INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018

Remote Data Integrity Checking Based On Cloud Storage System

[1] C.S.Vigneesh, [2]s.Rajalakshmi

[1] PG Scholar, [2] Assistant Professor, Velammal Engineering College, India.

Abstract

Safety in cloud computing is an area that needs most awareness in Current situation in IT Fields. Cloud computing storage provides the users to store and process their data in third-party data centres in cloud. In this paper, we are going to use the encrypt and decrypt the records or documents this is to be uploaded to the cloud. The Encryption process is presented with the novel property that publicly revealing an encryption key. But not reveal the corresponding decryption key to anyone. The Keys are entered separately and as a result the Data owner or User could be allowed to view the record or documents. This method could bring the better protection in the Cloud .This process may be carried out in the public cloud (Eg: Drop Box)

Index Terms*:* Cloud computing, Cloud security, Data storage, Security analysis,

1. INTRODUCTION

Cloud Computing is the next-generation architecture of IT field and also IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. Cloud computing allows the users and enterprises with various computing capabilities to store and process the data either in a private-own cloud, or on a third-party server located in a data centres. As a basic service of Iaas model in cloud computing [2] cloud storage enables the data owner to store their file into the cloud and deletes the local copy of the data, which reduces the burden of maintenance and management of the data [3]. From the data owner perspective both individual and IT field storing the data remotely into a cloud in flexible on-demand manner brings appealing benefits, relief of the burden for Storage management, universal data access with location Independence and avoidance of capital expenditure on Hardware, software, and personnel maintenances, etc., [3]. While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity [4]. Outages and security breaches of noteworthy cloud services appear from the time to time [5] – [7]. Examples are Amazon S3's recent downtime, Gmail's mass email deletion incident and Apple Mobile Me's post-launch downtime. Outsourcing data into the cloud is economically attractive for the complexity and cost of long term large scale data storage, it does not offer any guarantee on availability and data integrity. This problem, if not properly addressed may impede the successful deployment of the cloud architecture.

Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in the cloud environment can be formidable and expensive for the cloud users [8]. To ensure the data security and save the cloud user's computation resources, it is critical importance to enable public auditability for cloud data storage so that user may resort to a third party auditor (TPA), who as experise and capabilities that the user do not to check the integrity of all data stored in the cloud on behalf of the users which provides much more easier and affordable way for the users to ensure their storage correctness in the cloud. TPA could release an audit report which would not only help users to evaluate the risk of their subscribed cloud data services [8] – [11]. Enabling public auditing services will play an important role for this cloud economy to become fully established, where users will need ways to assess risk and gain trust in the cloud. RDIC enables the server to prove to an auditor the integrity of a stored file. It is a useful technology for remote storage such as cloud storage. Traditional cryptographic technologies for data integrity checking such as message authentication codes and digital signatures are not ideal to remote data integrity checking (RDIC) because the original file is required in the verification procedure. The cloud security technique is based on some encryption techniques. So we can use the public key cryptosystems.

II. WHY CLOUD COMPUTING?

The reason for Why we are concentrating on cloud computing is that Lately the use of cloud from running a service to storing information has been growing day by day. Therefore there desires to be more attention on Cloud. Additionally the necessity for safety in the cloud is likewise more. This is because numerous Cloud provider vendors provide free memberships and because of this, the security element is being compromised. So from the consumer point of view, it is vital that we implement or introduce a few protection functions to guard our statistics as lots as we could.

III. RELATED WORKS

Utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. TPA may concurrently handle multiple audit sessions from different users for their outsourced data files. TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. Users rely on the cloud server for cloud data storage and maintenance. They may also dynamically interact with the cloud server to access and update their stored data for various application purposes. To achieve the audit delegation and authorize cloud server to respond to TPA audits the user can sign a certificate granting audit rights to the TPA's public key and all audits from the TPA are authenticated against such a certificate. [13].A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Fuzzy Identity Based Encryption, which allows for error-tolerance between the identity of a private key and the public key used to encrypt a cipher text. Fuzzy Identity based encryption gives rise to two interesting new application. The first is an Identity-Based Encryption system that uses biometric identity. we can view a user's biometric, for example an iris scan, as that user's identity described by several attributes and then encrypt to the user using their biometric identity. [14].

In cloud storage systems, the server (or peer) that stores the client's data is not necessarily trusted. PDP Model, data is preprocessed by client, metadata used for Verification process. The file sent to untrusted servers for storage, client may delete the local copy of the file. In order to implement our first DPDP construction, we use a modified authenticated skip list data structure. This new data structure, which we call a rank-based authenticated skip list, is based on authenticated skip lists but indexes data in a different way. The possible updates in our DPDP scheme are insertions of a new block after a given block i, deletion of a block i, and modification of a block I. There is a hidden input and output client state in all functions run by the client, and server state in all functions run by the server. Some inputs and outputs may be empty in some schemes. For example, the PDP scheme of does not store any metadata at the client side. We can also extend our DPDP scheme for use in storage systems consisting of multiple files within a directory hierarchy [15].
Public Key Scheme K is Known, Secret key can be easily computed for a non-negligible fraction of the possible public key. Its main purpose is didactic, to serve as the first existence proof for identity based schemes. The scheme is based on a public key cryptosystem with an extra twist Instead of generating a random pair of public/secret keys and publishing one of these keys, the user chooses his name and network address as his public key. Any combination of name, social security number, street address, office number or telephone number can be used provided that it uniquely identifies the user in a way he cannot later deny, and that it is readily available to the other party. The corresponding secret key is computed by a key generation center and issued to the user in the form of smart card when he first joins the network [16].

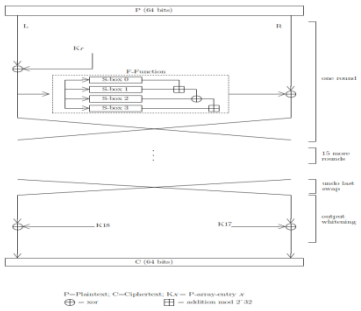
Public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Auditing services not only helps the data owner computation resources also provides transponent yet cost effective method for data owner to gain trust in the cloud. The challenging issues for public auditing services that need to be focused. Security in cloud computing an area full of challenges and of paramount importance is still in its infancy now but will attract enormous amounts of research efforts for many years to come. data owners no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted [17].

A secure cloud storage system supporting privacy-preserving public auditing. Enable the TPA to perform audits for multiple users simultaneously and efficiently. TPA can perform multiple auditing tasks in a batch manner for better efficiency. The public auditing scheme which provides a complete outsourcing solution of data, not only the data itself but also its integrity checking. Main scheme to support batch auditing for the TPA upon delegations from multiple users. MAC based solution which suffers from undesirable systematic demerits bounded usage and stateful verification, which may pose additional online burden to users, in a public auditing setting [18].

Encryption algorithms are divided in two categories, symmetric key encryption and public key encryption. Symmetric algorithms such as Blowfish, use the exactly the same key for encryption and decryption. This can be conveyed like a password that needs to be kept secret from everyone other than sender and receiver of the message. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both Encrypt and decrypt messages. Blowfish is also a block cipher meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits messages that aren't a multiple of eight bytes in size must be padded [23].

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16 round Feistel cipher and uses large key dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes. The diagram shows Blowfish's encryption routine. Each line represents 32 bits. There are five subkey-arrays: one 18-entry P-array (denoted as K in the diagram, to avoid confusion with the Plaintext) and four 256-entry S-boxes (S0, S1, S2 and S3).



Every round r consists of 4 actions: First, XOR the left half (L) of the data with the r th P array entry, second, use the XOR data as input for Blowfish's F-function, third, XOR the F-function's output with the right half (R) of the data, and last, swap Left and Right.

The F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output (see image in the upper right corner).

After the 16th round, undo the last swap, and XOR L with K18 and R with K17 (output whitening).

Decryption is exactly the same as encryption, except that P1, P2… P18 are used in the reverse order. This is not so obvious because XOR is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the cipher text block, then using the P-entries in reverse order).

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern (see nothing up my sleeve number). The secret key is then, byte by byte, cycling the key if necessary, XORed with all the P-entries in order. A 64-bit all-zero blocks is then encrypted with the algorithm as it stands. The resultant cipher text replaces P_1 and P_2. The same cipher text is then encrypted again with the new sub keys, and the new cipher text replaces $P_3$and P_4. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the sub keys about 4KB of data is processed.

Because the P array is 576 bits long, and the key bytes are XORed through all these 576 bits during the initialization, many implementations support key sizes up to 576 bits. While this is certainly possible, the 448 bits limit is here to ensure that every bit of every sub key depends on every bit of the key, as the last four values of the P array don't affect every bit of the cipher text. This point should be taken in consideration for implementations with a different number of rounds, as even though it increases security against an exhaustive attack, it weakens the security guaranteed by the algorithm.

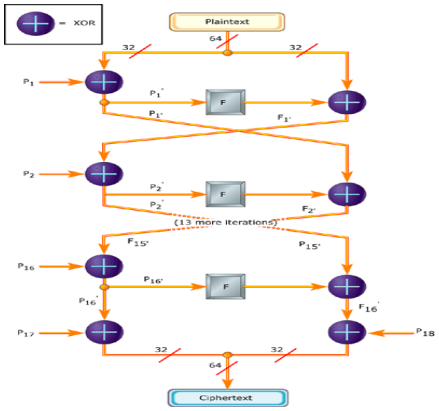
And given the slow initialization of the cipher with each change of key, it is granted a natural protection against brute-force attacks, which doesn't really justify key sizes longer than 448 bits [24].

BLOW FISH PSEUDOCODE

```
uint32_t P[18];

uint32_t S[4][256];

uint32_t f (uint32_t x) {

 uint32_t h = S[0][x >> 24] + S[1][x >> 16 & 0xff];

 return ( h ^ S[2][x >> 8 & 0xff] ) + S[3][x & 0xff];      }

void encrypt (uint32_t & L, uint32_t & R) {

 for (int i=0 ; i<16 ; i += 2) {

     L ^= P[i];

     R ^= f(L);

     R ^= P[i+1];

     L ^= f(R);

  }

  L ^= P[16];

  R ^= P[17];

  swap (L, R);

}

void decrypt (uint32_t & L, uint32_t & R) {

  for (int i=16 ; i > 0 ; i -= 2) {

     L ^= P[i+1];

     R ^= f(L);

     R ^= P[i];
```

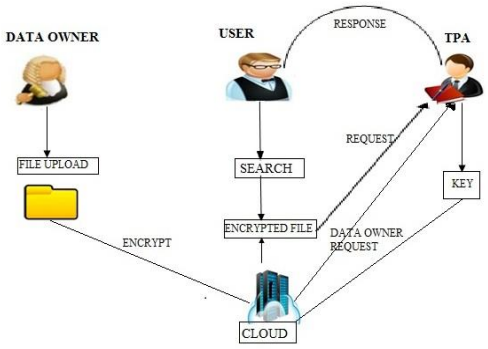
```
      L ^= f(R);
    }
    L ^= P[1];
    R ^= P[0];
    swap (L, R);
}
{
     for (int i=0 ; i<18 ; ++i)
       P[i] ^= key[i % keylen];
    uint32_t L = 0, R = 0;
    for (int i=0 ; i<18 ; i+=2) {
       encrypt (L, R);
       P[i] = L; P[i+1] = R;
    }
    for (int i=0 ; i<4 ; ++i)
       for (int j=0 ; j<256; j+=2) {
          encrypt (L, R);
          S[i][j] = L; S[i][j+1] = R;
}}
```

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018



III.PROPOSED WORK

In Encryption, First a key generated. Subsequent the cipher text is created. The phrases in the report are cut up into bytes and encrypted along with generated key. This can be decrypted handiest with the aid of getting into the proper key this is to be
gift within the user inbox that is sent by means of the admin



In Decryption, The equal process is repeated in the opposite order. The keys are generated and The key is deciphered and brought lower back to the identical layout which has all phrases split into bytes. Then The bytes are made into the example ultimately the decrypted price is were given and the decryption is whole. The decryption happens simplest after entering an appropriate key for an involved key price.

In the Existing system proposes the concept of Provable data possession (PDP) and gave two efficient construction using homomorphic verifiable tag (HVT) based on RSA algorithm. HVT aggregates response the challenge block into a single value. Symmetric-key algorithms are algorithms for cryptography that use the equal cryptographic keys for each encryption of plaintext and decryption of ciphertext. The keys can be same or there can be a simple transformation to move between the two keys. The keys, in exercise, constitute a shared secret among two or more events that can be used to maintain a private statistics link. This requires that each party have access to the name of the game key's one of the essential drawbacks of symmetric key encryption, in evaluation to public-key encryption (also known as asymmetric key encryption).

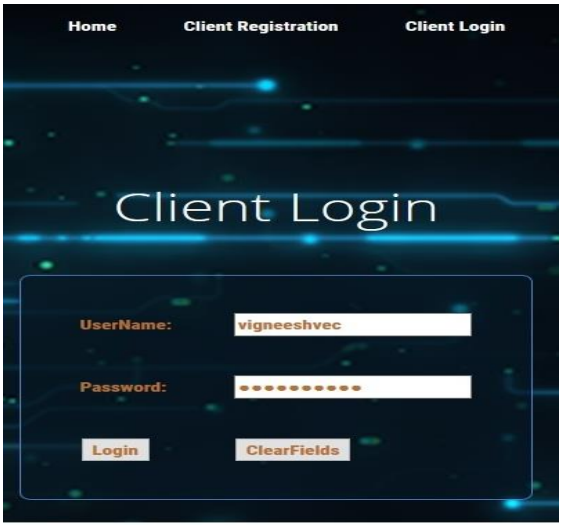
INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018

V. IMPLEMENTATION

Registration: In this module,the Data owner and user registers using his/her name,password,confirm password,mobile number and E-Mail Id which will be used when the Data owner and user is trying to upload and search a file.The user can act both as a user of the file and also as data owner of the file.

Logins: Login page we have to enter login
user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we cant enter into login window to user window it will shows error message. Before logging in we have to first register in the registration page with username, password, confirm password, E-Mail Id and register. This registration can be used for both user login and data owner login as well. So we are preventing from unauthorized user entering into the login window to user window.
Data Owner: In this module, the data owner process is to move into file upload window to upload file. The data owner process is to upload the files. Data owner uploads the file in the cloud storage for users view. While uploading the file the data owner generates the key for security purpose and upload into cloud.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018



Data owner is an authorized user who can upload, download and delete files from the cloud, data owner gives access to the user who has requested to view a particular file uploaded by the data owner, Data owner forwards the request by the user to the TPA admin and the TPA admin forwards the request to the server who generates a secret key and sends it to the data owner who then can forward the key to the user to view the file the user has requested for.

The TPA admin forwards the request sent by the data owner and the user to the server for further authentication where the server can generate a private key for the user to view the encrypted files.

A login generally requires the user to enter two pieces of information, first a user name and then a password. This information is entered into a login window on a GUI(graphical user interface)

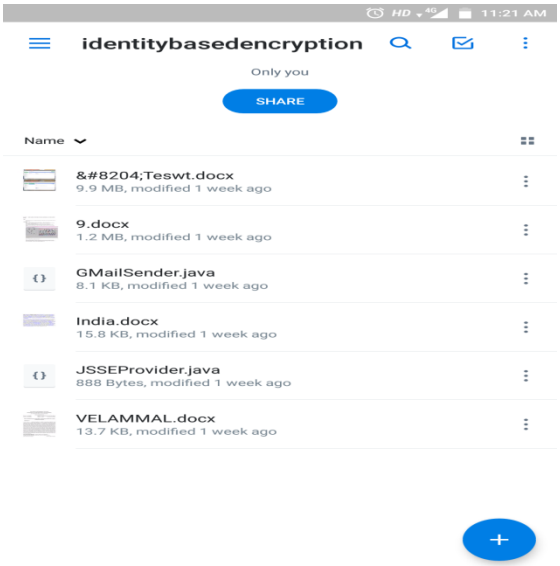
INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018

or on the command line in a console (i.e., an all-text mode screen), depending on the system and situation. A user name, also referred to as an account name, is a string (i.e., sequence of characters) that uniquely identifies a user. User names can be the same as or related to the real names of users, or they can be completely arbitrary. The user is only authorized to view and download files he cannot delete files from the cloud.

This sequence is used as an encryption key at one end of communication, and as a decryption key at the other end serves for the decryption process. The server authenticates the request generated. TPA to generate the key for the user and key will be send through the e-mail .Our experiment conducted on any free clouds.

For cloud we have used Dropbox. Once the file is uploaded that is explained in the data owner . The file gets uploaded into the dropbox directly. The file stored both locally and in the cloud as well.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3363 - 3375
RECEIVED : 15.03.2018 PUBLISHED : 23.04.2018
April 23, 2018



III.CONCLUSION

Thus Cloud data is secured in cloud using Blow fish algorithm. Cloud storage services have become an increasingly important part of the information technology industry in recent years.With more users getting involved in cloud storage, ensuring the integrity of data outsourced to the cloud is of paramount importance. A encryption key complement each authorization rule as cryptographic token to protect data against CSP misbehaviour. Guidelines for deployment in a Cloud Service Provider have been also given, including a hybrid approach compatible with Public Key Cryptography that enables the usage of standard PKI for key management and distribution. Future lines of research include the analysis of novel cryptographic techniques that could enable the secure modification and deletion of data in the Cloud. This would allow to extend the privileges of the authorization model with more actions like modify and delete. Another interesting point is the obfuscation of the authorization model for privacy reasons. But more advanced obfuscation techniques can be researched to achieve a higher level of privacy.

V. REFERENCES

[1] P. Mell and T. Grance, “Draft nist working definition of cloud computing,”Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[2] M. Hogan, F. Liu, A. Sokol and J. Tong, “NIST Cloud Computing Standards Roadmap,” NIST Cloud Computing Standards Roadmap Working Group, SP 500-291-v1.0, NIST, Jul, 2011.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A.Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech. Rep.

[4] Cloud Security Alliance, “Top Threats to Cloud Computing,” http://www.cloudsecurityalliance.org, 2010.

[5] M. Arrington, "Gmail Disaster: Reports of Mass EmailDeletions,"http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.
[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits-doors/, July 2008.

[7] Amazon.com, "Amazon s3 Availability Event: July 2008,"http://status.aws.amazon.com/s320080720.html, July 2008.

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.

[9] G.Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. ACMCCS '07, Oct. 2007, pp. 598–609.

[10] M. A. Shah et al., "Auditing to keep Online Storage Services Honest," Proc.USENIX HotOS '07, May 2007.

[11] G. Ateniese et al., "Scalable and Efficient Provable Data Possession," Proc.SecureComm '08, Sept. 2008.

[12] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Asia-Crypt '08, LNCS, vol. 5350, Dec. 2008, pp. 90–107.

[13] C.Wang, Q.Wang, K. Ren, andW. Lou, "Privacy-preserving public auditing for data storage security in cloud computing". Proc. of IEEE INFOCOM, pp.525-533, 2010.

[14] A.Sahai and B. Waters. "Fuzzy identity-based encryption". Advances in Cryptology-EUROCRYPT, pp.457-473, 2005.

[15] C. C. Erway, A. Kupcu and C. Papamanthou. "Dynamic provable data possession". ACM Transactions on Information and System Security (TISSEC), 17(4), 15, 2015.

[16] A. Shamir. "Identity-based cryptosystems and signature schemes". Advances in cryptology. pp.47-53, 1985.

[17] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services", IEEE Network, 24, pp.19-24,2010.

[18] C. Wang, S. S.Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage". IEEE Transactions on Computers, 62, pp.362-375, 2013.

[19] H. Q.Wang. "Identity-Based Distributed Provable Data Possession in Multicloud Storage". IEEE Transactions on Services Computing, 8(2), pp.328-340, 2015.

[20] Y. Yu, M.H. Au, Y. Mu, S.H. Tang, J. Ren, W. Susilo and L.J. Dong,"Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage"International Journal of Information Security.14(4), pp.307-318, 2015.

[21] R. L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Communicationsof the ACM, 21(2), pp.120-126, 1978.

[22] Y. Yu, J.B. Ni, M. H. Au, Y. Mu, B.Y. Wang and H. Li. "Comments on a Public Auditing Mechanism for Shared Cloud Data Service".IEEE Transantions on Services Computing, 8(6),pp.998-999, 2015.

[23] Ms NehaKhatri Valmik , V. K Kshirsagar "
Blowfish Algorithm" , IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83 www.iosrjournals.org

[24] https://en.wikipedia.org/wiki/Blowfish_(cipher)