International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Imperative Requirements for Data Security in Cloud Computing

Sambaiah. G
Asst.Professor, CSE Department,
Guru Nanak Institutions Technical Campus
Hyderabad, India.

E. Kiran Kumar
Asst.Professor, CSE Department,
Guru Nanak Institutions Technical Campus
Hyderabad, India.

***Abstract*—Cloud Computing is a popular buzzword currently in the market, the essential concerns for both Cloud providers and consumers are Confidentiality, Integrity, Availability, Authenticity, and Privacy . Security in Cloud computing is a crucial important and critical aspect, and involves numerous issues and problem associated to it. Cloud service provider and the cloud service consumer must and should make sure that the cloud is stay protected from all the external threats and risks so that the customer does not get any problem such as loss of data or data theft. There is also an instance where a malicious user can entered in to the cloud by acting like a legitimate user, in consequence infecting the entire cloud and that effects many customers who are sharing the affected cloud. In this we will discuss how to administer security for the data from the unauthorized users and accommodating integrity to the users.**

Keywords—Cloud,Cloud Computing, Data Integrity, Confidentiality, AES, Steganography.

I. INTRODUCTION

Cloud computing is an illustration for widely useful and on-demand network access to a shared pool of customize computing resources that can be quickly provisioned and released with simple management effort. In simple terms, Cloud Computing is an association of a technology and platform that provides hosting resources and storage service on the Internet. The primary goal of the cloud computing is to attire scalable and inexpensive on-demand computing infrastructures with excellent quality of service levels. A great number of companies developing and offering cloud computing services and products but have not legitimately considered the implications of storing, processing and accessing data in a shared and virtual environment. In reality, many developers of cloud-based applications work hard to provide security. In other cases, developers severely cannot provide real security with currently cheapened technological capabilities. Cloud computing is giving out of resources on a larger scale which is economical and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as google, amazon, IBM, rackspace, zoho, salesforce, Microsoft. It also shares needful software‘s and on-demand tools for different IT Industries. The advantages of Cloud computing are uncountable. The very most important one is that the customers need not to buy the resource from a third party vendor, rather than they can use the resource and pay for it as a service , Therefore helping the customer to save the time and money. Cloud is not only for Multinational or large scale companies but it is also being used by Small and medium enterprises.

The architecture of the Cloud Computing includes multiple cloud components collaborating with each other about the various data they are holding and providing services on too, that being so helping the user to get to the needed data on a faster transfer rate. When it comes to cloud it is more concentrated on the front-end and the back end. Here the front end is the User who provides the data, whereas the back-end is the number of data storage devices and server which makes the Cloud. There are three types of cloud based on the way of their usage. They’re public cloud, private cloud and hybrid cloud. The private cloud is maintained by a single company and public clouds are widespread on a larger scale however, private cloud provides better control and more flexible over public cloud. Hybrid cloud is a synthesized model of combination of Private cloud and Public Cloud which is used by most of the industries. The advantages of cloud computing may be very desirable but nothing is perfect. Cloud encountered many issues, in this paper we are talking about the security especially on Data theft, Data loss and Privacy, the parameters those influence on the security of the cloud and obstacles faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues.

A. Parameters affecting cloud security

There are a great number of security issues for cloud computing as it consists of many technologies including operating systems, networks, databases, resource scheduling, load balancing, virtualization, transaction management, concurrency control and memory management.

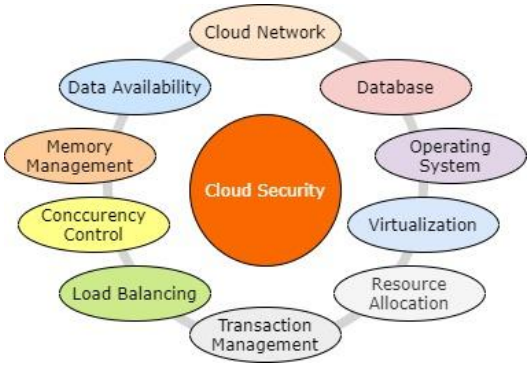

Fig.1. *Parameters affecting cloud security*

B. Security Issues faced by Cloud computing

In addition to the increasing popularity of the Could Computing environments, the security issues introduced

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

through customizing of this technology are also increasing. Regardless Cloud Computing offers lot of benefits, it is vulnerable to attacks and these attackers are always trying to find faults or weak points in the network to attack the cloud computing environment. The conventional security mechanisms which are used are reviewed because of these cloud computing spreads. Ability to control, visualize and inspect the network links and ports is needed to enhance security. Hence there is a need to support in understanding the challenges, loopholes and attacks associated with cloud computing, and by keeping all in mind come-up with a platform and infrastructure which is less vulnerable to attacks.

There are a great number of security issues for cloud computing as it consists of many technologies including operating systems, networks, databases, resource scheduling, load balancing, virtualization, transaction management, concurrency control and memory management.

1.Data Issues

2.Privacy issues

3.Infected Application

4.Security issues

1) Data Issues- Sensitive data in a cloud computing environment evolves major issues with aspect of security in a cloud based system. First of all, whenever a data is on a cloud, anyone from anywhere at anytime can access data from the cloud by taking into consideration data may be common, private and sensitive data in a cloud. However, many cloud computing service consumer and provider accesses and modify data. Hence there is a need of certain data integrity method in cloud computing. Secondly, data theft is a one of serious issue in a cloud computing environment. Many cloud service provider do not have their own server alternatively they procure server from other service providers due to it is cost affective and versatile for operation and cloud provider. So there is a more probability of data can be theft from the external server. Thirdly, Data loss is a universal problem in cloud computing. If the cloud computing service provider terminated his services due to some financial or due to any legal problem then there will be a chance to loss of data for the user. Furthermore, data can be damage or lost or corrupted due to natural disaster, miss happening and fire. As a result of above condition, users may not be able to access the data. Finally, data location is one another issues what requires focus in a cloud computing environment. Physical location of data storage is vital important and crucial. It should be unambiguous to user and customer. Vendor does not leak the physical locations where all the data‘s are stored.

Another important privacy challenge in cloud computing is the basic characteristics of information source; where data and information come from different sources. This requires that data be protected and organized carefully. Furthermore, information should be accessible only to licensed users and not for all users of the cloud, and avoiding from alteration at any time [11]. Privacy of users should be facilitated while data is collecting, stored and transmitted. The earlier conditions mentioned are essential to the providing privacy in the cloud and they are: Guarantee of availability, integrity and confidentiality [12]. The way of data collection from multiple sources as we said above is considered as one of the biggest challenge that face cloud computing in view of it reveals sensitive information about the consumers,. Such movement of accumulated data can lead to breach the privacy of users’ data [13]. On this basis, customers should be aware of the access policies to their data and utilities (called access control mechanisms). Moreover, users’ credentials must be defined early in the process and even edited by users when its mandatory. Conclusively, identification and authentication among users and the network is important and must be resolved [14]. After all these issues, we remains need to have a prescribed policy that defines the relations between the three important entities in the cloud: consumers, utilities and third parties involved [12]. To reach an adequate level of cloud privacy, many issues need to be identified like: incomplete user control over his data, information exposure in movement across the cloud, unauthorized duplication of sensitive data, uncontrolled data spread, and dynamic provision legal challenges [15].

2) *Privacy Issues*- Realizing the challenges facing cloud computing, we must manage the cloud using legal constraints, which are very essential because privacy intrusions on the Web are so common,. These difficulties may result from liberalization of Internet issues (government’s responsibility), to maintain an acceptable privacy levels and motivate users to use cloud computing. Additionally, researchers are worried that could computing environment will threaten online advertising industry and other related sectors. One more important issue to be considered is when we are treating with cloud computing environment in the social direction to control the domain. There are two options that can be used: directing the issues of market and self-regulation or by managing it by the government. Within the privacy perspective there are differences between a self-regulation and the government regulation. Some users says that government shouldn't give the legal instructions in privacy, demanding to avoid the standard view of the superior role of government. Other users said that self-regulation is difficult as no available equipment in the Cloud computing industry to select educated, logical , and significant policies to implement. Researchers concluded that regulations don’t help out in enforcing an significant Internet practices when we consider privacy point of view, where market impacts might be more effective than regulations in providing privacy [9]. Moreover, users thoughtful that rules don’t have major impact on privacy only but also could have a negative impact on providing privacy like reducing availability of information and improving transaction costs. Therefore many of cloud computing researchers concluded that making the administrative process more systematic and to solve the data privacy issues, cloud regulators need to discriminate personal and non-personal data [10]. The authors suggested a complaints department to handle this

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

issue, where users send their complaints on a service provider, then complaints can be forwarded anonymously to the public authorities, and finally, do its operations in a public cloud. Public departments need not to find any additional data about the sender.

3) Infected Application-It would be mandatory for the Cloud computing, service provider be the owner of complete access to the server with all permission for the intention of monitoring and maintenance of server. Therefore this will stop any malicious user from uploading any insecure application onto the cloud which will seriously affect the customer and cloud computing service.

The cloud computing service provider should have to make sure that the customer personal information is well secured from another providers, user and customer. Because of most of the servers are external, the cloud service provider must ensure that who is being access the data and who is maintaining the server such a way it enables the provider to protect the customer‘s personal information.

4) *Security issues*- Cloud computing security has to be done in two levels. First one is on provider level and another one is on user level. Cloud computing service provider should ensure that the server is well protected from all the external attacks it may come across. Although the cloud computing service provider has maintaining a well security layer for the customer and user, the user must make sure that there should not be any tampering or loss of data or stealing of data for other users who are using the same cloud due to its operation. A cloud is well defined only when there is an extremely good security measures provided by the service provider to the user.

II. EXISTING WORK

The limitations and difficulties toward the rapid growth of cloud computing are data security and privacy issues. No organizations accept to transfer their data or information to the cloud until and unless the assurance is built between the cloud service providers and consumers. This paper surveyed various techniques about cloud data security and privacy, keying on the data storage and use in the cloud, for data protection in the cloud computing environments to build a hope between cloud service providers and consumers. For building that trust worthiness Integrity, Confidentiality, Availability should be provided.

So in this paper we are providing

Confidentiality: In Cloud Computing, several sensitive data information shared in the cloud, it demands the cloud data storage and shared service to be trustworthy for secure, reliable and efficient distribution of data content to probably large number of authorized users on behalf of data service providers. To resolve this issue, one way is to presume the cloud servers and let them apply access control mechanisms such as Role-Based Access Control (RBAC) [20]. As access control mechanisms like RBAC are reliable techniques with capable of handling fine-grained access control in large scale systems, the aim of data access control can be achieved effectively . The main difficulty with this solution exists in two folds: Firstly, in access control mechanisms like RBAC, the server must have full access to all the user data when accomplishing their tasks. It requires that cloud users should completely trust the cloud servers, and hence the Cloud Service Provider (or even their employees). Secondly, due to the occurrence of serious outsider attacks at different layer of the cloud system stack, e.g., cross VM attacks and bluepilling attacks or subverting hypervisor attacks, it requires that cloud servers access control tasks should be well secured at every layer. In reality, this could be a challenging task in view of the fact that cloud servers exist in such an open Internet. An another possible way to provide secure data access service is based on cryptographic mechanisms. In this type of solutions, the cloud user encrypts data before storing them in the cloud and maintain the secret key to himself. Data access is accepted by distributing the data decryption key to the legitimate users. In this wise, we achieve “end-to-end” security without reveling data content to cloud servers. Apart from the first method, this type of solutions do not desire the cloud users to fully trust the cloud server. At the same time, cloud server can even take full charge of the control of the outsourced encrypted data because they are unable to compromise the data confidentiality. What makes the problem difficult is the implementation of fine-grained authorization policies, the support of policy get updated in variable scenarios, and the system scalability, when maintaining low 18 level complexity of key management and data encryption. Consequently, the main research work towards this direction is to at a time achieve fine-grainedness, scalability and data confidentiality of data access control in cloud computing, without involving significant computation headache on the cloud user.

Confidentiality is the way of protecting personal information,it means hiding a user’s information between other users, and not exposing to others including co-users, friends, family, etc.. For example providing confidentiality by authenticating the user by generating a Random number OTP (One time password) , checking the legality of the users.

Integrity: Integrity is the process of being honest and viewing a constant and uncompromising support to strong ethical and moral values and principles . We can provide Integrity by capable of storing the encrypted data in cloud service provider’s Drop box such as the normal multimedia, and used steganography for hiding most sensitive data like passwords.

In cloud computing, Data integrity service should be provided in the punctual manner. The reason is that in practical applications it is commonly too late for cloud users to find out data exploitation when they are actually retrieving the data. This is especially true for long term storage of large amount of data, in which many blocks of data could be rarely accessed in a long period of time. When some chunk of data is found corrupted while taking back, it could not be possible to recover as information which we want to recover may have been disappeared during the long interval. For example, disk

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

recovery is generally not possible when the physical location of the data in memory disk has been overwritten by new data. Further, it is since data corruption, the most probably it is that the data would not be recovered. To implement punctual data integrity service to cloud users to avoid the risk of data corruption or lost, it is mandatory to supply them with powerful data integrity check mechanism, it must be able to process the large volume of data without getting too much computation or communication overhead.

Availability:

The unlimited resources offered by cloud computing would greatly enhance cloud users' ability in data storage and dealing with. For example, by creating multiple copies of data in the cloud, cloud users can have robust data storage which may not be available locally because of restricted to limited resources. To provide better quality data services to their own customers, data owners (data users) may reproduce the data on geographically distributed cloud servers and permit their customers to access data easily via local cloud servers. Cloud users can also reduce the effort for data maintenance by authorizing it to the cloud service provider who may have more ability in doing this. In brief, with cloud computing cloud users could able to operate very effectively and large scale data services with 15 fewest local deployment and maintenance effort. Throughout this process, one of the main thing from the data user might be data availability in the following sense: First, cloud computing must ensure that user data stored in the cloud can be available immediately whenever accessed it. In particular, it is very essential to assure the availability of data services and consequently business continuity of cloud users in case of temporarily or permanently cloud interruption. In the real life, the unfortunate events are more likely to happen due to the interruption of cloud such as communication interruption, power interruption, bankrupt of the cloud service provider, etc. Second, cloud computing must provide the agreed service quality to cloud users. For example, for redundant data storage the cloud user may need to store k physical replicas in the cloud. In this case, it is failed to guarantee that the required replicas are really available in the cloud. This is also happen when cloud users need to store data replicas on topographically distributed cloud servers for providing quality of service. In these cases, the data may available but the quality of service would be reduced when the cloud service provider is not follow the agreement. We should pay the special attention in case of long term data storage. In such a scenario, it is very crucial to assure that the cloud service provider does not violate the service agreement by moving less frequently accessed data from on-site storage to secondary storage without knowing to any one. Such type of breakage in the service agreement is ordinarily easy to be ignored but will potentially reduces the service quality for cloud users. In many application prospects, the quality of data service such as data accessing speed is very important to the business success. It is important to give assurance for data availability at every aspect of data services as discussed. In order to providing faithful and trustworthy cloud data service to cloud users, appropriate action(s) should be taken place for cloud users to efficiently test the availability of their data. For the first case, the regular practice is to let cloud users store more number of replicas of data on distributed cloud servers or in different clouds. For assurance of data availability, we just need to have a way for cloud users to ensure that the multiple replicas of data do exist on allotted clouds or cloud servers, which is one of the objective for the second case. For the second case, the very important issue is how to create the trust between the cloud service provider and cloud users in the sense that the particular share of data does exist on granted storage sites/regions. Service level agreements (SLAs) can be employed to achieve this objective as is used in many application systems. For ensuring appropriate use of SLAs and preventing possible disputes, adequate verification mechanism(s) should be taken place. Along this direction, the research paper has proposed several cryptographic mechanisms to gives a strong security protection on data availability in cloud computing. Among these end results are two most hopeful ones: "provable data possession (PDP)" [17] and "proof of retrievability (PoR)" [18, 19]. In all these works and great efforts are compelled to design solutions that fulfil various requirements: high efficiency, effective verification, unlimited use of queries and retrievability of data, etc.When a system is repeatedly non-functioning, information availability is laid down and that impacts users. And also, if data is easily available, information security is get affected. Another factor that effecting availability is time. If a system cannot able to deliver information effectively, then availability is made effected.

Cloud user can use these services at anywhere and whenever needed by connecting to internet.

III. PRESENT WORK

Cloud computing and data storage solutions provide users and organizations with several capabilities to store and process their data in third-party data servers. Different organizations use the Cloud in a many of different service models and deployment models . Basically the service models are SaaS, PaaS, and IaaS and Deployment models are Private, Public, Hybrid, and Community.There are a huge number of security issues associated with cloud computing but these issues classified into two broad categories: security issues encountered by cloud providers such as organizations providing software- as-a-service , platform- as-a-service, or infrastructure-as-a-service via the cloud and security issues faced by their customers like companies or organizations who host applications or store data on the cloud. The responsibility comes in both ways, however the provider must make sure that their infrastructure is keep protected and that their client's data and applications are secure while the user should take measures to strengthen their application and use strong passwords and authentication measures.

In Cloud Computing environment it may involves three major potential threats namely

1.Security-for the stored data

2.Privacy-from the Unauthorized Users

3.Trust-Data Integrity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

A. Data Security and Privacy

Data is stored in the cloud shared by multiple users. The data location is transportable, that is, it can move from one location to another location dynamically. The users of cloud data may not be aware of the data location or regarding the access log of their data. The secret information is stored away from its owner, which increases its lack of protection. This results serious issues about the security of user‘s data.

B. Identity and Access Management

Data in the cloud is stored at multiple locations and the location of cloud data is mobile. The cloud accountant user may or may not be knowing of his data‘s location. The cloud being multi-way network in nature, the cloud user may have to login into cloud using different user credentials for different providers. This creates a potential threat to data as any individual may imitates as like the original owner in case the credentials are lost/intercepted outside the system. A cloud necessarily to have a strong and robust identity and access management system in place so as to attract more transfers to the cloud.

C. Proposed System

In this paper, we will analyse different security techniques and challenges for keep protect stored data and providing privacy protection in the cloud computing environment. The approaches used in the cloud computing describes data security aspects including confidentiality, data integrity and availability.

1) *Data Integrity:* Data integrity is one of the most critical function in any information database system. Basically, data integrity means safeguarding data from unauthorized deletion, fabrication or modification. Managing entity‘s entrance and allowance to specific enterprise resources make sure that valuable data and services are misappropriated abused or stolen.

Authorization is used to manage the access of data. It is the process by which a system provides what level of access to a particular authenticated user and it should have to keep protect the resources which are controlled by the system.

Data integrity in the cloud system environment means maintaining information integrity. The data should not be stolen or leak or modified by unauthorized users. Data integrity is the basis to implement cloud computing service such as SaaS, PaaS, and IaaS. In addition to this data storage of large-scaled data, cloud computing environment generally provides data processing service.

2) *Data Confidentiality:* Data confidentiality is another important feature for cloud users to store their private or confidential data in the cloud. Authentication and access control methodologies are used to ensure data confidentiality.

The data confidentiality, authentication, and access control issues in cloud computing could be addressed by enhancing the cloud reliability and responsibility. Due to the fact that the users do not trust the cloud providers and cloud storage service providers are virtually not possible to eliminate potential insider threat, it is more dangerous for users to store their perceptive data in cloud storage directly. Simple encryption will be encountered with the key management problem and cannot assistance complex requirements such as parallel modification, query and fine-grained authorization.

IV. DESCRIPTION

We are focusing more on Authentication and Data Integrity. Data Integrity means protecting data from unauthorized data modification and deletion, . Authentication means providing access only to the eligible users.

Random number generator is a one of method to authorize the users. The Random Number will be send to the mobile number which was given at the time of their Registration. When the user enters the code (Random Number) then they will allowed us to access the data, add data and to modify the data. If the User enters wrong code then the user is an Unauthorized User then he/she cannot access the data. Cloud service consumers can store any multimedia data in the cloud Service such facility is known as drop box. The very perceptive data of the users can be stored in more secured way using steganography. This multimedia data would be encrypted and then uploaded to cloud service provider. While downloading the multimedia from drop box then it will be decrypted and exposed to the users.

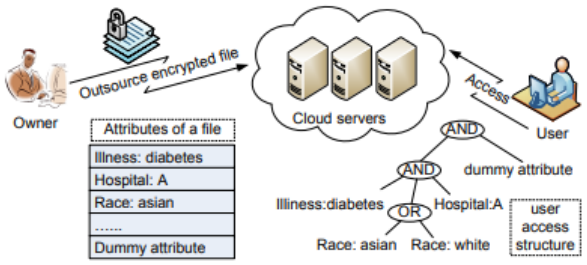

Fig.2. *Attribute-based encryption*

In this way the cloud data will be very much secured and not disclosed to other users

A) Existing Technologies

Steganography is a process of hiding the data at inside an image. Generally there are lot of steganography techniques used commonly to cover an information and this technique is also known as image steganography technique and is a

1) *LSB –2 Steganography-* In LSB-2 Steganography the data hiding process is slightly different. It modify the 2nd bit from right (2nd Least Significant Bit) for all pixels[5].

The algorithm is as follows:

Step1: Convert the data from decimal to binary equivalent.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Step 2: Read the data in the form of image.

Step 3: Convert the image data in to binary.

Step 4: Divide the byte to be hidden into bits.

Step 5: Take first 8 byte of actual data from the Cover Image.

Step 6: Exchange the least significant bit by one bit of the data to be hidden.

Step 7: Repeat the step 6 for all pixels.

E.g.:-

First byte of actual information from the taken Cover Image:

1 0 0 1 1 1 0 0

Here the first bit of the data to be hidden: 1

Replace the least significant bit

1	0	0	1	1	1	0	0
1	0	0	1	1	1	1	0

B) Key Enabling Techniques of Cloud Computing

In spite of the fact that the term Cloud Computing is new, the fundamental concept of cloud computing is actually not new. In the 1960s, John McCarthy said that "computation may some day be organized as a public utility" in his speaking at the MIT Centennial. Douglas Parkhill in his 1966 book [16] comprehensively explored the characteristics of the "Computer Utility" which are very comparative to those characteristics of the modern-day cloud computing. Anyway, cloud computing, or the "Computer Utility", had not changed in to a reality until the late 2000s when various critical enabling techniques at different levels of the system stack all made available: Service Oriented Architecture (SOA), broadband networks, Software as a Service (SaaS), the Web technology, virtualization, distributed computing and the plentiful of software and operating systems. The broadband networks act as a fundamental element in cloud computing for effectively combining physically distributed resources into a logically integrated service and results in smooth remote access for cloud users. The Web technologies provide platform independent techniques for users to visualize and configure remote services. SOA makes it possible to develop applications based on a loosely-coupled suite of services among multiple separate users/servers over the Internet. SaaS prescribes application level of services in a pay-as-you-go model. Virtualization summarizes logical devices from physical devices and permits co-residence of multiple logically hidden instances as like operation systems on a single physical machine. Distributed computing and Virtualization together make computing as utility and flexibility of computing resources possible. The attainability of high-performance and storage hardware devices and cost effective computing is fundamental to the ideal goal of unlimited resource.

V. AES ALGORITHM

In this segment, we propose a structure which involves securing of files through file encryption. The file existing on the device will be encrypted using AES algorithm. The user can download any of the uploaded encrypted files and read it on the system as well.

Flowchart:

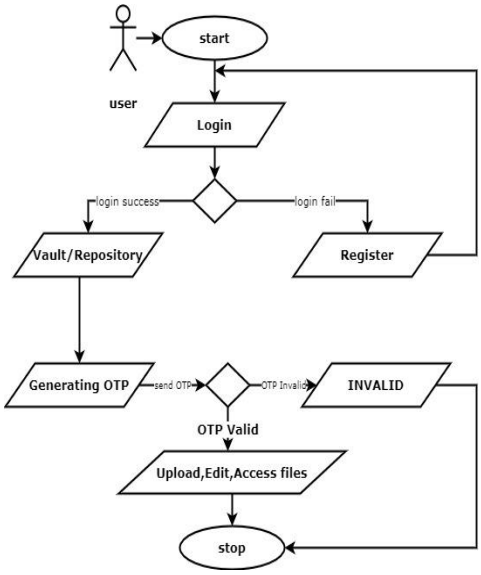

Fig.3. *flow chart: Key enabling technique*

A) AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher announced by the National Institute of Standards and Technology (NIST). The principles defined by NIST for selecting AES fall into three areas:

1.Security
2.Cost
3.Implementation.

AES is a non-Feistel cipher that encrypts and decrypts a 128 bits data blocks. It uses 10, 12, or 14 cycles or rounds. The key size, it can be 128, 192, or 256 bits, based on the specific round.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

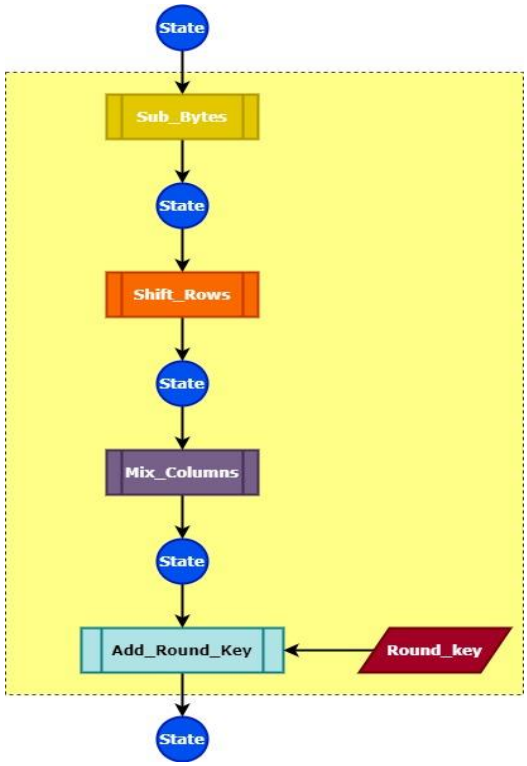

Fig.4. *AES Algorithm*

AES uses four types of transformations to provide adequate security: substitution, permutation, mixing, and key-adding.

Substitution-A non-linear substitution process where each byte is swapped with another according to a look-up table.

Permutation-A substitution step where each row of the state is shifted periodically a certain number of steps.

Mixing-A mixing operation which applies on the columns of the state, merging the four bytes in each column.

Key-Adding-In the Add_Round_Key step, the sub key is combined along with the state. For each round, a sub key is obtained from the main key using Rijndael's key schedule; each is the same size as the state. The sub key is obtained by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.

B) AES Encryption & Decryption Algorithm

AES is a conventional algorithm for performing encryption (and the reverse, decryption) which is a series of well defined comprehensive steps those can be proceeded as a distinct procedure. The actual information is known as plain text, and the encrypted data as cipher text. The cipher text message consists of all the information of the plain text message, but is not in a human readable format or computer without knowing the proper mechanism to decrypt it; it should resemble random gibberish to those not anticipated to read it. The encrypting procedure is varied based on the key which changes the detailed operation of the algorithm. Without having the key, the cipher text cannot be used to encrypt or decrypt.

1) AES Encryption Algorithm

Cipher (byte in [4*N_b], byte out [4*N_b], word w [N_b*(N_r+1)])

begin byte state[4,N_b]

state = in

Add_Round_Key(state, w[0, N_b-1])

for round =1 step 1 to N_r-1

Sub_Bytes(state)

Shift_Rows(state)

Mix_Columns(state)

Add_Round_Key(state,w[round*N_b,(round+1)*N_b-1]) end for

Sub_Bytes(state) Shift_Rows(state)

Add_Round_Key(state, w[N_r*N_b, (N_r+1)*N_b-1]) out = state

end

2) AES Decryption Algorithm

Inv_Cipher(byte_in[4*N_b],byte_out[4*N_b],word w[N_b*(N_r+1)])

begin

byte state[4,N_b] state = in

Add_Round_Key(state, w[N_r*N_b, (N_r+1)*N_b-1])

for round = N_r-1 step -1 down to 1

Inv_Shift_Rows(state)

Inv_Sub_Bytes(state)

Add_Round_Key(state,w[round*N_b, (round+1)*N_b-1])

Inv_Mix_Columns(state)

end for

Inv_Shift_Rows(state)

Inv_Sub_Bytes(state)

Add_Round_Key(state, w[0, N_b-1])

out = state

End

VI. CONCLUSION

Cloud computing is a hopeful and emerging technology for the next generation of IT applications. The limitations and difficulties toward the rapid growth of cloud computing are potential data security and privacy issues. Minimizing data storage and processing cost is a imperative requirement of any organization, at the same time, analysis of data and information is always the most essential tasks in all the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

organizations for decision making. So no organizations will transfer their data or information to the cloud until and unless buildup an assurance between the cloud service providers and consumers. A number of approaches have been proposed by researchers for data security and to gain highest level of data security in the cloud. However, there are still a lot of gaps to be filled by designing these techniques more effective. More efforts are required in the area of cloud computing to get it acceptable by the cloud service consumers. This paper surveyed various techniques about data security and privacy, finally concluded that to adopt a potential security in cloud, the data must be stored in encrypted form and different conventional encrypted algorithms keeps cloud data well secure.

REFERENCES

[1] Prince Jain, ―Security Issues and their Solution in Cloud Computing‖, International Journal of Computing & Business Research, Proceedings of _I-Society 2012‘ at GKU.)

[2] Rabi Prasad Padhy, Manas Ranjan Patra , Suresh Chandra Satapathy, ―Cloud Computing: Security Issues and Research Challenges‖, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[3] Harjit Singh Lamba and Gurdev Singh, ―Cloud Computing-Future Framework for emanagement of NGO's‖, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, ―CM- Measurement Facets for Cloud Performance‖, IJCA, Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5] Huiming Yu, Nakia Powell, Dexter Stembridge and Xiaohong Yuan, ―Cloud Computing and Security Challenges‖, 2012 ACM Publication.

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, DR. Atanu Rakshit, ―Cloud Security Issues‖, 2009 IEEE International Conference on Services Computing Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] Hassan Mathkourand, B. Al-Sadoon and Ameur Touir, ―A New Image Steganography Technique‖, IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2008

[8] A. E. Mustafa, A. M. F. ElGamal, M. E. ElAlmi and B. D. Ahmed, ―A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit‖, Research Journal Specific Education Faculty of Specific Education Mansoura University, pp. 752-767, 2011.

[9] Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. Wash & Lee L. Rev., Vol. 70(1), pp. 341-472.

[10] Deussen, P., Eckert, K., Strick, L. & Witaszek, D. (2012).Cloud Concepts for the Public Sector in Germany –UseCases. A publication by Fraunhofer Institute For Open Communication Systems.

[11] NIST-USA (2010). Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy Architecture, and High-Level Requirements (Vol. 1). A Report published by the National Institute of Standards and Technology, USA.

[12] Younis, Y., Merabti, M. & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep.

[13] Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud computing. International Journal of Information Technology, Vol. 5(2), pp. 243-246

[14] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, Vol. 34(1), pp. 1-11.

[15] Neela, T. J., & Saravanan, N. (2013). Privacy Preserving Approaches in Cloud: a Survey. Indian Journal of Science and Technology, Vol. 6(5), pp. 4531-4535.

[16] Parkhill, D.: The challenge of the computer utility. Addison-Wesley (1966)

[17] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D.: Provable Data Possession at Untrusted Stores. In: Proc. of ACM CCS. Alexandria, VA (Oct 2007)

[18] Juels, A., Burton, J., Kaliski, S.: Pors: Proofs of Retrievability for Large Files. In: Proc. of CCS. Alexandria, VA (Oct 2007)

[19] Shacham, H., Waters, B.: Compact Proofs of Retrievability. In: Proc. of Asiacrypt. Melbourne, Australia (Dec 2008)

[20] Role based access control, http://csrc.nist.gov/rbac/rbac-std-ncits.pdf