Megouache *et al. Hum. Cent. Comput. Inf. Sci.* (2020) 10:15
https://doi.org/10.1186/s13673-020-00224-y

Human-centric Computing and Information Sciences

RESEARCH Open Access

Ensuring user authentication and data integrity in multi-cloud environment

Leila Megouache[1], Abdelhafid Zitouni[1*] and Mahieddine Djoudi[2]

*Correspondence: abdelhafid.zitouni@univ-constantine2.dz
[1] University of Constantine2-Abdelhamid Mehri, Constantine 25000, Algeria
Full list of author information is available at the end of the article

Abstract

The necessity to improve security in a multi-cloud environment has become very urgent in recent years. Although in this topic, many methods using the message authentication code had been realized but, the results of these methods are unsatisfactory and heavy to apply, which, is why the security problem remains unresolved in this environment. This article proposes a new model that provides authentication and data integrity in a distributed and interoperable environment. For that in this paper, the authors first analyze some security models used in a large and distributed environment, and then, we introduce a new model to solve security issues in this environment. Our approach consists of three steps, the first step, was to propose a private virtual network to secure the data in transit. Secondly, we used an authentication method based on data encryption, to protect the identity of the user and his data, and finally, we realize an algorithm to know the integrity of data distributed on the various clouds of the system. The model achieves both identity authentication and the ability to inter-operate between processes running on different cloud's provider. A data integrity algorithm will be demonstrated. The results of this proposed model can efficiently and safely construct a reliable and stable system in the cross-cloud environment.

Keywords: Security, Multi-cloud, Authentication, Cryptography, Data integrity

Introduction

The National Institute of Standards and Technology (NIST) defines the fundamental of cloud computing as a concept for delivering a shared pool of configurable computing resources, which can be provisioned and released with minimum management effort and service provider interaction. Also, it enables convenient, on-demand network access to these resources [1].

Most companies today are increasingly interested in taking advantage of the flexibility and choice of multiple cloud offerings and adopt more than one cloud to make the best use of a variety of services [2].

Multi-cloud is a combination of multiple public clouds and private clouds [3]. Its goal is to enable cloud users to avoid vendor blocking and make the best use of multiple cloud services that can cooperate and interact with each other [4]. In 2018, the International Data Corporation predicted that more than 85% of IT companies would invest

in a multi-cloud architecture and adopt it [4]. Although this new technology has many advantages, it also presents significant challenges in terms of data security [5].

Therefore, before making the transfer of the data towards multi-cloud, the company owes to classify them and choose Cloud adapted according to her needs [6]. However, organizations are very worried about how security was being guaranteed in this distributed environment [7], especially when it comes to hosting their sensitive data and critical applications in the cloud [8], and also to know how to recover their data later. For that, we can consider that the first part of the problem resides in the fact that the companies do not have adequate security policies when they access the cloud [9], in this case, the problem was repeating throughout the cloud system [10]. Moreover, human errors can generate all sorts of risks, especially when running multiple instances across cloud or multiple cloud providers.

Moreover, with the development of the Internet of Things (IoT), security attacks have increased considerably. Several methods opt for the use of machine learning [11] as a solution to solve this problem, but so far they have not brought satisfactory results, because of the different constraints of the IoT, such as distribution, scalability, and low latency. Also, many researchers have proposed solutions and ideas to solve the security problem and, in particular authentication of users in multi-cloud environments. In [12], this paper investigated authentication mechanisms used in the Cloud Computing environment; the authors show that each type of cloud has its specificities in terms of authentication, and according to their classification, they explain that only certain authentication mechanisms are valid, but their classification does not seem to take into account a multi-cloud environment. In [13], the authors of this article use the features of multi-cloud computing to enhance the authentication mechanism, and this by dividing the verification tasks on different virtual machines and generate a new password for each new connection. This solution is obsolete in the case where one of the virtual machines breaks down.

Moreover, the use of a backup server, which communicates with the storage server, is a classic solution. There are, many other solutions that use the token [14–16], also named the USB key, these solutions are effective but require a periodic update of the token with cloud providers; or those based on the blockchain that guarantees the security and integrity of data inside and outside smart homes [17]. Note also, that currently many systems based on Artificial Intelligence (AI) for the protection of privacy are widely used in many fields [18], such as secure communication, a social network, data mining, etc. Although, the multi-cloud system is spreading more and more today over the world. New errors and attacks have been discovered, for example, when users click on the spam videos/photos, shared in facebook or Twitter, they may be redirected to the spammer websites. Later, spammers may steal the user's credentials using those websites [19–21]. Our motivation is to strengthen the protection of applications and data stored in this environment, and the use of authentication solutions that complicate the task of malware. For that, the main objective of our research is to improve the security in the level of authentication of the users in a multi-cloud system, knowing that the authentication is the first thing to do in all the systems clouds and, which protects the user's identity and this data [22]. For that, we will use the asymmetric encryption method, used for secure data in transmission and based on the algorithm of Rivest, Shamir and Adleman (RSA)

[23], which is very reliable in terms of security of data. The second goal is to maintain the integrity of the data saved in the different clouds by a hash algorithm.

In our framework, any user's need to access his data, he must first be registered in an authentication server; this server contains the information about the client, such as the username and password as well as other information. Only the user registered in this server of authentication is allowed to log in. The username and password authentication are encrypted. Dividing data across different clouds for secure ones are required. Secret information must be stored, in private clouds. A data integrity algorithm will present. The analysis and results of the proposed new model are analyzed, in relation, to security factors in cloud computing.

The remainder of this paper is organized as follows: In "Background" section, a brief description of security in multi-Cloud environment. "Related works" section, describes some related work in the field of security in multi-Cloud environment. In "Proposed solution" section, the authors elaborate a scheme to secure access of applications and services in the different clouds. In "Simulation and results" section, a simulation with results will be established. In "Discussion" section, the authors discuss the results and the performance of the system. Finally, in "Conclusion and futures works" section, the conclusions of this work are presented.

Background

Until now, the researchers study the security in only one sense [24]; that is to say, the customer works with one vendor Cloud, that he gives her sensitive data [8], but what will happen if the same customer decides to work in an open and distributed system that is the multi-cloud, and how will this data be restored afterwards.

Multi-cloud

Many of the public or private cloud networks are configured to work as closed systems which are not built to communicate with one another. The lack of integration between these networks makes it a hardship on organizations to combine their IT systems inside the cloud and realize productivity gains and cost benefits [21].

Unfortunately, with the current trend of using different services from different clouds, the frequency and improvement of cyber attacks are increasing at a time, knowing that the average now resides in a victim's network for more than 200 days before being detected [9]. Today, 75% of intrusions on the network are attributed to compromised user authentication, and authentication methods known to date, are not designed for distributed environments [9, 10]. However, when migrating of our data and applications to this multi-cloud model, users need to be protected in order to access their applications without problems.

Cloud service providers require customers to store their account information in the cloud. When a customer decides to use multiple cloud services, they will need to store their password in multiple clouds [25]. In this case, the number of copies of user information will be significant, and security threats will rise for both customers and cloud service providers. For this, cloud service providers will use several authentication mechanisms to recognize their customers.

Authentication

Authentication is a subdomain of security, as explained in [14]. Like security, authentication strongly depends on important aspects of confidentiality, integrity, and availability; they become obligations in the design of secure systems. As in a single cloud system, the multi-cloud must also guarantee [13, 25]:

- Ease of use: The cloud services can easily be used by malicious attackers, since a registration process is very simple, because we only have one valid credit card
- Secure data transmission: When transferring the data from clients to the cloud, the data needs to be transferred by using an encrypted secure communication.
- Insecure APIs: Various cloud services on the Internet are exposed by application programming interfaces. Since the APIs are accessible from any-where on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the enterprise customers.
- Malicious insiders: Employees working at cloud service provider could have complete access to the company resources.
- Shared technology issues: The cloud service SaaS,/PasS,/IaaS providers use scalable infrastructure to support multiple tenants which share the underlying infrastructure.

Related works

During the last years, a lot of researches and implementations on authentication and security for limiting the risk of data loss and corruption had been performed.

In their publication [26], the authors have proposed a distributed system based on replication, its objective is to be able to defend against failures, in which components of a system fail in arbitrary ways. Byzantine failure tolerant algorithms must cope with such failures and still satisfy the specification of the problems they are designed to solve, but its general problems are omission failure or execution failure or lying.

In paper [27], the authors in this article present a system called "CHARON", it is a cloud storage system able to store and share data securely and efficiently, using multiple cloud providers and storage repositories to comply with the legal requirements for sensitive personal data. CHARON implements three distinguishing features: (1) it requires no trust in any entity (2) it does not require any client-managed servers, and (3) it efficiently handles large files on a geographically dispersed storage set. With a data-centric leasing protocol, resilient byzantine way. But the use of byzantine-resilient for cloud storage implies increased latency compared to a single cloud, For this solution, the addition of a biometric solution can be more effective in terms of security and, more it allows benefits of functionality, control, verification and biometric authentication.

Authors in [28]: The model proposed which is the implementation of a secured multi-cloud virtual infrastructure consists of a grid engine on top of the multi-cloud infrastructure to distribute the task among the worker nodes that are supplied with various resources from different clouds to enhance cost efficiency of the infrastructure

set up and also to implement high availability feature. The Oracle grid engine is used to schedule the jobs to the worker nodes (in-house and cloud). Worker nodes will be acting like listeners to receive the job from the Oracle grid engine master node. The Client after proper authentication procedure submits the job to the grid gain engine. Access control is a key concern as attacks by hackers are of a great risk. A potential hacker can be someone with approved access to the Cloud.

Concerning user authentication framework, authors in [29]: They propose an access control mechanism to ensure confidentiality of data in the cloud. The mechanism is based on two protocols: ABE (Attribute Based Encryption) for data privacy and ABS (Attribute Based Signature) for user authentication. ABE is combined with ABS to ensure anonymity of users that store their data in the cloud. Key attributes and distribution is done in a Decentralized Manner. But several attacks have been discovered on DES and these methods are no longer effective with newer encryption algorithms due to the introduction of an avalanche effect.

Another approach has been proposed by researchers in [30]. The architecture consists of trusted client as well as three or more cloud service providers that provide Database as a Service. The Database as a service provider provides reliable content storage and data management, but is not trusted by the clients to preserve content privacy Authority. The client does not store any persistent data but stores a mapping table describing the storage of various fragments location.

In paper [31] the authors consider the existence of multiple CSPs (Cloud service providers) to collaboratively store and maintain the client's data. Moreover, a cooperative Provable data possession (cooperative PDP) is used to verify the integrity and availability of stored data in CSPs).The verification procedure is described as follows: firstly, the client (data owner) uses the secret key to pre-process the file, which consists of a collection of n blocks. It generates a set of public verification information that is stored in TTP (Trusted third parties), then transmits the file and some verification tags to CSPs, and may delete its local copy. This architecture could provide some special functions for data storage and management but these functions would increase the complexity of storage management. For example, there may exist overlap among data blocks and skipping.

In [32], the authors propose a solution for the confidentiality of recording location data. They build the structure multilevel query tree from the database to display the combination location data and access frequency, and then they add the noises to the query tree nodes and publish the new query as the end result. Which can improve protection location data.

The authors in [33] propose a data collection scheme preserving the confidentiality of Wireless Sensor Networks (WSNs). Their objective is to guarantee the confidentiality of sensory readings by preventing traffic analysis and flow tracing in the WSNs. They exploit homomorphic encryption functions (HEFs) in the collection of compressive data to thwart traffic analysis and maintain confidentiality. But the proposed scheme can only resist attacks from inside the network, but not from outside the network because an intermediate sensor node can be targeted by security attacks.

The authors in [34], have proposed a scheme which consists of three parts, namely selective HEVC video encryption, data integration in encrypted HEVC videos and data extraction. First, the content owner encrypts the original HEVC bitstream using stream

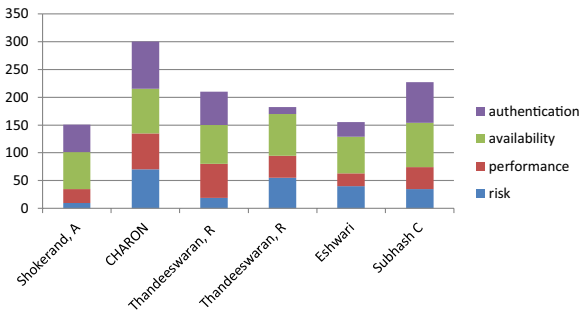

Fig. 1 Results of the degree of the fulfillment of the system comparison characteristics

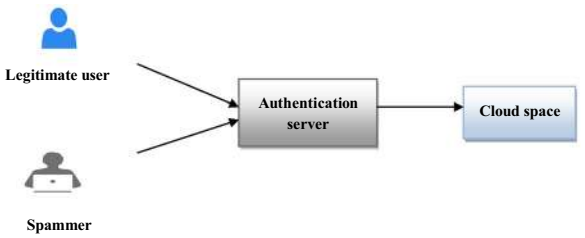

Fig. 2 Spammer's attack pattern

cyphers before sending it to the data cache. Then the data cache integrates some secret messages in the encrypted video using the coefficient modulation method. On the receiver side, data extraction and decryption are completely separable, i.e. they can be encrypted and decrypted domains. This mechanism has not been tested in complex IT environments such as cloud computing.

The authors made a comparison of these systems (Fig. 1) to better structure the authentication problem and to identify the different approaches and solutions established by the various authors cited above, for the management of security in multi-cloud environments.

Proposed solution

Despite the work cited above, as well as several other works carried in this area, the security problem still persists, and users are always afraid of losing their data, or that their data was illegally disclosed. As we know, spammers are at 80% responsible for this [35–37]. For example, a spammer can steal the identity of a legitimate user and subsequently, become the owner of a stolen account Fig. 2. But as a spammer never responds to the messages [19, 20] sent by the authentication server (such as secret questions that only the legitimate user knows), the server can filter users based on their behavior. But that was not enough to guarantee security in an open and distributed system.

In this section, the authors will present their scheme to secure access of applications and services in the different clouds. Our proposal framework contains three techniques: firstly, we create a private network virtual (VPN) between the customer and the provider; which minimizes the risk of data loss during its transfer, and to reduce the number of intrusions by offering a highly qualified security.

Secondly, we will use asymmetric data cryptography with the RSA algorithm [14, 38], to provide a high level of data security in transit. And finally, recover the information from several sources (clouds) by guaranteeing the integrity of the data using the hashing algorithm [22]. The Fig. 3 illustrates these three steps.

a. Create a Virtual private network

The first step to security is to create a virtual private network between the client and the host server, to ensure that only authorized users can access the network and that the data can not be intercepted by malicious software [24, 31]. Connecting to the VPN takes about 30 s to attempt to connect to the gateway. Sometimes a username and password are required to the user to login. In this step, two cases are possible: either the connection established successfully, or an error message occurs to indicate that the connection failed

Algorithm 1 presents method steps to connect vpn.

Algorithm 1: Steps for connect vpn customer

Connect "vpncustomer"
Input: (Username, password)
Output: (agree or refuse to connect)

```
1.  "contacting the security gate way"
2.   Initialization  Time=0;
3.  While (Time < 30) and State of connection is not known do
4.     "Wait for the connection"
5.       Time = Time + 1
6.  End while
7.  If Time >= 30
8.          "the connection is fail"
9.           "repeat the procedure"
10.  Else
11.         "The connection was successfully established"

End.
```

b. Access with authentication

The authentication mechanism plays a vital role in security controls by ensuring that only authorized users gain access to resources. Moreover, the security of any private cloud or public cloud service depends on the level of protection given to the cryptographic keys used to protect sensitive data [36].

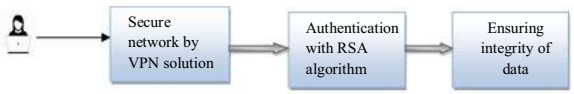

Fig. 3 The steps of proposed solution

Table 1 Defines the used annotations

Annotation	Definition
PU, PR	Public key, private key
M, C	Original message, encrypted massage
*Ai,Aj (i,j*ϵ*(1,n))*	User identity
F()	Stands for encryption
F′()	Stands for decryption
Φ(n)	The totient of n
PR(A)	A's private key
PU(A)	A's public key
PU(B)	B's public key
PR(B)	B's private key
p, q	Two different primes

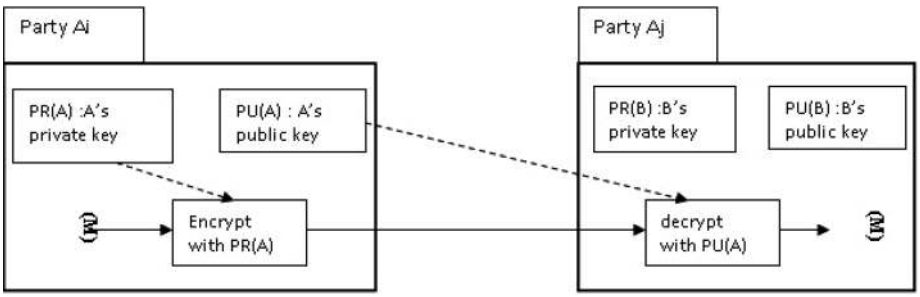

Fig. 4 Process of encryption and decryption

Encryption and decryption are carried out, using two different keys. The two keys was referred to as the public key (PU) and the private key (PR) [22, 37, 38]. If the client wants to send an authenticated message to provider, he would encrypt the message with the private key, and this message would only be decipherable with the public key, that would establish the authenticity of the message. The encryption method contains four steps, which was explaining in the following. Table 1 summarizes the most common abbreviations and Fig. 4 shows the process of encryption and decryption using the RSA algorithm.

Step-1: key generation: either the client part *Ai*, who wishes to send a message to another party who is *Aj*. The part *Ai* must convert its message which is: *M* in an encrypted form C, with the algorithm RSA: $C = F(PR(A), M)$.

The processing steps undertaken by the second part *Aj* to recover *M* of *C* is:

$M = F'(PR(B), C)$.

Now we suppose an integer M, $0 \leq M < n$, that represents our message, we transform M into another integer C who represent our ciphertext: $C = M^e \ mod \ n$ and $M = C^d \ mod \ n$, Then: $(M^e)^d \ (mod \ n) = M^{ed} \ (mod \ \_(n)) \equiv M \ (mod \ n)$.

Step-2: Generate two different primes (p,q), $n = p \times q$ and $\Phi(n) = (p-1) \times (q-1)$, $\Phi(n) = \Phi(p) \times \Phi(q)$.

Step-3: verification: The authors ensure that n is not factorizable by one of the modern integer factorization algorithms. Select for public exponent an integer e such as that: $1 < e < \Phi \ (n)$ and $gcd(\Phi \ (n), e) = 1$.

The mathematical requirement on e is that: $gcd(e, \ \Phi(n) = 1$(e, will not have a multiplicative inverse mod $\Phi(n)$) & gcd(e, $\Phi(p)) = 1$ & gcd(e, $\Phi(q)) = 1$. Or gcd(e, $p-1) = 1$ & gcd(e, $q-1) = 1$. Small values for e, are considered cryptographically insecure.

Step-4: calculate: this step is to calculate for the private exponent a value for d from e and the modulus n. Such that: $d = e^{-1} \ mod \ \Phi(n)$ or $d \times e \equiv 1$ (mod $\Phi(n)$). Since d is the multiplicative inverse of: e modulo $\Phi(n)$, Public Key = [e, n] and Private Key = [d, n].

Once the user is registered in VPN and in the authentication server, he can translate his authorized status into several applications and allows him to transition to a dispersed application environment.

c. Data integrity in multi-cloud

Here, the authors consider a data storage service composing with three different entities: Granted clients, who have the authorization to access and manipulate the stored data; and Cloud service providers (CSPs), who work together to provide security services and integrity of data and have enough storage space [14, 38]. The third-party auditor must handle the errors and must monitor the activities of the cloud server. Figure 5

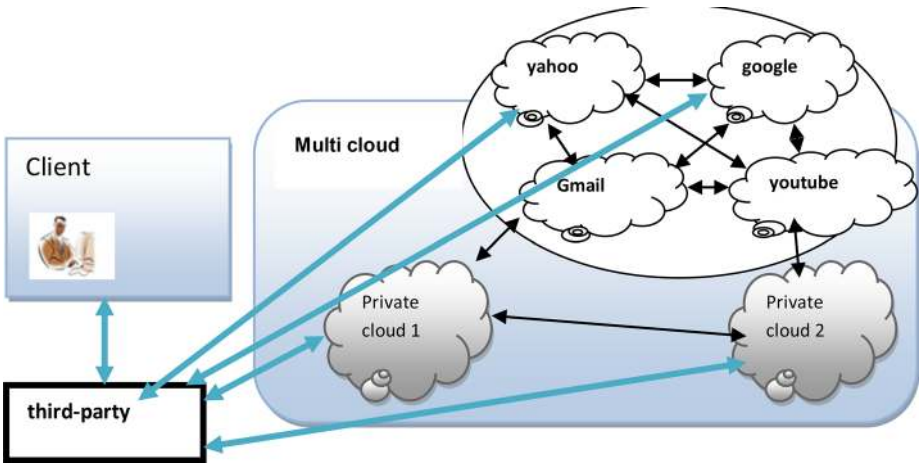

Fig. 5 An Integrity Schema in the Multi-Cloud

Demonstrates an Integrity Schema in the Multi-Cloud. Algorithm 2 presents the integrity of data method steps.

Algorithm 2: Data integrity

Input (file F)

1. **Splitfilen-blocks,indexing, {b1,b2,b3}**
   Generate key for each block ,
   public-secret key pair, KeyGen (b) {sk, pk}
   X = (r, s)
   Where X=r*s, product of two primes (*p,q*)
2. **Generate Tag for each block :**
3. **TagBlockGen(sk, Pk, bi) → {α,β,Ni}**
   α : is the secret of tag, β = (u,H),
   u :is a set of verification parameters ,
   H : Set of hash values; H = {hi}, i ∈ [1,n] ,
   Ni : index hierarchy
4. **Proof(P,V)**
   It is a protocol of proof of data possession between the CSPs
   P = {Pk}) and a verifier (V)
5. **For $p_i \in$ Pi, f_{pi}(V , (bi,pk, β,ni))= {0,1}**
   Ƒ returns a bit {0|1} denoting false and true
   where, Σf_{pi} denotes the collaborative computingin Pi ∈ P.

In the end, once the file has been approved by cloud,it can be downloaded by user.

Simulation and results

The simulation environment was built, based on the system of the national social security fund. This environment has a calculation centre which manages confidential data on insured persons such as sickness, disability.... As well, as public data such as family benefit records, drug reimbursements, and other benefits. In this organization, a very limited number of people know the access code to the information stored in Cloud servers (public, private).

So to eliminate the risk of data intrusion, we first secured the communication tunnel through a virtual private network. Once VPN access is complete, a username and password, are requested by the authentication server. This server plays a role of filtering different users according to their information (password, name, date of last access,...). The information provided by the legitimate user is encrypted by the RSA algorithm and stored at the user database on that server. Access to the database on the various public and private clouds will be authorised or refused by this server. Confidential data will be stored on private clouds and public data will be stored on the public clouds. Let's try to apply that system to that organization.

In the proposed system, the authors use two techniques to ensure authentication and security in cloud: Secure tunnel and a cryptography authentication.

1) Secure with vpn: VPN can increase security. To prevent the disclosure of private information, VPNs only allow authenticated remote access using encryption techniques.

2) Crypted authentication: At this level the username and password of the client will be encrypted and decrypted with the public and private key that are owned by both parties Fig 6. Illustrate the system.

Each function is explain as follows

- Open application and connect: the client connects to the application that has been configured at home before.
- Id user: a username and password will be requested by the application. An attacker in this system would only see encrypted data. Sender authentication is performed using the information provided when configuring the vpn on its own computer, such as the user name, password, and IP address.
- Identification and password: When the connection is established, a web page with the following IP address http:\\ 192.168.25.2 will be opened.
- Encrypt identification: in this second part the authentication will be encrypted with the RSA code.

We will now present an example based on what we have already demonstrated in the subsection 4.

Example: we select the following two primes **p, q** *where* $\mathbf{p} \neq \mathbf{q}$

$\mathbf{p} = 197$, $\mathbf{q} = 213$

$\mathbf{n} = \mathbf{p}^{*}\mathbf{q} = 197^{*}213 = 41{,}961$

For **e**:

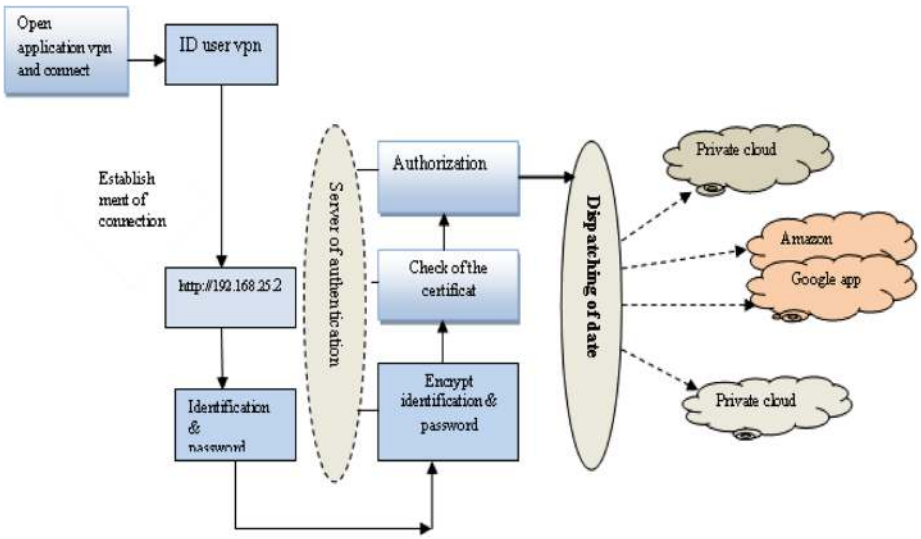

Fig. 6 An overview of the proposed system

$\mathbf{\Phi(n)} = 196 \times 212 = 41{,}552$

//**e** will also be relatively prime to 196 and 212//

Let's select e = 17 where gcd(17, 196) = 1 and gcd(17, 212) = 1

now choose **d**:

$\mathbf{d} = \mathbf{e}^{-1}$ mod Φ(n), **d** is the multiplicative inverse of: **e** modulo Φ(n), inverse of 17 modulo 41,552 is 9777.

17×9777 mod 41,552 = 1. Then e = 17, d = 9777, n = 41,961.

In our case, the two prime numbers p and q are very large, and the product of these two very large numbers is not practically factorizable. Indeed the known efficient algorithms which make it possible to verify that a number is not prime do not provide factorization.

- Check of the certificate: all the information concerning the customer is gathered in a database in the authentication server such as the name, the date of the last access, the remaining time of the contract, the password, the last operation to perform …etc., all this information is verified at every temptation to enter the client.
- Authorization: either access is allowed if all the information entered is correct, or refuse if there is a lack.
- Dispatching of data: if all permissions are acquired the data will be dispatched or query or update in the different clouds that is participating.

This system must ensure several parameters namely the availability of data, their integrity and the technology chosen for its organization (a centralized or decentralized management).

a) Availability and intégrity:

The first cloud that will receive the data (the cloud manager) of the client, he will record them on his RAID then, he diffuses them on all the other clouds of the system which will in turn save them [39–41]. But downloading one of the files must be check and without fail, for those CSPs must be cooperative [31]. The Fig. 4, showns this organization.

For the integrity, each cloud must verified this condition: If $\sum_{i=1}^{n} f_{\text{pi}}, f_{\text{pi}}(V, (bi, pk, \beta, ni)) = \{1\}$, this verification is iterative and **Proof(P,V)** is valid between CPS (show in Fig. 5). Then the file is correct and complete and there is no data loss between different clouds.

Here the different providers' hard drives work with "A Case for Redundant Arrays of Inexpensive Disks" (RAID) technology by placing data on multiple disks and allowing Input/Output operations to overlap in a balanced way, improving performance. As the use of multiple disks increases the average time between failures, redundant data storage also increases fault tolerance. With this system, if one or more drives fail, the entire

system remains functional and data integrity is available [42, 43]. The RAID meets the needs of reliability but also of high performance [44].

The most widely used redundancy system in the raid 5 is the parity calculation, it is based on the logical operation XOR (exclusive OR) and consists in determining whether on n data bits considered, the number of bits in the state1 is even or odd. If the number of 1 is even, then the parity bit is 0. If the number of 1 is odd, then the parity bit is 1. When one of the n + 1 data bits thus formed becomes unavailable, it is then possible to regenerate the missing bit by applying again the same method on the n remaining elements.

b) Organizational levels analysis:

Various organizational levels for a better distribution of controls in terms of data security in the cloud can be presented [14, 22, 42]. This organizational model represents a network model between applications and data. Figure 7 summarizes the different forms of organizational solution. The model of organizational is divided into four stages. The Fig. 8, shown the organization of model:

- Level 1: this level is characterized by completely centralized applications and data. It is an easy system to implement because there is only one governing party. Other parts are the executors of the system. The latest Internet platforms can be assigned to this level.
- Level 2: there is no centralized management, so each party must manage these applications and secure that data. Here the principle of data distribution to different participants is used in order to achieve high availability; also the maintenance of cooperation and interaction between the different parties must be ensured. This approach is similar to that of peer-to-peer.
- Level 3: decentralization of user data takes place. "Storage Cloud" technology is suitable for technological implementation because it allows for easy integration of user data storage into the system. Here the data is distributed and the central provider plays the role of authority and data management.

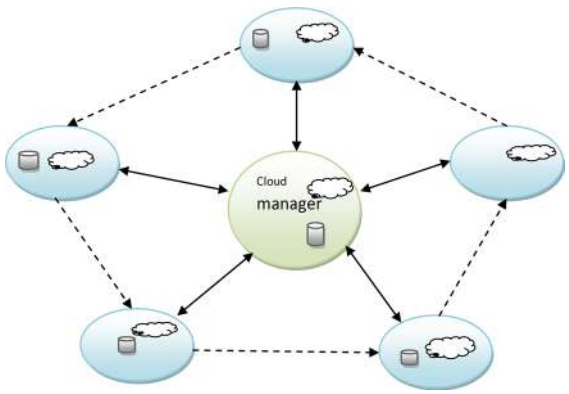

Fig. 7 Cooperation between cps

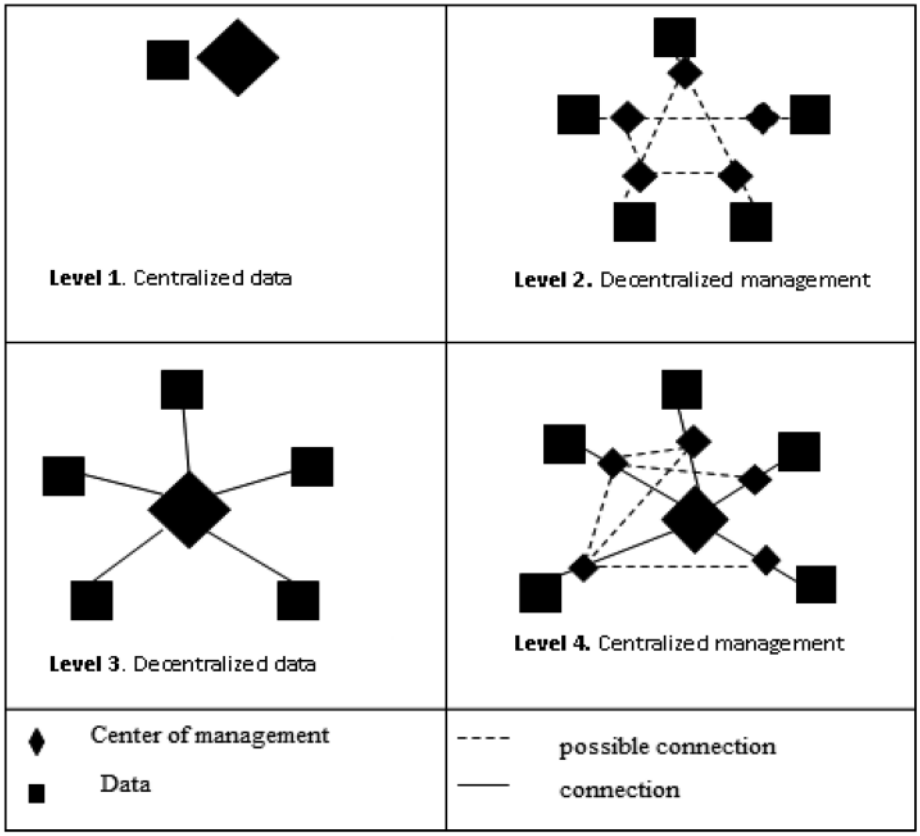

Fig. 8 Organizational levels

– Level 4: the applications and data are moved to other clouds with centralized management. The central provider maintains a register for connecting participants to each other.

This framework can be implemented by different methods and instruments appropriate. Therefore, we will use the simulation to evaluate this system according to the results obtained.

c) Evaluation:

We present our evaluation according to the criteria that we think are most important, namely: authentication and security, availability and performance, and the simplicity of its execution for the end user that we discuss in the next section.

Authentication and security level: to have a high level of security, we must have a very low probability of spammer intrusion, for this, we use the fish law, also called the low probability law, to check the credibility of our framework, this law uses two parameters:

A high number of intrusion attempts in a time interval (**t**) is: (**N**). and (**p**) the probability of occurrence of the event in a time interval (Δt) to give $\mathbf{p} > 10\%$.

Formulation with the random variable (N):
N: takes the positive value p
p: discrete, non-continuous values
λ: is a strictly positive real number
e: is the basis of the exponential (e ≈ 2718…)

$$P(N = p; \lambda) = \frac{\lambda^p \times e^{-\lambda}}{p!}$$

To test the validity of our simulation, we considered that there are two intrusion attempts per second (1S), and we want to know, what is the probability that there are exactly ten in 10 s?

2 by 1 s, that is $2 \times 10 = 20$ in 10 s
$\lambda = 2 \times 10 = 20$.

$$\mathbf{P(10; 20)} = 1\frac{20^{10} \times e^{-20}}{10!} = 0.0058$$

By this method, even if we take other values for λ, the probabilities of intrusions remain very low. Availability and performance: the distribution of data in fragments on the various clouds of the system minimizes the risk of loss and degradation of the latter. Add to that, by placing the data on multiple hard drives from different cloud providers using (RAID) technology, improving the performance of our system and also increasing our fault tolerance. The system remains functional even if a failure occurs on one of the server's.

Discussion

To validate the performance of our framework, we compared its results with other existing methods in terms of detecting attackers at the user authentication level [26–34]. The results were compared based on cryptology at the identification level, and on the validity of responses to user requests.

Then, the performance of our framework is better than other; the users can see virtual networking concept is used. In the same way, authentication server that contains the identity database is sources of truth, the exit procedures are simplified, just disable the user account which reduce errors and generate operational efficiency gains [45, 46]. If the user is an attacker then attacker has to block to the authentication server.

The main criterion is the trust relationship between all eco-systems. Therefore, centralized management is the most successful variant of trust. Basically, the goal is to better control sensitive data by offering more security than it already exists [47, 48]. In this system, when the file size is large the download time of this file by n users also increases, as formulated Fig. 9. Authors may also notice that the CPU usage is reduced a bit when the virtual network concept is used Fig. 10. In the same way, the control of the integrity of files by each provider is reduced to a minimum time.

The performance results are obtained by following the evolution of the authentication server about filtering, and security that it offers throughout the connection of the legitimate user. The authors also note the following classification in Fig. 11.

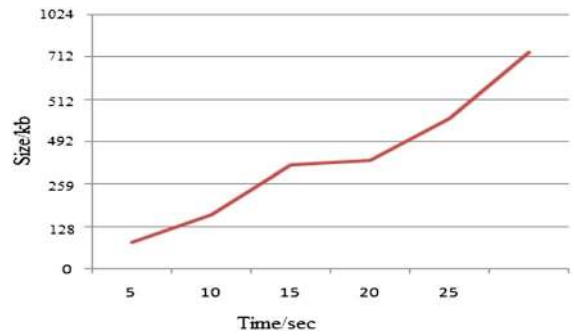

Fig. 9 Performance of server cloud

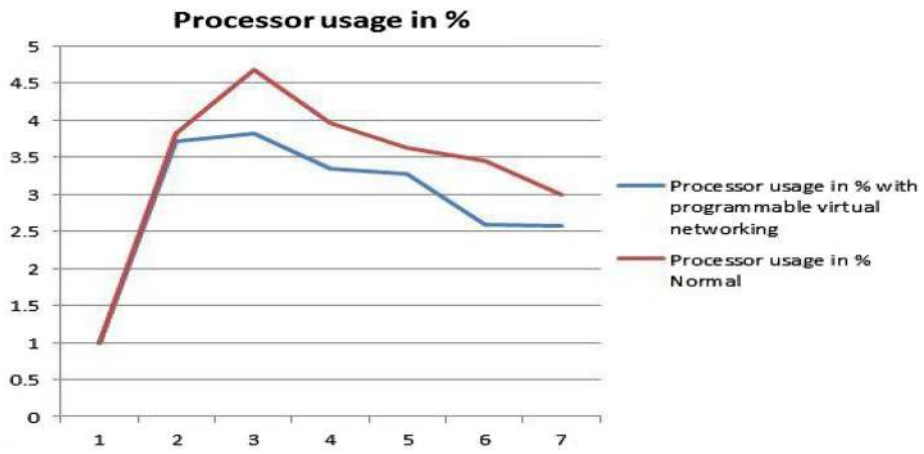

Fig. 10 Processor usage

- The first step vpn gives an efficiency between 90% and 72%, which reduce the risk of intrusion into the tunnel
- The second step authentication with asymmetric encryption (algorithm of RSA) results in a maximum efficiency of 90% and minimal 60%.
- The third step of data integrity the maximum of 80%, and the minimum of 60%.

Also, our system provides a high degree of confidence to better secure our data (90%). It is not complex (5%), responds to the budget of any organization (7%), the data remains consistent and correct (92%) with a reduced response time (8%). The authors can evaluate their system by the following diagram in Fig. 12.

In fact the Researchers are not able to adapt a system without taking into account the characteristics mentioned in this section.

In this proposition of solution the two most important properties is ensured:

1. Resistance against impersonation attacks: Communication between the user and the AS during authentication requires knowledge of the private key of one of the parts. But the private key PR is managed by the authentication server and it is impossible to have it. As a result, identity theft attacks become impossible.

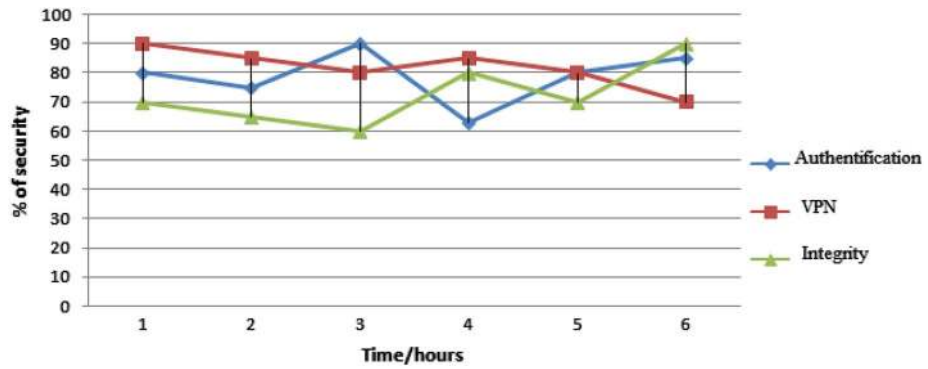

Fig. 11 Performance of system

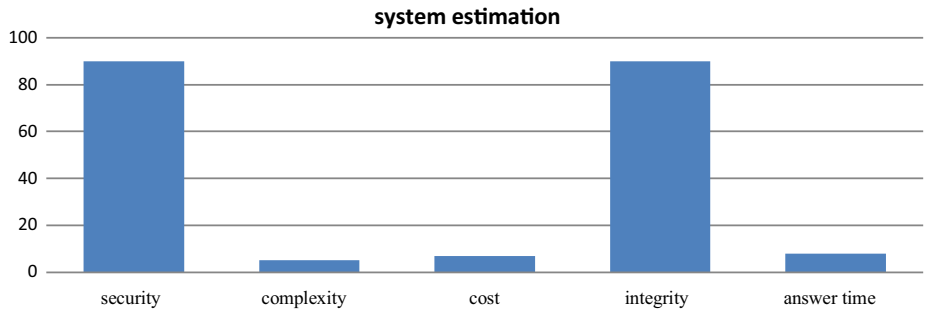

Fig. 12 Evaluation of proposed system

2. Impossibility: this property is related to the different phases of our system this is because only the user who owns the VPN application is able to generate a valid user login request. In the second part of the login phase of the user, the user communicates in encrypted form with the authentication server. And the third phase the data is segmented between different clouds. So even the risk of intrusion of the wrong-intentioned person is very low.

Note that in the case study, our company uses and generates data of different types such as text, images, video, audio…etc. Which will be stored on all the clouds in the system, this is multimedia data. Not to mention that some diagrams use the multi-level query tree to show the combination of location data and access frequency [32]. Our solution is based on the distribution and storage of data in each cloud of the multi-cloud system in a RAID type configuration, which allows to always have a copy of the original file. And with the data integration process, we can get images very similar to the original data.

Currently we can compare our system with some other mechanisms mentioned in section three, namely [26–34] (see Table 2). This table compares these systems with ours in terms of data security, availability, complexity and risk.

Table 2 Comparing and contrasting of system

Author (s)	%Authentication	%Availability	%Complexity	%Risk
Shokerand A	••	•••	••••	••
Bessani	•••	••••	•••	•
Thandeeswaran R	••	••••	••	•••
Thandeeswaran R	•••••	••••	•	•••
Eshwari J	•••••	••••	••	•
Kavitha M	•••••	••••	•••	••••
Our system	•••••	•••••	•	•

•••••: very good ••••: good •••: medium ••: weak •: very weak

The challenges for all decentralized architectures as in this study are the areas of security, data availability and data integrity. In addition, a reliable and trustworthy system must to be installed. For this, the aim is to develop a system with high data security and low complexity and at the same time, the user no longer needs to worry about the security of his data but must answer questions regarding the acceptance of data and reduced complexity.

Conclusion and futures works

A new secure multi-cloud architecture, preserving the confidentiality and integrity of data has been demonstrated. When you process sensitive information such as, in social insurance, which collects personal information about people or banking data, the confidentiality and authentication of users is of paramount importance. Also, the efficiency, the security and the integrity of the data that the multi-cloud could fear are essential criteria for the acceptance of these remote services.To meet these requirements, the authors have proposed a system that uses encrypted authentication, which guarantees that only the authorized person has the right to access the data as well as an algorithm that verifies the integrity of the data between the different clouds. Fragmenting data into pieces preserving confidentiality and integrity is used to minimize the risk of intrusion. The results of our simulation show that the proposed model reduces the number of intrusions of malicious people and reduces the time needed to establish a path by establishing the virtual private network.

In the future, we are looking to test the proposed method in a complex environment to test its scalability and design a system to enhance and extend current work using multi-agent systems.

Abbreviations

IoT: Internet of Things; AI: Artificial intelligence; VPN: Virtual private network; CPS: Cloud provider service; Di: Data; TTP: Trusted third parties; RAID: Redundant array of independent disks; PDP: Cooperative provable data possession.

Acknowledgements

Not applicable.

Authors' contributions

Authors contributed in various important aspects. All authors read and approved the final manuscript.

Funding

No funding was received.

Availability of data and materials
Not applicable.

Ethics approval and consent to participate
Not applicable.

Computing interests
They have no competing interests.

Author details
[1] University of Constantine2-Abdelhamid Mehri, Constantine 25000, Algeria. [2] TECHNE Labs, University of Poitiers, 1 rue Raymond Cantel, 86073 Poitiers Cedex 9, France.

Received: 16 December 2018 Accepted: 11 April 2020
Published online: 21 April 2020

References

1. Mell P, Grance T (2011) The NIST definition of cloud computing. National Institute of Standards and Technology, Special Publication, Gaithersburg, p 800
2. Jignesh S (2017) The 6 multi cloud architecture designer for an effective cloud. https://simform.com/multi-cloud-architecture. Accessed 15 Apr 2018.
3. Cloudenables C (2017) Managing multi-cloud security. https://www.corestack.io/blog/managing-multi-cloud-security. Accessed 22 Feb 2018
4. Robert P, Johnston E (2016) Worldwide cloud 2017 predictions. https://www.idc.com/getdoc.jsp? containerId = US41863916. Accessed 21 Oct 2018
5. Nicole H (2017) Security threats can come from anywhere: the multi-cloud world. http://itprotoday.com/hybrid-cloud/what-it-pros-need-know-about-multi-cloud-security. Accessed 10 Nov 2018
6. Travis W (2017) Five principles for running securely in a multi-cloud environment. https://threatstack.com/blog/5-principles-for-running-securely-in-a-multi-cloud-environment. Accessed 12 Nov 2018
7. Tweaks C (2013) Importance of cloud computing interoperabilitiy. https://cloudtweaks.com/2013/10/importance-of-interoperability-providerlockin. Accessed 15 Nov 2018
8. Bastiao Silva LA, Costa C, Oliveira JL (2013) A common API for delivering services over multi-vendor cloud resources. J Syst Softw 86(9):2309–2317
9. Data integrity service in multi-cloud and distributed cloud storage environment. In: The 5th international conference on advanced computing and communication technologies. IEEE, India, p 490–494
10. Brauer K (2011) Authentication and security aspects in: an international multi-cloud, https://theseus.fi/bitstream/handle/…/Karsten_Brauer.pdf. Accessed 12 Dec 2018
11. Abusitta A, Bellaiche M, Dagenais M, Halabi T (2019) A deep learning approach for proactive multi cloud cooperative intrusion detection system. Future Gen Comput Syst 98:308–318
12. Belbergui C, Elkamoun N, Rachid H (2017) Authentication mechanisms in cloud computing environments. Int J Inform Technol Secur 9(3):63–84
13. Zkik Ornahou, Elhajji S (2017) Secure mobile multi cloud architecture for authentication and data storage. Int J Cloud Appl Comput 7(2):213–230
14. Indu I, Rubesh APM, Vidhyacharan B (2017) Encrypted token based authentication with adapted SAML technology for cloud web services. J Netw Comput Appl 99(1):131–145
15. Munivel E, Kannammal A (2019) New authentication scheme to secure against the phishing attack in the mobile cloud computing. Secur Commun Netw 45:1–11
16. Obinna E, Faraz FM, Philipp W, Ramin Y (2017) A JSON token-based authentication and access management schema for cloud SaaS applications. In: The 5th IEEE international conference on future internet of things and cloud (FiCloud)
17. Lee Y, Rathore S, Park JH et al (2020) A blockchain-based smart home gateway architecture for preventing data forgery. Hum. Cent Comput Inf Sci. 10:9. https://doi.org/10.1186/s13673-020-0214-5
18. Ramotsoela DT, Hancke GP (2019) Abu-Mahfouz AM (2019) Attack detection in water distribution systems using machine learning. Hum Cent Comput Inf. Sci 9:13. https://doi.org/10.1186/s13673-019-0175-8
19. Shailendra R, Vincenzo L, Park JH (2017) SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook. J Appl Soft Comput 67:920–932
20. Shailendra R, Sharma PK, Park JH (2017) XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs. J Inform Process Syst 13(4):1014–1028
21. Shailendra R, Park JH (2017) Semi-supervised learning based distributed attack detection framework for IoT. J Appl Soft Comput 72:79–89
22. Siddeeq Y, Shayma W (2014) Firewall and VPN investigation on cloud computing performance. Int J Comput Sci Eng Survey 5(2):1–10
23. Ljubomir MV, Milan DS, Aleksandar S, Zoran DP (2019) Influence of encryption algorithms on power consumption in energy harvesting systems. J Sens 10:15–20
24. Arki O, Zitouni A, Dib AT (2018) A multi-agent security framework for cloud data storage. J Multiagent Grid Syst 14(4):357–382
25. Megouache L, Zitouni A, Djoudi M (2018) A new framework of authentication over cloud computing. In: Silhavy R, Silhavy P, Prokopova Z (eds) Cybernetics approaches in intelligent systems. CoMeSySo 2017. Advances in intelligent systems and computing, vol 661. Springer, Cham, pp 262–270

26. Yu H, Powell N, Stembridge D, Yuan X (2012) Cloud computing and security challenges. In: proceeding ACM-SE of the 50th annual southeast regional conference, India, pp 298–300
27. Qamar N, Ana S, Eran E (2018) Securing DICOM images based on adaptive pixel thresholding approach, computer-based medical systems (CBMS). In: IEEE 31st international symposium pp 280–285
28. Ricardo M, Tiago O, Vinicius C, Nuno N, Alysson B (2019) CHARON: a secure cloud-of-clouds system for storing and sharing big data, In: IEEE transactions on cloud computing p 19–39
29. Thandeeswaran R, Subhashini S, Jeyanthi N, Saleem Durai MA (2012) Secured multi-cloud virtual infrastructure with improved performance. J Cybern Inf Technol 12(2):11–22
30. Gawannavar M, Mandulkar P, Thandeeswaran R, Jeyanthi N (2015) Office in cloud: approach to authentication and authorization. In: recent advances in communications and networking technology, Bentham sciences 4(1): 49–55
31. Venkat RK, Avala AR (2013) Data integrity in multi-cloud storage international. J Sci Eng Adv Technol 1(7):219–223
32. Gu K, Yang L, Yin B (2018) Location data record privacy protection based on differential privacy mechanism. Inf Technol Control 47(4):639–654
33. Xie K, Ning X, Wang X, He S, Ning Z, Liu X, Qin Z (2017) An efficient privacy-preserving compressive data gathering scheme in WSNs. Inf Sci 390:82–94
34. Long M, Peng F, Li HY (2018) Separable reversible data hiding and encryption for HEVC video. J Real-Time Image Process 14(1):171–182
35. Subhash CP, Sumit J, Ravi S, Jyoti C (2018) Access control framework using multi-factor authentication in cloud computing. Int J Green Comput 121:1–15
36. Vengie B (2018) Privacy, security and Encryption. https://www.webopedia.com/TERM/V/VPN.html. Accessed 22 Sep 2018
37. Radford CJ (2017) Security in the multi cloud Era. In: Conference of the ComputerWeekly's coverage. https://linkedin.com/pulse/security-multi-cloud-era-cj-radford-laura-fernandez-dela-torre. Accessed 31 Oct 2018
38. Avi K (2018) Public key cryptography and the Rsa algorithm, lecture note on computer and network security. http://engineerining.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf. Accessed 22 Oct 2018
39. Dave K (2019) Micro- segmentation: securing complex cloud environments. Netw Secur 3:6–10
40. Latha K (2019) Sheela T (2019) Block based data security and data distribution on multi cloud environment. J Ambient Intell Hum Comput. https://doi.org/10.1007/s12652-019-01395-y
41. Chris C (2006) Introduction to the RSA and to authentication, MAT/CSC. https://nku.edu/christensen/section%2026%20RSA.pdf
42. Basappa B, Kodada BB, Prasad G, Pais AR (2012) Protection against DDoS and data modification attack in computational grid cluster environment. Int J Comput Netw Inf Secur 2074(9090):12–18
43. Max A, Eric V, Nuno N, Fernando MV (2019) Secure multi-cloud network virtualization. Comput Netw 661:45–60
44. Jon CC, Jennifer MS (2006) Prior family business exposure as inter-generational influence and entrepreneurial intent: a Theory of Planned Behavior approach. J Business Res Elsevier 60:1090–1098
45. Pritee P, Mayuri S, Prakash K, Sakshi S (2014) Public auditing: cloud data storage. In: The 5th international conference-confluence, the next generation information technology summit. IEEE Explore, pp 169–173
46. Fernandez L, Serrano A, Lastra MG (2014) Nuevas fronteras en la investigación en emprendimiento y en la docencia del emprendimiento. In:Workshop de la Sección de Función Empresarial y Creación de Empresas de ACEDE pp 223–241
47. Schaarschmid M (2012) Firms in open source software development: managing innovation beyond firm boundaries. Springer Books 1007:15–48
48. Shailendra R, Arun KS, Park JH (2018) A novel framework for internet of knowledge protection in social networking services. J Comput Sci 26:55–65

Publisher's Note