Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 5, Issue 7; October-December, 2018, pp. 545-550

http://www.krishisanskriti.org/Publication.html

# Cloud Computing Security Issues and Methods to Resolve: Review

**Mohd. Tajammul[1], Rafat Parveen[2] and Mohd Shahnawaz[3]**

*[1,2]Jamia Millia Islamia, New Delhi*
*[3]Glocal University, Saharanpur*
*E-mail: [1]mohammad8002@gmail.com, [2]rafatparveenjmi@gmail.com,*
*[3]ssshahnawaz.hussain@gmail.com*

**Abstract—***Data, an information generator is a sensitive element for an organization. It becomes more sensitive for those organizations which are involved in financial transactions. A large no of organizations are still in ambivalence whether to cloudify or not to cloudify because of security reasons. To remove this barrier and to provide robust and secure platform is the main aspect of cloud. Lots of algorithms have been designed and implemented for securing the data at cloud but the attack of 2014 on cloud in which 50 million users' accounts were hacked, shows that cloud is still not fully secured. Literature review shows that cloud storage is not even as secure as our normal system storage. The main focus of this paper is to draw an attention towards security issues, suggested tests and solutions in context of cloud computing. The paper suggests the next directions of security research in the field of cloud computing.*

**Keywords***: Cloud security, cloudify, security issues, security solutions.*

## 1. INTRODUCTION

The fundamental definition of cloud computing was coined by Professor John McCarthy in 1960, as " If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry" [9, 10]. Douglas Parkhill uncovers the features of cloud computing in 1966 in his book "The Challenge of the Computer Utility ". "Cloud computing is super-set of Virtual Private Network (VPN) along with network infrastructure that is utilized by telecommunication" [9, 10].

The National Institute of Standards and Technology defines "A model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models " [13].

### 1.1 Five basic characteristics

1. 24X7 on demand service
2. Resource pooling
3. Broad network access
4. Measured service – Pay per use service
5. Rapid elasticity

### 1.2 Three service models

**Software-as-a-Service (S-a-a-S)-:** In this provision dedicated software is given to the user on which customer can perform his operation. For instance someone wants to start his business and have no money to purchase costly software to run his business, in this situation he can go for S-a-a-S.

For instance NetSuite, SalesForce.com, Microsoft, IBM and Oracle.

**Platform-as-a-Service (P-a-a-S)-:** In this provision a dedicated platform is given to the user on which he can develop his applications. Suppose someone wants to start a software company to develop software but have no platform on which to develop that application, in this situation he can go for P-a-a-S.

Two famous examples are GAE, Microsoft's Azure.

**Infrastructure-as-a-Service (I-a-a-S)-:** Under this provision, infrastructure is given to the user for use. The infrastructure may be of many types like storage like server. More elaborately let us consider an organization having a website with the capacity to handle 100 users at a time. To host these 100 customer we need a server which can handle the request given by these users of the website and what happened if the server is very costly and out of the budget of the organization, in this case, the organization can go for renting a server from cloud and will pay for time the organization uses its services.

Examples are GoGrid, Joyent, Flexiscale and Rackspace.

### 1.3 Four deployment models

**Public cloud-:** Public cloud is available to all for storing data or performing computation. If data to be stored or to be computed is highly secure, it is highly recommended not to go for public cloud in this situation it is better to choose private cloud [8].

**Private cloud-:** This is the cloud which is available only for personal storage or personal computation of a particular organization or particular individual. This type of cloud is recommended if data is highly sensitive or financial [8].

**Community cloud-:** When some organizations have their own cloud for their use, this is an example of community cloud. This cloud is not owned by the community which uses its services rather its infrastructure is provided by the supplier [8].

**Hybrid cloud-:** This cloud satisfies the customer with heterogeneous requirements. Utilization of the cloud depends upon the nature of data, if it is very sensitive store it on dedicated server and if it is less sensitive upload it on cloud this is recommended because in hybrid cloud there is environment of multitenancy and hence fear of data leakage[8].

Cloud computing is an online service provided to the user as per requirement and pay-per-use basis by arranging the available resources in best possible manner in between different users to fulfill their needs. It dominants an important role in coming generation of Mobile Network and Services that is 5G and CPSC ( Cyber Physical and Social Computing). Producing the data within the boundary of organization and storing it outside the boundary of organization (at cloud storage), drastically reduce the burden of storage.

Nevertheless security, privacy as well as the trust between both the ends of cloud become the main issue that leverages a great impact on the success of cloud computing and also produce a hurdle in the development of CPSC and 5G. Four main points are here to draw attention.

**First –** As soon as the users store the data on cloud, the risk of its leakage and unauthorized access becomes more than that of as if it was stored at local machine storage.

**Second –** It become the centre point for the attackers and a place for inserting intrusions.

**Third –** Various operations like storage, recovery, deletion, migration, updating and searching in the cloud may not be fully trusted.

**Fourth –** Computation and processing f data on the cloud may uncover the privacy of data owner.

In starting when cloud computing was tossed, there were very small no of challenges in-front of cloud developer and cloud provider. As soon as the era of cloud grow rapidly, its issues and challenges grown more rapidly. These issues are as under:

1. Issue of Resource Scheduling and Management.
2. Issue of Portability and Interoperability.
3. Issue of Reliability and Availability.
4. Issue of Power Consumption.
5. Issue of Performance.
6. Issue of Security and Privacy.
7. Issue of Scalability and Elasticity.

Out of above seven issues security and privacy are the two basic and ongoing issues which have been listed here. To handle these fourteen security issues this paper discussed a lots of tests and also resolution techniques as below [9, 10].

1. Issues of Data confidentiality.
2. Issues of Web application security.
3. Issues of Data breaches.
4. Issues of Virtualization vulnerability.
5. Issues of Availability.
6. Issues of Data access.
7. Issues of sign-on process and Identity management.
8. Issues of Network security.
9. Issues of Data security.
10. Issues of Data segregation.
11. Issues of Authentication and authorization.
12. Issues of Data locality.
13. Issues of Backup.
14. Issues of Data integrity.

Remaining part of the paper is organized as: Section 2 discusses related works, Section 3 the classification of security issues, Section 4 discusses problem identification, Section 5 proposed an algorithm, Section 6 conclude the paper, finally Section 7 discusses future directions.

## 2. RELATED WORKS

In [1], Mansaf Alam et al. Proposed a covert channel detection technique in cloud computing. Where authors revealed, how information leads to covert channel and all the possible efforts have been made to detect covert channel and counter attack.

In [2], Subhashini and V. Kavitha discussed a survey on security issues on service models of cloud computing where authors discussed 14 security issues on SaaS and some on issues on PaaS some rest on Iaas. A large no. of solutions and tests has also been suggested to overcome these issues.

In [3], Dimitrias Zissis, Dimitrias Lekkas addressed cloud security issues in tabular form representation by discussing

levels of security users and security requirements and threats also.

In [4], Manas MN et al. discussed cloud computing issues and methods to overcome. Authors have discussed there isolation on the basis of SaaS, PaaS and IaaS and finally isolation at VM in memory and cache in multitenant environment.

In [5], Micheal Armbrust, shows a view of cloud computing where they proposed to clear the cloud away from the true potential and obstacle posed by cloud computing capabilities.

In [6], Manish M Potey et al. proposed a homomorphic encryption for security of cloud data. Authors showed that computation is performed on encrypted data in public cloud and results will be saved on users system.

In [7], P. Ravi Kumar et al. Discussed various data security issues as well as resolution technique in cloud computing.

In [14], Rao, B. T. (2016). Discussed a study on security issues in the field of cloud computing where authors' divided cloud security issues into three types (i) contractual and legal issues (ii) identity management and access control (iii) data storage issues, authors' has divided these issues further into eight issues.

In [15] Kumar, S., & Kumar, S. (2016). Discussed security vulnerability in cloud environment. Authors'have discussed security issues and challenges from various points of view like security at Network Infrastructure, security challenges at planning and administration level. Finally authors have discussed security vulnerabilities in various platforms like Xen, Virtual box, Hypervisor.

## 3. CLASSIFICATION OF SECURITY ISSUES

Security issues discussed above may be classified as under. Here we have design a tree like structure to clear the figure of security issues of cloud computing. All the issues of the given parent issue have been discussed. All these issues have been extracted from many sources and integrated together to form this hierarchical structure. First of all we have discussed all the parent issues and then child issues under that parent and then we have suggested a large no of solution to overcome those issues. Finally we have given table to show security requirements and related threats.

### 3.1 Traveling Packet Security

The bright face of the coin named Internet but it has dark face also and the face is that Network is considered as main carrier of attack against software applications running through cloud platform. Network based attack can be divided into two categories first one is the traditional attack and second one is the attack generated after the existence of cloud. One of the most dangerous attacks is DDoS (Distributed Denial of Services). DDoS is further of two categories that is application level and transport level. A well known attack in which network traffic is eavesdropped for stealing the information such as user id and password. It hampers the integrity as well as confidentiality. Other attack is SQL Injection flaws in which hacker insert a malicious code into applications; it hampers the speed of the system by occupying the controls over valuable resources.

**Counter Measures against travelling packet security [1]**

**Table 1**

| **Problem of travelling packet with solution** | | |
|---|---|---|
| **Problem** | **General Solution** | **Cloud Solution** |
| System | Filtering (Close to | TrendMicro, |
| availability, | destination, router, | Symantec, |
| Confidential- | source), Ingress | Kaspersky, |
| ity and | filtering, Egress | CloudLink, |
| Integrity | filtering, Router | Bitdefender, HP |
| | based packet | Atalla, |
| | filtering, History | CypherCloud, |
| | based filtering, | VLAN Network, |
| | Secured overlay | Network Intrusion |
| | service, Remote | Detection |
| | triggered black | System(NIDS) for |
| | hole and firewall, | fingerprint, SYN |
| | Intrusion Detection | Cookies, Network |
| | Prevention | Packet Filter, |
| | System(IDPS), | VShield Edge |
| | IDS, DIDS, SSL, | |
| | TLS, IPSec | |
| | Protocol, Data | |
| | encryption, Key | |
| | management, Data | |
| | backup and | |
| | Replication. | |

### 3.2 Data Storage Security

Cloud computing provide storage to customer to upload data into it. It is highly recommended to user to encrypt data before uploading it to cloud storage rather uploading plain data because cloud support multi-tenancy architecture and many users uses cloud storage. There are three types of attackers on data in cloud, external hackers, employee of the company offering cloud service and also owner of the company. Therefore it is intelligence to encrypt data before sending it to cloud and decrypt it while downloading. For making operation like encryption- decryption in cloud we use only symmetric algorithmavailable for example DES, AES, BLOW FISH.

### 3.3 Cloud Service Model Security

Existence of clod is just because of its service models. These models are available to provide service to the users as per service level agreement or as per service oriented architecture. If any of the company wants to develop its own cloud to serve others then it needs to develop any of the three models or all of the three models. These models are like the topology in computer networks and types of cloud may be thought as types of network. Topology is used to develop computer network and models are used to develop cloud deployment models. Cloud service model security has been further divided

into three sections, security at SaaS, security at IaaS and finally security at PaaS.

**Table 2**

| Security issues and suggested test at SaaS [11] | |
|---|---|
| **Issues** | **Suggested Tests** |
| Data security, data | Cross site scripting, OS |
| locality, network security, | and SQL injection flows, |
| data integrity, data | access control weakness, |
| access, data segregation, | cross site request forgery, |
| authentication and | hidden field manipulation, |
| authorization, web | insecure configuration |
| application security, data | and insecure storage |
| confidentiality, data | |
| breaches, availability, | |
| virtualization and | |
| vulnerability, identity | |
| management and sign in, | |
| backup | |

### 3.3.1 Security at P-a-a-S

Although pass gives some control to the nsr while building application. But command I still providers offer an assurance for example instruction reservation preoviders offer an assurance to the insert that the data is always inaccessible between applications Enterprize Service Bus (EBS) needs to be secure [11].

### 3.3.2 Security at I-a-a-S

If we improve the control of the security at pass, there is more control of insert on IaaS regarding security to the security aspects of both the providers and the consumers are different on different models of services for example Amazon EC2 Elastic compute cloud takes the responsibility in to the hypervisor from render side. It means that they can only interfere in environmental security, physical security and virtualization security [11].

### 3.4 Data processing security

When we send data to the cloud in encrypted from their at some point it will be decrypted, then common question arises how to protect it. For solving this problem an algorithm has been designed named Data processing security in this author has designed secured distributor file system. More over author has denote SccCloud for making cloud data storage more secure

### 3.5 Security at 3 levels

3 levels of security are at application level, security requirements at virtual level and security requirements physical level. All these three levels have their own requirements of security as well as the threats associated with them. Security at application level means security at SaaS, security at virtual levels means security at Iaas and at Paas and finally security at physical level which means security at data centre [12]. Security requirements at application level (SaaS Level) is very important because at this level a software is given to the user to use and pay or not pay for it. Like gmail service.

### 3.5.1 Security Requirement at Application Level [12]

**Table 3**

| Security Requirements | Threats |
|---|---|
| 1) Application Security<br>2) Access Control<br>3) Data Secondary<br>4) Secure Image<br>5) Cloud management control protection<br>6) Virtual cloud security | 1) Software notification<br>2) Programming Flaws<br>3) Software interruption<br>4) Session Hijacking<br>5) Impersonation<br>6) Proffice flow analysis |

### 3.5.2 Security Requirements at Virtual level [12]

**Table 4**

| Security Requirements | Threats |
|---|---|
| 1) Privacy in multitenant environment<br>2) Access control<br>3) Data security<br>4) Communication Protection<br>5) Service Availability<br>6) Software Security | 1) Interception<br>2) Data Interruption<br>3) Software interruption<br>4) Privacy Breach<br>5) Session Hijacking<br>6) Impersonation |

### 3.5.3 Security Requirements at Physical Level [12]

**Table 5**

| Security Requirements | Threats |
|---|---|
| 1) Hardware Security<br>2) Legal not abusive utilization<br>3) Hardware Reliability<br>4) N/W resource protection<br>5) Network Protection | 1) Connection Flooding<br>2) Network Attack<br>3) Distributed Denial of Services<br>4) Hardware modification, hardware flag, Natural disaster, Misuse of infrastructure<br>5) Hardware interruption |

## 4. PROBLEM IDENTIFICATION

On the basis of literature reviewed, it is clear that some of the authors are using only single one encryption –decryption algorithm to encrypt data before uploading it on cloud storage while others are using combination of two or three algorithm to encrypt data. All of them are using DES or AES or IDEA or Blow Fish. Either they are using these algorithms separately for single document or a combination of any two or three of these to encrypt different parts of document by different algorithm.

All of these algorithms are data independent, they are taking linear key from user and encrypting data. Now a question arises here: **Can we design an algorithm which can produce nonlinear key itself by sensing data rather than asking key from user?**

## 5. PROPOSED ALGORITHM

To answer the question raised in problem identification, we have proposed an algorithm which will sense data and will produce key accordingly.

### 5.1 Algorithm for Nonlinear Key Generation

This algorithm will produce a nonlinear key after sensing the document this key will subsequently be used to encrypt data by any of the pre-existing or newly discovered encryption-decryption algorithm.

**Algorithm Steps**

**INPUT:** Document/Text File

**OUTOUT:** Nonlinear Key

1. **START**
2. Read/sense the document.
3. Count the occurrences of each character in the document. Put these occurrences of each alphabet form ‘a’ to ‘z’ and from 0 to 9 in a matrix say M1 of size 6X6.
4. Take remainder division of the M1 by prime no greater than 26 and store in other matrix say M2.
5. Add ASCII of character ‘a’ to the first entry of M2, add ASCII of ‘b’ to the second entry of M2 and so on, add ASCII of 9 to last entry of M2.
6. Convert each entry of M2 into characters and store it into other matrix say M3.
7. M3 will obviously have 36 entries, convert this arrangement of 36 entries into key by taking entries from last to first.
8. **END**

## 6. CONCLUSION

Cloud computing is like a boon for those who want to start their own business but having no money for initial investment. This is a fruitful technology and growing rapidly. To make this technology as robust one, we need to make it more secure so that no unauthorized person can breach valuable information out of it. In this paper a no of issues related to the security o in cloud computing have been discussed with their solution. Though cloud computing is secure up-to a certain extent but there are some problems which needs to be address yet these problems are:

(I) Secure computation of data on cloud

(II) Session hijacking

## 7. FUTURE SCOPE

In Section 5 of this paper we have proposed a non linear key generation algorithm which senses the data and produce key. Now future work is to implement this algorithm to compute its efficiency and to use it in integration of encryption-decryption algorithm.

## REFERENCES


[1] Sethi, S., Alam, M. (2013). Covert Channel Detection Techniques in Cloud. Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), 3.02-3.02. https://doi.org/10.1049/cp.2013.2305

[2] Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 111. https://doi.org/10.1016/j.jnca.2010.07.006

[3] Zissis, D., Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems,28(3),583592. https://doi.org/10.1016/j.future.2010.12.006

[4] Manas, M. N., Nagalakshmi, C. K., Shobha, G. (2014). Cloud Computing Security Issues and Methods to Overcome. International Journal of Advanced Research in Computer and Communication Engineering, 3(4), 63066310.

[5] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Zaharia, M. (2010). of Cloud Computing. Communications of the ACM, 53(4), 5058.

[6] Potey, M. M., Dhote, C. A., Sharma, D. H. (2016). Homomorphic Encryption for Security of Cloud Data. Procedia Computer Science, 79, 175181. https://doi.org/10.1016/j.procs.2016.03.023

[7] Kumar, P. R., Raj, P. H., Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Proceedia Computer Science, 125(2009), 691697. https://doi.org/10.1016/j.procs.2017.12.089

[8] Manas, M. N., Nagalakshmi, C. K., Shobha, G. (2014). Cloud Computing Security Issues And Methods to Overcome. International Journal of Advanced Research in Computer and Communication Engineering, 3(4), 63066310.

[9] Tajammul, M. (2018). Comparative Study of Big Ten Information Security Management System Standards. International Journal of Engineering Research In Computer Science and Engineering, 5(2), 514.

[10] Tajammul, M. (2017). Comparative Analysis of Big Ten ISMS Standards and Their Effect on Cloud Computing. 978-1-5386-0627-8/17/$31.00_c 2017 IEEE 9001, 362367.

[11] Rasheed, H. (2014). International Journal of Information Management Data and infrastructure security auditing in cloud computing environments. International Journal of Information Management, 34(3), 364368. https://doi.org/10.1016/j.ijinfomgt.2013.11.002

[12] Zissis, D., Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems,28(3),583592. https://doi.org/10.1016/j.future.2010.12.006

[13] Ali, Arshad. (2016). A Relative Study of Task Scheduling Algorithms In Cloud Computing Environment. 978-1-5090-5256- 1/16/31.00c2016IEEE.

[14] Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science, 92, 128135. https://doi.org/10.1016/j.procs.2016.07.335

[15] Kumar, S., Kumar, S. (2016). A Study on Security Vulnerability on Cloud Platforms. Procedia Computer Science, 78(December 2015), 5560. https://doi.org/10.1016/j.procs.2016.02.010.