JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A NOVEL FRAME WORK DESIGN FOR ENHANCING SECURITY IN MULTI CLOUD SYSTEMS

Neela Vineeth[1] **Dr. G. Sharmila Sujatha**[2]

1. M.Tech Scholar, Dept. of CS & SE, Andhra University College of Engineering(A), Visakhapatnam, India,

2. Assistant Professor (C), Dept. of CS & SE, Andhra University College of Engineering(A), Visakhapatnam, India.

Abstract:

Earlier when cloud computing was introduced; very few business segments and enterprises welcomed the technology. Moreover those companies which accepted cloud technology are of massive and very large in nature. Gradually the next level of companies which are at large scale also got adopted to the giant technology and the current existing scenario shows that even small and medium scale enterprises not only are getting adopted to the technology but also it is of their prime agenda. That too, Cloud technology is being implemented in all business domains. Eventually cloud prospects led to dozens of domain based clouds. In this paper a novel security solution is proposed in storing the health care data where the health care centre subscribes for multiple clouds. Simulating three clouds as database storage, the proposed solution comprises storage in which the data is divided into pieces where in each fragment gets stored in specific encrypted format. While retrieving, the data gets decrypted after which it is combined and accessed by the intended user. For encryption and decryption the algorithms used in this project are Triple DES, AES and RC2, which means three algorithms are being used and hence the security when compared to the single cloud and earlier few multi cloud solutions certainly increase. Also the internal computations are simple so that the time consumption is also less.

Keywords: Multicloud solution, Multicloud security, Health cloud

1. Introduction:

1.1. About Cloud Computing:

In the current times every moment massive data is being generated which could not be handled by the traditional storage system. To handle such enormous data every business segment is utilizing the cloud services and hence cloud storage is of prime research aspect today. Cloud computing is the on demand delivery of computing services that includes servers, storage, databases, networking, software, analytics, and intelligence over the Internet to offer faster innovation, flexible resources, and economies of scale. Pay only for cloud services that are used, helping lower the operating costs, running the infrastructure more efficiently and scale the business according to the change in needs. Fig 1.1 shows the basic concepts of cloud technology.

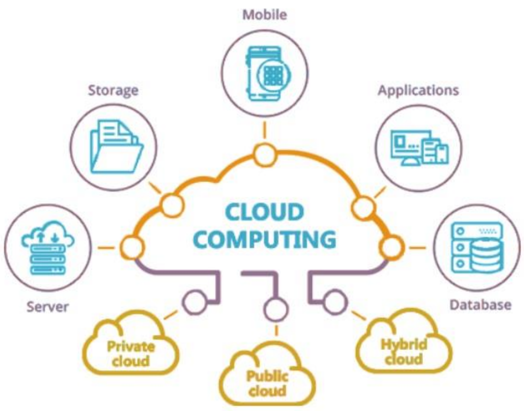


Fig 1.1: Basic concepts of Cloud technology

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data.

1.2 Cloud Services:

In a cloud-based system, if the primary server goes down, a secondary server powers up to ensure business continuity. In the event of a disaster, breach, or equipment error, this feature can significantly lower the risk of losing data and/or creating a work slowdown.

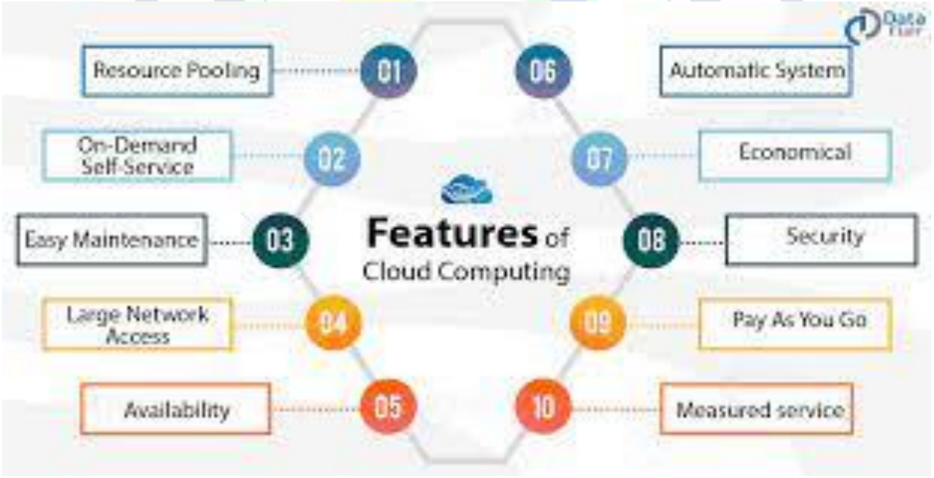


Fig 1.2: Cloud services

Data storage costs money in which maintaining legacy infrastructure to support internal backups raises the budget. Adopting cloud services certainly minimizes the costs. The services offered by cloud are as shown in the figure 1.2. Amongst, security is the prime concern of the digital assets (data) in any domain and hence secure storage of such assets is obligatory. Cloud Security is provided in several ways but the robustness in the architecture defines the strength of cloud. Security algorithms play a vital role in attaining the privacy for the data.

1. 3 Healthcare Cloud:

Nowadays Health domain is the most predominant and definitely needs the cloud support. Often in the taxonomy of Clouds we could see Health cloud as one category in which Haas (Health as a Service) is the cloud service. A health network comprises Hospital or Health care unit, Diagnostic centre, Patient and Doctor. Every element is connected. Examples for Health cloud include ClearDATA, Dell's Secure Healthcare Cloud and IBM Cloud. Using cloud computing, nurses, doctors, and administrators instantly share information from any location. In such a huge network if proper measures are not taken then definitely it leads to problems. A sample diagram of Health network connected to cloud is as shown in the figure 1.3.

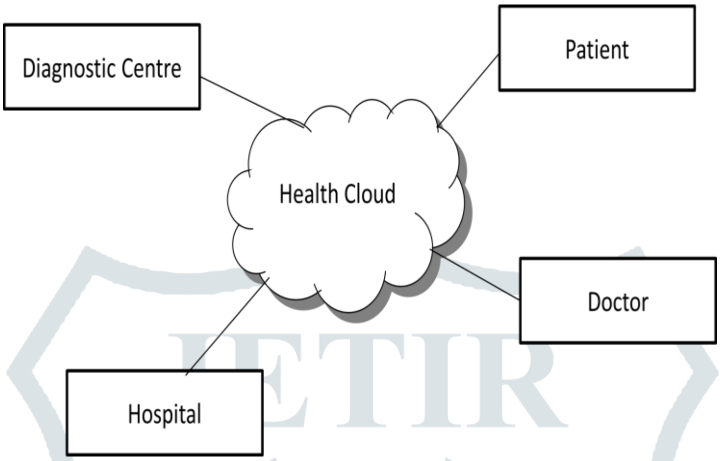


Fig 1.3: Health cloud prototype

A multi cloud network is the network of the entities which get connected to multiple clouds and are in connection. A sample multi cloud network could be seen in figure 1.4. The major assets in a cloud include Data centers, Data and Network infra such as routers, gateways, end user equipment, firewalls, cables etc... The major issues in multi cloud solution include Integration, Data distribution and Security. Data Privacy, Authentication and Integrity are the prime security aspects to be taken care while implementing a multi cloud.

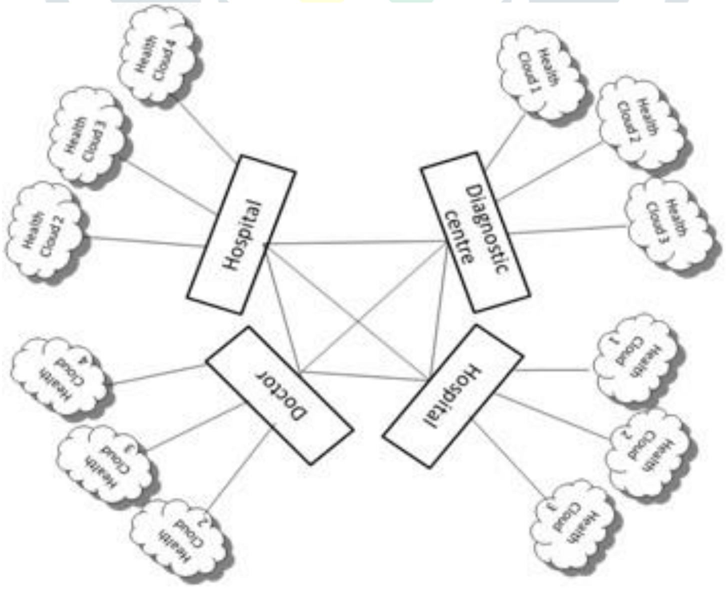


Fig 1.4: Multi cloud network

The next section addresses the already proposed solutions in favor of multi cloud security with respect to health cloud and in section 3 the proposed work is mentioned and finally conclusions are given in the last section.

2. Related work:

C.Wang et.al. [1] addressed how to enable public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. The result is further extended to enable the TPA to perform audits for multiple users simultaneously and efficiently.

Yunhong Gu et. al proposed [2] how to enable users to work with large datasets stored over multiple distributed nodes as if the files were on their local disk. Users do not need to locate data, manage data across multiple nodes, back up data, and manage the addition of new nodes or the deletion of existing nodes to the system.

Anwar Ghani et.al. [3] in their paper focused on issues related to the two categories data security and data management and analyzed the possible solutions to such issues. This distinction helped in understanding the challenges faced by cloud storage providers and tenants.

N. Velmurugan et.al. in [4] & [5] had given the concept of CPPD which is intended for security in cloud environment. They proposed an exclusive mechanism in the form of an algorithm in the multi cloud architecture so as to improve CPPD.

Kevin D. Bowers et.al. [6] proposed a distributed Cryptographic multi cloud security system HAIL which is a file integrity checking mechanism that operates in remote. It offers imperative features of multiserver application of Proof of Reliability (POR) protocols. HAIL exhibited better performance when compared to the available solutions.

HSDSA- Hybrid and Secure Data Sharing Architecture is an innovative and effective architecture proposed by **Tayssir Ismail et.al.** in **[7]**, which bridges the patient & e-health system requirements.

Balasaraswathi V.R. et.al. [8] & **R. G. Warhade et.al.** [9] proposed multi cloud storage models which enhanced the security through split-upload and club-download approaches. **Alisha Jindal et.al.** in [10] also proposed a multi cloud storage solution using Elliptic Curve Cryptographic (ECC) algorithm for encryption and decryption processes.

Yogita M Pattan et.al. proposed a solution in [11] that provides a secure mechanism for file storage. In the solution the process of storing files is abstracted which is done across multiple servers enhancing the security and privacy of data with a trustworthy environment to the users.

3. Proposed Work:

The proposed work comprises the design of a framework which enhances the security in multi cloud systems in which the data is encryption and decryption is done using the three algorithms namely Triple DES, RC2 and AES algorithms. The design solution is developed using Java, NetBeans IDE, MySQL.

The core part of this project is upload and download processes. The overall design of the data upload and download processes is as shown in figure 3.1. It is presumed that the data stores into three clouds. The project is a simulation where the three clouds are considered as database/s.

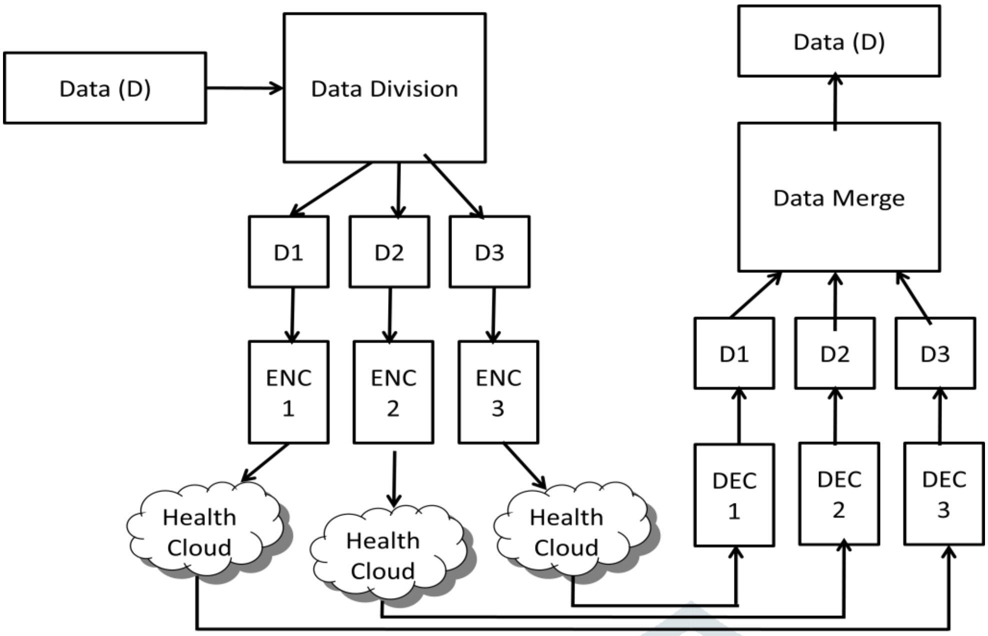


Fig 3.1: Design model

The data is divided into three parts D1, D2 and D3. These 3 parts are given to three encryption algorithms and the output is stored in three clouds. When the data is to be retrieved the data from three clouds is obtained and the respective decryption algorithm is applied with which we get three decrypted parts. Finally the three parts will be merged to get the original data. The mathematical representation is as shown below. The algorithms used in this project are Triple Data Encryption Standard (3-DES), Advanced Encryption Standard (AES) and RC2 algorithms.

Data upload to cloud:

D=D1+D2+D3

ED1=TDESk1(D1)

ED2=RC2k2(D2)

ED3=AESk3(D3)

Data retrieval from cloud:

D1=TDESk1 (ED1)

D2= RC2k2 (ED2)

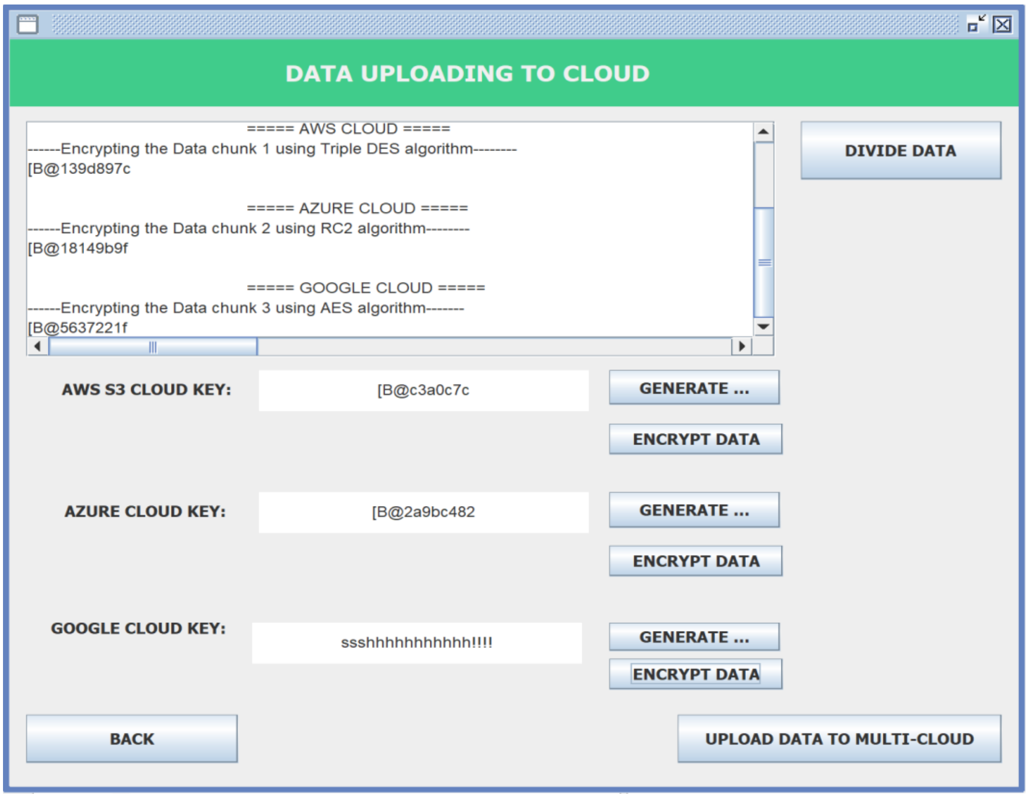
D3=AESk3 (ED3)

D1+D2+D3=D

In the above mechanism k1, k2 and k3 are the keys used for encryption. Below equations represent the key computations in which r1, r2 and r3 are random numbers of size 168 bits, 128 bits and 192 bits respectively. 'C1' & C2 are constants of size 128 and 192 bits respectively.

$k1 = r1$
$k2 = r2 \oplus C1$
$k3 = r3 \oplus C2$
$\oplus$ - XOR operation

Following are the implementation screenshots (Fig 3.2, 3.3 and 3.4) of the design solution among which the data upload process could be observed. The data is divided, three keys are generated for each part to be encrypted and then the parts are encrypted.



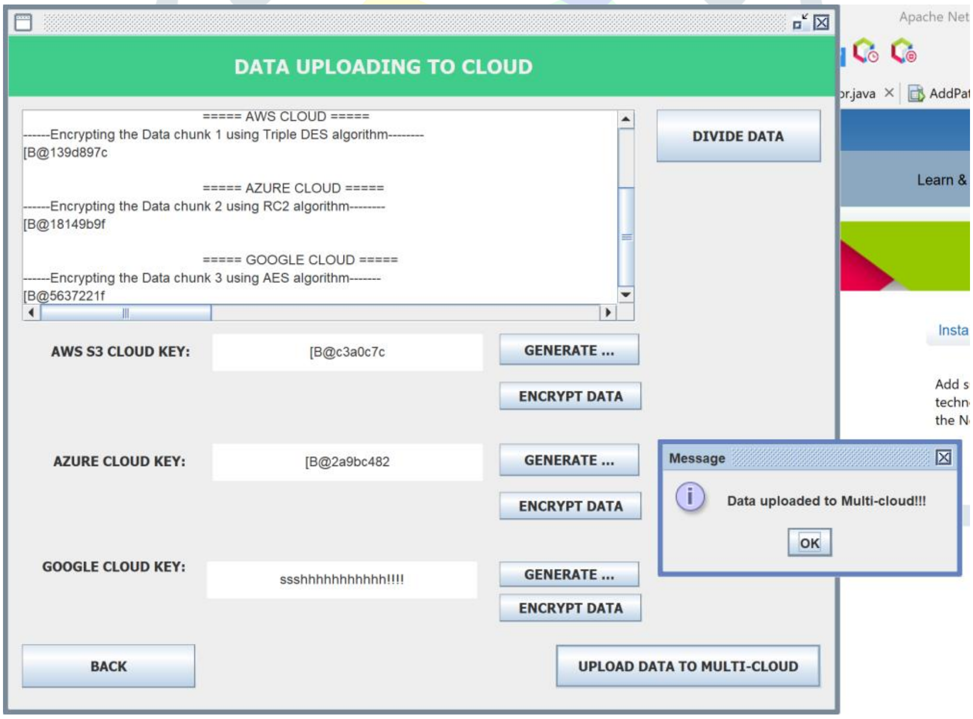
```
===== AWS CLOUD =====
------Encrypting the Data chunk 1 using Triple DES algorithm--------
[B@139d897c

===== AZURE CLOUD =====
------Encrypting the Data chunk 2 using RC2 algorithm--------
[B@18149b9f

===== GOOGLE CLOUD =====
------Encrypting the Data chunk 3 using AES algorithm-------
[B@5637221f
```

AWS S3 CLOUD KEY: [B@c3a0c7c

AZURE CLOUD KEY: [B@2a9bc482

GOOGLE CLOUD KEY: ssshhhhhhhhhhh!!!!

Fig 3.2: Encryption of the data



```
===== AWS CLOUD =====
------Encrypting the Data chunk 1 using Triple DES algorithm--------
[B@139d897c

===== AZURE CLOUD =====
------Encrypting the Data chunk 2 using RC2 algorithm--------
[B@18149b9f

===== GOOGLE CLOUD =====
------Encrypting the Data chunk 3 using AES algorithm-------
[B@5637221f
```

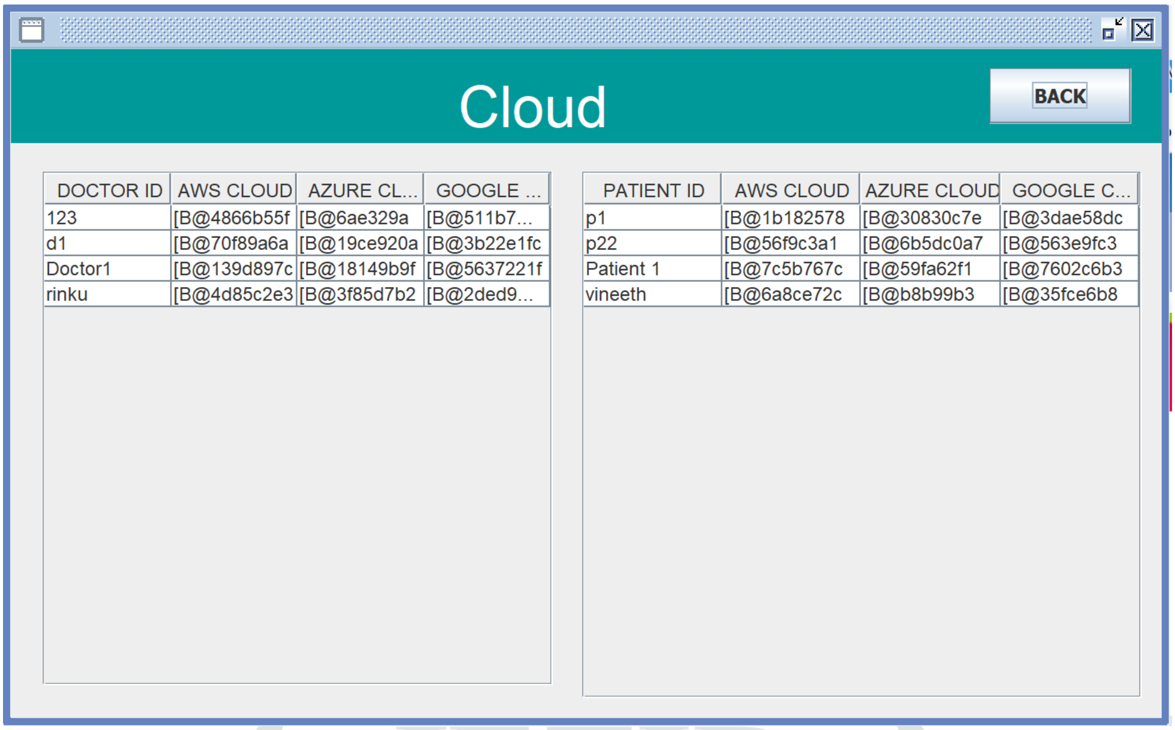
AWS S3 CLOUD KEY: [B@c3a0c7c

AZURE CLOUD KEY: [B@2a9bc482

GOOGLE CLOUD KEY: ssshhhhhhhhhhh!!!!

Data uploaded to Multi-cloud!!!

Fig 3.3: Data uploaded to cloud successfully



DOCTOR ID	AWS CLOUD	AZURE CL...	GOOGLE ...
123	[B@4866b55f	[B@6ae329a	[B@511b7...
d1	[B@70f89a6a	[B@19ce920a	[B@3b22e1fc
Doctor1	[B@139d897c	[B@18149b9f	[B@5637221f
rinku	[B@4d85c2e3	[B@3f85d7b2	[B@2ded9...

PATIENT ID	AWS CLOUD	AZURE CLOUD	GOOGLE C...
p1	[B@1b182578	[B@30830c7e	[B@3dae58dc
p22	[B@56f9c3a1	[B@6b5dc0a7	[B@563e9fc3
Patient 1	[B@7c5b767c	[B@59fa62f1	[B@7602c6b3
vineeth	[B@6a8ce72c	[B@b8b99b3	[B@35fce6b8

Fig 3.4: Sample Cloud data details

3.4.2 Performance analysis:

Although the solution is designed, it is necessary to check the effectiveness of solution. Firstly the algorithms which are considered for encryption and decryption are efficient and hence the security issues are highly preserved. Next, the security is said to be enhanced due to the reason that data is partitioned; each part is encrypted separately. The probability of security is improved. Moreover the key computation for the three algorithms is simple due to which the time consumption becomes less. Lastly due to the random numbers considered in key generation, the probability of security with Encryption algorithms shall be high.

Most importantly, performing brute force attack will also be difficult because the number of all possible keys required is $2^{(168+128+192)}$. Similarly time consumption also is less when implemented.

4. Conclusion:

Multi cloud is a vast area in which the security features are very much crucial. In this project a model is developed which implements a multi cloud security architecture. The architecture comprises of secure storage and accessing the Electronic health data of patients on to multiple clouds. The data is partitioned into chunks encrypted with different algorithms. The dynamic, simple and robust key generation process; data division and merging processes; multiple encryption algorithms and multiple clouds offer high security to the data assets in clouds.

As a part of future direction, which data is to be distributed to which cloud, how many clouds are apt for the security implementation, key distribution etc…

REFERENCES

[1] C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," in IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013, doi: 10.1109/TC.2011.245.

[2] Yunhong Gu, Robert L. 2009. Grossman. Sector: A high performance wide area community data storage and sharing system. Future Generation Computer Systems, 20 May 2009.

[3] Ghani, Anwar & Badshah, Afzal & Jan, Saeed Ullah & Alshdadi, Abdulrahman & Daud, Ali. (2020). Issues and challenges in Cloud Storage Architecture: A Survey.

[4] N. Velmurugan and S. Godfrey Winster, "An Invincible Rudimentary Architecture for Data Security in Cloud Environment Using Multi Cloud", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-11, September 2019

[5] N. Velmurugan and S. Godfrey Winster, "An Inimitable Mechanism and Architecture for Security in Cloud using Multi Cloud", International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-5, January 2020

[6] Kevin D. Bowers, Ari Juels, and Alina Oprea. 2009. HAIL: a high-availability and integrity layer for cloud storage. In <i>Proceedings of the 16th ACM conference on Computer and communications security</i> (<i>CCS '09</i>). Association for Computing Machinery, NewYork, NY, USA, 187–198. DOI:https://doi.org/10.1145/1653662.1653686

[7] Ismail, Tayssir & Touati, Haifa & Hajlaoui, Nasreddine & Hassen, Hamdi. (2020). Hybrid and Secure E-Health Data Sharing Architecture in Multi-Clouds Environment. 249-258. 10.1007/978-3-030-51517-1_21.

[8] Balasaraswathi V.R. and Manikandan S., "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014, pp. 1190-1194, doi: 10.1109/ICACCCT.2014.7019286.

[9] R. G. Warhade and B. Vankudothu, "Enhancing Cloud Security Using Multicloud Architecture and Device Based Identity," 2015 7th International Conference on Emerging Trends in Engineering & Technology (ICETET), 2015, pp. 34-39, doi: 10.1109/ICETET.2015.16.

[10] Alisha Jindal and Kaur Gagandeep. (2019),"Enhancing Data Integrity in multi cloud storage", Int. Journal of Engineering Research and Applications, Vol. 4, Issue 9

[11] Yogita M Pattan, Peruru Vanaparthi Sai Likhitha, Prof. Raghavendra Prasad and Prof. Smitha G R, "Implementation of Secure Multi Cloud File Storage", International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 05 (May 2020), pp 7138-41.