Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

Multi-dimensional security in cloud using Encryption & Authentication

Meenakshi Shrivastava[1], Mr. Ravindra Gupta[2]

[1]M. Tech. Scholar, Department of Computer Science & Engineering,
RKDF Institute of Science and Technology, Bhopal (M.P.), INDIA.

[2]Assistant Professor, Department of Computer Science & Engineering,
RKDF Institute of Science and Technology, Bhopal (M.P.), INDIA.

Abstract – In today's world where every dimension of human life is witnessing new developments almost every day, the traditional computing is also improving exponentially. One of the most revolutionary improvement is the conception of Cloud computing. Cloud computing systems are the need to time and way to go forward with technological improvements in world of IT. It has a wider variety of solutions for various IT user/developer communities. It not only offers a high degree of mobility, flexibility to its user, it provides a hassle free computing environment as well.
However as with every distributed computing platform, it is also not un-touched with a set of concerns, biggest of which is security and data privacy. In order to provide a secure cloud environment where every user has its own data privacy and integrity intact, cloud system have to be absolutely security complaint and able to overcome any kind of intrusion or malicious activity against them.
As the cloud computing is gaining maturity, there have been widespread advancements in securing cloud systems, by providing various security measures. Various organizations, researchers and authors around the world have come up with distinct ideas to secure cloud systems and have benefitted the world with their ideas.
In this paper we have provided an overview of cloud computing systems, common security issues, and their solutions and have subsequently proposed a solution for providing multi-dimensional security for cloud system, up to a certain extent the proposed work also caters to the need of cloud system availability. We have used AES and RSA as encryption techniques and CHAP authentication techniques to achieve some of the security goals.

Keywords – Cloud computing, security, encryption, authentication, service availability

I. INTRODUCTION

In Simple terms, we can define **Cloud Computing** as a way of addressing all our computing needs with the help of internet, without possessing any costly hardware, software or any other infrastructure component.
It has emerged as a key trend of current computing era, and has been envisioned to be the future of modern computing and IT infrastructure.
Cloud computing has brought a paradigm shift in the way IT organizations (big or small) used to address their IT needs. Cloud Computing can provide software, or a development platform or complete IT infrastructure as a service over the internet and can handle all the related overheads. The end users or organizations need not to worry about the software licensing, maintenance, or any scheduled software upgrade. It will be taken care by the cloud service provider. Amazon, Microsoft, Google are among the top Cloud Service providers.

To better understand the concept of Cloud computing, let's review some of the definitions provided by various Cloud research organizations.

As per the *Cloud definition provided by Cloud Security Alliance Group [3]*, Cloud computing advocates the usage of collection of services, applications, data and infrastructure which comprises of a reusable pool of computers, processors, information and storage media. These reusable components can be rapidly provisioned, implemented and decommissioned, scaled-up or down to provide an on-demand utility model of allocation and consumption of resources.

As per the cloud definition provided by U.S. National Institute of Standards and Technology, cloud computing [4] can be described by its five vital characteristics, three service model and four deployment models. Below visual model represents various aspects of cloud computing paradigm, followed by their details.

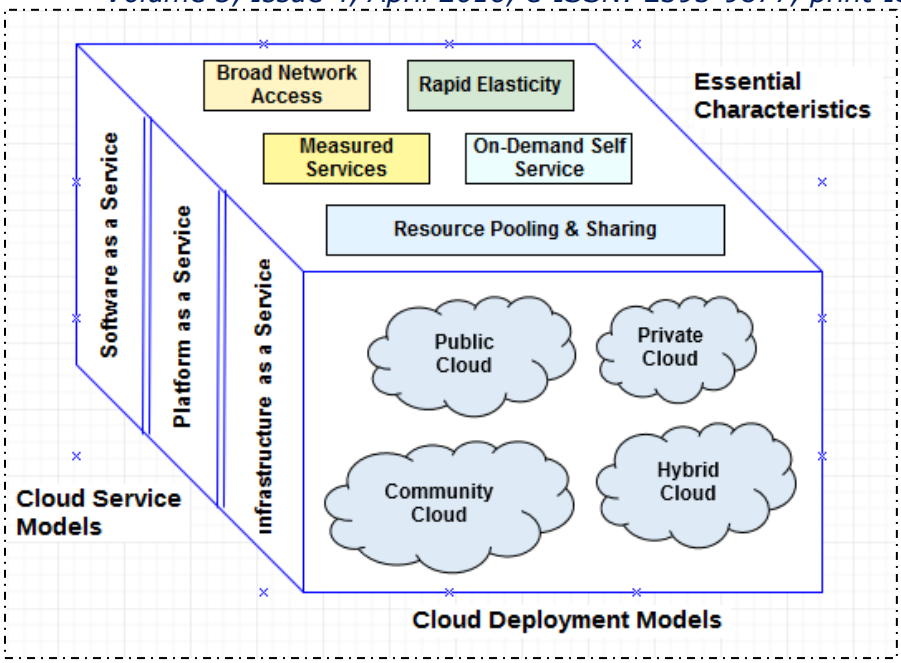

Figure 1.1 – Cloud Computing

A. Cloud characteristics:

Following inherent characteristics of cloud computing makes it a highly promising computing platform to use.

On-demand self-service–Users of cloud computing have the flexibility to easily manage the resources like processors, storage media and network resources as per their need, and more surprisingly it does not require any manual intervention of any administrator or service provider.

Broad network access – Cloud capabilities are distributed over the internet which makes it broadly available and increases its usability to any remote or local area. These services are accessed via standard mechanisms and users have the flexibility to use any thin or thick client applications (from their Desktops, laptops, PDAs, mobiles etc.) to leverage cloud service.

Resource pooling – CSP's resources are pooled to serve multiple end users using a multi-tenancy model with the ease of allocating and de-allocating the resource based on the consumers need. Due to the distributed nature of cloud services, these resource provisioning is transparent to the end users.

Measured service – Cloud enabled systems have the capability to track & optimize the use of pooled resources according to consumers' usage, and the users are charged on fair usage policy.

B. Cloud Service models:

Cloud service models are:

Software as a Service (SaaS) – This service model enables users to use software/applications running on CSP's infrastructure. Users are free from the hassles of buying, upgrading and maintaining these software's on their systems. These applications can be access via any thin or think client interfaces.

Platform as a Service (PaaS) – As part of PaaS, consumers are provided with the ability to deploy their self-developed or acquired application (written using the APIs, libraries supported by CSP) onto the hosting applications provided by their CSP. Consumers need not to manage any related resources prior to or during the life of deployment, all these things are managed by cloud provider. Consumers are only required to deploy and/or do any type of configuration setting which is required for the deployed application. PaaS service model opens a gate of opportunity to many developers, organizations (small or large) by providing the required platform at a reasonable cost.

Infrastructure as a Service (IaaS) – This service model is aimed to provide various fundamental computing resources like storage, processors, network and other related entities to the consumers to be able to leverage these virtual infrastructure components to host and manage their business applications. Though the consumers do not maintain or control the basic cloud infrastructure, however has complete control over OS, network topology and storage mechanisms.

Following table lists down cloud service models from perspective of type of user community which will mostly leverage that service.

Table 1.1 – Cloud Services

Cloud Service Type	Examples of service providers	User Community
Software as a Service [SaaS]	Google Docs, Gmail, Microsoft SkyDrive	End users
Platform as a Service [PaaS]	Microsoft Azure, Amazon EC2	Developers
Infrastructure as a Service [IaaS]	Rackspace, Amazon AWS	System Administrator

Apart from these basic service model, there are many emerging extensions which are intended to provide specific set of services e.g. *Storage as a service* **(STaaS)**, *Security as a service* **(SECaaS)**, *Data as a service* **(**DaaS**)**, *Test environment as a service* (TEaaS), *Desktop as a service* **(DaaS)**, *API as a service* **(APIaaS)**etc.

C. Cloud Deployment models:

Following are ways in which cloud environments can be deployed.

Private cloud –This type of cloud infrastructure is established to be used by a single organization which may contain a set of cloud consumers (big or small). Private cloud is usually owned and managed by the organization itself or any third party cloud provider or a combination of both (inside or outside the organization).

Public cloud – Public cloud infrastructure is established to be used by general public i.e. basically internet users. This type of cloud infrastructure is owned, managed, and operated by a commercial, academic, or government institutions, or some combination of them. It is hosted inside the premises of the cloud provider.

Community cloud –Community cloud infrastructure is established to be specifically used by a community of users from various organizations who have common concerns or job interests (e.g., mission, security requirements, policy, and compliance considerations). It may be owned and managed, and operated by one or more the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Hybrid cloud –The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

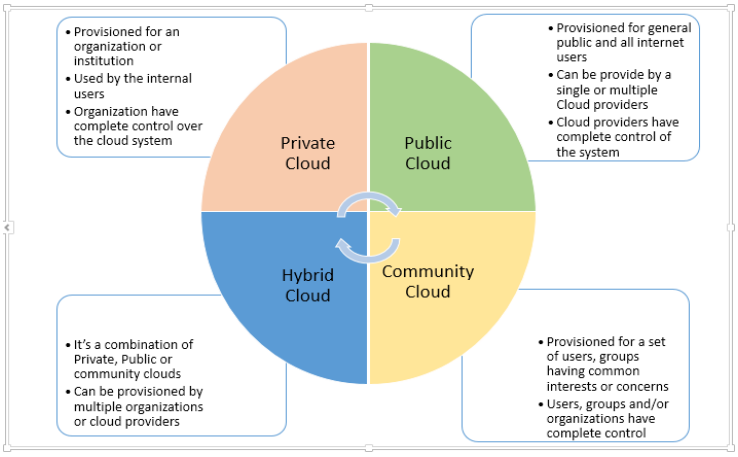

Figure 1.2 – Cloud Deployment models

As we can see Cloud computing has lot of potential to serve IT community in a much better way than the traditional computing, it can serve them with faster and omnipresent access of data, software and services, on a cost-effective pricing, and without any hassles of maintaining any type of hardware or software components.

Considering the fact that internet community is growing day by day and the data volumes are reaching beyond all the estimated limits, Cloud computing is certainly a way to go.

However one can also imagine that all these services cannot be provided effortlessly, if not the individual users then someone (i.e. Cloud providers) have to bear all the overheads to provide an effective cloud service.

And there are various factors which can lead to increased complexity in managing those overheads. One of the most common and highly discussed aspects is **Security** in Cloud systems.

In the next section we will explore more, on common cloud issues, followed by a detailed discussion on Cloud security issues, their severity and impact on cloud user community.

II. COMMON ISSUES IN CLOUD COMPUTING

Before going into the details of threatening issues for cloud computing, let's have a look on some high-profile cloud system outages in recent past, caused due to various reasons.

Amazon EC2 Cloud outage *– [8] [30] [31] In April 2011, Amazon EC2 cloud services suffered a major outage which led to a number of services like Quora, Foursquare and Reddit going offline.*

EMC's Security component attacked *– [9] In Feb, 2011, RSA, the security component of EMC suffered a major data breach in which the hacker stole the intellectual property concerning company's authentication technology. RSA admitted that the information was stolen.*

Microsoft's Azure cloud outage *– [10] In Nov 2014, Microsoft Azure based cloud services went down for nearly 40 hours. The outage knocked many online businesses offline, including several of Azure-based services such as Microsoft Office 365, Visual Studio Online, OneDrive for Business, the Windows Store and Xbox Live.*

Google's Compute Engine outage *– [11] In Feb 2015, Google's Compute Engine, suffered an outage due to network connectivity issues, affecting many enterprise consumers who use the Google cloud infrastructure.*

Sony PlayStation data attack*– [12] In April 2011, Sony PlayStation network data was compromised which exposed personal data of many users along with their payment information.*

Above mentioned are only a few incidents. And if the CSPs fail to provide a robust cloud infrastructure then it may cost millions of dollars to consumers as well as the providers.

Cloud computing paradigm is based on a service delivery and usage model, and to make it cost effective, services and/or resources are pooled as well as shared between multiple cloud users. E.g. a Cloud Service provider may have a set of data centers, where data from various users or organizations is stored, a set of virtual machine instances to rapidly allocate and de-allocate computing resources like memory & processors to meet dynamic needs of a set of users; and many more.

Due to this very nature of cloud computing it is exposed to many issues, which if not taken care properly, can hinder the smooth operation and service availability for the end users. Some of the major aspects, which should be appropriately handled in cloud computing are:

- **Cloud Service related**
  - Multi-tenancy & Co-residency
  - Identity management
  - Upgrades & patch management
  - Service level agreement
  - Service and Data availability
- **Cloud Security related**
  - Confidentiality (Secure information management)
  - Data integrity and privacy
  - Secure Data access (or Data transmission)
  - Data intrusion
  - Virtualization vulnerability

Multi-tenancy & Co-residency: [6] Multiple users and organizations use the shared resources of cloud service provider. As long as everyone is accessing their resources in an ethical manner, everything is fine, however in case someone gets access to other's confidential data intentionally or accidentally, then it opens up a whole lot of privacy risk for cloud users.

Identity management: [7] Cloud computing uses multiple methods and technologies to serve user needs, hence there is an immense requirement to identify the user and the requested service/technology uniquely, otherwise it may adversely impact the user experience.

Upgrades & patch management: CSPs own a wide variety of hardware and software components to support their cloud users. This brings an associated liability to perform time to time upgrades for various components to keep them up-to-date

and to fix any kind of known issues or security vulnerabilities. These patches/upgrades involve down-time of the system, hence it should be pre-planned in such a way that it removes any chance of outages to end users.

Service Level agreements:[7]Service level agreements (aka SLAs) are the legal terms & conditions agreed between Cloud Service Providers and cloud users to define their business obligations towards each other. It accumulates the list of agreed services offered by CSP, and the legal measures to be applied in case those are not met up to the level of satisfaction.

Service availability: In order to meet service level agreements, CSPs are required to provide measures to make their services highly available by replicating them on multiple servers and by increasing duplication of resources. This will enable CSP to provide services in an un-interrupted manner in case of a server crash or a local site failure.

Cloud security related aspects: Data Confidentiality, data integrity & privacy, secure data access etc. are the vital needs of any transactional distributed system, and due to the shared and widely distributed nature of cloud computing these becomes one of the most non-negotiable aspects of any cloud computing implementation.
Multiple users and organizations use the shared resources of cloud service provider. As long as everyone is accessing their resources in an ethical manner, everything is fine; however in case someone gets access to other's confidential data intentionally or accidentally, then it opens up a whole lot of privacy risk for cloud users.

Severity of cyber-attacks is well known to us, and when it comes to Cloud world, which is already open for a wider range of users via wider channels like notebooks, smart phones PDAs etc. [7] If a cyber-criminal can identify the weaknesses of a cloud computing infrastructure then he can do a un-imaginable hazardous to the user & provider community. Bigger CSPs like Google, Microsoft, Amazon have matured overtime and now have the capability to overcome this types of attacks, however for various emerging CSP, it is a key requirement to keep their security considerations up to the mark and provide a protected cloud service experience to end users.
Following table enlists the security requirements for various types of cloud service models:

Table 2.1 – Cloud Security requirements

Security Requirements		IaaS	PaaS	SaaS
1	Availability, Resource management, Trust, Protecting communications, Network protection and its resources, Compliance, Secure architecture, Reliability, Images management	√	√	
2	Control and administration, Continuity of operations, Risk management, Protecting virtual private cloud, Hardware security, Hardware reliability, Trusted third party, Basic configuration, change control configuration, Key management, Connection to information systems, Storage and computing	√		
3	Identifying security threats, Monitoring configuration changes, Security planning procedures and policies, Fairness, Security accreditation		√	
4	Identity and access management	√		√
5	Anonymity property	√	√	
6	Privacy, Confidentiality, Non-repudiation, Security and software engineering, Security training and security awareness, Internet and service			√

Hence we can understand the essence of Security in cloud computing and providing appropriately strong measures for various integral components; a cloud system can be safe guarded from external world, up to a good extent.

In the next sections of this paper we will discuss about some of related research work done for targeting various types of security issues in cloud computing systems. Will also provide the detailed of propose our approach to mitigate the cloud security issues.

III. RELATED WORK

Being one of the most vital aspect of Cloud computing, there has been a lot of research in this area and may advancements have been made since the conception of Cloud computing. We will review some of the solutions proposed by various authors/researchers in this direction.
Faraz Fatemi et al. [2] have proposed an approach where they have used client based encryption and sharing the encrypted key between communicating parties for a secure and confidential data sharing. They have also used an authentication

mechanism to validate user's legal identities and allow them to access the resources as per their allocated role & privileges. RSA Small-e algorithm has been used for encryption and a modified version of Diffie-Hellman algorithm to generate and share the secret key between users.

AlZain, Eric, & Ben, [5] suggested the Concept of Multi-clouds Databases (MCDB), which uses multiple clouds instead of a single cloud. In addition to this, authors have also incorporated Shamir's secret key sharing approach. It explains how the data is managed and distributed within multi clouds and is shared among different clouds inside a cloud service provider. Though having multiple clouds increases redundancy, still it's a useful technique to provide a reliable cloud system.

M. Sugumaran & BalaMurugan, [1] proposed an architecture based on block based symmetric cryptography algorithm, to provide data encryption & decryption using a shares private key between the user and Cloud system. This architecture can help in providing better data security however if it is mixed with a strong authentication mechanism, it can be made more effective. The solution provided by ***Hamid, Alireza & Elham*** [14], is based on trusted computing architecture, using trusted components at various levels like cloud nodes, clusters, user VMs, & UTEs etc. This solution is specifically aimed to provide better security to IaaS systems.

As per another study [15] carried out by ***Nahid and Zohreh***, to provide a secure cloud system with adequate SLA adherence, we must define key security requirements for the system implementations and they should be mapped to systematic parameters of the system design. This analysis will help CSPs and cloud consumers to define & select the appropriate system behaviors in terms of Cloud system security. In order to strengthen cloud system security ***Feng Zhao, Chao Li,Chun*** have proposed a solution [16] using Homomorphic encryption technique which tries to solve the encryption problem. It has four methods-key generation algorithm, Encryption algorithm, decryption algorithm and additional evaluation algorithm.

Another solution suggested by ***S. Srinivasan & K. Raja*** for securing a cloud system [17], is to use strong encryption and authentication mechanism with a mix of RAID [Redundant array of independent disks] technology, it also provides the facility to safeguard the data even in case of a disk failure or crash. Apart from these standard solution, there are some biometric measures have also been proposed by ***Akshay Pawle & Vrushsen Pawar*** [29], where the Face recognition technology is used for authentication purposes. Though it's an advanced technique, however it may restrict the users from authenticating in case of absence or malfunctioning of camera device.

There are many more such mechanisms which have been proposed by various authors/researchers to fight the security issues in cloud. In the next section we will describe our proposed work.

IV. PROPOSEDWORK

As part of the proposed work we will try to mitigate some of the security issues in cloud computing. Following visual representation highlights the area of our work.

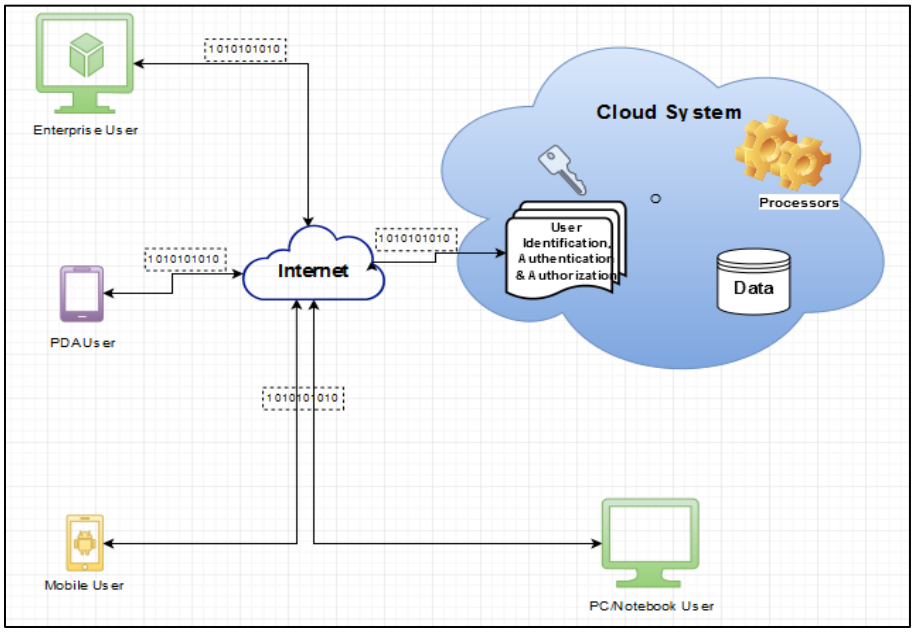

Figure 4.1 – Cloud Security aspects

As indicated in above visual, the proposed work is targeted to secure following design aspects of secure Cloud computing environment:

1) **Data residing inside the cloud storage**
   Cloud resident data can be protected by providing appropriate data encryption mechanism. Securing this aspect will result in achieving Data privacy and integrity.
2) **Data transmitted over the network**
   Transmitting encrypted data over the network (instead of plan text) will result in achieving this aspect as well.
3) **User identification and Authentication**
   By providing an appropriate authentication mechanism, user identity & authenticity problems can be targeted.
4) **User authorization control**
   This design aspect can be achieved by defining confidentiality flags and access control measures for data components, and allowing only intended users to access the data.

As part of the proposed solution, following techniques have been identified for achieving the above mentioned design aspects:

Standard Encryption techniques for Data Security

A combination of following standard encryption techniques have been used to provide multi-level data security:

1) **Advanced Encryption Standard [aka AES]**
   The AES cipher [18][19] was chosen because it seems to be the best performing algorithm in a variety of different systems of all bit sizes tested, and it is also extraordinarily secure. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a ***symmetric-key algorithm***, meaning the same key is used for both encrypting and decrypting the data.
2) **RSA encryption**
   RSA is a public-key cryptography, also referred as **asymmetric cryptography** [21][22]. It uses two different but mathematically linked keys, one public and another private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

These 2 algorithms are considered to be the most secure ways to provide data encryption, and are highly used in complex systems for providing data security.

Challenge Handshake Protocol for Authentication

Extensible Authentication Protocol, or EAP, is standard an authentication framework frequently used in wireless networks and point-to-point connections. In the proposed work one of its flavor called CHAP (Challenge Hand-shake protocol [23][24]) is being used as the authentication mechanism.

This authentication protocol is based on a standard TCP three-way hand-shake mechanism between requester and authenticator (i.e. server). On successful authentication requester is given access to the resource he has asked for. Benefit of CHAP protocol is that the user password is never sent over the network during authentication process and hence it one of the most preferred PPP authentication protocol.

Following data flow diagram shows the logical sequence of our proposed solution:

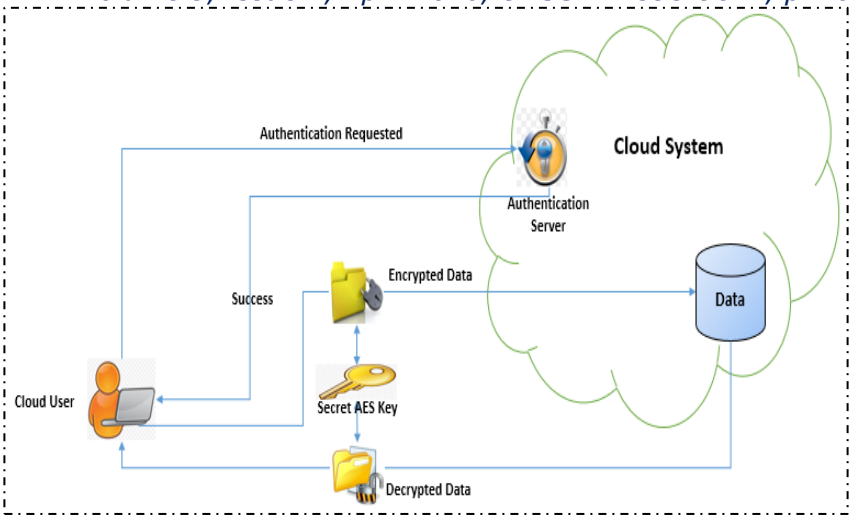

Figure4.2 – Secure Cloud architecture

We can describe the sequence of events in case a user wants to add/update/retrieve cloud data using the proposed solution:

a) User opens the client application or user interface to login to Cloud system
b) User requests for authentication from server or tried to access any file
c) Authentication server at CSP end, sends a challenge message to the user
d) User then generates hash value of the message (using predefined hash function), and then sends back the generated message to the authentication server
e) Server then calculates the hash of the same challenge text (using the same hash function) and check if the hashed value of challenge message sent by user is same as generated at server's end
f) If both of the hashed values matches, then CHAP server sends success notification to the user
g) Upon successful authentication, user tries to upload a file to server,
   a. At the time of upload, user has an option to set the Security Level of the document being uploaded it can be any of the following –*Unclassified (or Non-confidential), Confidential & Top Secret*.
   b. Based on the selected security level the encryption technique will be used to encrypt the file and then the encrypted data is sent to the server and gets uploaded.

> *Concept of assigning security level on the documents to be uploaded has been introduced to get the optimized performance from the system. Due to this categorization, only documents which are really confidential will be uploaded in encrypted form, unclassified (non-confidential) documents can be uploaded as it is (without encryption). This will provide a kind of filter to encrypt the confidential documents only.*

h) Similarly if user tries to retrieve any file/data from server (which is in encrypted form), then it is transferred to users end in encrypted form and then gets decrypted. The decryption is done on the basis of security category of the document.

Following are the detailed overview of the technologies used:

CHAP Authentication Process:

CHAP authentication [23] scheme is mostly used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP server periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial communication link, and may happen again at any time afterwards. The verification is based on a shared secret (could be user's password).

1. After the completion of the link establishment phase, when the requester or initiator performs an action like login or document access, then the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function (using a predefined hashing mechanism) on the challenge and the secret combined.
3. The authenticator checks the response against its own calculation of the expected hash value (using the same hashing technique). If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.Overall process [25] is depicted below:

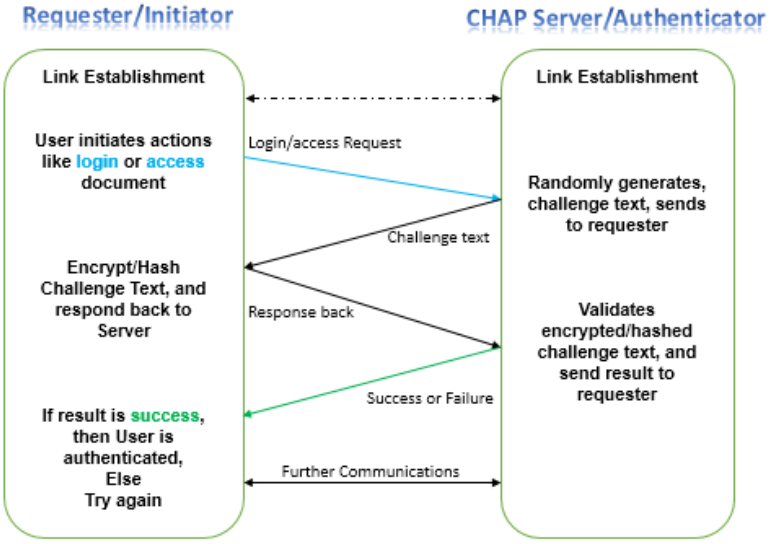

Figure4.3 – CHAP Authentication process flow

In the proposed work, we have also tried to improve the availability of the authentication mechanism by increasing the number of CHAP servers, i.e. instead of having only 1 CHAP server, we will have **N** instances of CHAP servers and during authentication process, response from the user will sent to all **N** instances of CHAP servers, and if the user authenticates successfully with **(N/2+1)** servers (called success threshold limit), then he will be given access to the requested resource. This process will have following two benefits:

1) **Enhanced Security** –
   Instead if authenticating to 1 CHAP server, now user will be authenticated against N/2+1 server, it will definitely increase the security and will reduce the chances of password hack by any malicious attacker.
2) **Increased Availability**–
   If we have only one CHAP server and that goes down due to some issue, then all the users will be impacted and no one will be able to access cloud data due to authentication failure. However if we have N CHAP servers and out of which if any one or two goes down, then also user can get through the authentication from the remaining set of servers. Success threshold limit (i.e. **N/2+1**), can be reconfigured or changed by the system administrators according to the availability of servers and complexity of the system.

V. CONCLUSION & FUTURE WORK

In the coming future as the computing era keep growing rapidly, we will certainly see many challenges, improvements, and enhancement in cloud computing; however the security and service availability aspects are always going to be the key for the success of Cloud environments. There have been many such proposed solutions to fight with Security issues, having improvements over one or the other. Similarity we need to keep improving the technologies and find new ways of securing the systems, and make the user experience better and better.

From the perspective of the current work, as of now we have proposed mechanisms to secure the cloud data, effective user authentication/authorization, and securing data in transit up to a certain extent.

As a future improvement work of the solution proposed in this paper we can further make it more secure using the SSL (Secured Socket Layer) or TLS (Transport Layer Security) features, which will certainly secure the data in transit as well. Another aspect for improvement will be to work on achieving better performance of the overall system.

REFERENCES

[1] M. Sugumaran, BalaMurugan. B, D. Kamalraj – "An Architecture for Data Security in Cloud Computing" 2014, IEEE.
[2] FarazFatemi, Iman Ghavam, Shirin Dabbaghi, SoroushMobedi – "A Client-Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers", Dec-2013, IEEE
[3] Cloud Security Alliance – "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Dec-2009.

[4] "The NIST Definition of Cloud Computing", Sep 2011.National Institute of Standards and Technology, USA, 2011.
[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom —"Cloud Computing Security: From Single to Multi-Clouds" IEEE Transactions on cloud computing, 9(4), IEEE 2012.
[6] Daniel W.K. TSE – "Challenges on Privacy and Reliability in Cloud Computing Security", 2014, IEEE.
[7] Rameshwari Malik &Pramod Kumar - "Cloud Computing Security Improvement using Diffie Hellman and AES", May-2015.
[8] Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee – "From System-centric to Data-centric Logging – Accountability, Trust & Security in Cloud Computing" IEEE.
[9] Z. Zorz – "RSA hacked, SecurID users possiblyaffected", 2011 – [http://www.netsecurity.org/secworld.php?id= 10763]
[10] Azure outage disrupts cloud services across the globe – [http://searchcloudcomputing.techtarget.com/news/2240235048/Azure-outage-disrupts-cloud-services-across-the-globe]
[11] http://www.ibtimes.co.uk/google-compute-engine-down-cloud-service-suffers-major-worldwide-outage-1488606
[12] "User data stolen in Sony PlayStation Network hack attack", 2011 - [http://www.theregister.co.uk/2011/04/26/sony_playstation_network_security_breach].
[13] Prashant Rewagad & Yogita Pawar - "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013, IEEE
[14] Hamid Banirostam, Alireza Hedayati, Ahmad KhademZadeh, Elham Shamsinezhad –"A Trust Based Approach for Increasing Security in Cloud Computing", 2013, IEEE.
[15] Nahid Bohlol, Zohreh Safari–"Systematic Parameters vs. SLAs for Security in Cloud Computing", 2015, IEEE
[16] Feng Zhao, Chao Li,Chun Feng Liu – "A cloud computing security solution based on fully Homomorphic encryption," [pp. 485-488],2014, IEEE.
[17] S. Srinivasan, K. Raja – "Security Challenges in Cloud Computing", 2014.
[18] Advanced Encryption Standard – [NIST]http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[19] Advanced Encryption Standard – [https://en.wikipedia.org/wiki/Advanced_Encryption_Standard]
[20] Rijndael key schedule – [https://en.wikipedia.org/wiki/Rijndael_key_schedule]
[21]RSA algorithm (Rivest-Shamir-Adleman) – [http://searchsecurity.techtarget.com/definition/RSA]
[22] RSA Cryptosystems – [https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29]
[23] Challenge-Handshake Authentication Protocol– [https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol]
[24] RFC for Challenge-Handshake Authentication Protocol – [https://www.ietf.org/rfc/rfc1994.txt]
[25]PPP Authentication Protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) – [http://www.tcpipguide.com/free/t_PPPAuthenticationProtocolsPasswordAuthenticationPr-3.htm]
[26] Abdul Muttalib Khan, Dr. Shish Ahmad, Mohd. Haroon –"A Comparative Study of Trends in Security in Cloud Computing", 2015, IEEEs
[27] Amlan Jyoti Choudhury, Pardeep Kumar,MangalSain ,Hyotaek Lim, Hoon Jae-Lee – "A Strong User Authentication Framework for Cloud Computing". 2011, IEEE.
[28] Sumathi M, Sharvani G.S, Dinesha H A – "Implementation of Multifactor Authentication System for Accessing Cloud Service", 2013.
[29] Akshay A.Pawle, Vrushsen P. Pawar – "Face Recognition System (FRS) on Cloud Computing for User Authentication", 2013.
[30] http://www.crn.com/news/cloud/229402004/amazon-ec2-goes-dark-in-morning-cloud-outage.htm
[31] http://www.infoworld.com/article/2624084/iaas/the-failure-behind-the-amazon-outage-isn-t-just-amazon-s.html