ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Online Data Sharing Using Cloud Computing

Santanalakshmi Somasundaram[1]

U.G. Student, Department of Computer Science and Engineering, Kumaraguru College of Engineering, Coimbatore, India[1]

ABSTRACT: Data sharing is associate necessary practicality in cloud storage. In this paper, we show however to firmly, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems that turn out constant-size cipher texts such that economical delegation of secret writing rights for any set of cipher texts is feasible. The novelty is that one can mixture any set of secret keys and build them as compact as a single key, but encompassing the power of all the keys being mass. In other words, the secret key holder can unleash a constant-size mixture key for versatile decisions of cipher text set in cloud storage, but the different encrypted files outside the set stay confidential. This compact aggregate key will be handily sent to others or be hold on in an exceedingly} revolving credit with very restricted secure storage. We offer formal security analysis of our schemes within the commonplace model. We conjointly describe different application of our schemes. In particular, our schemes give the 1st public-key patient-controlled encoding for versatile hierarchy, which was nonetheless to be noted.

KEYWORDS: Data stream, Computation outsourcing, Storage outsourcing, multiple keys, Public verifiability

I. INTRODUCTION

Cloud Computing has been envisioned as the next- generation design of IT enterprise, due to its long list of unprecedented blessings within the IT history: on- demand self-service, ubiquitous network access, location independent resource pooling, rapid resource physical property, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the terribly nature of however businesses use info technology. One fundamental side of this paradigm shifting is that information is being centralized or outsourced into the Cloud. From users' perspective, including each people and enterprises, storing data remotely into the cloud in a versatile on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with freelance geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances,

etc.. While these blessings of victimization clouds square measure inarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of cloud service providers (CSP) might not be notable by cloud users—data outsourcing is additionally relinquishing user's final management over the fate of their information. As a result, the correctness of the data within the cloud is being place in danger owing to the subsequent reasons. First of all, although the infrastructures beneath the cloud square measure abundant additional powerful and reliable than personal computing devices, they are still facing the broad vary of each internal and external threats for information integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, for the benefits of their own, there do exist various motivations for cloud service suppliers to behave unreliably. Towards the cloud users regarding the standing of their outsourced information. Examples include cloud service suppliers, for monetary reasons, reclaiming storage by discarding data that has not been or is seldom accessed, or even hiding information loss incidents thus on maintain a name . In short, although outsourcing information into the cloud is economically engaging for the price and complexness of long-run large-scale information storage, it does not supply any guarantee on information integrity and accessibility. This problem, if not properly addressed, may impede the winning preparation of the cloud design.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

II. PREVIOUS METHOD

The single key distribution center used for distributes secret keys and attributes to all users. Unfortunately, one KDC isn't only a single purpose of failure however tough to take care of owing to the massive range of users that area unit supported during a cloud setting. In Cipher text-policy contain the secret key which will decrypt the file. So once the user tries to access a file, the system will match the user attributes that associated with user key. If those attributes satisfies the access policy associated with the file, the system will decipher the file, otherwise it will not be decrypted.

III. DISADVANTAGE

• The problem here is that the information records ought to have keywords related to them to alter the search.

• The key distribution center is a single key management uses a symmetric key approach and doesn't support authentication.

• The KDC is not only one purpose of failure however tough to take care of owing to the massive range of users that area unit supported during a cloud setting.

• The user will produce and store a file and different users can solely browse the file. Write access was not permitted to users aside from the creator.

IV. PROPOSED WORK

In this paper, we study however to build a coding key additional powerful within the sense that it permits coding of multiple cipher texts, without increasing itssize. Specifically, our problem statement is ―To style associate degree economical public-key coding theme that supports versatile delegation in the sense that any set of the cipher texts (produced by the coding scheme) is decrypt able by a constant-size coding key (generated by the owner of the master-secret key).‖ We solve this drawback by introducing a special kind of public-key coding that we tend to decision key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not solely below a public-key, but additionally below associate degree symbol of cipher text referred to as category. That means the cipher texts area unit more classified into completely different categories. The key owner holds a master- secret called master-secret key, which will be wont to extract secret keys for various categories. More significantly, the extracted key have can be associate degree mixture key that is as compact as a secret key for one category, but aggregates the power of the many such keys, i.e., the decryption power for any set of cipher text categories.

V. ADVANTAGE

• The delegation of decryption will be expeditiously enforced with the combination key, which is solely of mounted size

• The Multiple Key Distribution Centers used for distributing secret keys and attributes to users.

• It is provide the high security by mistreatment coding and coding keys for sensitive info.

• The cipher text is sent to the cloud supported the attributes and therefore the cloud verifies the key and stores the cipher text.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

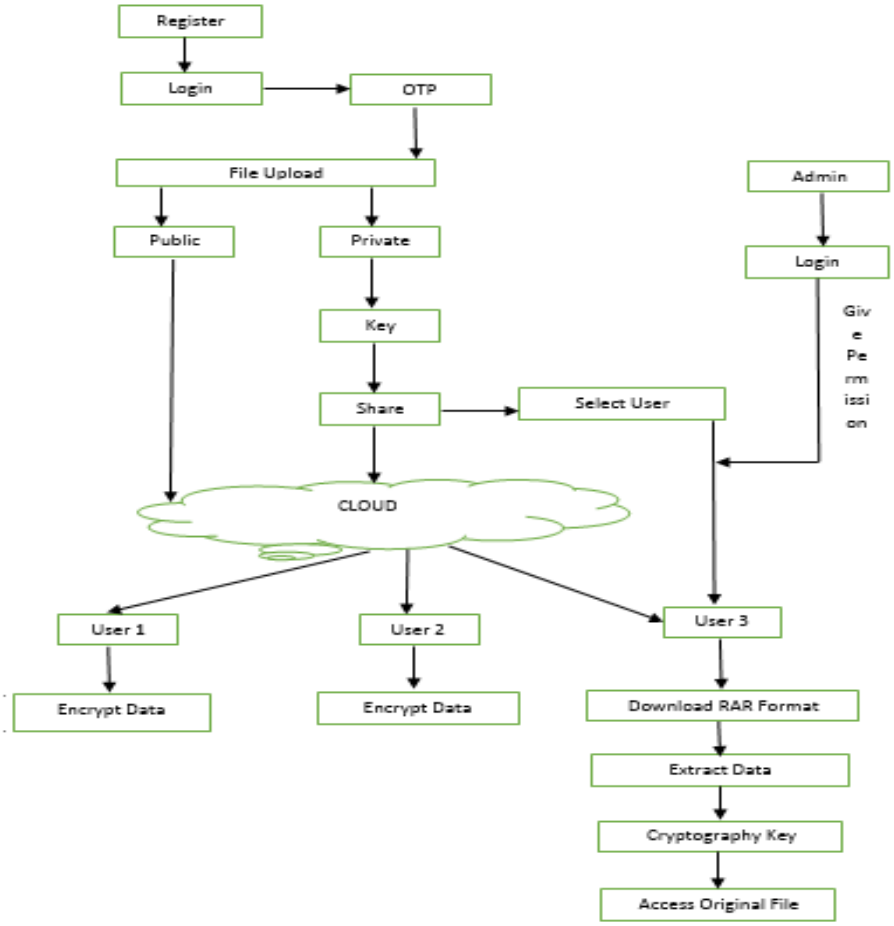
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

• The user wants the information, the cloud sends cipher text. If the user has key matching with access policy, it can decipher and get back original message.

VI. ARCHITECTURE DIAGRAM



VII. RELATED WORK

A. Performance Evaluation Of Public- Key Cryptosystem Operations In WTLS Protocol

WTLS (Wireless Transport Layer Security) is a vital commonplace protocol for secure wireless access to net services. WTLS employs public-key cryptosystems during the hand shake between mobile shopper and WAP entry (server).Several cryptosystems at completely different key strengths will be utilized in WTLS. The trade-off is security versus processing and transmission time. In this paper, an analytical performance model for public- key cryptosystem operations in WTLS protocol is developed. Different acknowledgment protocols, different cryptosystems and key sizes are thought of. Public-key crypto systems are enforced mistreatment state-of-the–art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and the analytical model are accustomed calculate the value of mistreatment public-key cryptosystems in WTLS. Results for different cryptosystems and acknowledgment protocols are relatively pictured and understood. It has been observed that ECC

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

(Elliptic Curve Cryptography) performs higher than its rival RSA cryptosystem in WTLS. Performance of some stronger ECC curves, which are not thought of in WTLS commonplace, is also analyzed. Results showed that some of those curves might be utilized in WTLS for prime security applications with a suitable degradation in performance.

B. Privacy-Preserving Public Auditing For Data Storage Security In Cloud Computing

Cloud computing is the long dreamed vision of computing as a utility, where users will remotely store their knowledge into the cloud therefore as to fancy the on-demand top quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be alleviated from the burden of native knowledge storage and maintenance. However, the fact that users now not have physical possession of the probably giant size of outsourced knowledge makes the information integrity protection in Cloud Computing a really difficult and doubtless formable task, especially for users with unnatural computing resources and capabilities. Thus, enabling public auditability for cloud knowledge storage security is of crucial importance therefore that users will resort to associate degree external audit party to envision the integrity of outsourced knowledge once required. To securely introduce associate degree effective third party auditor (TPA), the following two elementary necessities have to be compelled to be met: 1) TPA ought to be ready to with efficiency audit the cloud knowledge storage while not demanding the native copy of knowledge, and introduce no additional on- line burden to the cloud user; 2) The third party auditing method ought to bring in no new vulnerabilities towards user knowledge privacy. In this paper, we utilize and unambiguously mix the public key primarily based homo orphic critic with random masking to realize the privacy-preserving public cloud knowledge auditing system, which meets all on top of necessities. To support efficient handling of multiple auditing tasks, we additional explore the technique of linear combination signature to extend our main result into a multi-user setting, where TPA will perform multiple auditing tasks at the same time. Extensive security and performance analysis shows the projected schemes are demonstrably secure and extremely economical.

C. An Improved Dynamic Provable Data Possession Model

Cloud computing is becoming more and more standard. Many firms, organizations and individuals select to source their computing demands and storage demands. In order to confirm the integrity of the information within the Cloud, especially the dynamic files that will be updated on-line, we propose associate degree improved dynamic demonstrable knowledge possession model: It divides file into blocks, generates a tag for each block, computes a hash value for every tag, use stags to ensure the integrity of the file blocks, and uses hash values to ensure the integrity of the tags. Compared with previous works, it reduces the computational and communication complexness from to constant. Although shopper desires to store some secret values which can produce some further storage expense, it only takes up about0.02% of the original file size. Hence it is acceptable in most cases.

D. Hybrid Provable Data Possession At Untrusted Computing Stores In Cloud

In recent years, cloud computing has gradually become the thought of net services. When cloud computing environments become a lot of excellent, the business and user will be a vast quantity of knowledge hold on within the remote cloud storage devices, hoping to achieve random access, data assortment, reduce prices, and facilitate the sharing of other services. However, when the information is hold on within the cloud memory device, a long time, enterprises and users inevitably will have security issues, fearing that the information is really hold on within the cloud continues to be within the memory device or too long while not access to, has long been the cloud server removed or destroyed, resulting in businesses and users within the future can't access or restore the information files. Therefore, this scheme goal to analysis and style for information storage cloud computing environments that are evidenced. Stored in the cloud for information storage, research and develop a security and economical storage of proof protocol, also will delegate or authorize others to public verifiability whether or not the information truly hold on within the cloud storage devices.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

E. Robust Dynamic Provable Data Possession

Remote Data Checking (RDC) permits shoppers to expeditiously check the integrity of information hold on at global organization sure servers. This allows information house owners to assess the chance of outsourcing information within the cloud, making RDC a valuable tool for information auditing. Robust RDC theme incorporates mechanisms to mitigate discretionary amounts of information corruption. In particular, protection against small corruptions (i.e., bytes or even bits) ensures that attacks that modify a couple of bits don't destroy an encrypted file or invalidate authentication info. Early RDC schemes have focused on static information, whereas later schemes such as DPDP support the total range of dynamic operations on the outsourced information, including insertions, modifications, and deletions. Robustness is needed for each static and dynamic RDC schemes that bank on spot checking for potency. However, under associate adversarial setting there is a basic tension between economical dynamic updates and also the coding needed to attain hardiness, because change even a tiny portion of the file might need retrieving the whole file. We determine the challenges that want to be overcome once attempting to feature hardiness to a DPDP theme. We propose the first DC schemes that offer hardiness and, at the same time, support dynamic updates, while requiring tiny, constant, client storage. Our first construction is economical in coding, but has high communication value for updates. Our second construction overcomes this drawback through a combination of techniques that has RS codes supported Cauchy matrices, decoupling the encoding for hardiness from the position of symbols in the file, and reducing insert/delete operations to append/modify operations when change the RS- encoded parity information.

VIII. A SURVEY ON MODULES

A. Access Control

In this module, the user registration process is done by the admin. Here every user's offer their personal details for registration method. After registration each user can get Associate in Nursing ID for accessing the cloud area. If any of the user wants to edit their info they have submit the small print to the admin at that time the admin can do the edit and update info method. This process is controlled by the Admin.

B. Sharing Information's

In this module, every user's share their info and data's in their own cloud area provided by the admin. That information might be sensitive or necessary data's. For providing security for their information each user's storing the knowledge in their specific cloud. Registered users only will store the knowledge in cloud.

C. Multi Encryption Process

In this module, the information and data's shared by the user within the cloud is encrypted by victimization MES (Multi cryptography Standard) algorithmic program. All the information shared by each user is encrypted supported the information sensitivity and keep within the cloud. Involves in client facet configuration, performs two actions. The two actions area unit access management and permission management. Access control - MES algorithmic program. Permission control –Iconic cryptography algorithmic program. Access management method is based mostly on the server control options. Permission management method is based mostly on the shopper control options.

D. Integrity Checking

Integrity checking is the process of examination the encrypted info with altered cipher text. If there is any change in detection a message can send to the user that the cryptography method isn't done properly. If there is no change in detection suggests that then it'll enable doing consequent method. Integrity checking is mainly used for anti-malware

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

controls. In this module, the encrypted data is decrypted by the user victimization the public key of owner of the information. Decryption is the method of changing cipher text into plain text. MES algorithm is used for encrypting and decrypting the knowledge. The user can read {the knowledge theinfo the information} and can also transfer the data with high security.

E. Data Forwarding

In this module, the encrypted data or info keep in the cloud is forwarded to a different user account by victimization that user's public key. If any user wants to share their info with their friends or somebody they will directly forward the encrypted knowledge to them. Without downloading the knowledge the user will forward the knowledge to a different user.

Secure Data Forwarding is enforced by police investigation flag generation wherever for sharing flags can be 0-1 and wherever for forwarding flags 1- 1 is detected. Is flag 1-1 is detected then by applying Filtering technique data's are filtered out

F. Mathematical Analysis

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.)In January of 1997, a process was initiated by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, to find a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques. The entire selection process was fully open to public scrutiny and comment, it being decided that full visibility would ensure the best possible analysis of the designs. In 1998, the NIST selected 15 candidates for the AES, which were then subject to preliminary analysis by the world cryptographic community, including the National Security Agency. On the basis of this, in August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- †RC6, submitted by RSA Security
- †Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- †Serpent, submitted by Ross Andersen, Eli Biham and Lars Knudsen
- †Twofish, submitted by a large team of researchers including Counterpane's respected cryptographer, Bruce Schneier

  Implementations of all of the above were tested extensively in ANSI C and Java languages for speed and reliability in such measures as encryption and decryption speeds, key and algorithm set-up time and resistance to various attacks, both in hardware- and software-centric systems. Once again, detailed analysis was provided by the global cryptographic community (including some teams trying to break their own submissions). The end result was that on October 2, 2000, NIST announced that Rijndael had been selected as the proposed standard. On December 6, 2001, the Secretary of Commerce officially approved Federal Information Processing Standard (FIPS) 197, which specifies that all sensitive, unclassified documents will use Rijndael as the Advanced Encryption Standard.Also see cryptography, data recovery agent (DRA)RELATED

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

GLOSSARY TERMS: RSA algorithm (Rivest-Shamir-Adleman), data key, greynet (or graynet), spam cocktail (or anti-spam cocktail), fingerscanning (fingerprint scanning),munging, insider threat, authentication server, defense in depth, nonrepudiation

IX. EXPLANATIONS

AES is based on a design principle known as a Substitution permutation network. It is fast in bothsoftwareandhardware. Unlike its predecessor,DES, AES does not use a networkers has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the *state* (versions of Rijndael with a larger blocksize have additional columns in the state). Most AES calculations are done in a special field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryptionkey.

X. HIGH-LEVEL DESCRIPTION OF THE ALGORITHM

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule
2. InitialRound
    1. AddRoundKey—each byte of the state is combined with theround key using bitwisexor
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with anotheraccording to alookuptable.
    2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certainnumber ofsteps.
    3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in eachcolumn.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

Examples

In this appendix, twenty examples are provided for the MAC generation process. The underlying block cipher is either the AES algorithm or TDEA. A block cipher key is fixed for each of the currently allowed key sizes, i.e., AES-128, AES-192, AES- 256, two key TDEA, and three key TDEA. For each key, the generation of the associated sub keys is given, followed by four examples of MAC generation with the key. The messages in each set of examples are derived by truncating a common fixed string of 64 bytes. All strings are represented in hexadecimal notation,with a space (or a new line) inserted every 8 symbols, for readability. As in the body of the Recommendation, K1and K2denote the sub keys, M denotes the message, and T denotes the MAC. For the AES algorithm examples, Tlen is

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

128, i.e., 32 hexadecimal symbols, and K denotes the key. For the TDEA examples, Tlen is 64, i.e., 16 hexadecimal symbols, and the key, K, is the ordered triple of strings, (Key1, Key2, and Key3). For two key TDEA, Key1 = Key3. D.1AES-128

For Examples 1–4 below, the block cipher is the AES algorithm with the following 128 bit key:

K 2b7e1516 28aed2a6 abf7158809cf4f3c. SubkeyGenerationCIPHK(0 128)7df76b0c 1ab899b3 3e42f047 b91b546f K1 fbeed618 35713366 7c85e08f7236a8de K2 f7ddac30 6ae266cc f90bc11ee46d513b

Example Explanations

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption convertsdatatoanunintelligibleformcalledciphertext; decryptingthe cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

XI. CONCLUSION

Motivated by the sensible desires in knowledge sharing, We have reserved enough cipher text categories for the long run extension additionally, we expand the public-key the parameter will be downloaded with cipher texts, it would be better if its size is freelance of the most range of cipher text categories. On the other hand, when one carries the delegated keys around in a mobile device while not victimization special trusty hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem nevertheless permits economical and versatile key delegation is additionally a stimulating direction. We planned a new notion referred to as Forward Secure key primarily based Filtering. It allows associate ID-based Filtering theme to have forward security. It is the primary within the literature to own this feature for filtering in ID-based setting. Our scheme provides unconditional namelessness and will be verified forward-secure memorable within the random oracle model, assuming security downside is laborious. Our scheme is terribly economical and doesn't need any pairing operations. The size of user secret secret's only 1 integer, while the key update method solely needs associate mathematical process. We believe our theme can be terribly helpful in several alternative sensible applications, especially to those need user privacy and authentication intensive security and performance analysis shows that the planned schemes are incontrovertibly secure and extremely economical. We believe all these blessings of the planned schemes can shed lightweight on economies of scale for Cloud Computing.

REFERENCES

1) EricZavattoni, Luis J. Dominguez Perez, Shigeo Mitsunari, Ana H.S´anchez- Ramirez, Tadanori Teresa, and Francisco Rodr´ıguez-Henr´ıquez. Software implementation of an attribute-based encryption Scheme. IEEE Trans. Computers, 64(5):1429–1441, 2015.
2) Erik C Shall man. Up in the air: Clarifying cloud storage protections. Intell. Prop. L. Bull., 19:49, 2014.
3) Cheng-Kang Chu, Sherman SM Chow, Wen- Guey Zeng, Jitneying Zhou, and Robert H Deng. Key-aggregate cryptosystem for Scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions on, 25(2):468–477, 2014.
4) Ming Li, Shucheng Yu, Yao Zheng, KuiRen, and Wending Lou.Scalable and secure sharing of personal health records in cloud Computing using attribute- based encryption. Parallel and Distribute Systems, IEEE Transactions on, 24(1):131–143, 2013.
5)ChitchanokChuengsatiansup, Michael Naehrig, PanceRibarski, And Peter Schwa be. Panda: Pairings and arithmetic. In Pairing- Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers, pages 229–250, 2013
6)K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Paral- lel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, Sept. 2013.
7) Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859-25, May 2011.
8) C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

9)L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing with Anonymous ID Assignment," IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.
10)K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept./Oct. 2010.
11)J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.
12)Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
13)H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.