Data security In Cloud from the user end to the cloud and vice-versa using different techniques

[1]Er. C.P.Patidar, [2]Prasiddhi Khanna, [3]Mayank Saharan,[4]Abhishek Modi
[1]Assistant Professor Information Technology Department ,[2]B.E ,Information Technology ,
[3]B.E ,Computer Engineering,[4]B.E ,Information Technology,IET DAVV ,Indore,India

***Abstract*—** Cloud computing is a technology that has brought revolution in IT industry because of its performance ,availability, accessibility etc.It doesn't require any new infra structure and it maximize the capacity of new personnel or licensing new software. It provides big storage for data and computation power is very fast and it is serving large amount of customers. It necessarily shift the database and application to the large data base centers which is known as cloud where data is not completely secure. Because of which companies do not prefer to deploy their business to cloud even when it offer so many things. The data security in cloud is one of the major issue we are facing in the implementation of the cloud. So we present a paper in which we provide a solution for the security of cloud.We try to give complete security i.e from the data owner to the cloud and from cloud to the user of data. We use the classification of data on the basics of 3 parameter presented by the user i.e Confidentiality (C), Integrity(I) and Availability(A).The strategy followed to protect the data utilizes various measures such as the SSL (Secure Socket Layer) 128-bit encryption and can also be raised to 256-bit encryption ,the MAC (Message Authentication Code) is used for integrity check of data, searchable encryption and division of data in cloud for storage.

IndexTerms*— *Cloud security,Message authentication code, Confidentiality,Availability,Integrity

I. INTRODUCTION

Cloud primarily is referred as saving of user’s data to an off site storage system that is maintained by a third party. The data of the user is stored on a remote database where internet provide the connection between user and the database and not on the user's hard disk or other storage device. Computers are configured to work simultaneously in the cloud and the various applications use the collective computing power as if they are running on a cloud using the concept of virtualization. In this model customers are required to demand the services and for only that services they have to pay. Essentially, IT resources are shared by many tenants like office space, apartment, storage etc and they are rented. Delivered on an internet connection, the cloud eliminates the company’s data center or server. Cloud computing services for eg.Amazon EC2 and Google App Engine area unit engineered to require advantage of the already existing infrastructure.
The cloud model revolves around three things:

1. Cloud service provider: It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients data and high computation power.
2. Client/owner:It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.
3. User: The user is the data owner who wish to upload the data on the cloud.

The main concern are:
1. External assaulter (any unauthorized person) will get to the essential knowledge, because the management isn't within the hands of the owner.
2.Cloud service provider himself can breach the owner, as data is to be kept in his premises.
Anything which breaches security is critical and produce consequences. As soon as cloud privacy issues are further organised and strict regulations and governance for cloud operation are in position, more and more business owners will feel safe to opt for cloud computing.The proposed model has been made by using various techniques and use them to perform the task of data security in cloud. This This combination stood as wall in the security challenges which is drawback in effective functioning of cloud . This model is reported in such a way so it provides a complete view of data at different levels. The model uses encryption as the main fundamental protection scheme and data sent to cloud is in encrypted form.Encryption is that the conversion of information into encrypted kind referred to as a cipher text that can't be simply understood by unauthorized person and may be decrypted by the licensed person having a valid decryption key. Apart from this, the model positively handles the security issues by employing strict authentication parameters, digital signatures, storing encrypted data in cloud according to sensitivity rating, building of index, using of MAC for integrity check and keyword search for data in cloud.Thus of these parameters result into an outlined mechanism that encourages the right functioning of cloud computing.The owner sends the encrypted knowledge to cloud wherever it's keep in numerous sections looking on the sensitivity rating then the information are often retrieved by user from the cloud when requested.However, this is often possible solely when passing the authentication parameters then looking out the information by the utilization of keyword obtained from the owner.

II EXISTING SYSTEM

The cloud could be a nomenclature with an extended history in telephone, that has within the past decade, been adopted as a figure for net based mostly services, with a typical depiction in network diagrams as a cloud outline.The underlying thought dates back to 1960 once John McCarthy opinion that ‘‘Computation might sometime be organized as a public utility’’; so it shares characteristics with service bureaus that date back to the 1960s.In 1999, sales- force.com was established by brandy Benioff, Parker Harris.They applied several technologies of shopper websites like Google and Yahoo! to business applications.They additionally provided the thought of ‘‘On demand’’ and ‘‘SaaS’’ with their real business and triple-crowncustomers. IBM extended these ideas in 2001, as elaborated within the involuntary Computing pronunciamento, that describes advanced automation techniques like self-monitoring, self-healing, self-configuring and self-optimizing within the management of advanced IT systems with heterogeneous storage, servers, applications, networks, security mechanisms and other system elements that can be virtualized across an enterprise.Amazon.com played a key role in the development of cloud computing by modernizing their data centers.It found that the new cloud design resulted in vital internal potency enhancements and providing access to their systems by means of Amazon internet Services in 2005 on a utility computing basis.2007 saw raised activity with Google, IBM and a number of universities embarking on a large scale cloud computing research project, around the time the term started gaining popularity in the main stream press .

In August 2008, Gartner analysis determined that ‘‘organizations square measure shift from company-owned hardware and software package assets to per-use service-based models’’.The projected shift to cloud computing can end in dramatic growth in IT product in some areas and in vital reduction in alternative areas.Despite all the hope of gaining most advantage from this cloud computing, it seems to have born with security and management concerns, which time to time hinders its growth.For this, heap of analysis work has been done to secure the info in cloud computing (primary concern) from each perspective, but everything seems to face a new challenge as soon as it employed.

Juels. (2007)[1] described a formal Proof of Retrievability (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error-correcting code to ensure both possession and recovery of files on archive service systems.Shacham and Waters(2008)[2] engineered on this model and created a random linear perform based mostly Homomorphic appraiser.This enables unlimited number of queries and requires less communication overhead. Bowers. (2008a)[1] proposed an improved frame- work for POR protocols that generalizes both Juels[1] and Shacham’s work. Later in their subsequent work, Bowers. (2008b)[3] extended POR model to distributed systems.However, of these schemes square measure that specialize in static information.The effectiveness of their schemes rests totally on the pre-processing steps that the user conducts before outsourcing the info file.Any change to the contents of data file, even a few bits, must propagate through the error-correcting code, thus, establishing significant computation and communication complexity.

Chor. (1995)[4] proposed private information retrieval (PIR) so that clients can access entries in a distributed table without revealing which entries they are interested in. The PIR literature usually aims for very strong information theoretic security bounds, which makes it harder to find practical schemes. PIR schemes often require multiple non-colluding servers, consume large amounts of bandwidth, do not guarantee the confidentiality of the data, do not support private keyword searching and do not support controlled searching or query isolation. The schemes (Cachin., 1999[5]; Chor., 1998[6]; Gertner., 1998[7]; Kusilevitz and Ostrovsky, 1997[8]) are important exceptions which allow removing some but not all these Recently, Wang. (2009)[9] described a homomorphism distributed verification scheme using Pseudo random Data to verify the storage correctness of user data in cloud.This theme achieves the warranty of information convenience, dependableness and integrity. However, this scheme was also not providing complete protection to user data in cloud computing, since pseudorandom data would not cover the entire information.Prasad. (2011) and Sood. (2011)[10] discussed different security aspects in computing. Prasad.

(2011) technique provides a brand new thanks to demonstrate in third-dimensional approaches.

It provides availability of data by surmounting many existing problem like denial of services and data leakage etc. Additionally, it also provides more flexibility and capability to meet the rising demand of today’s complex and diverse network. But in this model, the data stored is not in encrypted form and once the username and password is lost, the data can easily be retrieved by any unauthorized user.Kamara and Lauter (2010)[11] worked over public cloud infra- structure and proposed a model which is well suited for preserving integrity with the help of cryptographic primitives.This technique is only supported scientific discipline storage services.In planned procedure, when a user wants to send data to other user, they first generate a master key that encrypts their message.The secret key for coding is keep on receivers’ system for decrypting a similar message.They use the idea of index secret writing and tokens are generated with the data of secret key.The looking technique isn't terribly economical for encrypted knowledge.They mentioned parallel searchable secret writing (SSE) and uneven searchable secret writing (ASE).These techniques are used for encrypted data searching but increase complexity and make the system cumbersome.Wang.(2010)[12] mentioned the drawbacks of mistreatment standard cryptography techniques and urged that these techniques don't seem to be helpful over cloud as a result of for this user ought to have pre information concerning the encrypted cloud data.Their model is predicated on parallel searchable secret writing technique.They gave design for existing cryptographic primitive and order preserving symmetric encryption (OPSE). Security analysis shows its success rate for one to many mapping and for ranked keyword search.This model didn't offer any data regarding the protection attacks, confidentiality and integrity.This model is not well suited for preserving security.Popa. (2010)[13] presents Cloud Proof, a secure storage system for increasing security over cloud.In this model users will discover violations of integrity, confidentiality, write serial ability and freshness.Model use cryptographic tools and engineering efforts to obtain an efficient and scalable system which
Allow users to detect and prove cloud misbehavior.

Cloud computing is a layered technology and the data in cloud computing has to go through different processing levels, so the security mechanism should be efficient and provided at each step, i.e., from owner to cloud and cloud to user or back to owner.Data shouldn't succumb to the attackers attempting to retrieve or tamper with it and not even the cloud supplier ought to be able to damage the info in any possible manner, because cloud service provider cannot be trusted with data of high sensitivity.

Hereby we are able to say that the planned model has been designed by keeping of these things in mind and for certain as compared to previous works, provides all these required measures to protect data in a very efficient and organized manner.

III. PROPOSED SYSTEM

Proposed framework has been structured to supply complete security to the information throughout the whole method of cloud computing, be it in cloud or in transit.Thus, multiple mechanisms and available techniques area unit applied to defend the vital info from unauthorized parties.

The proposed frame work is divided into two phases. First part deals with method of sending and storing knowledge firmly into the cloud.Second part deals with the retrieval of knowledge from cloud and showing the generation of requests for data access, double authentication, verification of digital signature and integrity, thereby providing authorized user with knowledge on passing all security mechanisms.

3.1.storing of data-This part deals with mechanisms and ways to store and secure the information from starting and sending it firmly to the cloud in encrypted type.It is further divided into sub-sections (Classification, Index Building and encryption, Message Authentication Code (MAC) which provide stepwise details of action on the data). 3.1.1.Classification-As the data in the cloud is intended to be stored, an approach is introduced for storing the data in different sections in the cloud (public, private, limited access) basis of three cryptographic para- meters viz: Confidentiality, Availability and Integrity.These values are going to be listed by the consumer himself and sensitivity rating (SR) are going to be calculated victimization the planned algorithmic program shown ahead.The value of C (confidentiality) is based on the level of privacy needed at each step of data processing, value of I (integrity) is based on how much accuracy of data, reliability of information and protection from unauthorized modification is required, and value of A (availability) is based on how frequently data is accessed and should available immediately when requested

3.2 ALGORITHM

```
1.  Input: Data, protection section ,D[] array of n integer size.Where D[] array consisting of C,I,A,SR of n integer size.
2.  Output: categorize data for corresponding section.
3.  For I=1 to n
        3.1 C[i]=Value of confidentiality
        3.2 I[i]=Value of integrity
        3.3 A[i]=Value of availability
        3.4 Calculate SR[i]=(C[i]+((1/A[i])*10+I[i])/2
4.      For j=1 to 10
         For i=1 to n
          If SR[i]==1|2|3 then
           SR[i]=3
           If SR[i]==4|5|6 then
            SR[i]=2
           If SR[i]==7|8|9 then
           SR[i]=1
```

In the algorithmic rule listed higher than, the first job of the owner is to reason the info on the idea of cryptographical parameters viz: C, I and A.Here D [ ] represents the info and also the user must provide values of C, I and A.After applying the projected formula as shown higher than, the value of Sensitivity Rating (SR) is calculated.This ‘‘SR’’ value is used to allocate the data to one of the three sections in cloud, i.e., S3 [Public], S2 [Private] or S1[Owner’s Limited Access] Index building and encryption. After the triple-crown allotment of values to information, the information currently has to prepare for an additional process mechanism.As the data on cloud will be stored in encrypted form and searching over encrypted data is a complicated issue, so we need to build up an index, using Index builder while retrieval, we can perform searching over encrypted data. Possible way to build up an index is that, for each word W (keyword) of interest, list the documents that contains W. Building up an Index provides faster retrieval of files.To provide a lot of security against revealing any style of info to cloud we'll write the index additionally.This index can primarily contain a listing of keywords, with each keyword contains list of pointers to the documents where key- word appears.The keywords area unit words of interest that a user might want to go looking later.Best follow is to create Associate in Nursing index of clear documents then write each document and index and store the encrypted knowledge onto the cloud.The index ought to be encrypted, by encrypting keywords moreover as document pointers in every list within the index.After this we need to encrypt data. Now, to code the data, the model uses encryption.Encryption is that the method of turning intelligible data into useless data

3.3 MAC authentication code

After encryption the data, a message authentication code (MAC) is generated which it transmits along with the encrypted data to cloud. MAC is a small fixed size block of data that is generated based on message/file F of variable length using any secret key. It is called cryptographic checksum and is used to check whether data has been tampered throughout the transmission and this check can be made by the user or owner of data on retrieving the file . Now, as the encrypted data on reaching cloud is to be stored in particular sections, the data will be distinguished on the basis of the Sensitivity Rating calculated i.e., SRr3 will go into public sections (S3), 3oSRr6 will go into private sections (S2) and 6oSRr10 will go into owner's limited access sections (S1).

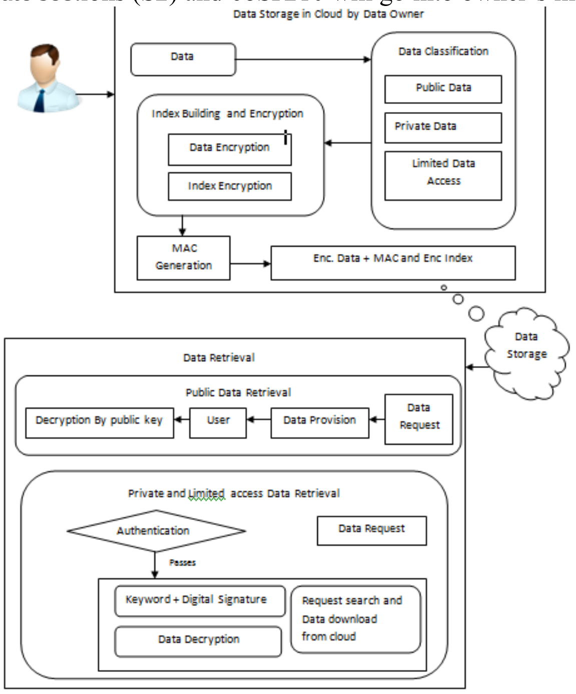

Figure 1 Data Storage and retrieval

3.4 Retrieval of Data

Now when the data has been stored in cloud in secure manner, the retrieval of data should be supported with equally best possible mechanism and techniques.First the retrieval of knowledge needs the user to register him with the owner/organization by obtaining a username and a arcanum.The user can register to urge its username and arcanum at organization, which will further forward the username to cloud to let it store the username into its directory.In this model, when the user requires accessing the data in cloud, he sends a request along with the username to cloud.Cloud check the request and if it is for public section , then without authentication access is granted and user after retrieving can decrypt this data by the public key provided in the section only. If the request is for private section and limited access section , authentication is necessary and cloud looks for username provided by user into its directory of user- names, provided by the owner.The sectional information utilized in this model can offer access below the subsequent guidelines:

1.The user granted access to higher section isn't allowed to access lower section, i.e., no read/write is in lower section.
e.g.: if user has access for information publicly section, then the information of same owner obtainable in cameraand restricted access section won't be obtainable to
the user.
2.The user granted access to lower section is allowed to access higher section.e.g.: if user has access for information in restricted access section, then the data of same owner available in private section will also be available to the user.if the username matches, cloud forwards the username to the owner/organization for authentication, here the important thing is that primary authentication process is kept with the owner only because criticality of the process is such that even the cloud cannot be trusted. Now as the company receives the username from cloud, it has to authenticate the username .For authentication, the user first sends the password to the owner and on clearing this parameter, user is prompted with a security question from owner and after answering it correctly, user is authenticated.The owner additionally sends the user identity together with the digital signature to cloud in order that cloud arecertain that owner has given the access of knowledge to particular user identity for this session only.
Afterwards user sends the request for information to owner that successively sends the owner's ''Digital Signature'', keyword of requested data and a master key to decrypt the data provided by cloud.On receiving the digital signature and keyword from the owner, the user forwards the same to the cloud with a search request for data corresponding to the keyword.The cloud initial verifies the digital signature, and if verified, cloud processes the search request using the keyword.Basically searching over encrypted data provides easy retrieval of file and without revealing any critical information to the cloud.As explained earlier we have a tendency to have already got hold on Associate in Nursing encrypted index containing an inventory of

keywords and with every keyword list of tips to the document wherever keyword seems.Whenever the cloud gets a keyword to search over encrypted data, it finds a match and then returns the user encrypted list of matching positions from the index. The user can then decrypt the encrypted entries by the decrypting key provided by owners of data and sends cloud download request to retrieve relevant file or document which user was looking for. The cloud replies the user with encrypted file it requested for and then user can decrypt the file by decryption key of file F, already shared by owner with user.One potential advantage for this theme is that the request might be embedded in alternative retrievals in order that cloud might need uncertainty regarding the correlation of the search request and the retrieval request for cipher text.Now, as the user has received his data from cloud, the question or doubt arises in the mind regarding its integrity. As this model uses MAC for integrity check, the user can assure him by deriving the MAC of encrypted file received using secret key, already shared with user and comparing it with MAC received along with the encrypted file

IV SECURITY ANALYSIS

The analysis of the proposed model for security of data through- out the whole traversing into this cloud computing paradigm comes up with the following mentioned steps where data can be terribly at risk of threats like knowledge escape, modification, privacy of users and confidentiality etc.The projected model is intended to tackle of these security problems terribly expeditiously.

4.1. Unauthorized server

As the knowledge has to be transmitted over a network to the cloud, there are numerous means through which an attacker can easily get into the internet based network and act as a cloud server to the owner of data, hence resulting into the loss of data.To prevent the loss of knowledge during this scenario, SSL certification in this model is used.Certificate Authorities (CAs) issue each certificate, which is a credential for the online world, to only one specific domain or server.The cloud server 1st sends the identification info to the owner once it connects then sends the owner a duplicate of its SSL Certificate.The owner verifies the certificate so sends a message to the server and therefore the server sends back a digitally signed acknowledgement to begin AN SSL encrypted session, enabling encrypted knowledge transfer between the browser and therefore the server.Moreover, the info and keywords ar hold on on the cloud in encrypted kind.

4.2. Brute force attack

The data whereas in transmission to cloud over an online network are often attacked by numerous unauthorized interceptors.Since SSL offers secret writing that forestalls interceptors from reading knowledge traversing the cloud.It is not troublesome to crack mistreatment today’s computers which may crunch sizable amount combos quickly so as to work out each doable key in an endeavor referred to as a brute force attack.Thus, in projected model we tend to ar mistreatment 128-bit SSL secret writing that provides additional bits of key length than the previous one SSL (40 bit) and can also be shifted to 256-bit whenever required.128-bit SSL is complicated enough to create a brute force attack largely useless at this point.The proposed model uses double encryption, one being done by owner and other using SSL.The process power required, among other things, would render most attackers ineffective.Hence this approach not solely safeguards knowledge wherever it lives, however conjointly helps assure customers that knowledge is secure whereas in transit.

4.3. Threat from cloud service provider

The cloud is that the place wherever the info resides when being transmitted by the owner.Suppose the info in cloud is safe from any third party, as the cloud service provider will use strict measures to protect it.The cloud service supplier will flip against the owner.As the knowledge isn't within the management of owner once in cloud, anything can be possible or cloud service provider can manage any leakage of data even by helping the rival parties.So, the cloud service supplier (CSP) can not be sure blindly.For this the simplest doable answer utilized in projected model is secret writing of knowledge hold on in cloud.SSL Certificates as used in the proposed model encrypts private communications over the public Internet.Using public key infrastructure, SSL consists of a public key (which encrypts information) and a private key (which decrypts information), so that only the key owners can read it.128-bit SSL secret writing encrypts the info in such how that it's nearly not possible for AN aggressor to decode it by a brute force attack.

4.4. Tampering of data

The data is often underneath the threat of being tampered by any unauthorized fighter aircraft.As all the preventive measures like encoding of knowledge, keywords and SSL encoding are taken within theplanned model to not let anyone tamper the info, but still knowledge has to be checked when the transmission.

For this, raincoat (Message authentication code) has been employed in planned model.MAC of encrypted data is generated by the owner before sending it and this MAC is transmitted along with the encrypted data. On the other hand, when receiver downloads or receives the data, can generate the MAC of received data and compare it with the MAC received along with the received data that was generated by the owner and if each the raincoat codes square measure same then user is assured of the integrity {of knowledge|of knowledge|of information}, i.e., data has not been tampered.

4.5. Loss of user identity and password

For unauthorized access, authentication is required to be there in the cloud computing security structure.Thus, just in case any user looses or by mistake reveals his user identity and arcanum to any unauthorized person, the data can be in danger.To protect the info, we have added another parameter, which is a must to clear in order to access the data in cloud.Here the user will be asked a security question whose answer is known to the authorized user only, so the unauthorized user will face Disappointment only even after having the correct user identity and password.
Moreover, assaulter should grasp the key to decipher the encrypted knowledge received from the cloud.

V. CONCLUSION

The planned technique provides the simplest way to safeguard the info, check the integrity and authentication by following the best possible industry mechanisms.It introduces the division of data into different sections, Index builder,128-bit SSL encryption, Message authenticate code and a double authentication of user one by owner and other by cloud and verification of digital signature of the owner.It provides handiness {of knowledge|of knowledge|of information} by surpassing several problems like data leak, change of state of knowledge and unauthorized access even from the cloud service supplier.Pro- posed method achieves the availability, reliability and integrity of data traversing through owner to cloud and cloud to user. In addition to this, it also provides more flexibility and capability to meet the new demand of today’s complex and diverse network and also enable the user to retrieve files from cloud by searching over an encrypted data.

REFERENCES

[1] Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive. Report 2008/175; 2008a.

[2] Shacham H, Waters B. Compact Proofs of Retrievability, Proceedings of Asiacrypt ’08, 5350, p. 90–107, 2008.

[3] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print Archive. Report 2008/489, 2008b.

[4] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval, In Proceedings of the 36th annual symposium on foundations of computer science, IEEE, p. 41–51, 1995.

[5] Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication, LNCS Springer Verlag, Advances in Cryptol- ogy- EUROCRYPT’99, 1592, p. 402–414, 1999.

[6] Chor B, Gilboa N, Naor M. Private information retrieval by keywords. Report 98-03.Theory of Cryptography Library, 1998.

[7] Gertner Y, Ishai Y, Kushilevitz E. Protecting data privacy in private information retrieval schemes, In Proceedings of the 30th annual ACM symposium on theory of computing, ACM, p. 151–160, 1998.

[8] Kusilevitz E, Ostrovsky R. Replication is not needed: single database, computa- tionally-private information retrieval, In Proceedings of the 38th annual symposium on foundations of computer science, IEEE, p. 364–373, 1997.

[9] Wang C, Wang Q, Ren K, Lou W. Ensuring data storage security in cloud computing, quality of service, 2009, IWQoS IEEE 17th international workshop, p. 1–9, 2009.

[10] Prasad P, Ojha B, Shahi RR, Lal R. 3-dimensional security in cloud computing. Computer Research and Development (ICCRD) 2011;3:198–208.

[11] Kamara S, Lauter K. Cryptographic cloud storage. Lecture Notes in Computer Science 2010;6054:136–49.

[12] wang C, Cao N,Li J Ren K, Lou w. secure ranked keyword search over encrypted cloud data. Journal of the ACM 2010;43(3):431–73.

[13] Popa RA, lorch JR, Molnar D, Wang HJ, Zhuang L , Enabling security in cloud storage SLAs with cloudproof. Technical report. Microsoft Research May 2010.