International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Cloud Security Issues and Challenges: Important Points to Move towards Cloud Storage

Dr. Firas A. Abdulatif [1], Maan zuhiar[2]

[1]College of education Ibn Al-Haitham, Iraq

[2]Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate, Iraq

Abstract: ***Cloud computing is a new paradigm in which resource delivered as a service through the internet and you pay just for what you use, The cloud is exposed to many security attacks like Login page, cloud APIs.one of the important services delivered by the cloud is a storage in witch customer can store privet data in remote data center and arrival this data from anywhere and at any time if connected to internet. Security and Privacy of cloud storage are very important because of that after moving data to cloud storage the control of data will be share by customer and cloud service provider, In this paper, we will focus on the cloud part and leave the subject of network security, it will discuss some of the methods used to protect cloud storage, while discussing some useful instructions on how to choose the cloud provider and deal with penetration types.***

Keywords: cloud security; cloud attacker; security of cloud storage.

1. Introduction

Cloud Computing is not a new technology Rather, it is a new method such as applications, software and hardware provided as services over the Internet [1]. The major features of cloud computing services are **on demand self-service, broad network access, resource pooling, measured service and rapid elasticity**[2]. The most important services provided by the cloud is storage; data is stored and managed on remote servers over the internet, organization use the cloud to reduce the cost, and rapid scaling[3][4]. So that when we want to use the cloud must choose the cloud provider in a precise manner to avoid some future problem [5], Store data on cloud must be done with high accuracy to avoid data breaches, In case of some security rules are not considered, the main kinds of security concern are:[6,7]

- Confidentiality: termed as the pledge that data is be kept secret.
- Integrity: described as incapability to change or destroy data by accident or violation.
- Availability: it is ability to reach that data every time it is needed. Figure1. Explain the main types of security concern

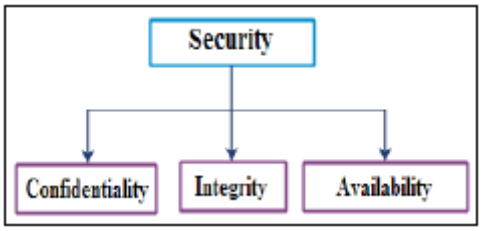

Figure 1: basic types of security concern[5]

This paper contain in addition to section one section two, will present the cloud computing service model and cloud computing deployment model, section three will present cloud security attacker, Section four will present methods for protect data stored on the cloud , section five will present important points towards cloud storage and section 6 the conclusion of this paper.

2. Cloud Computing

In cloud computing there is many services and deployment models

a) Service Models
Three Services Models provided by cloud.

Software as Service
The ability to use the provider's applications running on the cloud.

Platform as Service
In this kind of service the user can develop tools and applications using programming languages and tools provided by cloud provider [6].

Infrastructure as Service
The ability provided to the user to use storage, processing, networks and other computational resources that enable user to run and deploy a software. User can request operating systems, storage, some applications, and some network components[7]. Figure2. Show the cloud computing service model

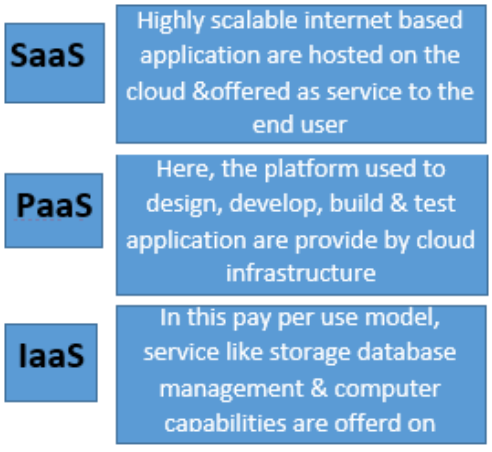

Figure 2: cloud computing service model[8]

b) Deployment models
Four deployment models in cloud computing as below

•Private cloud
The cloud infrastructure is provided for special use by a single organization including multiple consumers. It may be owned and managed by the organization this type considered expensive but more security than other types [9].

• Community cloud
The cloud infrastructure is provided for special use by a certain community of consumers from organizations that have shared concerns. It may be owned, managed, and functioned by one or more of the organizations in the community[10].

• Public cloud
The cloud infrastructure is provided for public use by the general public. It may be owned, managed, and functioned by any A profitable organization, government or some combination of them[11]. That provides services to public users for different use with different concerns. This type considered less security and cost.

• Hybrid cloud
The cloud infrastructure is provided for two or more cloud infrastructures may be private, community, or public that stay unique objects, but they are linked together by a unified technology or proprietary technology that enables data and application portability [12]**.** Figure3 Show the cloud computing deployment models

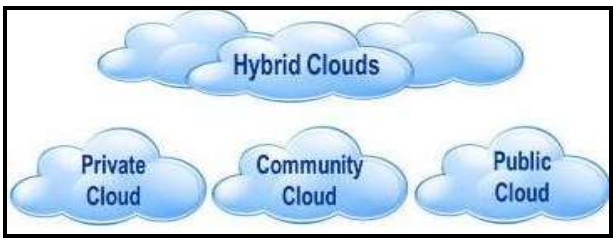

Figure 3: cloud computing deployment model[13]

3. Cloud Security Attackers

There are many types of attackers bellow the common types of them

- **Insecure Interfaces and APIs**

Cloud computing providers a set of APIs that user used to interact with the services provided by the cloud so that this APIs must be secure enough to avoid the threat[14].

- **Vendor lock-in**

One of the concerns that is often overlooked when choosing a cloud provider is Vendor lock-in, cloud service provider Block the services provided to the customer such that customer cannot access his data and use any services provided by the cloud[15]**,**or cannot move to other cloud provider.

- **Malicious Insider**

Granting powers to the current or former employee or partner to access user data and misuse this access in a way that negatively affects the confidentiality, integrity of data [16].

- **SQL injection**

It is done by inserting SQL orders in a database of an application from the web to Smashing that database[17].

- **Guest-hopping attack**

The attacker tries to access to virtual machine by breakthrough other virtual machine hosted in the same hardware.

- **Side Channel Attack**

This type of attacker put a malicious virtual machine on the similar physical machine as the victim machine so that attacker can access all the private data on the victim Machine. can overcome this by Working with well-known service providers[12].

4. Some Method to Secure the Cloud

Many concerns that led to the reduction the use of the cloud by companies because when transferring data on the environment of the cloud storage and this environment may be a multi-tenant environment so that the customer concerned that another user getting their data[18]. So that will show many studies to enhance the security of cloud computing.

A. Cloud Computing Adoption Framework[19]**.**
It is proposed by Chang,VictorRamachandran, Muthu to secure the cloud by developed a framework known as Cloud Computing Adoption Framework (CCAF).it consist of multi-layers of security mechanism to maximize protection. It also ensures reduction in the infections by Trojans, virus, worms and unauthorized access and denial of service attacks. Each layer has its own protection and is in charge of one or multiple duties in the protection, preventive measurement and quarantine action. CCAF consist of:

The first layer is Access Control and firewall to allow restricted members to access.

The second layer consists of the IDS and IPS. The aim is to detect attack, intrusion and penetration, and also provide up-to-date technologies to prevent attacks such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning.

The third layer is Encryption
This layer is protect data by encrypting data using one of the encryption algorithm and store it to cloud so any one access data cannot read it.

B. Quick response (QR) code and Triple data encryption standards algorithm (3DES) [10].
Mahroosh Irfan and Muhammad Usman propose new method to secure the cloud by integrating quick response (QR) code and Triple Data Encryption Standards Algorithm (3DES).

QR cod is Universal little square that uses four standardized encrypting modes (numeric, alphanumeric, binary, and kanji) to efficiently store data. figure4, explain quick response

Figure 4: quick response cod

This suggest method uses 3DES algorithm the encryption key consist of three key the first key is quick response code, the second key is mirage quick response cod and 8-digit pass cod and the third key is merge of quick response cod and another 8-digite pass cod each user have unique QR code, thus the key will be unique and will reduce opportunity Data Access the encryption algorithm will work as follows

Cipher text = ENKey3 (DEKey2 (ENKey1 (plain text))) where (EN) mean encryption and (DE) mean decryption. During the creation of a user account on the cloud the three keys will be stored in the database and no one can access them nor the cloud service provider.

C.Applying Chiphertext - Policy Attribute-Based Encryption(CPA-BE) [20].

Ke Han, Qingbo Li and Zhongliang Deng Beijing propos a new way to secure the cloud by applying Chiphertext - Policy Attribute-Based Encryption (CPA-BE),it is a good cryptography method that provide well access control to data. The most important think in Attribute-Based Encryption is key generation and how to keep it from theft they separate the validity key to several key authority centers (KAC) this is responsible for great confidential factor for user's characteristics confidential factor from different KACs are combined together to make users' confidential keys. User encrypt his data locally before uploaded it to cloud. Any recorded user on the cloud can easily query for any encrypted text but only when the user's characteristics met the access structure included in the Cipher text, it is capable to decrypt the Cipher text When a user with U_i receives the Cipher text C from cloud server, it can decrypts the cipher text using its confidential keys in recursive way. For every leaf node $x \in \Gamma_R$, if $\lambda_x \in S_i$ compute the V_x else set $V_{x=0}$

$$V_x = \frac{e(D_x, C_x)}{e(D'_x, C'_x)} = \frac{e(g^{u_i} H(\lambda_x)^{r_x}), g^{q_x(0)})}{e(g^{r_x}, H(\lambda_x)^{q_x(0)})}$$

$$= \frac{e(g^{u_i}, g^{q_x(0)}) e(H(\lambda_x)^{r_x}, g^{q_x(0)})}{e(g, H(\lambda_x))^{r_x q_x(0)}}$$

$$= e(g, g)^{u_i q_x(0)}$$

Records children nodes set of all non-leaf node y as N. For every node z ∈ N, if |N| < k y or V z = 0 sets V y = 0. CPA-BE provide efferent way to secure the cloud and flexible method to access data.

D.Depend on RSA and AES encryption algorithm[21].

Nasrin Khanezaei and Zurina Mohd Hanapi propose method to secure the cloud depend on merge of tow encryption algorithm RSA (Rivest-hamir-Adleman) and AES (Advanced Encryption Standard) encryption algorithm to share data between users in a secure way. Overview of the suggested framework is displayed in Figure 5. The objects of the system are: sender, receiver and cloud storage system (CSS). In order to make the cloud storage service safe enough, firstly sender demands from cloud system his public key and then the cloud service creates the private key, the file identifier , the public key and an offer random number. And then cloud service sends the made public key and the file identifier of file to user. And then, sender sends the encrypted file and its file identifier to the system, the method of sending file is encoded by RSA algorithm. Part two of this system is sending file from cloud storage system to the receiver. For this reason, receiver directs a request for the list of files and then cloud system will send the list of files to the user. Receiver can select any file want from cloud system and download it and after creation the download demand, the user directs the file name to cloud system and user directs his public key to the system as well. The use of this public key is to encode the confidential key of the symmetric encryption algorithm. The final part is search the demanded file by (CSS) and then encoding this file using AES encryption algorithm.

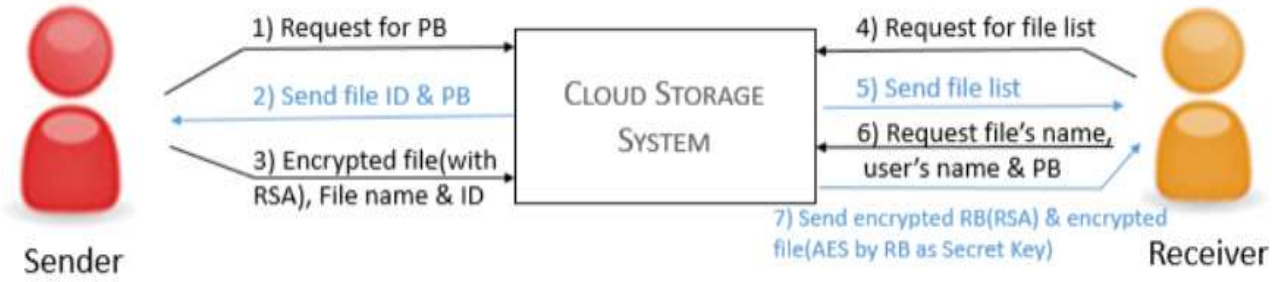

Figure 5: Framework to secure the cloud[21]

E. Trusted computing[1].

Saakshi Narula, Arushi Jain and Ms. Prachi Proposed strategy to secure the cloud by involving third parity this method called trusted computing (TC)**,** The main reason for the companies don't using the cloud is lack of trust on the service delivered in cloud computing. To get this trust by involvement of third party who attest both the consumers and cloud provider and this is identified as remote server

attestation.TC system is very significant due data security is core operation and not the add-on operation. TC system encodes the data and application and offers the decryption key to the trusted program. Trust Computing Platform (TCP) The two services delivered by TCP are authenticated boot and encryption. The TCP has two ingredients: Trusted virtual machine monitors [TVMM] and trusted coordinator. TVMM hosts the customer's virtual machines [VMs] and also give protection against inspection and modification of customer's VM. Trusted coordinator is responsible for running customer's VM securely by some set of nodes. These nodes should be within security perimeter and should run the TVMM then only these nodes are said to be trusted node.

F. One time password and hash function[22]

Mr. Nilesh R. Patil and Prof. Rajesh Dharmik propose a new method to secure the cloud by using one time password for authentication and Generation of hash for integrity check and using Advanced Encryption Standards (AES) algorithm for encryption/decryption user data .figure 6, explain the flow architecture of proposed method

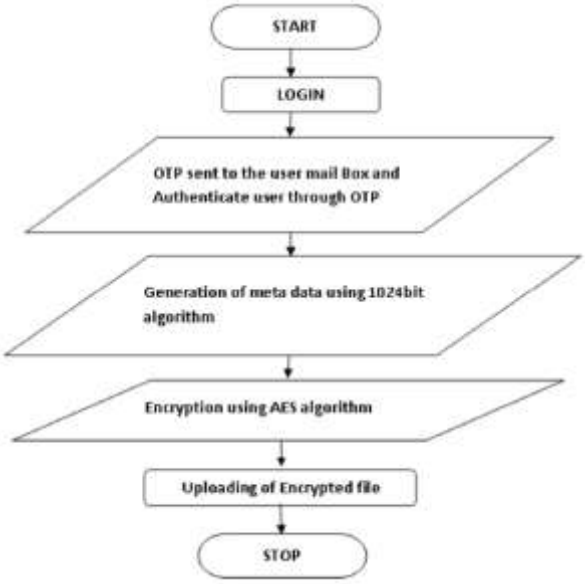

Figure 6: Download Flow [22]

One Time Password is password that is valid for only one time. OTP is more secure than static password. In the proposed method, cloud service provider (CSP) will authenticate user through OTP. CSP generate the OTP and send it to the user mail box. Hashing is the method of taking data and creating unpredictable, Irreversible output. Hash used to ensure the integrity of data transferred to the cloud. The proposed System will use SHA-2 algorithm. This modified algorithm will run on digest size of 1024 bit and also produce the hash value of 1024 bit). Using hashing algorithm we are going to generate hash value of the user file. When user is uploading his file hash will be calculated and file will be pass to the encryption algorithm. When the user is accessing file or downloading file after decryption of that file hash will be calculated to check whether data has been manipulated or not . In proposed system, after generation of hash user file is going to upload on cloud. Before storing file in cloud will be Encrypted using standard AES algorithm. That encrypted file will be stored on cloud not the original file. When user want to access that file or download that file, encrypted file will be decrypted using AES decryption algorithm. Hash will be calculated.

G. Authorization access for secure multi-tenancy based on AAAS protocol[23]

Azizol B HJ Abdullah and Salman Yussof use authorization model Based on AAAS protocol to create safe communications among cloud computing tenants in respects to its authority and priority. The AAAS protocol can be divided into the following categories: Client-to Policy Enforcement- Point(PEP), PEP to Policy Decision Point (PDP), Client to PDP, and PDP to Policy Information Point (PIP).The system has two layers which are authorization services and Cloud services. Figure7. Show these tow layer

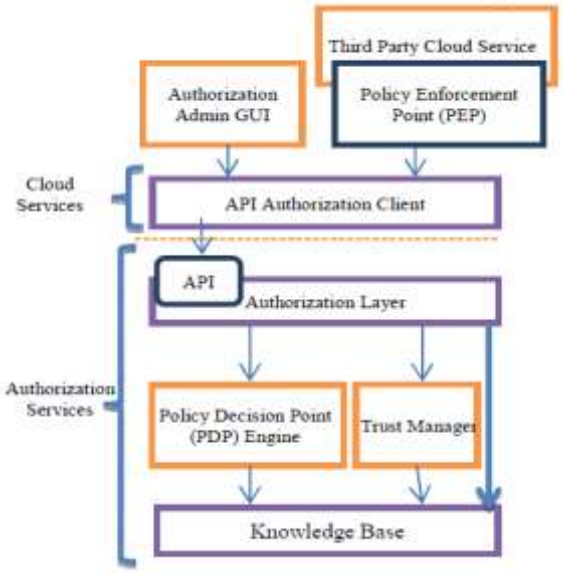

Figure 7: Authorization Architecture of cloud security system[23]

The authorization method can be termed in Figure.8. An object B safe recourse managed by cloud service PEP is requested to access by object a client. The authorization client API is used by object B PEP to start a safe communication with the authorization system which leads the authorization request to be redirected to the PDP component. Then, the entity B trust relationships can be retrieved from the trust manager using this PDP (that is, the list of objects that allow B to use their authorization statements for authorization decisions. After that, the authorization process can utilize the authorization statements from the knowledge base depending on these trust relationships retrieving by PDP. Therefore, the only authorization statements that can be retrieved by PDP are the ones that allowed to access by B entity. Finally, the authorization decision is made by authorization model that applied by PDP.

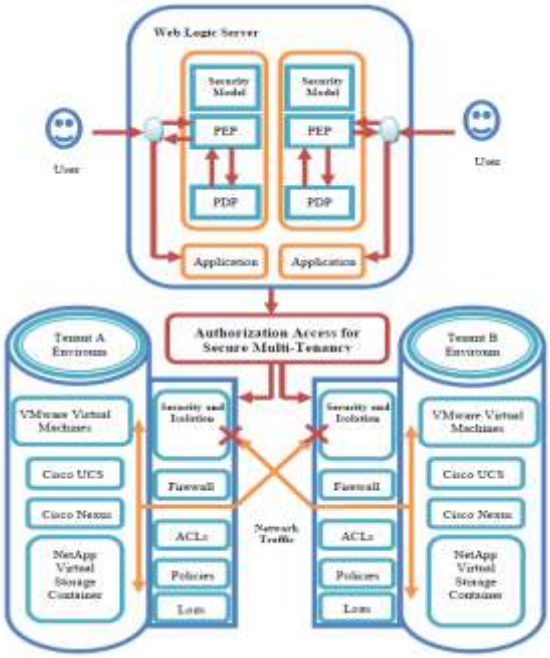

Figure 8: Authorization Access for Secure Multi-Tenancy[23]

H. Asynchronous challenge response authentication solution based on smart card[24]

Hash function, symmetric algorithm and one time password are proposed by Guifen Zhao, Ying Li, Liping Du and Xin Zhao to secure the cloud this proposed method displays time element as a challenge to the user while it attempts Signing in cloud server. Every time cloud server produces a new challenge for user when he wants to sign in. the challenge create by client software. The client software uses the smart card to produce a unique random number, then use the cryptography method to produce a unique password according to challenge and random number. Cloud server scan username and password, and the authentication server scan the made one-time password. Only the legitimate legal user can reach cloud resources. The authentication protocol is displayed in Figure 9. And described as follow:

1) $S_C \rightarrow U_C$: T if user wants to sign in, cloud server makes a time element *T* as new challenge for user. The time element is year- month- day- hour- minute- second.

2) $K = U_{ck} = C_{T, R}(U_{ID})$. The time element *T* is got by client software. Then the client software uses the smart card to generate a unique random number element *R* , then use the collective secret key algorithm on the basis of user's key seeds *Ks U* to produce a one-time secret key *cK U* rendering to time element and random number element.

3) H1= H ($U_N \| U_{Pw}$). Using hash function to create the digest of username and password.

4) H2= H ($U_{ID} \| T \| R$). Using hash function to produce the digest of user identity, time factor and random number factor.

5) E_k (H ($U_{ID} \| T \| R$)). Using encryption algorithm to encode the digest of user identity, time element and random number element. The generated Collective secret key *k* is the encryption key. The symmetric algorithm is proposed in the solution.

6) $U c \rightarrow S_C : E_k (h2) \| h1 \| T \| R \| U_{ID}$ Transfer the cipher text of user identity, time element and random number element, the digest of username and password, the time element, random number factor and user Identity to cloud server.

7) $H (U_N \| U_{pw}) = H (U_N' \| U_{pw}')$

Cloud server produces a new digest of username and password according to the username and password stored in database and check the expected hash value and the generated hash value are the similar or not. If they are the same, continue the authentication process. If not, terminate the authentication

And refuse user access.

8) $S c \rightarrow S_A E_k (H (U_{ID} \| T \| R)) \| T \| R \| U_{ID}$

Cloud server convey the digest of user identity, time factor and random number factor, the time factor, random number factor and user identity to authentication server.

Where U_C Cloud user, U_N Username, U_{ID} User Identity, U_{Ks} User Key Seeds, U_{cK} Combined Secret Key, U_{Pw} Password, S_C Cloud Server, S_A Authentication Server, E_k ( ) Encryption algorithm, k is the encryption key, H ( ) Hash function, $C_{T, R}$ ( )

Combined Secret Key Algorithm, T Time factor, R Random number factor

Smart card Terminal cloud server authentication server encryption card

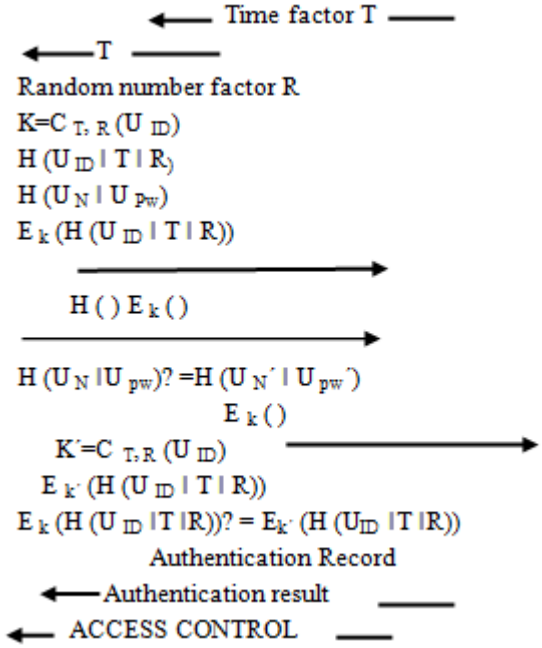

Figure 9: Schema of cloud based authentication[24]

I. A Framework to Ensure Data Storage Security in Cloud Computing[25]

Mrinal Kanti Sarkar and Sanjay Kumar suggested new Schema to secure the cloud by encrypt the data stored in cloud this model shown in figure10.

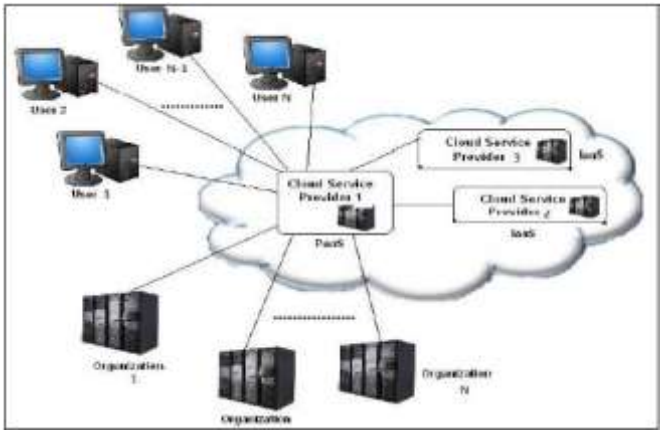

Figure 10: System Architecture for Cloud[25]

- **User:** who wish to use cloud infrastructure
- **Cloud Service Provider-1(CSP-1):** is the platform as a service supplier. User interact the CSP-2 and CSP-3.
- **Cloud Service Provider-2(CSP-2):** Encryption algorithm, decryption algorithm and key generation methods are kept here.
- **Cloud Service Provider 3(CSP-3):** That is the Infrastructure as a service supplier: every data are kept here.in this data will be encrypted by using encryption algorithm the key generation of this encryption algorithm shown in procedure1.

Procedure 1: Key generation of propose encryption algorithm

1. Start procedure
2. A and B are two small prime numbers where (gcd (A, B) =1).
3. Prime number sets m= (A+1) (B+1).
4. Let F_1 is the sum of the above (A_i, B_i) (starting from smallest prime number).
5. Sum of all prime number sets up to m.
   $N_{sop} = \sum_{i-1}^{m} F_I$ Where N_{sop} is an integer (positive).
6. Now average value of sum of all prime set.
   $N_{avg-sop} = \frac{N_{sop}}{III}$ Where $N_{avg-sop}$ is an integer (positive).
7. Calculate the R, a small random value such that $R \epsilon Z_{N\ age\text{-}sop}$ {R|1<R<= $N_{avg\text{-}sop,\ gcd}$(R, $N_{avg\text{-}sop}$) =1}
8. Let U is the number of existing users of cloud, Users sets are
   $\{U_1, U_2, U_3 \ldots U_K\}$
9. Select two small odd numbers B_i ,B_j from $F_i < B_i < N_{avg\text{-}sop}$, $F1 < B_j < N_{avg\text{-}sop}$ respectively where gcd (B_i, Bj) =1
10. $\varphi = B_i + B_j$
11. Let Q is positive number where Q=U*([φ(B) mod N_{sop}])
12. Now secret key K_S= ((R*Q) %256).
13. Return K_S
14. End procedure.

The encryption algorithm that used to encrypt data shown in procedure2.

1. **Start procedure2**
2. File FTemp, FEncod;
3. Count Ch=Char (FTemp)
4. Ks=Key_Gen ();
5. Set Counter=Position (Ch, FTemp)
6. FEncod =KS+Ch+Counter
7. Delete FTemp
8. End procedure.

And the decryption algorithm is:

1. Start procedure
2. File FTemp, FEncod;
3. Count Ch=Char (FEncod)
4. Ks=Key_Gen ();
5. Set Counter=Position (Ch, FEncod
6. FEncod =KS-Ch-Counter
7. Delete FEncod
8. End Procedure

J. A New Framework for Cloud Storage Confidentiality to Ensure Information Security[26].

Deepak Singh and Harsh K Verma suggest framework, this framework use AES, SHA-1, and Station-to-Station Key Agreement protocol. The proposed framework will used different servers and every server in a cloud network performs same operation. The consumer data that stored in cloud can be tested in terms of privacy and integrity. The server in the cloud network communicate to each other in shape of a ring these servers are performing operations as follows: First user need to be authenticated by the server and server is authenticated by the user, which is done by station-to-station key agreement protocol. Then for integrity of data server will compute SHA-1. And finally server encrypts the data using AES to maintain confidentiality of data. We will using station-to-station key agreement protocol as a key exchange mechanism. This protocol an outstretched version of Diffie Hellman Key exchange algorithm, but Diffie Hellman algorithm is exposed to Man in Middle attack. In station-to-station key agreement protocol. This protocol avoids man-in-the-middle attack so validity of the user and server is kept. Working of the suggested system as in algorithm 1 for upload file. User Sign Up or Sing In to/from the Cloud Service Provider, Keys Interchange among users and cloud servers via station-to-station key agreement protocol and user chooses the data file to Upload or Download.

Algorithm 1: Propose system upload algorithm

Input: any type of file
Output: encrypted file

1) Consumer encodes the data with their key and directs it to the authentication server.
2) Authentication Server decodes the file with his keys.
3) It calculates the SHA-1 algorithm for the native file and inserts the result called digest with the native file.
4) Lastly the certification server encodes the file using AES and sends the encoded data to the customer.
5) Currently customer can access to storage server and uploads the encoded file to cloud storage

Customer downloads the data file by directing request to server by clicking on download pin algorithm 2 explain how user can download his file.

Algorithm 2: Propose system download algorithm

Input: encrypted file
Output: plan text file
1) Downloaded file is sent to the verification server by the customer. And verification server decodes the file using its key.
2) It calculates the SHA-1 on data ration of the file and matches it with the digest insert with the data file.
3) If the match was found true then file is confirmed and file is send back to the customer, else error message is direct to the customer tell him that the data file is immoral or changed

We chose these methods to protect the cloud because it provides data security and thus ensure that the data remains confidential and protected from all types of threats

5. Important points towards cloud storage

Cloud storage is an important service to provide data, documents and other sources of knowledge continuously and everywhere. One of the most important things that prevent the spread of cloud storage is a large sense of security breaches and data disclosure, especially when the data is important, sensitive and valuable, so we will try in this section Focus on some important points to increase user knowledge to deal with some security problem and what steps to follow when choosing a cloud storage service provider.

1) At first you have to think about the amount of data that will be transferred to cloud storage and its value, the private clouds are considers secure and more expensive cloud types at the same time. If this option expensive, it is better go to the community cloud, this share service with users has same concerns, with different security perceptions, if this option also expensive, go to the public cloud that consider less security from above but still have acceptance degree for security but need more attention.
2) In all types of deploy, enable Encryption techniques from service provider consider an additional layer of security, and can customize the Encryption techniques to make different in all user, or make user able to use it from third party.
3) Interfaces and APIs as important to connect and interact with the services provided by the cloud but the insecure APIs make it from easy points to penetrate , for that must work with provider that provide the secure control environment to working with APIs.
4) Also work with service provider that store my data in standard form and that let change the provider and service without loss in data, time and money.
5) Access controls and firewalls with multi-layer secure systems are the power tools to deal with granting powers and power that using to penetrate.
6) Also access control with firewalls uses to separate virtual machines and not insert a malicious virtual machine on the physical machine.
7) The service provider has a mechanism to translate the sentences entered to the cloud accurately to detect any codes that can be implemented leads to data revealed.

All these characteristics must be ascertained that they are present at the service provider. In the final, neglected the security concerns that related with network in this paper.

6. Conclusion

Cloud computing and cloud storage provides very important services, poor security and privacy in the cloud storage has made many users do not want to upload data on the cloud, in this paper we tried to identify the main points in the cloud computing in general, and some of the attacks on the cloud and cloud storage service and how to deal With it and some characteristics that must be provided by the service provider before the transfer of data to the cloud. We ignored in this paper the security problem of networks and the Internet to the large volume of the subject

References

[1] S. Narula, A. Jain, and Prachi, “Cloud Computing Security: Amazon Web Service,” *2015 Fifth Int. Conf. Adv. Comput. Commun. Technol.*, pp. 501–505, 2015.
[2] G. Docs, “Cloud Computing Security and Privacy Issues,” no. 10, pp. 2–5, 2011.
[3] R. Saleem, “Cloud computing’s Effect on Enterprises in terms of Cost and Security,” *Computing*, p. 89, 2011.
[4] T. M. Evans, T. Huynh, K. Le, and M. Singh, “C l o u d S t o r a g e,” 2011.
[5] V. S. Arjun U, “Issues in Cloud Computing,” *IEEE*, 2016.
[6] S. Barakovi, “Short and Sweet : Cloud Computing and Its Security,” 2016.
[7] H. Sirtl, *Cloud Computing*. 2009.
[8] D. Wu, P. Hugenholtz, K. Mavromatis, R. Pukall, E. Dalin, N. N. Ivanova, V. Kunin, L. Goodwin, M. Wu, “CLOUD COMPUTING – An Overview An Overview,” *White Pap.*, vol. 462, no. 7276, pp. 1–5, 2009.
[9] R. Sharma and R. K. Trivedi, “Literature review: Cloud Computing –Security Issues, Solution and Technologies,” *Int. J. Eng. Res.*, vol. ISSN, no. 34, pp. 221–225, 2014.
[10] M. Irfan, M. Usman, Y. Zhuang, and S. Fong, “A Critical Review of Security Threats in Cloud Computing,” *Comput. Bus. Intell. (ISCBI), 2015 3rd Int. Symp.*, pp. 105–111, 2015.
[11] Y. R. K. Ch Chakradhara Rao, Mogasala Leelarani, “Cloud Computing Services and Applications,” *Int. J. Eng. Comput. Sci. ISSN2319-7242*, vol. 3, no. 12, pp. 963–967, 2013.
[12] N. M. Turab, A. Abu, and T. Shadi, “Cloud Computing Challenges and Solutions,” *Int. J. Comput. Networks Commun.*, vol. 5, no. 5, pp. 209–216, 2013.
[13] N. Kshetri, “Cloud computing in developing economies,” *IEEE Comput.*, vol. 43, no. 10 April, pp. 47–55, 2012.
[14] Cloud Security Alliance, “Top Threats to Cloud Computing,” *Security*, no. March, pp. 1–14, 2010.
[15] A. Gordon, “The Hybrid Cloud Security Professional,” *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 82–86, 2016.
[16] C. M. R. Da Silva, J. L. C. Da Silva, R. B. Rodrigues, G. M. M. Campos, L. M. Do Nascimento, and V. C. Garcia,

"Security threats in cloud computing models: Domains and proposals," *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 383–389, 2013.

[17] S. Iqbal, M. L. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, and K. K. Raymond Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, 2016.

[18] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud Computing Security--Trends and Research Directions," *2011 IEEE World Congr. Serv.*, no. October, pp. 524–531, 2011.

[19] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," vol. 9, no. 1, pp. 138–151, 2016.

[20] K. Han, Q. Li, and Z. Deng, "Security and efficiency data sharing scheme for cloud storage," *Chaos, Solitons & Fractals*, vol. 86, pp. 107–116, 2016.

[21] N. Khanezaei and Z. M. Hanapi, "A framework based on RSA and AES encryption algorithms for cloud computing services," *Proc. - 2014 IEEE Conf. Syst. Process Control. ICSPC 2014*, no. December, pp. 58–62, 2014.

[22] N. R. Patil and R. Dharmik, "Secured cloud architecture for cloud service provider," *IEEE WCTFTR 2016 - Proc. 2016 World Conf. Futur. Trends Res. Innov. Soc. Welf.*, pp. 1–4, 2016.

[23] S. K. Abd, R. T. Salih, S. A. R. Al-Haddad, F. Hashim, A. B. H. Abdullah, and S. Yussof, "Cloud computing security risks with authorization access for secure Multi-Tenancy based on AAAS protocol," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2016–Janua, 2016.

[24] G. Zhao, Y. Li, L. Du, and X. Zhao, "Asynchronous challenge-response authentication solution based on smart card in cloud environment," *Proc. - 2015 2nd Int. Conf. Inf. Sci. Control Eng. ICISCE 2015*, pp. 156–159, 2015.

[25] M. K. Sarkar, "A Framework to Ensure Data Storage Security in Cloud Computing," *IEE 2*, pp. 3–6, 2016.

[26] D. Singh, "A New Framework for Cloud Storage Confidentiality to Ensure Information Security," 2016.