International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2018/49433 Volume 5, Issue 3, May – June (2018)

RESEARCH ARTICLE

A Diffie-Hellman and Two Step Verification based Secure Cloud Computing Paradigm

Mir Shahnawaz Ahmad
Institute of Technology, University of Kashmir, J&K, India.
mirshahnawaz888@gmail.com

Syed Rameem Zahra
Shri Mata Vaishno Devi University, J&K, India.
rameemzahra@gmail.com

Published online: 26 June 2018

Abstract – The foundation of cloud computing has been laid on five important traits: self-service on appeal, wide network access, pooling of resources (location independence), quick elasticity and quantified service. In least complex terms, it is to say that any cloud product (whether infrastructure, platform or software) is offered in a way that it can be rented by consumers over the internet (pay for what you use on demand). Owing to all these characteristics, there are enormous advantages from the viewpoint of both the vendor and the user and hence the cloud is gaining limelight day by day. However, it should not be forgotten that every coin has two sides; the level of dangers against IT frameworks is specifically corresponding to the level of developing technology. In order to make any new reliable technology, the security professionals need to pay attention to discover any new threats that could possibly be launched against it. Cloud computing has various issues, like privacy issues, confidentiality of user's data etc. which majorly depress the extensive benefits of cloud computing is restricted. Also, the concept of multi-tenancy offered by cloud computing poses new challenges to the security professionals. In this research article, we enlighten the security issues related to cloud computing and propose the corresponding possible solutions to balance out these threats.

Index Terms – Cloud Computing, Security Issues, multi-tenancy, privacy, confidentiality.

1. INTRODUCTION

Representing a standout amongst the most explored technologies, Cloud Computing has seen a quick evolution and is imagined as the cutting edge design of IT enterprise [1]. Traditionally, computations used to be performed on the mainframe computers which were owned by IT giants like IBM, Amdahl and Hitachi. The customers would buy the services of these companies to perform their computational tasks which took days to complete. Cloud computing revolutionized the way computations were performed in the way that its computational speed is higher, memory is larger, the service cost is lower and the hardware is smaller. Cloud Computing offers uniform and on-demand access to the pool of shared common resources that are configurable (like network, storage space, servers, applications and services.) and could be temporarily discharged with negligible administration efforts or service provider interactions [2]. This develops the interests of technical giants in this technology e.g. Google, Amazon, IBM, Microsoft, Yahoo to develop new trade models so as to enhance the efficiency of their services. There is currently no consensus on the definition of cloud computing [3].

National Institute of Standards and Technologies (NIST) characterize 5 fundamental attributes of cloud computing to be: on-request self-service, wide access to network, asset pooling, fast versatility and estimated service benefit [4]. [5] Define cloud computing as a dynamic and easily scalable technology that has the ability to provide shared resources to its customers via the internet. The user remains unaware of the technicalities of the cloud working and gets a direct access to its services.

Some authors describe cloud computing as the combination of services given over the web and hardware equipment and frameworks programming in datacenters that are utilized to give those services. From the user's perspective, the cloud computing can also be defined as the blend of software as a service (SaaS) and utility computing. The utility computing includes services available on the public cloud.

2. CLOUD COMPUTING KEY IDEAS

The main aim of cloud computing is to combine the fiscal value model and the development of prevailing approaches and computational techniques, which may include applications, distributed services, networks, storage resources and much more. Cloud computing has a greater impact on the reduction of costs since it makes use of the optimal techniques. Also, cloud computing has a significant influence on the collaboration, agility and scale, thus providing a true computing model on internet. For better understanding, the key features, service and deployment models of cloud computing need to be understood first.

2.1. Principal Features of Cloud Computing

The key features of an efficient cloud computing paradigm embrace: infrastructure scalability, rapidly available resources without increased overhead, broader network access, independence of location, high reliability, cost efficiency and security.

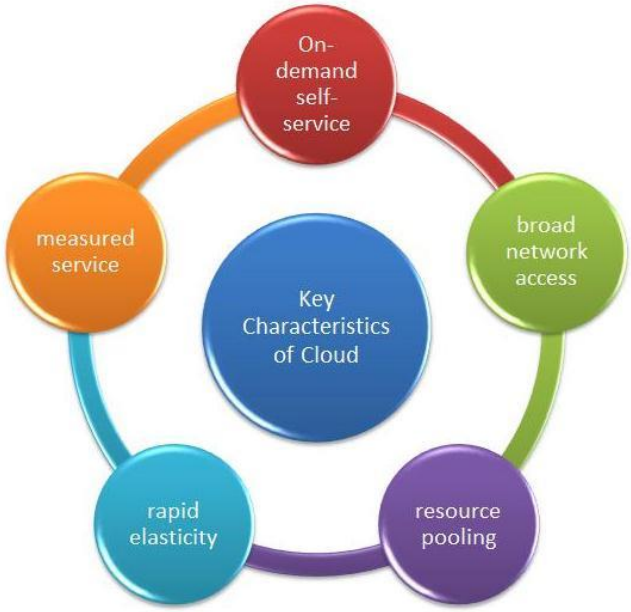

Figure 1 Principal Features of Cloud

With all these benefits, the cloud computing also has some security issues [6-9] that we have discussed in this paper and are also proposing different methods to solve those issues. A cloud acts a black-box to the user, so when the user has no information about who is providing the cloud services, what is cloud provider doing with user‘s data and what processing is done on cloud. With all these properties of cloud we need to make the cloud user feel secure in availing the services of cloud, only then we can effectively increase the gains and uses of cloud computing. Without the implementation of different security protocols and techniques in cloud computing, the cloud computing will be a total failure. One can also get confused between the grid computing and cloud computing, while grid computing has a five layered architecture comprising of fabric layer, connectivity layer, resource layer, collective layer and the application layer, cloud computing has only four layers: fabric layer, unified layer, platform layer and application layer. Also, the grid computing provides a shared access to storage and computing power from the desktop, whereas cloud computing provides a leased access to storage capacity and computing power from a desktop. The services provided by a cloud can be depicted as a layered architecture in figure-2.

2.2. Service Model

Three types of service models are included in the world of cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [10]. In IaaS, the cloud provider avails the customer with virtual machines and storage space, where the customer can run its applications and pays only for what he uses. PaaS aides in getting access to and make use of the added application block in the programming environment. Here, the cloud provider offers services such as software development framework, operating system support etc. using which the user can create his/her own application directly by using the cloud’s development environment. In SaaS, the cloud provider provides the on-demand application software to the users. The users get the option of renting the software instead of buying it, thereby benefiting them economically. Each of the layers can be seen as a service for the layer above and as a consumer of the layer below in figure – 3.

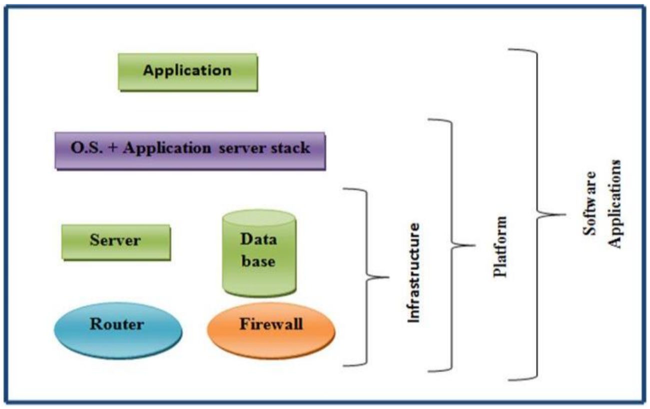

Figure 2 Cloud Services as Layered Architecture

2.3. Deployment Models

There are essentially 4 types of cloud deployment models depending upon who owns them via: Public cloud, private cloud, community cloud and the hybrid cloud [11]. A public cloud can be used by anyone and is owned, controlled and managed by a public cloud provider. It typically exhibits an open structure and hence displays a weaker security base. A private Cloud on the other hand, is owned, controlled and administered by a private group and hence only the users from within that organization can use its services. Since, the structure is not clearly open, it has a good security line. A community cloud is created and owned by multiple organizations that share some common needs and interests. By doing so, they reduce their individual utilization costs by cutting on the requirement of owning individual private clouds. Finally, the hybrid cloud is a unique mixture of a private and public clouds brought together by some proprietary or standardized technology. The organizations benefit from such hybrid clouds by transcending their side businesses into the public cloud while managing their core businesses on their privately owned cloud.

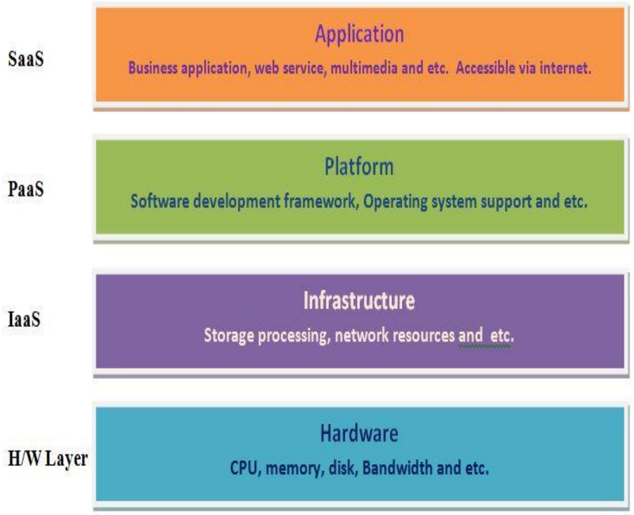
SaaS
Application
Business application, web service, multimedia and etc. Accessible via internet.
PaaS
Platform
Software development framework, Operating system support and etc.
IaaS
Infrastructure
Storage processing, network resources and etc.
H/W Layer
Hardware
CPU, memory, disk, Bandwidth and etc.

Figure 3 Layered architecture and service models.

3. CLOUD COMPUTING SECURITY THREATS

Due to the opportunities provided by new applications like mobile interactive applications, parallel interactive processing and with the introduction of web 2.0, the cloud has got more importance and greater use. The characteristic features, service models and deployment models of cloud explained earlier indicate that cloud is essentially an open system and thereby vulnerable to a lot of security threats like data loss, downtime, phishing, password cracking, botnets and other malwares. On a broader perspective, the security issues in cloud computing could be classified along 3 directions: User data security issues, Virtualization related security issues and Application related Security issues.

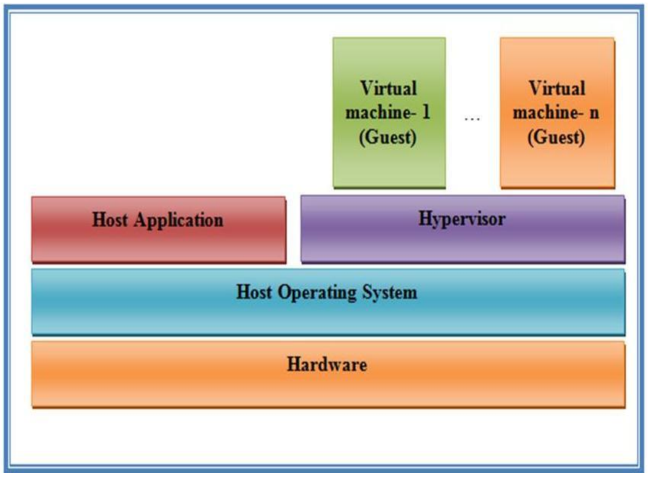

Figure 4 Location of Hypervisor in Cloud Architecture

User data Security Issues: In cloud computing paradigm, the data of user gets stored and processed on the cloud and thus the owners of data have no control on the management of their data causing multiple threats. The common user data security threats are tabulated in table-1.

Application related Security Issues: Application security pertains to the security of applications running on any system by utilizing its software and hardware resources. Presently, spoofing the identity of a trusted user is one of the most common attacks. By doing so, the attackers get an open access into the system and can carry out any type of malicious activity afterwards. The security potholes at the levels of API's or interfaces with cloud services make the cloud less secure at the application level. The common threats related to application security are tabulated in table 2.

Virtualization related security issues: To overcome the above issues we can use virtualization security [22] that includes the use of a virtual machine (VM) i.e. a software counterpart of the actual physical computers that too runs an operating system as well as the various applications for each guest, managed by a hypervisor running on the top of host operating system as shown in figure-4. Therefore, virtualization as the rooting technology of cloud computing is not ideal, as it has got some limitations like: state restores increase complexity, vulnerable hypervisor security, inter-virtual machine attacks and scaling. In state restores, the cloud restores a state after performing some series of tasks, due to which a worm can survive on the cloud and thus compromise the security of cloud data. Also, the hypervisor manages the multi-tenant virtual machines and the applications which reside on them [23] and has the ability to touch and affect anything running on these virtual machines [24] which increases the security risk because all an attacker needs to do is to take the control of hypervisor and then it can compromise anything running on that host system. With the use of hypervisors, an additional component is introduced, thus increasing the complexity of the cloud computing environment. Also, the hypervisors execute code in privileged mode, increasing the probability of executing vulnerable code by a hypervisor. One more problem with the addition of hypervisor component is the escape of malicious code from within the level of VMs and interface with other guest VMs or hypervisors [25]. The virtual machines use the shared folders to interact with each other; therefore, one can later use the image of a particular virtual machine. The security system of cloud has got a particular capacity and adding a virtual machine is as easy as copying a file, but with a climb in the quantity of virtual machines the security capacity of the cloud gets effected and the data on the cloud is exposed to security threats. Also, virtualization takes an advantage of snapshots, but this advantage decreases the performance of the cloud, because the snapshots retain the deleted data on the cloud. Lack of audit-ability has also been an issue in cloud computing, because it is just the cloud provider that has the full ease of access on the network traffic, hypervisor logs and physical machine data. So, we also require the mutual audit-ability, which can improve the security efficiency of the cloud.

User Data Security Issue	Violated Security Property	Cause	Solution	Problem with existing solution
Data Breach	Integrity, confidentiality	Employee/hacker	Strong encryption like AES, DES	Heavy Computation overhead on owner, only exact keyword search possible [12-14]
Data Lock-In	Data Access, privacy	Owner/ Bug	Standardization of cloud API e.g. GOGRID API [15]	No complete solution available.
Data Remanence	Integrity	Attacker/ server breakdown	Encrypt data and fragment the key, making administration of devices important [16]	Complex
Data Recovery	Integrity, Data Access	Server Breakdown	Backing of important data on local computers [17]	Back-up related issues like redundancy.
Data Locality	Privacy	Cloud Features	Privacy laws laid by Governments [18]	Laws not there/ less stringent

Table 1 User data security issues

Application related Security Issue	Definition and Importance	Security Issue	Probable solutions
Cloud Browser Security Issue	The universal application that satisfies the need of IO, sending/receiving in SaaS models where the client’s computations are sent to distant servers is the browser and hence of utmost importance. Its security is also therefore very crucial.	The existing internet browsers simply use TLS encryption and TLS Signatures that are not enough for defending against malicious users.	TLS and XML based cryptography to be used as suggested by [19].
Cloud Malware Injection	Here, the attacker generates an infectious VM or a service implementations and injects it onto the cloud System. The Security against this attack is crucial because the purpose of attack can range from executing tiny wiretaps to entire functionality modifications.	Legitimate user requests are forwarded to the illegitimate VM instance where the malicious code gets executed	Perform integrity check
Backdoor and Debug option security issue	The developers often intentionally/unintentionally keep backdoors in their codes. They also keep debug options for future software developments [20].	These debug points can be exploited by hackers to make entry into the system.	Tackling at the level of development.
Cookie Poisoning	Making an unapproved ingress into a website/application by modifying the constituents of a cookie.	Unapproved users obtain right of entry into the application	Cookie encryption/cookie cleansing.
Distributed Denial of Service (DDOS)	An attack is launched from diverse sources that have already been compromised.	Multiple VMs could be employed to launch attack. The server services become inaccessible to legitimate users	Intrusion detection systems on the entire traffic/ every VM [21].

Table 2 Application related security issues

4. RELATED WORK

The lack of proper security stands as a hurdle in the development of cloud computing. Various security challenges have been studied and identified in [6]. In addition, with the proliferation of mobile devices in the lives of common masses, mobility of users introduce additional security threats-ones that already exist in the domains of Ad hoc and sensor networks. In 2011, [7] presented different cloud computing security concerns which include: right of entry to server & applications, data transmission, network security, data security, data privacy, data integrity, data availability, etc. that led to focus on various facets of cloud computing environment and the need to provide secure techniques and methods concerning these aspects. Based on these concerns, the security issues include: service level agreement, data management in cloud, encryption standards, interoperability, access control, reliability and several other issues and challenges. Diogo et al [8] introduced profound security issues in a cloud computing environment and talked about numerous security dangers and assaults conceivable in it. It has categorized the security issues of cloud computing environment in different areas as: software, cloud storage, virtualization, services provided by cloud, network connectivity, access to data on cloud and mutual trust between cloud provider & customer.

Also, the user Data security issues include integrity, confidentiality, privacy and data access. The solution to the data access and privacy problem in cloud computing is given in [15], but the solution is not complete, it only emphasizes on particular issues and neglects other issues. Also, [16] proposes the method of encrypting the data and fragment the shared key, making administration of devices important, but this techniques is a bit complex and hence requires more computational power and overhead. [17] Also provides solution for data access and integrity problem, by backing of important data on local computers, but this approach results into data redundancy. The details regarding the user data security issues, their probable solutions and applicability of these solutions are given in Table – 1.

The security issues in cloud computing are also at application level, which include Cloud Browser Security, Cloud Malware Injection, Backdoor and Debug option security, Cookie Poisoning and DDOS etc (discussed in Table – 2). All these security issues are directly related to the applications used for accessing the services provided by cloud computing environment. [19] Proposed the use of TLS and XML based cryptography for securing the cloud browsers. [21] Presented an Intrusion Detection Systems, which needs to be implemented on the entire traffic/every VM, for detecting the malicious behavior. Again these solutions provide protection against a particular type of attack/security issue, one need to propose a general security mechanism for securing the entire cloud computing environment. So, in the next section, the paper presents a general security cloud computing paradigm, which makes the cloud data as well as the applications, using the services of cloud, more secure.

5. PROPOSED SECURITY AND PRIVACY IMPLEMENTATIONS

Owing to the popularity of cloud computing, the security and privacy has become a critical area of concern, henceforth, continuous attempts are being made to improve the security of cloud based computing environment. A multitude of security challenges come up in cloud computing paradigm that may include: the malicious insider, data breach, man-in-the-middle attack, data loss, account hijack and many more. In malicious insider, an attacker having the authority to access the cloud data can damage the cloud data, to avoid this type of attack, cloud provider has to be cautious in granting authorities to different people who can access cloud data or who are in the vicinity of the cloud. Another type of attack is data-breach, where an attacker can breach the cloud and can destroy or attack the data in a cloud, to avoid it cloud providers and the clients have to implement the security protocols which will authenticate the legitimate users, or we can also use audit-ability to avoid such attack. The man-in-the middle attack can be avoided by transferring only encrypted data between cloud and client. Generally the research on security in cloud computing falls in two categories: one which deals with the security of stored data on the cloud, and another includes the security of cloud computations. In this paper we will be discussing security issues in both the categories and will propose different security and privacy techniques which will improve the security of cloud data and the computations also. In this section, three security issues will be discussed in three perspectives of cloud computing: storage, processing and transfer of the message.

5.1. Data Integrity and Authentication

In a cloud computing model, there are many cloud servers that are controlled by one or more cloud providers. The cloud service provider allocates the cloud resources to the user when the cloud user requests for the storage or the computational services. The major issue here is to check the faithfulness of the cloud provider, i.e. how proficiently and safely the cloud provider will store the client data on the cloud, which has been explained by [26]. This issue can be solved either by using the public key encryption or by saving the information in cryptic form on the cloud, but the data stored on the cloud is very huge, and to encrypt it, we need a lot of pre-processing, but the capability of client to encrypt such amounts of huge data is very less because of limited processing capability. Hence, we have used the symmetric key cryptography, which will not require the bulk encryption of huge data on the cloud.

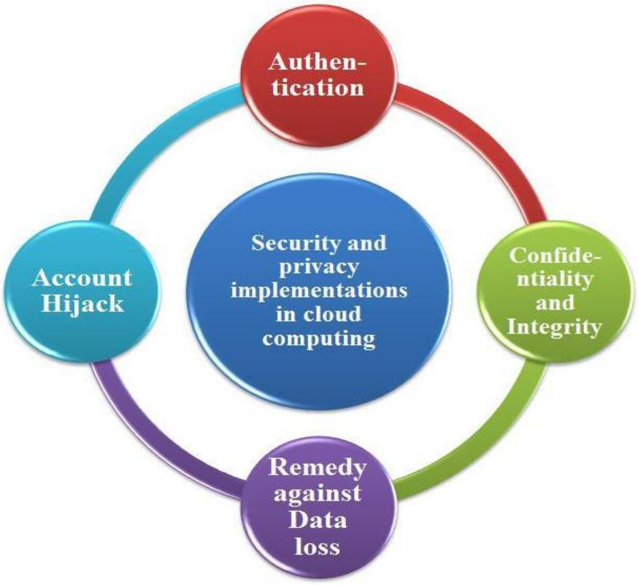

Figure 5 Security and Privacy Implementations in Cloud Computing

The basic idea behind this scheme is that the client before sending the data to cloud performs certain pre-computations. The client pre computes certain brief ownership verification tokens where every token shelters certain data blocks. After this the data is being sent to the server in which it is stored. At whatever point the customer needs to acquire the confirmation of the information ownership, it sends some arbitrary block indices, over which the server must register certain checks and send reaction to the customer. If the response matches the desired response at the client side, then the server is authentic and the data stored on the server belongs to the client whose tokens matched the tokens sent as a response by the server. The pre-computed tokens by the client can also be mounted on the cloud in an cryptic form that are small in size, and then can be decrypted by the client at the time of verification. Thus, with this scheme the client‗s storage and processing overhead are reduced, together with the achievement of integrity and authentication. In the detailed view, the whole scheme is divided into different steps.

1) *Initialization step:*

The first step being initialization part, where the client generates in advance different random challenges (sent by client to server) and tokens (sent by the server as a response). To produce a token, the client generates a set of indices as follows:

a) Compute the index of the particular data block.

b) Generate the permuted key and a challenge number using AES and a pre-defined encryption key ―X.

c) Compute the hash of different data blocks using challenge-number.

The hash, thus computed will act as a token which we expect to receive from the server when we request for our data (for which the token was created). The challenge number is being calculated by the client so as to shun the pre-computation of cloud server. Also, each token is generated using the hash function implying that its size is small and hence the storage overhead of server is alleviated. Once the token for every single data block is generated by the client, the data along with the tokens are sent to the server where they are stored. Also, each token is sent in encrypted form to the cloud using a symmetric key encryption technique (AES).

2) *Confirmation step:*

To verify the particular data block, the client re-generates the token for that data block, for which it only need to know the encryption key (X) and the index of the data block. The server only retrieves the data block for which request is being sent by the client, together with its token. Then the client will compare the regenerated token with the received token, and if the comparison is successful, then the received data blocks are in intact form and belong to that client who stored them previously on the cloud, otherwise the data block will be rejected.

5.2. Confidentiality

Confidentiality is one of the most serious concerns in cloud computing. Due to the increase in the number of access points, the threat of compromise of data mounted onto the cloud increases since the number of cloud users also increase. Due to this, a lot of issues emerge, which may include: multi-tenancy (resource sharing), data security and privacy. Once the user mounts the data on a cloud, the user has no control on it, so the confidentiality, privacy and integrity are main concerns here. Confidentiality of cloud data is correlated to user authentication, sine confidentiality also deals with hiding the user‗s account from thefts. Disclosure of information stored in a cloud is also an important issue in cloud computing. An additional concern is that of integrity meaning that the information placed on the cloud should only be allowed to be deleted or modified by a legitimate user. But, there is a certain type of data which does not require confidentiality or integrity like simple audio or video clips. Hence, there is a need to develop a technique that will offer diverse levels of security for different types of data, rooted on the demand of cloud user. For this the data stored on the cloud needs to be classified into three types, which include:

1) The first type of category includes that data where no privacy is needed. So, here the cloud provider is fully trusted and no encryption is needed.

2) The second category is met for those cloud users who completely put their faith on the cloud provider and do not doubt its intentions, but the data stored on the cloud is important and needs to be hidden. For this we can use encryption, which is done by the cloud provider using its own cryptographic key. Therefore, this type of data can be sent by the client without encryption over the secure network. Finally, the cloud provider will perform encryption on it and save it on the cloud.

3) The last category includes that type of user, who does not trust the cloud provider and also the data requires to be hidden. A provable data possession scheme was proposed in [27], a similar scheme has been presented in this paper, where the customer can encrypt the data with its own cryptographic key and then send it to the cloud. This type of data cannot be viewed by anybody except client who has encrypted it (not even the cloud provider).

```
Algorithm – 1: For achieving data integrity and server
authentication in cloud computing environment.

1) Generate random Token for each data block at the
   client side as:
   a) Generate encryption key X.
   b) Construct challenge-number with the help of
      AES using pre-computed key.
   c) Compute the index of the data block.
   d) Compute Hash for each data block using
      challenge number.
2) Store each data block along with its token at cloud
   server.
3) Confirmation step:
   a) Generate tokens at the server using an
      encryption key (X).
   b) Send the tokens & respective data to the client.
4) If token received by client & the token embedded
   with received data is same, then data is
   authenticated.
```

Now to implement security on these three types of data on a cloud, the cloud provider can use different logical pools to store different types of data, and implement different techniques and security protocols on these different types of data. To store the first and second category data, no special technique is to be implemented in the data. But, for the third category, a technique is presented that will allow the cloud user to store the data on the cloud and achieve confidentiality and integrity. To implement this technique we use different variables or tags, they include:

CID: It is a unique identification tag generated by the cloud provider, when the customer gets registered to the cloud.

AID: It is another unique identification tag which is generated by the customer for each of its applications.

K: It is a symmetric key generated by the customer.

PUC: is the customer‘s public key.

We also use digital signatures, which has been also explained by [28], where an encrypted digital signature scheme can be used for cloud computing environment. The use of digital signature, together with timestamp can be used for avoiding replay attacks, and identifications inform the cloud about the type of information sent by the customer. For huge volumes of data, a short signature scheme [29] can also be used. We use public key encryption [30] to share the secret key between cloud provider and customer. At the customer end, the customer classifies the data according to the above mentioned three categories. Only for the third type of data, the customer uses Diffie-Hellman key exchange [31] to generate the secret key between cloud provider and the customer, using which the customer can encrypt the data and send it to the cloud, thus ensuring the confidentiality of data. For integrity, we can use message authentication codes, which are again generated using the secret key developed by the Diffie-Hellman key exchange mechanism.

```
Algorithm – 2: For achieving confidentiality and
integrity in the cloud computing environment.

Assumptions:
• Each customer has CID (generated by the cloud
  provider at the time of registration).
• The algorithm executes on client side which ensures
  the secure transfer of data to the cloud.

Input: data item (d)

1)  Compute the category of data item (d).
2)  If category = I, then
3)  Send _d‘ to the server without encryption
4)  end if
5)  If category = II, then
6)  Send _d‘ to the server without encryption.
7)  Encrypt _d‘ at the server before storing it on the
    cloud
8)  end if
9)  if category = III, then
10) Generate K, PUC
11) Use Diffie-Hellman algorithm to exchange K
    between client and server.
12) Generate MAC for data block _d‘, using PUC
13) Encrypt _d‘ using _K‘ .
14) Send encrypted data block to the cloud
15) end if.
```

We can also use a trusted third party, which will ensure a secure storage and processing on the cloud and will remove the additional processing overhead from customer [32]. A trusted third party is an element that is responsible for the secure communication among the cloud provider and customer, by using digital certificates [33]. The digital certificates are distributed among the communicating parties. The trusted parties are connected with each other through certificate paths, thus forming a web of trust with the help of public key infrastructure. The use of trusted third party for implementing secure communication between cloud provider and customer can also provide authentication, confidentiality, privacy and integrity for data stored on cloud. Also, public key infrastructure [34] implemented on a single-sign-in mechanism is ideal for cloud computing environment, because with this the customer has to only sign-in for once (without repeated entering of passwords), resulting in smooth, less complex and secure communication with cloud. Also, with the help of trusted third party we can incorporate different levels of security for different types of data to be stored or retrieved from cloud. All these methods are summarized in figure-7.

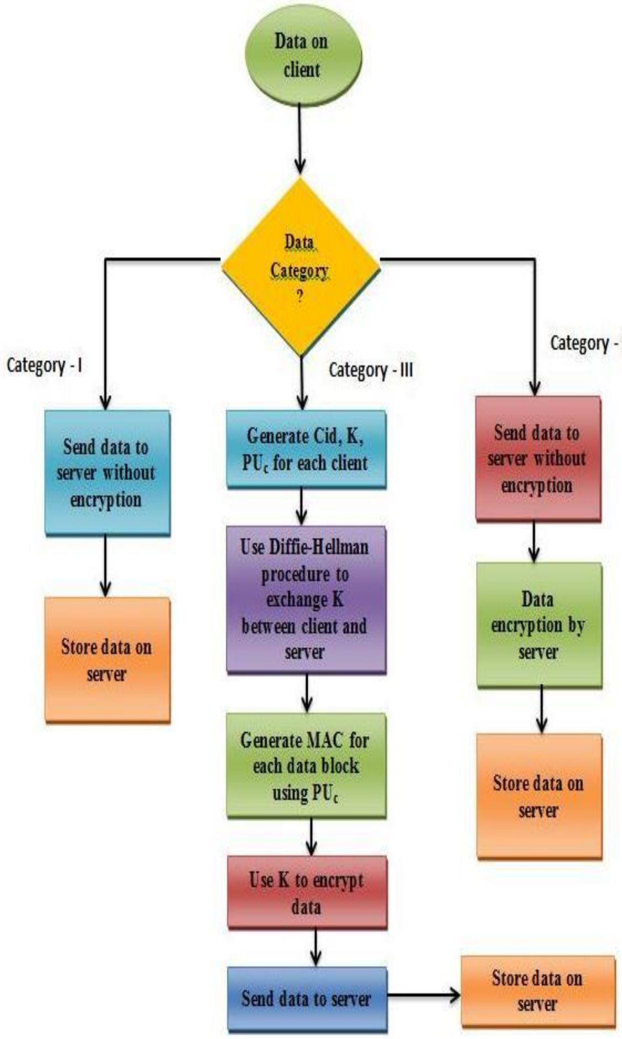
Data on client
Data Category ?
Category - I
Category - III
Category - II
Send data to server without encryption
Store data on server
Generate Cid, K, PU$_c$ for each client
Use Diffie-Hellman procedure to exchange K between client and server
Generate MAC for each data block using PU$_c$
Use K to encrypt data
Send data to server
Store data on server
Send data to server without encryption
Data encryption by server
Store data on server

Figure 6 Proposed approach to achieve Confidentiality & Integrity in Cloud Computing

5.3. Remedy against Data loss

When the customer stores data on a cloud, there are chances that the data can be lost because of accidental deletion or by accidental deletion of the customer subscription. Hence, this form of loss can occur either from the cloud provider side or from the client side. To overcome this type of loss, we can implement following techniques:

a) Data after getting deleted by the customer should remain on the cloud for some pre-defined period, so that even if there is accidental delete the data can be retrieved.

b) We should implement customer-level recycle-bin, where from we can retrieve the accidentally deleted data.

c) Another method is to use redundancy, where a copy of the data stored on the cloud should be stored on another cloud.

All these techniques can be cost ineffective, but to overcome data loss one has to implement one of the above techniques, either at the customer level or at the cloud provider level or at both levels.

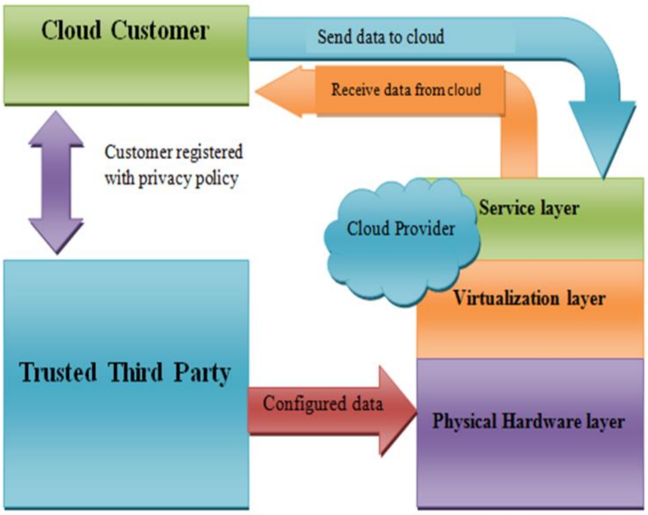

Figure 7 Confidentiality and Integrity in cloud computing

5.4. Account Hijack

Once the customer has mounted his/her information on the public cloud, it is available to all. So, any unauthorized customer can easily breach the system, hijack the customer credentials and can access the user‘s data or can destroy it. Hence, this is again a grave issue in the realm of cloud computing. In 2004, a foolproof scheme for grid computing [35] was proposed, which tries to overcome the account hijack problem in grid computing that explains how the customer‘s account can be hijacked in order to deceitfully access and modify the legitimate user‘s credentials. The similar problem can also occur in cloud computing. [36, 37]

Explain different intrusion detection techniques for cloud computing, that also gives us an idea of dealing with such problems in cloud computing. So, in this work, we have proposed a scheme that avoids the account hijack problem in cloud computing. To allevaite such attacks, the use of two-step verification while interacting with the cloud provider, has been proposed. In this two-step verification process, the phone number or the e-mail of the customers are registered with the cloud provider and when the client will request for the data stored by him/her on the cloud, the cloud provider will start this two-step authentication scheme, which is discussed below:

a) The unique phone number or the e-mail address of the customer is to be registered with the cloud provider at the time of registration.

b) When the customer requests for the data access, the customer will provide the user name and password to the cloud provider. The cloud provider will check the submitted username and password and will generate the one-time OTP and will send this to the registered phone number or e-mail registered by the customer. Once the legitimate customer will receive this one-time OTP, the customer will submit it to the cloud provider, where it will be matched with the previously generated OTP. If the match is successful, then the access will be granted to the customer.

By adopting this scheme the customer‘s data stored on the cloud will be safe from unauthorized access and thus will avoid the account hijacking problem in a cloud computing environment.

6. CONCLUSION

Cloud Computing has seen a tremendous growth through the past decade and enjoys a rapid adoption. Nonetheless, every coin has two faces, on the one-hand it provides user with a lot of services at the service, platform, and infrastructural levels but on the other hand it faces a lot of security and privacy challenges. This paper talks about major issues related to cloud computing, especially security. Also, the various security issues in cloud computing environment and different techniques to overcome such issues have been proposed. Moreover, it was observed that major security threat on the cloud computing is on the SaaS deployment model, where customer has no control on the data stored on cloud, and as such, different techniques to achieve confidentiality, integrity, privacy and many more security services to cloud computing were proposed. By implementing these solutions to security problems in cloud computing, it can become leading promoter of secure and economically viable solutions for secure service providing & data storage in future.

REFERENCES

[1] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, etal, A view of cloud computing, Communications of the ACM 53 (4) (2010) 50–58.
[3] Jun-jie Wang and Sen Mu, “Security issues and countermeasures in cloud computing,” in 2011 IEEE International Conference on GreySystems and Intelligent Services (GSIS), 2011, pp. 843–846.
[4] “Final Version of NIST Cloud Computing Definition Published.”[Online]. Available: http://www.nist.gov/itl/csd/cloud-102511.cfm.[Accessed: 18-Mar-2012].
[5] Haoyong Lv and Yin Hu, “Analysis and Research about Cloud Computing Security Protect Policy,” in 2011 International Conference on Intelligence Science and Information Engineering (ISIE), 2011, pp. 214–216.
[6] H. Takabi, J. Joshi, G. Ahn, Security and privacy challenges in cloud computing environments, IEEE Security & Privacy 8 (6) (2010) 24–31.
[7] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, Cloud Computing: Security Issues and Research Challenges, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
[8] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. 13:113–170 (2014) DOI 10.1007/s10207-013-0208-7.
[9] Aguiar, E., Zhang, Y., Blanton, M.: An Overview of Issues and Recent Developments in Cloud Computing and Storage Security, pp. 1–31, Springer, Berlin (2013).
[10] “T. Grance, and P. Mell, ‘The NIST definition of Cloud Computing,’ National Institute of Standards and Technology (NIST), 2009.”
[11] B. Gowrigolla, S. Sivaji, and M. R. Masillamani, “Design and auditing of Cloud computing security,” in 2010 5th International Conference on Information and Automation for Sustainability (ICIAFs), 2010, pp. 292–297.
[12] C. Wang, Q. Wang, and K. Ren, “Towards Secure and Effective Utilization over Encrypted Cloud Data,” in Proc. of ICDCS’11 Workshops, 2011.
[13] P. Samarati and S. De Capitani di Vimercati, “Data Protection in Outsourcing Scenarios: Issues and Directions,” in Proc. of ASIACCS, 2010.
[14] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in Proc. of ICDCS, 2011.
[15] GoGrid API, http://www.gogrid.com/company/press-releases/gogridmoves- api-specification-to-creativecommons.php, 2011.
[16] Storage Network Industry Alliance, http://www.snia.org, 2011.
[17] Amazon Web Services, “Amazon Simple Storage Service (Amazon S3),” http://aws.amazon.com/s3/, 2009.
[18] H. Lo, R. Wang, J. P. Garbani, E. Daley, R. Iqbal, and C. Green, Forrester report, The State of Enterprise Software: 2009, 2009.
[19] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On Technical Security Issues in Cloud Computing,” in Proc. of IEEE International Conference on Cloud Computing, 2009.
[20] Hacker4Lease, “Backdoor and Debug Options,” http://www.hacker4lease.com/attack methods/backdoor/, 2011.
[21] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, “A Survey on Security Issues in Cloud Computing,” in ArXiv 2011.
[22] Q. Duan, Y. Yan, A.V. Vasilakos, A survey on service oriented network virtualization toward convergence of networking and cloud computing, IEEE Transactions on Network and Service Management 9 (4) 373–392 (2012).

[23] W. A. Wayne, "Cloud hooks: Security and privacy issues in cloud computing," in Proc. of Hawaii International Conference on System Sciences, 2011.
[24] Texiwill, "Is Network Security the Major Component of Virtualization Security?," http://www.virtualizationpractice.com/blog/?p=35, 2009.
[25] Sabahi and Farzadl, "Virtualization-level security in cloud computing," in Proc. of IEEE International Conference on Communication Software and Networks, 2011.
[26] Slawomir Grzonkowski and Peter M. Corcoran "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", IEEE Transactions on Consumer Electronics, vol. 57, no. 3, 2011.
[27] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, Provable data possession at untrusted stores, in: Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07), Alexandria, Virginia, USA, October 28–31, 2007.
[28] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003), Warsaw, Poland, May 4–8, 2003.
[29] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, Journal of Cryptology 17 (4) 297–319 (2004).
[30] R. Merkle, Protocols for public key cryptosystems, in: IEEE Symposium on Security and Privacy, Oakland, California, USA, April, 1980.
[31] P. Rewagad and Y. Pawar "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", IEEE International Conference on CSNT, pp.437 – 439, 2013.
[32] Dimitrios Zissis, Dimitrios Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems 28 583–592 (2012).
[33] B. Kang, C. Boyd, E. Dawson, A novel identity-based strong designated verifier signature scheme, Journal of Systems and Software 82 (2) 270–273 (2009).
[34] VeriSign. Directories and public—key infrastructure (PKI), Directories and Public—Key Infrastructure, PKI.
[35] W. Du, J. Jia, M. Mangal, M. Murugesan, Uncheatable grid computing, in: Proceedings of the 24th International Conference on Distributed Computing System (ICDCS'04), Hachioji, Tokyo, Japan, March 24–26, 2004.
[36] Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, A survey of intrusion detection techniques in Cloud, Journal of Network and Computer Applications, 36(1), pp. 42-57 (2013).
[37] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, ―Intrusion detection techniques for Grid and Cloud Computing Environment,‖ IT Professional, IEEE Computer Society, vol.: 12, issue 4, pp. 38-43, 2010.

Authors

Mir Shahnawaz Ahmad received the B.Tech. degree in Computer Science and Engineering from University of Kashmir, Srinagar, J&K, India, and the M.Tech. degree in Computer Science and Engineering from SMVDU, Katra, J&K, India. He is currently working as Lecturer at Institute of Technology, University of Kashmir, J&K, India. His main research focus lies in Database Systems, Software Defined Networks, MANETs, IoT, Cloud Computing and Data Sciences.

Syed Rameem Zahra received the B.Tech. degree in Computer Science and Engineering from University of Kashmir, Srinagar, J&K, India, and the M.Tech. degree in Computer Science and Engineering from SMVDU, Katra, J&K, India. She is currently pursuing the Ph.D degree with the department of Computer Science and Engineering, National Institute of Technology Srinagar, J&K, India. Her area of research is Database Systems, Wireless Sensor Networks, VANETs, Cloud Computing and IoT security.