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

Cloud Computing - An Overview of Architectures, Security Threats and Their Solutions

Ashwini Phadke[1], Devashree Jadhav[2]

[1]SUID: 575445713

[2]SUID: 244997526

Abstract: ***World is connected by the large web of internet and everyday tremendous amount of data is generated across different transactions. Management, storage and processing of this huge amount of data over the 'internet cloud' has become the most frequently used buzzword in the technology space. As the data size increased so did the necessity to transfer it over a network which led to the development of 'Cloud Computing '. The cloud has taken the load away from local servers and hard drives to help tech companies make the data accessible from anywhere across the globe. It can, therefore, be viewed as an extensive data sharing platform made available to ensure that no data is lost due to space deficiency. This technology is extensively used in many areas of engineering to enhance the data storage ability of the system. The applications of cloud range from emails, photos, data backup, databases for various applications etc. However exposing critical data to a third party vendor for storage makes it vulnerable and insecure. In this paper, we discuss various threats associated with cloud computing systems and possible solutions for the same. We address the issues pertaining to data confidentiality, data integrity and availability. We review the existing cloud infrastructures, services and deployment models. This paper also investigates various optimized architectures for implementing energy efficient cloud systems.***

Keywords: Cloud Computing, Internet, Security Threats, Architectures

1. Introduction

1.1 Why Cloud Computing?

Variation in the given networks and increasing speed of service makes data transfer a vital part of the entire facility [1]. We create a huge amount of data due to the continuous use of social media in corporate as well as social environment. Traditional media is put at competition by digital media almost every day [1]. Newer aspects of digital media lead to the requirement of more and more amount of storage capacity for all kinds of data [1]. As amount of data increases, the storage of this huge amount of data starts becoming a bigger concern. Hard drives provide a promising performance, but they have space constraints. Due to space constraints many hard drives would be needed and that would increase the cost of hardware in a system exponentially. Besides hard drives always involve the risk of getting affected by virus. The best solution to this problem is 'Cloud Computing'. Clouding Computing avoids the overhead of external data storage and provides the user a space on the internet which is not bound by a limit. Thus the user will be able to store data on a Cloud without getting bothered about the space limitation.

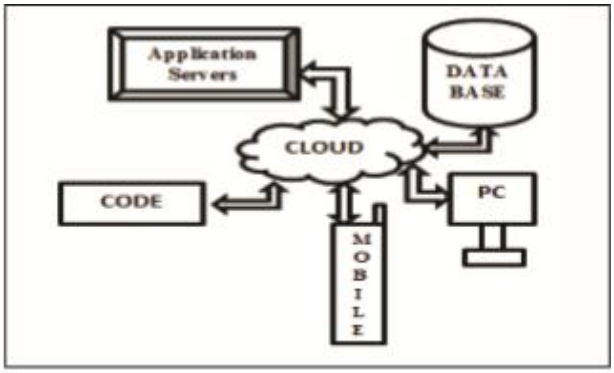


Figure 1: Data flow in a cloud computing architecture

1.2 What is Cloud Computing?

The term cloud computing can be broken into two basic concepts - the word 'Cloud' which refers to Internet and 'Computing' which means the computer technology [1]. Thus, the most straightforward definition of the term would be making use of the internet to store all types of data which would otherwise occupy huge amount of space in local devices. Cloud computing makes computing much more centralised by decreasing dependency on local computers. It is a highly efficient platform as it enhances innovation, development and business agility which reduces costing. It allows users to access large amount of data, information and various other computing resources. Thus it can be imagined as a model which provides access to a shared pool of services as and when required [1]. The management of this data is easy and manual or third party interruption is minimum. The idea of cloud computing can be summarised as a third party with large-scale storage servers and data centres used to provide infrastructures, software development and distribution platforms with low costs in the computing technology.

1.3 Services provided by Cloud Computing [1]

The cloud services can be classified into following:

Software as a service
Software as a service or SaaS is any cloud service which provides the user the facility of accessing the software application over the internet. 'The cloud' here plays the role of hosting the application when a huge amount of users are accessing it. Utilising SaaS is just like renting a software rather than buying it. Unlike traditional applications that require the user to download the package and install it on individual machines, the SaaS types of applications are used online and the respective files are saved on the cloud thus

sparing the user the overhead of occupying the space in local machines.

Platform as a service

Development of any kind of an application requires a specific platform. This platform can also be the choice of the developer based on experience. The PaaS services are hosted in the cloud and users all over the world can access these platforms for development of applications. Thus, by using PaaS the user is assured of working on the required environment without investing a lot in creating that on their own. Thus, the cost of investing in physical infrastructure is negligible. This brings teams working on the same project across the world virtually closer. Flexibility and adaptability are the other few benefits.

Infrastructure as a service

IaaS or Infrastructure as a service provides the user with all the hardware and network required for execution of any given software. This helps in avoiding the expense of buying a server or datacenter. IaaS gives the user the authority to decide the size of the resources in order to make sure that the user pays only for what they use. Thus any resources required by the user can be found on the cloud which can be rented for the duration it is needed. This provision helps user in reducing the pain of the process of purchasing, installing, configuring and maintaining any software, middleware or application. High performance computing, Storage and backup, Big Data Analysis, Web apps etc , use the facilities offered by IaaS.

Cloud computing has made every service available to the user online and transformed localised work environment into a globalised one. It has found its application in almost all areas due to the flexibility of its structure. Every organisation uses the concept in one way or other. Different implementations can be categorised in different types.

2. Types of Cloud Computing [1]

1. Public Cloud

This type of service is made available by the service provider to the people or a collection of organisations for access. This service can be used by everyone and those using this service share identical infrastructure pool with the same security settings, selected configurations and a few variances [7]. Examples of such a service are Google, Amazon and Microsoft. These organisations offer their own infrastructure to be shared by all the other users wishing to make use of them.

2. Private Cloud

If an organisation uses a cloud infrastructure for operation designed only for the organisation then such an arrangement is called Private Cloud [7]. In this setup, the cloud storage is not available to the public and anyone outside the organisation cannot access it. It is a protected infrastructure and any confidential data, pictures or media which is shared on this cloud remain within the network of the organisation [1]. As compared to other organisations, the security threats are lesser in this type of a cloud infrastructure.

3. Community Cloud

If a group of organisations is required to share specific data within themselves a community cloud infrastructure is formed [7]. The security of information becomes a concern when multiple organisations are involved in sharing of important information. However, this is the simplest technique of sharing required data in least time possible within specific organisations even if the size is huge.

4. Hybrid Cloud

A combination of two types of clouds is termed as Hybrid Cloud [1]. This infrastructure is often used to improve the usability of a given cloud by using specific characteristics of different types of clouds and combining them into one. Due to the involvement of different types of infrastructures, the risk of security issues is increased.

Effects of Transition to Cloud Computing:

As Online processing and networking has increased the necessity of Cloud computing to manage these resources online has increased double fold. Few scenarios where Cloud Computing is put to use to enhance the process are:

Test and Development

Configuring an environment online and using the same for development is a very common approach due to the services offered by Cloud computing. Thus, test and development environment can be created as required according to an individual or organisation's specifications.

Big Data Analysis

Big Data refers to the exponentially growing structured and unstructured data. Cloud Computing helps in the analysis of the data and derive the patterns of any search made by the consumer in a way that would be helpful for the organisation. Extracting behavioural patterns from huge amount of data to understand the nature of customer and use this analysis for designing better sales policies. This also helps in understanding the requirements of the consumer better.

File storage

Different organisation have different preferences when data storage is concerned. Due to cloud storage, the organisation has the flexibility in storing data on or off the premises. Any type of data can be stored on cloud storage with availability, scalability and speed of retrieval ensured.

Disaster recovery

Cloud storage involves the benefit of easy disaster recovery compared to specific applications which are more expensive than the suggested technique. Disaster recovery is much faster when cloud computing is involved in the process as data availability is ensured.

However, as utility and availability of a system increases the possibility of threats also increases. Even Cloud Computing cannot be an exception to this possibility. Thus, with all the advantages of the technology, the security aspect stands as a challenge to it which needs to be addressed along with the benefits of the implementation. Various ways are being used to make Cloud Computing more secure for usage, few of

which can be seen as a part of our study in the later sections of this paper.

In the next section we will be discussing about a proposed architecture using Cloud Computing for managing the continuously incoming flow of huge amount of data.

3. Related Work and Analysis

Architecture involving Cloud Computing
In order to study the usability of cloud computing we will discuss an architecture which is experimented and tested for its usefulness in classifying data acquired from satellites.

Cloud Computing architecture for remote sensing data [4]
A huge amount of data is generated each day due to the advances in modern earth observation technologies. Many sensing satellites launched in orbit are acquiring a huge quantity of information about spatial resolution, revisit frequency, and number of spectral bands [4]. Due to the improvement in the technology the resolution of images captured is also improved which thereby increases the size of the data received. In this study we explain a new architecture using cloud computing which will classify the data received from the remote sensors in such a way that it forms three layers each of which targets different types of users. This architecture supports network communication, fault tolerance and distributed execution in such a way that the user is not aware of it. The layers of this architecture are independent of each other and different users can work on different layers without the knowledge of the architecture being worked upon at an individual level by multiple users.

The name of the proposed architecture is *InterCloud Data Mining Architecture*. This design consists of the following three layers [4]:

- **Project definition layer**

This layer is specifically designed for end user interaction. People working at this layer need not have programming knowledge. The information provided by the end user at this layer is used in the classification layer. The interface lying between project definition layer and classification layer is the translation process. The translation process as the name suggests is required for translating the instructions coded in the classification layer.

- **Classification layer**

This layer applies the classification algorithm on the acquired data for further processing. Only a person with appropriate programming knowledge can work on this layer of the architecture. Working on this layer would mean designing classification algorithms in such a way that the person in project definition layer is able to select these algorithms.

- **Distribution layer**

The distributed programming models are used by the users who are experts in the specific distributed model. The distributed layer is required for the execution of each of the distributed process. The translation process between classification layer and distribution layer translates the programming code in classification layer to distributed programming.

4. Execution framework of proposed architecture:

Each layer requires a specific execution plan and framework for ensuring maximised results. Keeping the requirements and expected outcome in mind each layer uses different implementation strategies.

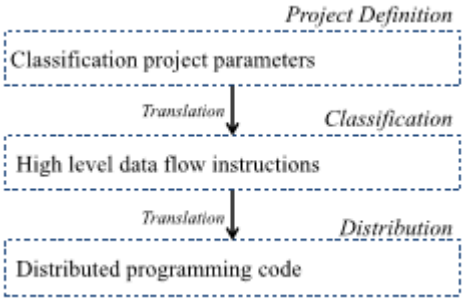


Figure 2: InterCloud Data Mining Architecture [4]

Starting from the lower most layer, the distribution layer is implemented using MapReduce *[4]* which is a most commonly preferred model used for datasets which are huge in size. The classification layer is the layer that has to manage the incoming data and perform appropriate processing but also interfaces with distribution layer. These requirements indicate that a framework which would permit the use of user defined functions should be used. Thus, the Pig Framework is used for the classification layer *[4]*. The language Pig Latin provided by this framework makes it easy for the programmers to interact with MapReduce.

Experimental Design and Results
The following tests were performed for experimental purposes in order to verify the correctness of the approach :

1) Amazon Web Services for verification of the cloud environment.
2) Hyperspectral images - Pavia and Indian Pines as Datasets for testing.
3) Random Forest and SVM (Support vector Machines) algorithm for verifying the classification approach.

5. Results Obtained

The experiments performed on the classification approach found an accuracy of 78.26 % for Pavia dataset and 64.41 for Indian Pines dataset [4]. The speed ups obtained for Pavia datasets for 2Gb size were 2.56, 3.57, 4.27, and 4.23 for 5, 10, 20, and 50 nodes respectively [4]. This implies that as more cluster nodes were added the speed up obtained increased accordingly. The results obtained from the experiments validate the fact that the proposed architecture is scalable. The increase in speed up with increase in the number of nodes verifies the accomplishment of an almost accurate distributed network [4]. As larger datasets can exploit the distributed the distributed resources better and higher level of parallelism can be achieved. This architecture has therefore proved the usefulness of cloud computing in any given system. It can be noted from the given

observations that cloud computing forms the basis of the architecture and how any data mining application can make use of it with a few variations in the given model [4].

After studying the given paper, it can be observed that data management and data handling is an important process in Cloud Computing. Processing of huge amount of data requires various approaches and few of which are used in the architecture that we studied. We studied various algorithms and their processing and their experimental outcome. Also, the proposed algorithm, uses a high level of abstraction to ensure parallelism in the execution. The necessity of abstraction is any given implementation is a take away from the proposed solution. It uses classification, distribution and user interface in different layers to make the architecture as easy to use as possible. The user, developer, distribution expert can perform their own work without disturbing the working of the other. This technique maybe in its initial phase, but the idea gives rise to myriad possibilities of solution to problems other than data coming from remote sensing.

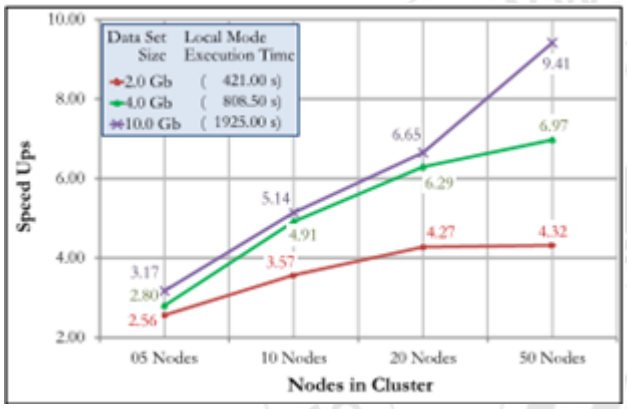


Figure 3: Pavia Datasets and speed up

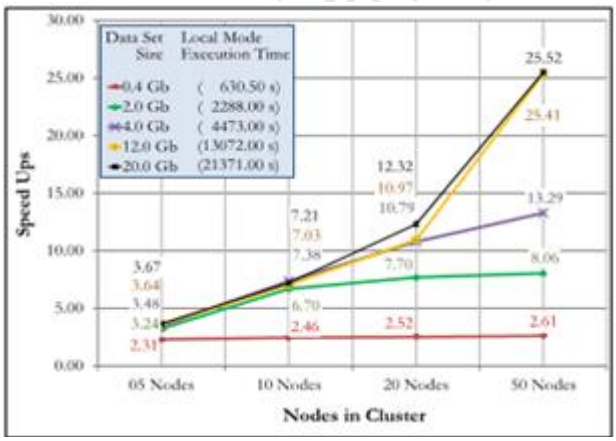


Figure 4: Indian Pines datasets and speed up [4]

As the huge amount of this data is being processed and the entire process is done online, the system is susceptible to a few threats and removing the risk of these threats from the system is an important aspect of the given architecture. In the following section we will be discussing the various threats to any system involving Cloud Computing

6. Security Threats

Ironically the biggest advantage of the cloud which is the ability to store large amounts of data makes it most vulnerable to hacking and security breach attempts. Moreover the cloud market thrives on multi tenant approach which means that the cloud services are rented out to third party vendors which makes it all the more susceptible to hackers. It is this security concern that is keeping the current IT departments from venturing into the cloud space.

The types of attackers in cloud computing are internal attackers or external attackers. Internal attackers are classifies as employees within the organization who have some classified user access to information. They can attack the availability and integrity if the data stored in cloud. An external attacker has no access to any of the company's data. The attacker exploits the shortcomings of the company's security policies and executes attacks.

In order to develop a strategy against such breach in security protocols certain basic security principles are defines. These principles are discussed in the upcoming paragraphs.

1) Confidentiality
Since cloud services are mostly given to third party vendors it is all the more important to have strict authorization polices to access the sensitive data. Confidentiality could be achieved by data encryption.[2].Also data leakage through either human or hardware errors directly affects confidentiality. User identification through passwords, biometric verification and security tokens is necessary.

2) Accountability
Accountability refers to accuracy, consistency and responsibility for the data. It eliminates possibility of any intruder hacking in the data. Data is safe due to both cryptographic and physical measures taken by the vendors.[2] This guarantees minimum loss in event of any hacking in the system. Since cloud hosts user data of many users, data integrity is of prime concern.

3) Availability
Availability refers to access to data, software and hardware on demand. [2] There can be loss of data due to natural disasters, communication and network errors and bottlenecks In such times 'backup data' would prove helpful. Such threats can potentially result into ' denial of service' which can adversely affect the system.

4) Trust
Customers trust their highly confidential data with the cloud service vendors . So trust plays a very important role in these services. It is the responsibility of the service provider to adhere to the norms of confidentiality, integrity and availability. The principles discussed above form the basis of data security in cloud computing .Cloud computing includes virtually shared resources, services and utility based computing [7]. These properties makes it susceptible to many security threats. Security threats in interfaces of APIs, technology sharing issues due to malicious elements, loss or leakage of data or risking the confidentiality of the

user's data are some of the primary security issues in cloud. These threats are discussed below.

a)Privacy Issue
Sometimes there are instances where the consumers do not directly have access to the data on cloud. In such cases there is a probability that the vendors may misuse the data. The data can be sold for junk advertisements or for third party vendor's benefit when the customer's opinion is not considered. [2]

b) Multi-tenacy and it's threats
Single software is shared among various users. But, weak security arrangements can lead to resource sharing among unauthorized subscribers leading to malpractices.

c) Data disposal
Having a secure backup of data is extremely important in cloud computing applications. Natural disasters or any manmade error could lead to loss of data.

d) Phishing
Phishing messages attack on social behavior aspects of the users and are often disguised in form of emails, messages etc.
Whenever the user clicks on the link the malware gets automatically installed on the system and there is high chance of theft of passwords, credit card details and other confidential information of the user.[2]

e) Issues in data location
Users must be kept in the loop about the location of the data it's whereabouts . A user trusts the vendor by keeping a lot of personal, sensitive or confidential data with the cloud. This helps the user in developing the trust factor with the company. Users can also decide upon the choice of location where the data is to be stored according to the bylaws mentioned in the contract. The capacity of data protection in a certain region may be affected by the location transparency and laws implemented in that particular region.[7]

f) Legal Issues
The third party vendor must honor the terms mentioned in the contract between the clients and the company. The clarity in legal issues ensures that there are no conflicts in the future. Lack of well defined standards makes it difficult to bring cloud services under law. It will be difficult for users to transfer data from private cloud to public cloud in absence of open standards.

g) Portability and Mobile Computing issues
The features introduced with cloud portability could introduce various levels of API based security threats. Processing large volume of data is a problem created with mobile computing which further risks the vulnerability of data. This has pushed researchers to develop new technology , ' mobile cloud' to deal with these applications.

h) Data stealing
Data stealing mainly affects cloud integrity. The security models in cloud depend on the various types of service models like Saas, PaaS and IaaS. [5] The two states where data is most susceptible to intrusion is when data is at rest or in transit. Data at rest refers to the data in cloud or any data accessible by the Web. Data in transit refers to the data moving in and out of the cloud. Data at rest could be protected by using private cloud. Data in transit is at higher risk of hacking since it is being communicated over the network [5].The best strategy to protect the data in transit is to use encryption over the communication channel.

7. Cloud Computing Attacks

With many technology companies adopting the cloud computing technologies to store the data, care must be taken to protect the data against the hackers. The major types of attacks which the hackers may attempt are discussed further.

1) Denial of Service Attack (DoS)
[2] Users are more susceptible to DoS attacks as many users are involved in the usage of cloud services and resources. With the increasing workload the service tries to provide more power to users in form of virtual machines, more service instances to cope with additional workload. The attacker utilizes this to send messages in bulk to the victim to verify the requests which returns invalid addresses when accepted. When the victim verifies the request, the server is paused before closing the connection. During the time the connection is closed, additional messages are sent by the intruder which makes the server busy again. This makes the resources of the cloud inaccessible to the victim.[2]

2) Wrapping attack
The wrapping attack is carried out by attacking the login procedure initiated by the user, This attack utilizes xml signature wrapping technique to duplicate user id and login password so that the SOAP messages transferred between user and server are affected.

3) Man in middle cryptographic attack
This attack is caused when the attacker positions himself in middle of the communication network between server and user. The attacker can intercept the data and modify the communications. This type of attack can be prevented by a secure authentication process to check the identity of every user of the service. Also the data sent over the channel should be encrypted over the network.[2]

4) Malware injection attack
In malware injection attacks, the attacker mimics the services provided by the cloud. When the user agrees to all the terms and conditions presented the attacker executes it's malicious software and uses the access to either steal or modify data for nefarious motives. These attacks can be prevented by installing hypervisor at t each end of the system. A hypervisor checks the integrity of all the services from the File Allocation Table of the user's machine.

5) Authentication attack
In this type of attack the authentication of existing users is either interrupted or terminated. This can be avoided by data encryption. Also the passwords should contain combination of alphanumeric data and special characters to make it difficult to guess.

6) Side channel Attack
Side channel attack occurs commonly in IaaS, as it provides a huge collection of virtual machines to the user. This attack takes place in two stages, In the first step the malicious software is placed in users machine and in the second stage the information and documents are extracted. Virtual firewall and random encryption or decryption techniques are applied to solve this attack.

8. Cloud Security Classification

The functionalities provided by various layers in the cloud computing sphere can be classified into four prominent layers namely user layer, virtualization layer, service provider layer and data center layer. Each layer has associated functionalities to it which are discussed below.

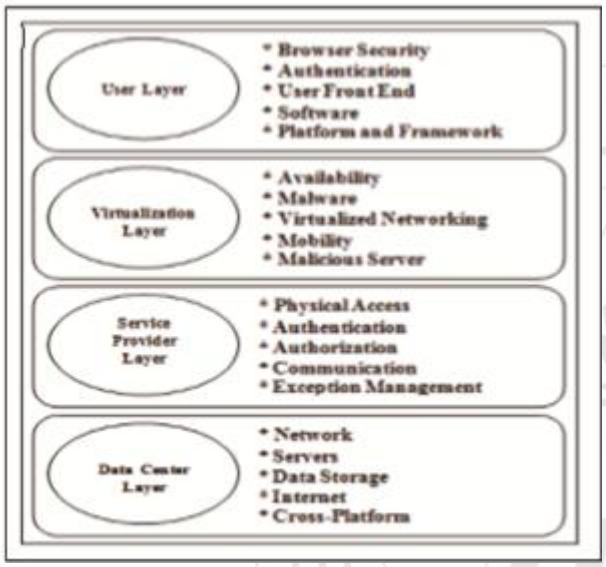


Figure 5: Mapping of cloud layer and security Characteristics [6]

1) User Layer
[6]This layer involves browser security, authentication , user front end software and software , platform and framework layer.
The browser security layer deals with the network data protection while browsing on the web. It secures the system from pop up advertisements, identity theft or data procurement tools etc.

The authentication layer verifies the identity of the user by either verifying their username and password or by validating via digital signature or other identification means. User front end refers to the application window that the client sees at his machine. It is designed for various web browsers. Various softwares are developed to help with the scalability of the cloud computing environment. This layer refers to all the cloud service providers who work on reducing the barriers in cloud services.

2) Virtualization Layer
The fundamentals of cloud computing technology are dealt in this layer. It processes requests for additional virtual machines on the existing hardware. The availability aspect of cloud computing is used to include various service levels. The businesses are rapidly adopting to virtual systems and technology to avoid malware attacks. Virtualized networking is a method of spitting the resources into various chambers with each designated server. Mobilization has increased the demand of the technology in every aspect. Malicious server is a very serious threat, The state of the client is remotely altered without any valid permissions by attackers.[6]

3) Service provider layer
This layer is concerned with the authentication, authorization ,physical accessibility and communication dealings with various services[6]Physical access to the system by the intruders has to be prevented by implementing various methods like narrowing the access to particular assets etc. Authentication mechanism allows the usage of one cloud service by other, it helps in maintaining data confidentiality. Authorization is required for security and reliability of the system. Communication strategies and type of communication required is also decided in this layer. The system designed should be bug free and not crash under load cases. This requires excellent planning of exception management.

4) Data Center Layer
This layer includes all the platform and network requirements needed by the user while utilizing services of the cloud. The network has to be secured to protect users from DoS attacks and network breaches. Server selection is a important aspect of this layer since it fulfills the hardware and software demands of the virtual and physical environment. Data storage facilities should be cost effective and secure. Internet security is essential to be taken into consideration to protect the channel against data theft and fraud. Cross platform refers to cross network connections and coupling facility of the network.[6] As the scope of the service increases the administration security is moved across various platforms which becomes challenging to provide security.

In the next section we will be studying an architecture proposed to ensure that the data stored on cloud is protected from any possibility of threats.

9. Secure data transference Architecture

The basic requirement for designing the architecture is the understanding about cryptography. The concept of creating secret codes so as to maintain the integrity of the original message is termed as 'Cryptography' [8]. This technique is often used to protect sensitive data from attacks. The process of cryptography can be summarised in the following image.

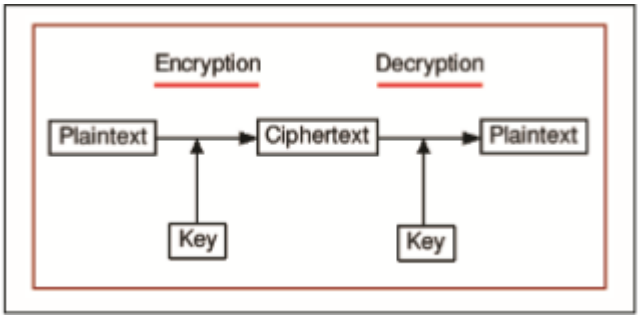


Figure 6: Cryptography [8]

The process of cryptography consists of 2 parts:

Encryption:
The sender uses an algorithm to convert the message in plaintext to cipher text using a secret key. Plaintext is written in normal language which can be read by anyone. Cipher text is encrypted text which cannot be deciphered without knowing the algorithm involved in encoding it.

Decryption:
The receiver on receiving the message decodes the encrypted message using the secret key so as the read the message sent by the sender.

The proposed architecture uses the 'cryptography' as a basic idea while implementing a security mechanism for data on cloud. There are three steps involved in the execution of the architecture

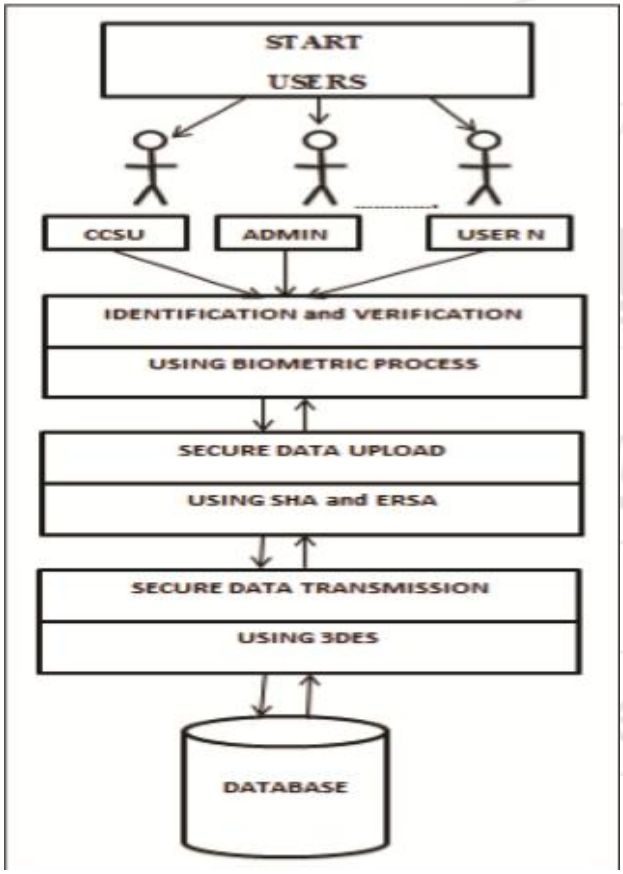


Figure 7: Secure Data transference Architecture [8].

1) User Identification and Verification
In this step the user is verified against the various entries in the database of different users so as to make sure that the said user is authorised to enter into the system. The user could be any person having access to the system and need not know about the details of the verification process. The process of identification can be done using various approaches. In this architecture, the biometric identification technique is used.

2) Secure Data Uploading
This part implies that the data uploaded should be uploaded in a secure way. This is done using the ERSA algorithm which is considered to be more secure than the traditional and more popular RSA algorithm.

3) Secure Data Transmission
This step ensures that the data travels safely and reaches the appropriate endpoint with minimum invasion by imposters. This is executed by using 3DES algorithm which has been proven to be better than the regular DES algorithm when number of attacks is considered.

Algorithms used [8]:

1. RSA Algorithm
The most popular encryption and decryption algorithm currently in use is RSA algorithm. This provides maximum protection from third party invasion. Most importantly it develops a completely secure path for data transmission.

Part 1: Key generation
- Select 2 large prime numbers suppose p1 and p2
- Multiply these numbers and save the result in 'res'.
- Multiply the p1-1 and p2-2 and save the result in 'res2'
- Select 'num' such that 1<num<res2
- The public key is (num,res1)
- Calculate m such that m = num^(-1)mod res2. m is the public key.

Part 2: Encryption and Decryption

- When the encryption and decryption is performed, the sender 'S' would send the message in encrypted form using public key for the specific receiver 'R'.
- On the receiving the receiver will decrypt the message using its private key.

2. SHA
The SHA is a family of algorithms for secure encryption of data which was created by NIST (National Institutes of Standards and Technology). These algorithms provide better online security and were created as cyber invasion and threats increased.

3. 3DES algorithm
Data Encryption Standard is used for designing a key for encryption. The 3DES is just an extension of DES where it is used 3 times. The process is as follows [8] :
- Encrypt with key K1
- Decrypt with key K2
- Encrypt with key K3

While decryption,
- Decrypt with key K3
- Encrypt with key K2
- Decrypt with key K1.

After studying these algorithms, the actual idea of the architecture can be formulated in the following manner.

10. Results

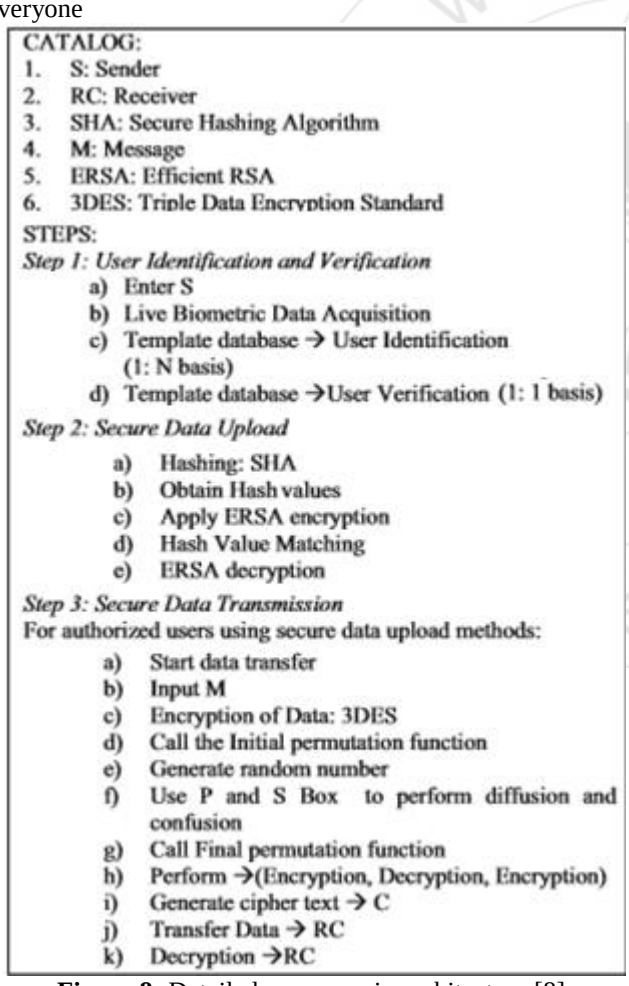
As Cloud Computing is the upcoming revolution in the field of IT, it is a necessity to make it secure to improve and

increase reliability. The proposed algorithm is the best approach to obtain a highly secure Cloud Computing environment.

From this paper we have studied the following algorithms :

- 3DES Algorithm
- SHA Algorithm
- RSA algorithm

The requirement of security in the system increases exponentially when the number of users, consumers, enterprise involved increases. Given the popularity of Cloud Computing, its safety for use has always been in question due to the involvement of 'internet' in the process. Traditionally data used to be stored in hard disks and people were comfortable with the arrangement. They found passwords to their storage as the best way of protecting their details. However, when the world went online, multiple issues started revealing themselves which needed to be curbed. Thus, the initially comfortable people now found it unusual to store all their important information online. The fact that the data is not stored in a physical device, made everyone


CATALOG:
1. S: Sender
2. RC: Receiver
3. SHA: Secure Hashing Algorithm
4. M: Message
5. ERSA: Efficient RSA
6. 3DES: Triple Data Encryption Standard

STEPS:

Step 1: User Identification and Verification

a) Enter S
b) Live Biometric Data Acquisition
c) Template database → User Identification (1: N basis)
d) Template database →User Verification (1: 1 basis)

Step 2: Secure Data Upload

a) Hashing: SHA
b) Obtain Hash values
c) Apply ERSA encryption
d) Hash Value Matching
e) ERSA decryption

Step 3: Secure Data Transmission

For authorized users using secure data upload methods:

a) Start data transfer
b) Input M
c) Encryption of Data: 3DES
d) Call the Initial permutation function
e) Generate random number
f) Use P and S Box to perform diffusion and confusion
g) Call Final permutation function
h) Perform →(Encryption, Decryption, Encryption)
i) Generate cipher text → C
j) Transfer Data → RC
k) Decryption →RC

Figure 8: Detailed processes in architecture [8]

question the reliability of the architecture. To ensure the people about the security, the developers had to come up with more and better solutions. This paper is one such attempt. From this paper we studied, the various algorithms used in data encryption. We also studied how to uses these algorithms in an efficient way to build a secure cloud architecture.

11. Future Scope

The security threats as discussed in the paper can be either of data type or network type. It is seen that prevention of attack is can be best achieved by intrusion detection system. IdS is used to critically inspect the network packets by applying various pattern identification techniques to identify both external and internal attacker. It notifies the system in presence of any impending threat to the system. The two detection schemes used in this system are anomaly detection and misuses detection. The success of IDs lies in its placement in the server. It can be positioned in the server cloud or in a separate cloud server . There were experiments carried to check the performance of the system under attack when the IDS was placed in various different server positions. It is observed that IDS successfully detects any attack either from outside or inside when it is placed separate from the server cloud. This position does not increase the CPU computing loads as compared to the scheme where IDS is places within the server cloud. The only disadvantage of this scheme is that a separate IDS server is needed. This scheme can be applied to detect both internal and external threats,

12. Conclusion

In this paper we have studied and analyzed the requirement of cloud computing in the current scenario. We have understood the necessity of this architecture in data management and processing by studying the architecture using cloud computing . We studied the various security threats in the cloud computing domain and discussed the various possible attacks which can affect the cloud system. The possible solution to these attacks and the intrusion detection schemes were reviewed. We emphasized the need of security against various threats in the sphere of cloud computing. We also studied how these threats can be tackled using a security architecture with cryptographic algorithms which ensured the integrity of data transmission in a cloud environment.

References

[1] Omar Ali, Jeffery Soar and Jian Ming, “Improved Media Management Through Cloud Computing Technology”, *Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design*
[2] Rajat Soni, Smrutee Ambalkar and Dr Pratosh Bansal, "Security and Privacy in Cloud Computing" , *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*
[3] Aryachandra A A, Fazmah Arif Y and Novian Anggis S "Intrusion Detection System (IDS) Server Placement Analysis in Cloud Computing", *2016 Fourth International Conference on Information and Communication Technologies (ICoICT)*
[4] Victor Andres Ayma Quirita, Gilson Alexandre Ostwald Pedro da Costa, Patrick Nigri Happ, Raul

Queiroz Feitosa, Rodrigo da Silva Ferreira, D´ario Augusto Borges Oliveira, and Antonio Plaza, "New Cloud Computing Architecture for the Classification of Remote Sensing Data", 2016, *IEEE journal of selected topics in applied earth observations and remote sensing*.

[5] Ahmed Albugmi, Madini O. Alassafi, Robert Walters and Gary Wills "Data Security in Cloud Computing ", *Fifth International Conference on Future Generation Communication Technologies (FGCT 2016)*

[6] Manju Khari, Sana Gupta and Manoj Kumar , "Security Outlook for Cloud Computing: A Proposed Architectural- Based Security Classification for Cloud Computing",*2016 InternationalConference on Computing for Sustainable Global Development(INDIACom)*

[7] Komal Gandhi and Dr. Parul Gandhi, "Cloud Computing Security Issues : An Analysis", *2016 InternationalConference on Computing for Sustainable Global Development(INDIACom)*

[8] Manju Khari, Manoj Kumar, Vaishali ," Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithm", *2016 InternationalConference on Computing for Sustainable Global Development (INDIACom)*

APPENDIX