography. User authentication takes many forms, but all are based on a combination of authentication factors: something a person knows (such as a password), something they own (such as a security token) or a measurable quality that is intrinsic to them (as a fingerprint)[24]
2. Access control: Access control:Access control mechanisms are an essential tool to maintain a complex IT environment that supports the separation and integrity of different levels or categories of information belonging to multiple parties.But the controls They are supported by many other security features.Access controls are generally described as discretionary or non-discretionary,and the most common models are: Discretionary access control (DAC), Role-based access control (RBAC),Mandatory access control (MAC)[24]
3. Encryption: Is a key component to protect data at rest in the cloud.It is important to use an appropriate reinforced chipping:Strong chipping is preferable when inactive data has a continuous value over an extended period of time.If surgical data of this long-term value is obtained by a third party and they have a long period of time to break or tear the chirement,the reward is worth it[24].
4. Integrity: In the context of cloud computing,data can be distributed or copied across multiple cloud provider datacenters,information integrity mechanisms

must be in place.To be implemented.Thus,in the context of information exchanges between an organization and its As a cloud provider,SSL/TLS protocols also help to ensure data integrity,by implementing either a hash function in addition to a chipping algorithm(this is the mode called Hash-based Message Authentication Mode (HMAC)),or to use an algorithm(this is the mode called Galois/Counter Mode (GCM)).And at the level of the resources and data stored in a cloud,it will be appropriate for an organization to focus on the integrity protection and monitoring tools provided by its service provider cloud.[25]

5. Traceability: As a general rule,any application in production (whether deployed and then used in a cloud environment or not) generates traces or logs,allowing to obtain information related to this one.Since the applications will be based on digital data of an organization,the information contained in the logs will make it possible to know in particular the users who have manipulated this data.The objective is to have concrete elements allowing to locate the digital data of an organization.Thus,it should be verified that its supplier cloud offering Paas and/or SaaS solutions makes APIs available,so that the organization can collect the traces for processing.[25]

8 Preview

To ensure non-repudiation, a new data tracking usage technique is proposed.How?

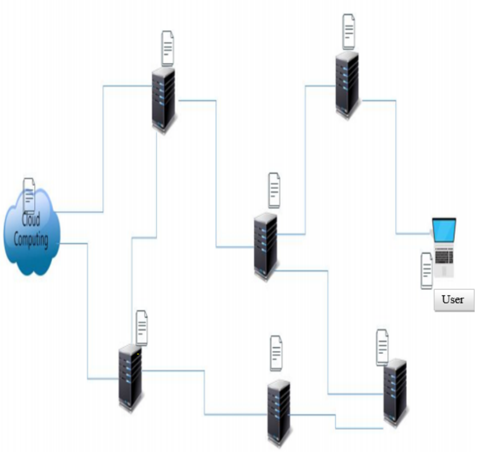


Fig. 3. Sends text data via hosts

- Text data must be sent via hosts (see figure 3);

- Mark the data by adding the ip address of each host in an encrypted this encryption is done in a way:
  - Convert the ip address to binary in the middle of eight bits(four on each side);
  - Convert the result into ascii which will be translated into characters;
  - Distribution of these characters in the data.

8.1 Case Study

1. **User side:**
   The user transmits text data via the Internet and from hosts.
2. **On the course side:**
   The original text becomes encrypted and signed with the IPs of each host during its passage through our proposal of a part of a new protocol followed by the cloud data D(SDCD).
3. **Cloud side:**
   The cloud saves encrypted and signed texts.When the text data will be attacked, the cloud can recognize the attacking host through its IP. SDCD protocol helps the cloud to do secure routing.

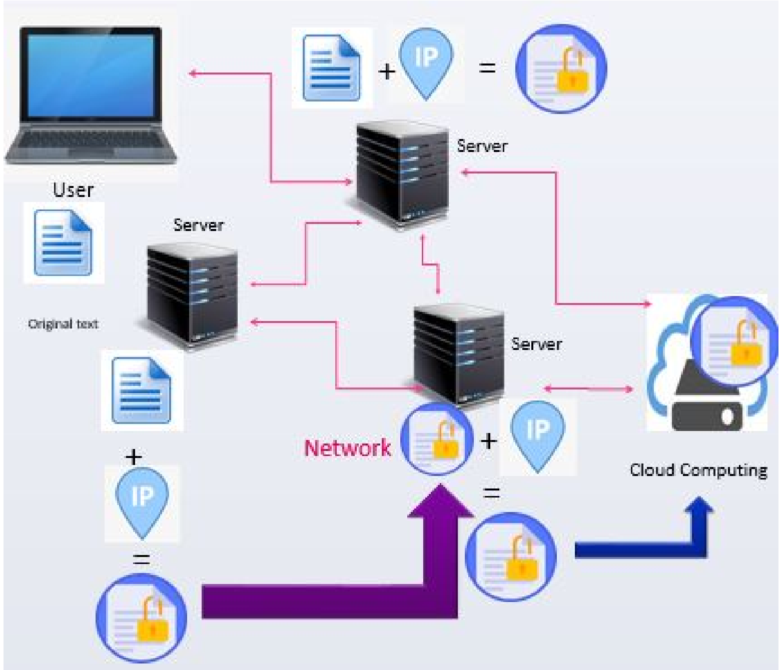
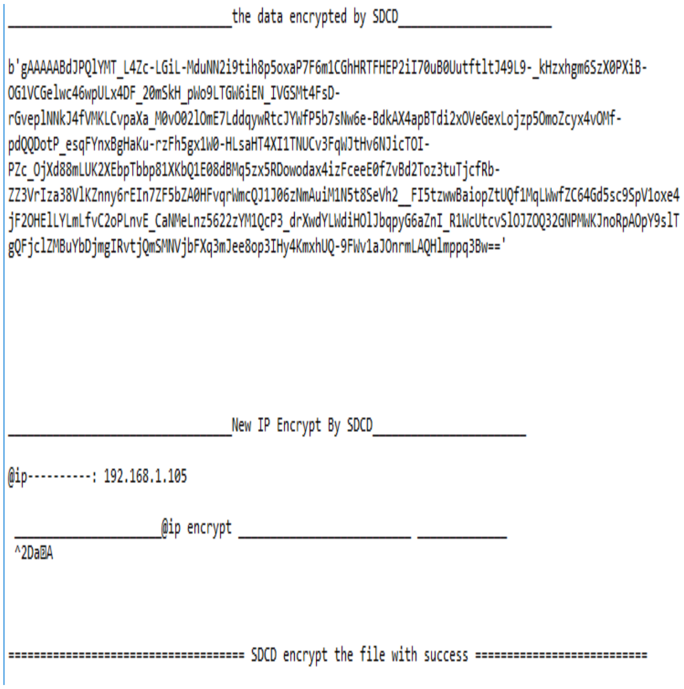


Fig. 4. Cloud security through data tracking



```
__________________________the data encrypted by SDCD__________________

b'gAAAAABdJPQlYMT_L4Zc-LGiL-MduNN2i9tih8p5oxaP7F6m1CGhHRTFHEP2iI70uB0UutftltJ49L9-_kHzxhgm6SzX0PXiB-
OG1VCGelwc46wpULx4DF_20mSkH_pWo9LTGW6iEN_IVGSMt4FsD-
rGveplNNkJ4fVMKLCvpaXa_M0vO02lOmE7LddqywRtcJYWfP5b7sNw6e-BdkAX4apBTdi2xOVeGexLojzp5OmoZcyx4vOMf-
pdQQDotP_esqFYnxBgHaKu-rzFh5gx1W0-HLsaHT4XI1TNUCv3FqWJtHv6NJicTOI-
PZc_OjXd88mLUK2XEbpTbbp81XKbQ1E08dBMq5zx5RDowodax4izFceeE0fZvBd2Toz3tuTjcfRb-
ZZ3VrIza38VlKZnny6rEIn7ZF5bZA0HFvqrWmcQJ1J06zNmAuiM1N5t8SeVh2__FI5tzwwBaiopZtUQf1MqLWwfZC64Gd5sc9SpV1oxe4
jF2OHElLYLmLfvC2oPLnvE_CaNMeLnz5622zYM1QcP3_drXwdYLWdiHOlJbqpyG6aZnI_R1WcUtcvSlOJZOQ32GNPMWKJnoRpAOpY9slT
gQFjclZMBuYbDjmgIRvtjQmSMNVjbFXq3mJee8op3IHy4KmxhUQ-9FWv1aJOnrmLAQHlmppq3Bw=='





__________________________New IP Encrypt By SDCD__________________

@ip---------: 192.168.1.105

 ________________@ip encrypt ___________________ __________
 ^2Da□A



=================================== SDCD encrypt the file with success ==========================
```

Fig. 5. the result of a part of the SDCD protocol

9 Conclusion

Despite the features and benefits of the cloud.The user is always afraid because of several security challenges that can be summarized by:

- data security,
- Network security,
- data integrity,
- data segregation and access to data,
- authorization and authentication,
- data availability,
- security of virtual machines.

So from the study of cloud security solutions,informatics security and cloud security challenges,we propose a new security system based on data tracking with digital signature.We choose to realize this system with Deep Learning. This system addresses cloud security in the form of external communication (between customers and the cloud) and two informatics security objectives (non-repudiation and integrity).

References

1. Z. Al Haddad,M. Hanoune,A. Mamouni, Sécurité de cloud computing : approches et solutions,REINNOVA Vol 1 no.1, pp.67-71,Mars 2016.
2. Qu'est-ce que le cloud computing ,https://azure.microsoft.com/fr-fr/overview/what-is-cloud-computing/Last accessed17/12/2018.
3. P. Pankaj and C. Inderveer, "A Secure Data Transfer Technique for Cloud Computing," THAPAR UNIVERSITY, August 2014, 2014.
4. C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing,"Comput. Electr. Eng., vol. 39, no. 1, pp. 47–54, Jan. 2013.
5. K. Arjun, G. L. Byung, L. HoonJae, and K. Anu, "Secure Storage and Access of Data in Cloud," InternationalConference on ICT Convergence (ICTC), 15-Oct-2012.
6. S. Maninder and S. Sarbjeet, "Design and Implementation of Multi -tier Authentication Scheme in Cloud,"IJCSI Int. J. Comput. Sci., vol. 9, no. 2.
7. K. Satish and G. Anita, "Multi-Authentication for Cloud Security: A Framework," Int. J. Comput. Sci. Eng.Technol. IJCSET, vol. 5, no. 04, Apr. 2014
8. A. S.Ezhil, G. B, and A. S, "Privacy –Preserving Public Auditing In Cloud Using HMAC Algorithm," Int. J.Recent Technol. Eng. IJRTE, vol. 2, Mar. 2013.
9. P. Kalpana and S. Singaraju, "Data security in cloud computing using RSA algorithm," IJRCCT, vol. 1, no. 4, pp. 143–146, 2012.
10. U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing,"2010, pp. 211–216.
11. V. R. Balasaraswathi and S. Manikandan, "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach," in Advanced CommunicationControl and Computing Technologies (ICACCCT), 2014International Conference on, 2014, pp. 1190–1194.
12. X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," 2009, p. 127
13. D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, Apr. 2014.
14. M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci., vol. 305, pp. 357–383, Jun. 2015.
15. B.-H. CARINE, "Cloud computing, la sécurité en question."
16. J. Guillaume, "securite-des-donnees-5-points-averifier- avant-de-signer-son-contrat-de-cloud-computing," Sep-2014.
17. S. Pascal, "Cloud Computing et Sécurité, Cycle de conférences sur cloud computing et virtualisation, Sécurité de la Virtualisation et du Cloud Computing," Paris, 2010.
18. K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilité des données entreposées dans les nuages," in 9ème atelier Fouille de données complexes (EGCFDC2012), 2012.
19. E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th InternationalConference on, 2012, pp. CC–12.
20. Institute of Electrical and Electronics Engineers, Ed., "Enhancing Data Security during Transit in Public Cloud," Int.J. Eng. Innov. Technol. IJEIT, vol. 3, Jul. 2013.

21. D. Chen and H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” 2012, pp. 647–651.
22. Balakrishnan.S, Saranya.G, Shobana.S, and Karthikeyan.S, “Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud,” Int. J. Comput. SciEnce Technol., vol. 2, Jun. 2011.
23. F. Aloul, S. Zahidi, and W. El-Hajj, “Two factor authentication using mobile phones,” in Computer Systems andApplications, 2009. AICCSA 2009. IEEE/ACS InternationalConference on, 2009, pp. 641–644.
24. Data security in cloud computing - Part 3: Cloud data protection methods,:https://www.eetimes.com/document Last accessed 28/12/2018.
25. K.Boisaubert,P.Gérard:Protection des données et cloud computing,pp.38-48, 2017-2018