*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 11 – No. 8, January 2017 – www.ijais.org*

# A Proposal on Cloud based Data Centre using Shared Memory of Mobile Storage by Virtualization

Nazmus Sakib
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka- 1208, Bangladesh

Raihan Ahmed
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka- 1208, Bangladesh

Tanvir Ahmed
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka- 1208, Bangladesh

Fahad Bin Islam
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka- 1208, Bangladesh

Bijoya Das
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka- 1208, Bangladesh

## ABSTRACT

Cloud computing is a broadly used technology which serves users with resources on specific demand enhancing manageability, minimizing the data management and operational cost. Basically, cloud allows users to store their valuable data on the cloud storage so the security of the data center and easy access are considered as focusable parts in cloud computing. In the study we spot light to a new approach of cloud computing where mobile storage is used to build the data center of cloud and easy access having a preferable security. We deliberate that it is possible to lower the cost if the data center is built using user's mobile storage so a 3-tier technology is proposed. Firstly, a layer is user's mobile devices, second layer is server with different virtual machines and last layer is again the user's mobile device which is used to build the data center of cloud (mobile-server-mobile). A mobile app implements the initial security and management issues. Users can oscillate data between first layer and third layer with the help of virtual machines that ensure secure transaction of data, reduction of power consumption, maintenance cost, bandwidth consumption and fast data sharing.

## Keywords

Cloud, shared memory, virtualization, encryption, synchronization, RAID, security, Virtual Machine(VM), Media Access Control(MAC), Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES).

## 1. INTRODUCTION

Cloud computing is a technology which has created a buzz in the modern era, having both technology and business model it is widely used in different approaches and for different purposes by any organization based on how they use it [1]. Recently it is empowered as a model which is provisioning with the smallest possible operational effort over the network component [2] [3]. Cloud computing has come into view of providing reliable and fast access to the resources that is why it is popular as a service oriented network where users are being served from different organization based on the service they offer [4] [5]. Though the organizations are providing on demand services, they may face a strong challenge with the different issues in future for which many question may rise: 1) How the cloud storage will be maintained with the increasing need of storage for the increasing users and what can be the role of user's unused mobile storage for this purpose? 2) How the power consumption by the server can be lowered? 3) How the file sharing can be faster to save time and cost? 4) Can the specific bandwidth utilization be maximized? 5) How data can be more secured against the activities of the intruders?

The study of this paper would like to propose a new approach of using cloud with mobile based data center that would be able to cover the back of the rising issues. If we consider using user's mobile storage rather than server storage it would result in low storage at the server side then the maintenance would be simple causing lower load and processing time at the server virtual machines, that may end up using low power consumption by the server to maintain the low storage which may increase the data reliability, availability [6].

In consequence, user's mobile unused storage can be utilized to provide additional storage to the cloud server solving the emerging need of storage for the increasing users. Moreover, data on the mobile storage can be transferred using mobile bandwidth specifically by pairing two mobile devices using MAC addresses results efficient use of bandwidth of mobile internet and faster file sharing between them which can maximize the utilization of the specific bandwidth of mobile devices [7]. Meanwhile, a two-layer security is introduced for a secured file sharing. Above all, a mobile app installation is mandatory for the users within the cloud network. The uniqueness of our proposal is that the use of mobile storage to minimize the cost of introducing large storage at server side. Moreover, it reduces the required server side bandwidth by using mobile device bandwidth instead. And also it will process faster file sharing between users by pairing two mobile devices through mac addresses based on a particular file request. This papers follows in section 2 about the literature review, then our proposal is on section 3 and so on.

## 2. LITERATURE REVIEW

### 2.1. Cloud Data Centre

Cloud computing is a popular use of the recent technology. Cloud computing is an internet based working process through which data can be accessed and stored. In cloud computing system devices are virtualized and made a connection through which it acts like a single Personal Computer (PC). In some case clouds are consisted with clusters grid. Cloud computing can be explained as a data center with end devices which acts like a single PC through hypervisor technology which offers services to multiple users by sharing resources. The most important part of the cloud computing is that the users don't need to think about the location, they just need their internet connection [8]. And also It has become familiar for its reliable architecture consisting of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Data-as-a-Service (DaaS) and Software-as-a-Service(SaaS) which provides easy access, high computing power, storage ability, cheap cost, easy management, works like a single end device [9].

Three models are mainly used for this cloud computing. Firstly private cloud: some organizations are using private cloud which are using the same benefits of public cloud but in this process the system only works for a single organization where the data is not shared by all, it is shared by a limited number of people and for that reason the security issues minimizes. Secondly public clouds: The main difference between the public cloud and private cloud are in public clouds the shared data can be used by general users through an internet connection but in private clouds by a limited permitted users only. Here security issues are different from private cloud. And the latest technology is hybrid cloud. We can define it is a combination of public cloud and private cloud. It is more beneficial as it offers multiple deployment models. Moreover, hybrid cloud increases the capability of data sharing [10].

## 2.2. Virtualization

Virtualization is the core approach to operate cloud computing in an easier and flexible way that has gained a priority to distribute the work load within the cloud network. Recently combining newer approach of virtualization and cloud computing different organizations has been benefitted by minimizing their cost at server side. Besides, virtual software is used to allow several software running under a single operating system which is like Linux and windows in the same PC [11]. Along with managing large data center, sometimes it is impossible for the server to serve different requests on the same data center and for which virtualization is used to distribute the load of the requests within the virtual machines created from the server machine. Resulting, the processing of the users request separately within different virtual machines and it reduces the server response time as well as scalability [12].

Three types of virtualization: Server virtualization, desktop client virtualization and storage virtualization. In server virtualization, a server controlling a cloud is divided by resources which allows multiple works can be operated resulting high utilization of server resources and minimizes the expense. Desktop client virtualization allows the operator to keep the users machine up to date and track the record which improves the security. Storage virtualization is the most valuable part in the cloud computing that has three approaches known as: Direct Attached Storage (DAS), Network Attached Storage (NAS) and Storage Area Network (SAN). Each of the approaches has different method of storing data in the storage and maintaining with the help of the server [13].

## 2.3. Security

Cloud is a service based network where client is served on demand and the variety of services are attracting clients to be interested of. Cloud computing is the recent era of technology where people are getting more and more used to relying on this technology. Moreover, the different approach of using cloud is now getting much attention of the users to get involved with this newest practice of modern era. In the case of Cloud computing, the first and foremost concern is the security that is to assure the client to be relaxed about the reliability. The stronger security a cloud networks provides the more it becomes reliable and trustworthy, also the users can get their minds off the data security. Data security is now the core feature to define the level of a cloud network which is the most focusing point for the cloud organizations. Currently many organizations are following some common approach of security to secure the data of the user and maintain a level of security [14].

In the study of this paper, security is being taken as the major attention where the user's data are given two layer of security [15]. Here AES (Advanced Encryption Standard) as Encryption-1, 2048 bit RSA as Encryption-2 are used to serve the standard of the security. RSA asymmetry algorithm is now a day widely used to secure data transmission within the cloud network. RSA asymmetry algorithm has to be done by a key generation, distribution, encryption and decryption. It has an encryption key that is public to everyone within the cloud and a decryption key that is kept secret within the cloud to maintain the rules of security. In asymmetry RSA, two large prime numbers are used for to find a public key with the auxiliary value that prime numbers are kept secret but the public key is freed to everyone. Anyone within the cloud network can encrypt data using the public key and cover the data with one layer of protection, but the private key is the main concern of secret that is kept hidden from everyone, the one holding the private key can only decrypt the encrypted data [16]. AES stands for advanced encryption standard, which is a preferable encryption differing from RSA is that is symmetric as it uses only one key to encrypt and decrypt data. Implementation of AES must be followed by using one of the key lengths e.g. 128,192,256 bits [17].

## 2.4. Synchronization

In the cloud server all the data are stored in a synchronized way and whenever the data are uploaded in the server those files will be automatically synchronized enabling the user to upload and download data in an easy way. Synchronization is the method of ensuring compatibility and the reliability of the data objects throughout all the applications and those devices which stores data [18].

Moreover, it guarantees that similar copy of data are used in some selected devices from source to destination. Data synchronization is empowered through a specific software that records data when they are created and used. This process is being put into practice in the cloud servers when the valuable data are stored in the virtual machines. Whenever the data are modified in the original source synchronization ensures that all the data are updated with the original one. In some case, synchronization also performs mirroring of data where each of the data sets are absolutely duplicated within another device [19] [20]. And there are two types of synchronization rules are available one of them is declarative another one non-declarative synchronization rules.

The rules which is needed to apply the synchronization is known as declarative provisioning. And declarative provision is applied in the Forefront Identity Manager (FIM) portal which is an architecture that provides flexible and customizable architecture to define the data and its attributes. Those rules ensure that data is flowed between the virtual machines and destination devices. And one of the important benefits of synchronization is that it improves the response time because retrieval rates are faster as it can fetch data from nearby data storage. Another important factor of the synchronization is that it has to maintain a consistency of the data throughout the server though it has loose consistency over the entire cloud, that some of the virtual machines can up to date with the recent data but some fail to replicate in a consistent manner [21].

## 2.5. Mirroring

Mirroring is a process to ensure the data reliability in case of failure or recovery which is a core support for every storage. Mirroring has variations like: RAID 0, RAID 1, RAID 5 and so on having different techniques storing data and mitigating fault tolerance. Here RAID-5 is preferable in the study of this paper. The idea of the RAID-5 cloud came from the storage cost which need to be minimized before it was done by coding practices by designers and now it is completely banned when the RAID-5 was introduced in the cloud. An ideal cloud raid system provides a best balance between the production, reliability and storage.

In addition data security is a prime interest now-a- days. Cloud storage changes the view of storing data in the virtual machines by centralization where all the data are spread in the cloud. There are some noticeable benefits of storing data all over the cloud which are known as flexible data management, data can be accessed all over the globe resulting the minimization of the cost. RAID-5 increases the performance of the data storage and recovery scope of those data [22]. In addition, those files are saved in the disks of RAID-5 if one of the disks are damaged it is possible to retrieve data from another disks this is how RAID -5 ensures data reliability and availability. And that is one of the special capability of the RAID-5 in other case if the data are stored using RAID-1 then all the data are mirrored. In case of data failure all data would lost as no data are mirrored in another disks. So RAID-5 has much better space efficiency than all other RAIDS [23].

## 2.6. Shared Storage

The term shared storage stands for a kind of storage that is shared among multiple users and all users can access multiple time in the shared storage. But in the study shared storage is nothing but the user’s mobile device's storage which is partitioned and the partitioned portion is shared among the cloud users. So, the shared storage is main storage which build the data center in our study. Upon the agreement of user, the mobile device's storage is partitioned and a strong encryption is applied in the partitioned part of the storage and then make it accessible only by the users through the app and by the servers [24]. SAN, NAS etc. are some kind of storage sharing approaches that have been accepted wisely. As well as the mobile device's storage portion that is shared among the cloud users is accessible through the internet with the app. The users need to be connected with the internet all the time in this concept.

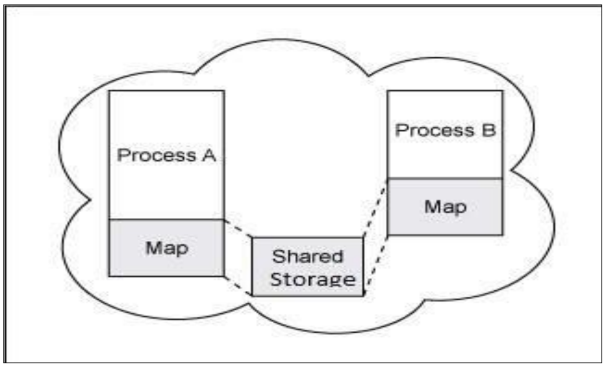

**Fig 1: Shared Storage**

Whenever user wants to access the shared storage an authentication process is required to be fulfilled completely by the user. The authentication process can take input some identity, password, MAC of device etc. and the user is able to access in the shared storage only when the information given by user is declared as valid by the server. Power is consumed by the storage sharing approach and also the pressure in the server is highly decreased moreover it becomes portable and decreases the cost for maintenance of data center [25].

## 3. PROPOSED IDEA

In the study a new approach of cloud management is proposed which is a 3 tier technology that is upper and lower layer are consisted with mobile devices and the middle layer is virtualized servers. Though the upper and lower layer are built with mobile device but the purposes of the two layer’s mobile devices are not same. The first layer’s mobile device is used by the users to access the cloud where the third layer’s mobile device is nothing but the storage of cloud. The middle layer which is virtualized servers performing specific tasks such virtual machines are: user authentication, encryption/ decryption, and mapping, mirroring, process request, device and data control.

So, first of all the user’s mobile devices in the first layer that can access the cloud with the help of an application which should be installed in the mobile device that is mandatory. Whenever the app is installed in the mobile device a portion of the device storage is separated and encrypted by the app which become accessible only by this app. Upon installing the app, the MAC address of the particular device is fetched from the mobile device and after that the users are required to provide necessary information for the registration purpose which will provide them a unique authentication identity and that is the key for the users to access the cloud further. Then the additional information of the user and MAC address of the device is stored in the server. In addition, the app also possesses encryption – decryption mechanism which is a part of security of this model [16] [17] [26].

Now when a registered user wants to upload his valuable data to the cloud, user’s unique authentication identity is checked by the server user authentication virtual machine to determine the user’s validity which contains all the users’ authentication identity and corresponding MAC addresses for the particular device. Upon the validity check the user is able to upload data to the cloud. First the user’s data is encrypted by AES that is encryption-1 then data is then sent to the server device and data control virtual machine for the validity check of the data which is completed by matching the MAC address of the user’s device that is already stored in the server user authentication virtual machine at the time of registration period with the MAC address of the device that has sent the current data. After confirming that the data is valid, the device and data control virtual machine transfers the corresponding data to the Encryption/Decryption-2 virtual machine that performs RSA security on the valid AES encryption-1 data by the app, now the user's data contains a two-layer security [16].

Now the two layered secured data transfer back to the device and data control virtual machine. In the meantime, the mapping virtual machine of the server is activated for mapping the nearest available layer-3 mobile devices using Global Positioning System (GPS) technology and the information including MAC address is transferred to the device and data control virtual machine [27]. Later on the best two devices of layer-3 is selected by the device and data control virtual machine. And data is mirrored by mirroring virtual machines in the selected two mobile devices' shared storage of layer-3 and in the server side.

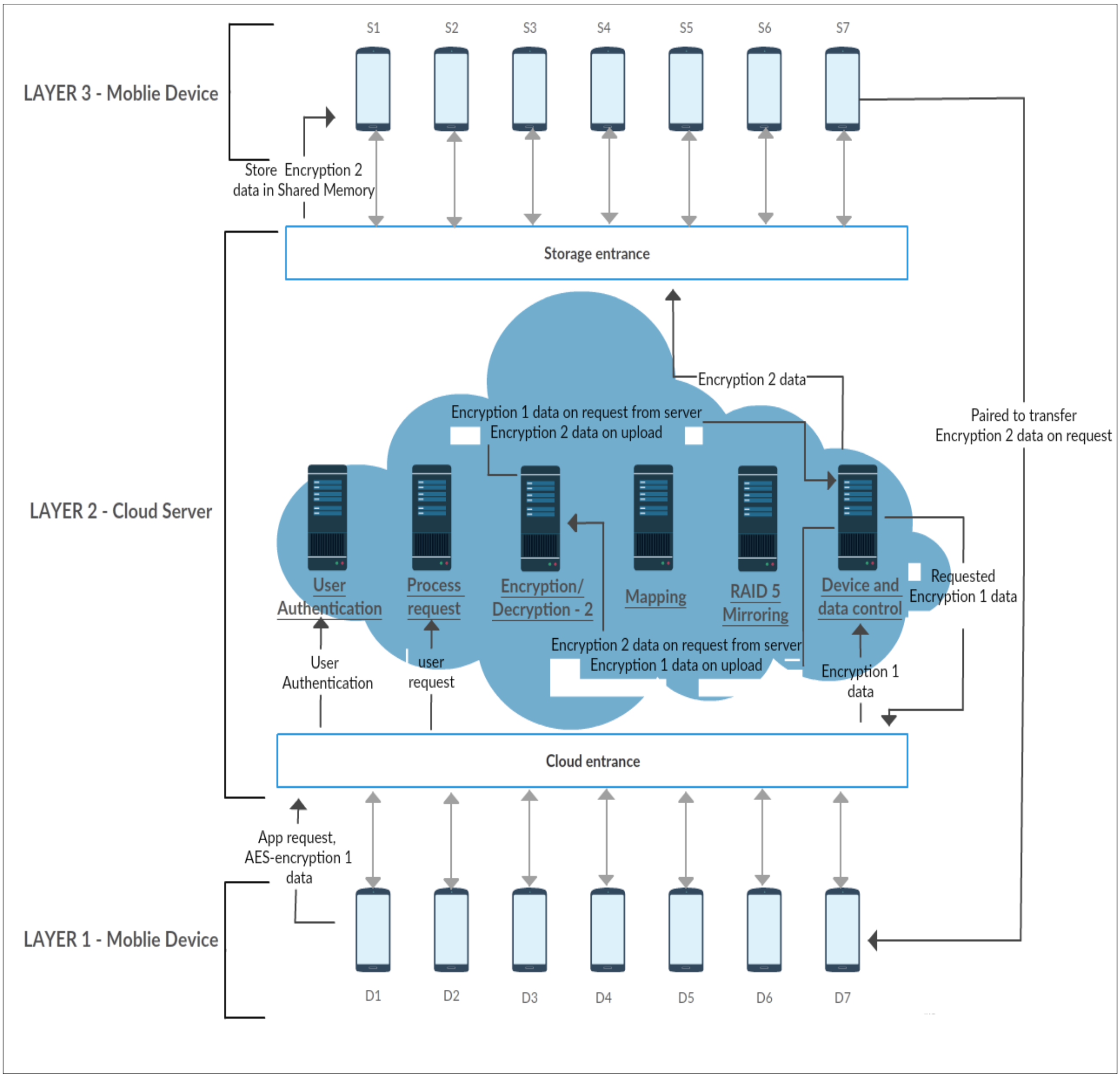
LAYER 3 - Moblie Device
S1
S2
S3
S4
S5
S6
S7
Store Encryption 2 data in Shared Memory
Storage entrance
Encryption 2 data
Encryption 1 data on request from server
Encryption 2 data on upload
Paired to transfer Encryption 2 data on request
LAYER 2 - Cloud Server
User Authentication
Process request
Encryption/ Decryption - 2
Mapping
RAID 5 Mirroring
Device and data control
Requested Encryption 1 data
User Authentication
user request
Encryption 2 data on request from server
Encryption 1 data on upload
Encryption 1 data
Cloud entrance
App request, AES-encryption 1 data
LAYER 1 - Moblie Device
D1
D2
D3
D4
D5
D6
D7

**Fig 2: Three Tier Technology**

The data is stored in the server side for ensuring data reliability and availability and also recovery of data in case mirrored two mobile device's failure [23]. The whole mapping information and data history is saved and updated in the log file according to the sending user's MAC address information. Device and data control machines check repeatedly after a fixed time period whether the mirror devices data and the server side data is up to date for particular user using the log file.

Moreover if it is found that mirror device for particular user is offline for a certain period then the Mapping virtual machine performs another mapping for the particular user's data to be mirrored by the Mirroring virtual machine and the LOG file is updated accordingly [20] [28]. For user to download a specific data, a user request is sent to the specific virtual machines which is processed request virtual machine at the server side with the help of user authentication virtual machine the user is authenticated. Upon authentication, the device and data control virtual machine will check the LOG file for the particular data and layer 3 devices that holding the requested data. Then the nearest device using the LOG is selected and check either the MAC of the nearest device and MAC in the LOG is matched fully or not, if it is matched then a pair is made between the selected mobile device in layer 3 and the requested mobile device in layer 1 then the data is directly downloaded by the requested device from the mirrored layer-3 device which allows the file sharing between the two mobile devices using the mobile devices' data network, this may result a faster file sharing within the cloud.

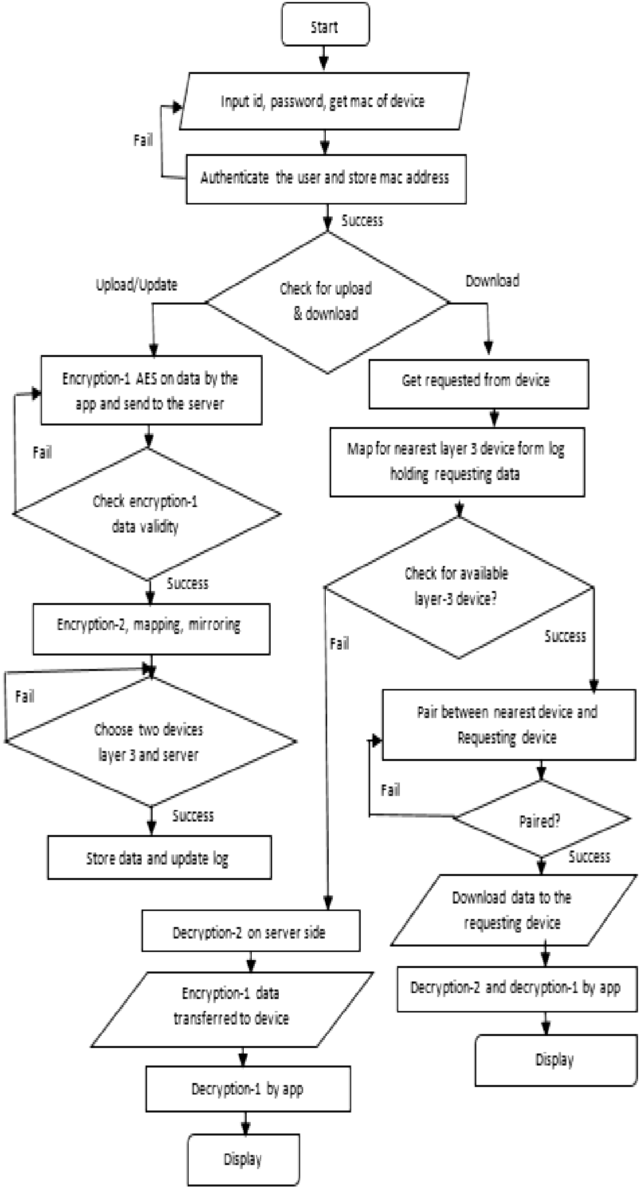
Start
Input id, password, get mac of device
Fail
Authenticate the user and store mac address
Success
Upload/Update
Check for upload & download
Download
Encryption-1 AES on data by the app and send to the server
Get requested from device
Map for nearest layer 3 device form log holding requesting data
Fail
Check encryption-1 data validity
Check for available layer-3 device?
Success
Encryption-2, mapping, mirroring
Fail
Success
Fail
Choose two devices layer 3 and server
Pair between nearest device and Requesting device
Fail
Paired?
Success
Store data and update log
Success
Download data to the requesting device
Decryption-2 on server side
Decryption-2 and decryption-1 by app
Encryption-1 data transferred to device
Display
Decryption-1 by app
Display

**Fig 3: Flow Chart Download and Upload Data**

Here the downloaded data in the requested device at first undergo decryption-2 then AES lock is removed by the app itself, after that requested data is readable. But in case of failure to fetch data from layer 3 device due to offline situation of the layer-3 device or requested data which is mirrored on the layer-3 device is not updated as the server data in this case server side data is used to serve request for a particular user device. In this situation the file sharing a bit slower than the previous one. At server side the decryption-2 is applied on the data then transferred to the requested device based on MAC address. The data is received by requested device then the AES lock is removed to make the data readable for the user.

Suppose from fig-2, Device D1 is configured with the app and proceeds to upload data in cloud. First of all, D1 is blocked by the User authentication VM to provide its authentication details to be checked whether it is valid or not and upon validation it is decided that D1 can proceed to next step for uploading data to cloud. Now the data is encrypted by AES

which is done by the app and then data is transferred to the server where the encrypted data is again encrypted by RSA

2048 algorithm this is how two-layer security is given. In the meantime, the mapping VM map for the nearest devices available for storing the data and the device list including MAC addresses is transferred to the Device and data control VM to select the best two devices where the data can be stored in an efficient manner. Suppose, some devices in the layer-3 S3,S4,S5,S6,S7 are listed as available by the mapping VM and then from the list S5 and S7 is selected as the best devices for  based on their available storage, distance from server etc. Based on the selection, Mirroring VM stores the data with its mirroring algorithm in the selected two devices S5 and S7 also one mirror in the server and finishes the upload process for the data of device D1 in the Device S5 and S7. The data's identity like MAC address of D1, user id of D1 is saved in the LOG file with information like MAC addresses of S5 and S7.

In other case D1 proceeds to download file, again D1's validity is checked and then the request is proceeded to the Process request VM. Then Device and Data control VM is activated to search in the LOG file to find out either there is any storing history of the requested data and then checked whether the data is available by checking availability of device S5 and S7. If S5 and S7 is available, then nearest device is paired with D1. Suppose S5 is chosen and then a pair is made between S5 and D1 as a result the requested data is downloaded directly from S5 by D1 but in case of failure to reach S5 and S7 data is provided from the server site. Now the data is in the D1 device but still it cannot be viewed by user of D1 because of its strong two-layer security. So, the encrypted data is first decrypted with RSA 2048 algorithm and then by AES. The study on the paper includes, a two-layer security on the users' data and the maximum utilization of the mobile devices shared memory that is used as a storage of the cloud network that roughly minimizes the large storage cost, moreover decreases the storage maintenance complexity at the maintenance side which increases the scalability and flexibility of the cloud network. As mobile storage substituting as server storage so that server side having comparatively lower storage than needed resulting low power consumption at the maintenance side. Moreover, mobile bandwidth is properly used for file sharing resulting high optimization of specific mobile bandwidth.

## 4. CONCLUSION

Cloud computing is now the biggest hotspot for introducing new technological approaches as it is getting more and more interest across the world at different purposes and also the cloud computing is now adopting to the newest technological approaches. Moreover, the trend of using cloud for different purposes with different arena has taken it to a whole new level where cloud based service has become a challenging among different organizations. Though, cloud computing is a key technology, it is still revolving and some more wide variations of the use of cloud are still to be declared. Beside using cloud intensely people are also dependent on smartphone, using the affinity to the cloud the study of the paper reveals the new approach that is 3-tier technology which merges the use of smartphones with cloud. Here the 3-tier technology introduces that smartphones can be operated as both client and storage for the cloud network which specifies that the unused storage of the smartphone can be used at some purpose efficiently different from the usual trend of use. And the specific bandwidth of the mobile device is used with maximum utility that reduces the bandwidth required for the server, moreover, downloading a file two mobile devices can be paired to share files between them resulting faster file sharing within the cloud which increases the flexibility and scalability of the cloud. Due to reduction of storage need at the server, power consumption and storage cost are gone under a relaxing situation at the server side. Along with these, the 3-tier technology also provides two level of security on the data for the clients to be ensured of.

## 5. FUTURE WORK

In future, we are targeting to strengthen the reliability and manageability of the shared memory of mobile devices. Moreover, finding more secured and faster approach of sharing data along with reducing the bandwidth required that would decide the cost to be reduced. In addition, a simulation work and an implementation of the proposed system would be highly prioritized.

## 6. REFERENCES

[1] E. Gorelik, "Cloud Computing Models," Massachusetts Institute of Technology, USA, 2013.

[2] K. Hashizume, D. G. Rosado, E. Fernández-Medina and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 5, p. 1, 2013.

[3] A. Holt, K. Weiss, E. Gelblum, S. Flannery, S. Devgan, A. Malik, N. Rozof, A. Wood, P. Standaert, F. Meunier, J. Lu, G. Chen, B. Lu, K. Han, V. Khare and M. Miyachi, "Cloud Computing Takes Off," MORGAN STANLEY RESEARCH Globa l, 2011.

[4] J. SRINIVAS, K. VENKATA, S. REDDY and M. QYSER, "CLOUD COMPUTING BASICS," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 5, pp. 1-3, 2012.

[5] S.-i. Kuribayashi, "Optimal Joint Multiple Resource Allocation Method for Cloud Computing Environments," International Journal of Research and Reviews in Computer Science (IJRRCS), vol. 2, no. 1, pp. 1-2, 2011.

[6] S.-i. Kuribayashi, "Reducing Total Power Consumption Method in Cloud Computing Environments," International Journal of Computer Networks & Communications (IJCNC), vol. 4, no. 2, pp. 1-2, 2012.

[7] K. Patel and M. Rathod J., "Effective Utilization of Bandwidth for Mobile Ad Hoc Network," Indian Journal of Science and Technology, vol. 9, no. 27, pp. 1-2, 2016.

[8] K. Kaur and K. Rai, "A Comparative Analysis: Grid, Cluster and Cloud Computing," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 3, pp. 1-3, 2014.

[9] Q. Hassan F., "Demystifying Cloud Computing," Cross Talk, Cross Talk, 2011.

[10] M. Amini, S. Safavi, D. M. Khavidaki and A. Abdollahzadegan, "Type Of Cloud Computing (Public And Private) That Transform The Organization More Effectively," International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 5, pp. 1-5, 2013.

[11] K. Khajehei, "Role of virtualization in cloud computing," International Journal of Advance Research in Computer

Science and Management Studies, vol. 2, no. 4, pp. 1-8, 2014.

[12] M. Liaqata, S. Ninoriyab, J. Shujaa, W. Ahmada and A. Gania, "Virtual Machine Migration Enabled Cloud Resource Management: A Challenging Task," University of Malaya, kualalampur and Jabalpur ;, 2016.

[13] D. M and K. P, "A Study On Virtualization Techniques And Challenges In Cloud Computing," :International Journal Of Science & Technology Research, vol. 3, no. 11, pp. 1-3, 2014.

[14] YunchuanSun, J. Zhang, Y. Xiong and G. Zhu, "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks, vol. 2014, 2014.

[15] K. Hashizume, D. G. Rosado, E. Fernández-Medina and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 5, pp. 1-5, 2013.

[16] U. Naik and V. Kotak, " Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing," IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), vol. 9, no. 1, pp. 1-5, 2014.

[17] M. Pitchaiah, P. Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm," International Journal of Scientific & Engineering Research, vol. 3, no. 3, pp. 1-5, 2012.

[18] "Techopedia," [Online]. [Accessed 26 july 2016]. Available: https://www.techopedia.com/definition/1006/data-synchronization.

[19] N. Malhotra and A. Chaudhary, "Implementation of Database Synchronization Technique between Client and Server," International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 3, no. 4, pp. 1-5, 2014.

[20] S. S and B. K, "Data Synchronization Using Cloud Storage," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 11, pp. 1-4, 2012.

[21] "Techopedia," [Online]. [Accessed 27 july 2016] Available:https://www.techopedia.com/definition/1006/data-synchronization.

[22] "nsk inc," [Online]. Available: http://blog.nskinc.com/IT-Services-Boston/bid/77545/When-to-Use-Mirroring-as-a-Data-Recovery-Solution. [Accessed 28 july 2016].

[23] H. Jin and K. Hwang, "Stripped mirroring RAID architecture," Journal of Systems Architecture, vol. 46, no. 543±550, pp. 1-6, 2000.

[24] "Android developers," [Online]. [Accessed 20 july 2016] Available:https://developer.android.com/guide/topics/data/data-storage.html..

[25] S. Arianfar, P. Sarolahti and J. Ott, "Reducing Server and Network Load with Shared Buffering," Aalto University, FRANCE, 2012.

[26] "WD support," [Online]. [Accessed 15 july 2016] Available:http://support.wdc.com/KnowledgeBase/answer.aspx?ID=10624..

[27] M. Singhal and A. Shukla, " Implementation of Location based Services in Android," IJCSI International Journal of Computer Science, vol. 9, no. 1, pp. 1-4, 2012.

[28] D. Vadlamudi, K. Chaitanya, T. Srikanth, B. Venu, U. Joseph and T.-h. Kim, "An Applicative Approach for Collecting and Fortifying History of Data in Cloud Environment," International Journal of Software Engineering and Its Applications, vol. 9, no. 5, pp. 1-7, 2015.