ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Securing Data against Pollution Attacks through SAAS-An Implementation of Cloud Computing Application

A Maheswararao[1], B Aswini[2]

Assistant Professor, Dept. of CSE, Satya Institute of Information Technology and Management, Vizianagaram, Andhra Pradesh, India

B.Tech, Dept. of CSE, Vignan Institute of Information Technology, Vishakapatnam, Andhra Pradesh, India

ABSTRACT: Software as a Service (SAAS), a class of Cloud processing permits both large and small scale associations to have a chance to utilize Intranet-based administrations. The across the board dissemination of appropriated and distributed storage arrangements has changed significantly, the way clients, framework fashioners, and specialist co-ops deal with their information. Security assaults, whereby a lot of malignant elements endeavour to degenerate put away information, are one of the numerous dangers that influence cloud data security. Lamentably, the impacts of a security assault on information can be awful, since a solitary dirtied part can spread unavoidably, therefore hampering the entire data. These are one of the numerous dangers that impact information security. The effect of these assaults can be appalling. At the point when sender sends specific information to the recipient, in the midst of this procedure the assailant attempts to degenerate or control the information. This is called as pollution attack. Here, we can use an asymmetric cryptographic algorithm which can detect the presence of an attack while getting the information from cloud storage.

KEYWORDS: Cloud storage, cloud data security, Pollution attack.

I. INTRODUCTION

Cloud storage systems give the substrate enabling clients and applications to connect their figuring assets to remote, progressively provisioned capacity assets. Extensive informational collections can be put away without causing into possibly critical capital and operational costs. Be that as it may, to open their maximum capacity, different issues should be appropriately tended to, including execution of information access, just as information accessibility and security. Security of outsourced information to the cloud represents to a key concern for clients, framework originators, and service providers. State - of-the-craftsmanship privacy systems for cloud storage depend on encryption that are computationally costly while the arrangement given by ENIGMA causes in a much lower computational expense [2]. State-of-the-art integrity mechanisms focus on just checking the integrity of data, while ENIGMA is able to tolerate the modification of sector fragments [2]. Among the many risks to information security, pollution attacks represents to a standout among the most risky dangers to information integrity, i.e., the capacity of guaranteeing information dependability. In this sort of assault, vindictive substances take control of at least one stockpiling resource to degenerate (contaminate) information (or parts of it) in order to thwart information accessibility. As Network coding allows intermediate (possibly malicious) nodes to actively mix packets it introduces new challenges in the detection of corrupted (or polluted) packets, it[4]. This is vulnerable and widely used to corrupt the data. Unfortunately, the very nature of packet mixing makes network coding systems vulnerable to a severe security threat known as pollution attacks, in which attackers inject corrupted packets into the network [4]. It is a sort of registering that depends on shared figuring assets as opposed to having local servers or personal devices to deal with applications. It is only sharing of data, stockpiling and recovery of information. In ENIGMA privacy is accomplished by uncovering just coded data,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

while the coding key is securely put away by the intermediary as it were [2]. The principal cloud computing services was given by Amazon in 2006 through the primary open cloud. These administrations are additionally called as AWS (Amazon Web Services). It gives administrations to applications, for example, long range interpersonal communication locales, email sites and web indexes. The upsides of cloud computing are versatility, dependability and proficiency. It saves money and time. The data at cloud isn't actually lost. Reliability: Services utilizing multi-repetitive locales can bolster business congruity and debacle recovery. Reduce Maintenance: Cloud specialist organizations do the framework upkeep that does not require application establishments onto PCs. Mobile Accessible: Mobile labourers have expanded efficiency because of frameworks open in a foundation accessible from anyplace [10]. It decreases organize multifaceted nature and no need of purchasing software licenses. The cloud client (U), who has expansive measure of information records to be put away in the cloud; the cloud server (CS), which is overseen by the cloud service provider (CSP) to give information stockpiling administration and has noteworthy storage room and calculation assets the outsider reviewer (TPA), who has mastery and abilities that cloud clients don't have and is trusted to evaluate the distributed storage administration dependability in the interest of the client upon demand. Clients depend on the CS for cloud information stockpiling and support. They may likewise powerfully communicate with the CS to access and refresh their put away information for different application purposes. To spare the calculation asset just as the online weight, cloud clients may depend on TPA for guaranteeing the capacity honesty of their redistributed information, while planning to keep their information private from TPA [8].

II. RELATED WORK

Trust Service Providers (TSPs) are partitioned over the cloud, and they inspire crude trust confirmation from various sources and in various organizations. This verification is data concerning the adherence of the cloud service providers (CSPs) to the Service Level Agreement (SLA) for the offered administrations and the input sent by cloud service users(CSUs). Utilizing this information, they determined a target trust and a subjective trust of CSPs. TSPs interconnect between themselves through a trust diary arrange that allows a TSP to get trust data about a CSP from different TSPs. Examinations demonstrated that their proposed structure is compelling and generally consistent in separating reliable and deceitful CSPs in a multi-cloud setting. It offered reasonable security, unwavering quality, and dynamicity, yet it experienced low reliability, low honesty, low secrecy, and low wellbeing [5]. The fundamental work of Cloud information capacity is to keep up the information given by the customer since this information can't be kept up on customer's machine. So the information given by customer ought to be kept up by cloud framework for this reason cloud ought to act naturally reasonable in nature, this self-managing of the cloud, the framework will lessen the weight of the customer [7].

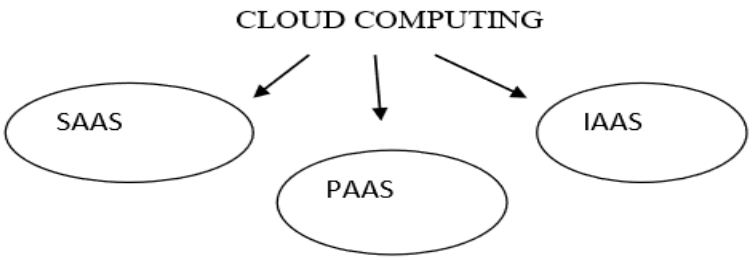

Fig.1 Types of Services in Cloud

The three primary classifications of cloud computing are SAAS (Software as an Service), PAAS (Platform as an Service) and IAAS (Infrastructure as an Service). This is a web application that utilizes SAAS in it. SAAS is only a product dispersion show. In SAAS, specialist organizations have applications and make them accessible to clients over web or intranet. Homomorphic encryption which hypothetically permits performing the calculation on scrambled

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

informational indexes, applying current calculations are somewhat costly because of their wastefulness [12].The fundamental work of Cloud information capacity is to keep up the information given by the customer since this information can't be kept up on customer's machine. So the information given by customer ought to be kept up by cloud framework for this reason cloud ought to act naturally reasonable in nature, this self-managing of the cloud, the framework will lessen the weight of customer [6].A novel privacy-preserving range query (PaRQ) scheme over encoded metering information to address the protection issues in budgetary reviewing for the shrewd lattice. A PaRQ enables a private client to store metering information on a cloud server in a scrambled structure. A PaRQ builds an Elgammal calculation for scrambling the information. The PaRQ develops a shrouded vector encryption based range inquiry predicate to scramble the accessible traits and session keys of the encoded information [9] . when running at low use, servers normally need up to 70% of their greatest power utilization. Such administrations can be virtualized and kept running inside a virtual machine (VM) bringing about huge increments in general vitality productivity. Virtualization innovation enables one of the approaches to make a few Virtual Machines (VMs) on a physical server and subsequently, lessen the measure of equipment being used and improves the use of assets[11].

II.I. DATA SECURITY ISSUES OF PRIVACY DATA

The objective is to give security to the data against different dynamic and passive attacks. Information security has turned into a vital angle in the modern world. With the wide spread of networks i.e, web, numerous web based business, web based banking, email and a lot more administrations have turned out to be basic spot. Regardless of whether they give us the simplicity of many things, they come at an incredible danger of protection and security. The ease, with which we can benefit these facilities, is only equivalent to another person profiting those facilities in our name. Precedent: If somebody i.e., X is to access the bank username and secret word of somebody i.e., Y, at that point X could without much of a stretch do exchanges as though it is Y itself. This is the issue which impacts cloud - information security. The answer for this can be given utilizing Cryptography

II.II. POLLUTION ATTACK ON THE DATA TRANSFER

Other than confirmation, mistake adjustment of adulterated coded sections is another essential way to deal with manages contamination assaults in coding-based frameworks, e.g., All these techniques depend on the addition of coding data that empower the coded piece collectors to distinguish and naturally recreate the first information. The cost to be paid is a wonderful increment in the coding overhead; moreover, the viability of these methodologies vigorously relies upon the measure of adulterated data. They are a lot of noxious entities and are a type of security assaults that endeavours to corrupt the stored information. These are one of the numerous dangers that impact information security. The effect of these assaults can be deplorable. At the point when sender sends a specific information to the recipient, in the midst of this procedure the aggressor endeavours to degenerate or control the information. This is called as pollution attack.

II.III. DETECTION AND RECOVERY FROM POLLUTION ATTACKS IN CODING-BASED DISTRIBUTED STORAGE SCHEMES

Pollution attacks in coding-based distributed storage frameworks. In a pollution attack, the enemy malignantly adjusts a portion of the put away encoded bundles, which results in the off base interpreting of a vast piece of the first information upon recovery. We propose calculations to recognize and recuperate from such assaults. Rather than existing ways to deal with tackle this issue, our methodology did not depend on adding cryptographic checksum or marks to the encoded parcels, and it doesn't acquaint any extra repetition with the framework. The calculations are reasonable for down to earth frameworks, particularly in remote sensor systems. Power is conveyed from providers to purchasers through an interconnected system called Grid. It comprises of creating stations that produce electrical power, high-voltage transmission lines that convey control from inaccessible sources to request focuses, and conveyance lines that interface singular clients. The pollution detection algorithm ready to recognize the nearness of an assault while bringing the information from distributed storage amid the typical circle perusing tasks [4]. Therefore each piece is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

check for malevolent substance and ignored to the server for preparing. The alert triggers a methodology that finds the dirtying hubs in beginning time of handling to stay away from the interruption. Likewise to distinguish the dirtied substance hashing strategies are utilized [4]. A pollution detection algorithm that identifies, with high likelihood if a course of action of untrusted storing resources gives no short of what one dirtied coded part. The figuring relies upon a changed adjustment of the LT unravelling estimation mishandling Gaussian Elimination[1] ; An illustrative model for disentangling (and disclosure) execution is out of reach in the composition we fall back on diversions to assess the area likelihood [1].

III. CRYPTOGRAPHY

Cryptography is typically alluded to as "the investigation of mystery". Encryption is the way toward changing over typical content to unintelligible structure. Decoding is the way toward changing over encoded content to ordinary content in the meaningful structure.

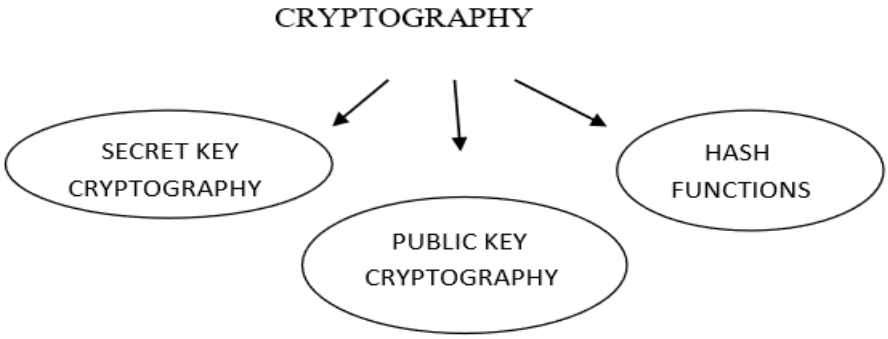

Fig.2. Types of key in Cryptography

Secret Key Cryptography is likewise called as symmetric cryptosystem on the grounds that it comprises of a solitary key. The most generally utilized symmetric cryptographic calculation is DES (Data Encryption Standard).

Hash Functions: These are irreversible capacities which give information respectability. Precedent: MD5 calculation is a cryptographic hash work that conceals the content and shows dabs in the content region box of secret key. A hash work is any capacity that can be utilized to delineate of subjective size to information of fixed size. The qualities returned by a hash work are called hash esteems, hash codes, digests, or basically hashes. One use is an information structure called a hash table, broadly utilized in PC programming for quick information query. Hash capacities quicken table or database query by identifying copied records in a huge document. A model is finding comparable stretches in DNA successions. They are likewise valuable in cryptography.

Public Key Cryptography is also called as asymmetric cryptosystem. Asymmetric implies it comprises of two diverse keys. One of them can be shared to everybody; it is called as Public key. The other key must be kept private and is called as Private Key. Public key is utilized for Encryption of information though private key is utilized for decoding process. The private key is additionally called as mystery key or message key. The most broadly utilized asymmetric cryptographic calculation is RSA calculation. R represents RON RIVEST; S represents ADI SHAMIR and A represents LEONARD ADLEMAN.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

IV. EXISTING SYSTEM

Gaussian Elimination Algorithm: The calculation depends on a changed form of the interpreting calculation misusing Gaussian Elimination or Row Reduction. GE is named after CARL FRIEDRICH GAUSS (1777-1855).Since an analytical model for deciphering (and discovery) execution is inaccessible in the writing, we resort to re-enactments to evaluate the detection probability. Long division of polynomial to be tackle, bringing about slower advance .GE has the drawback in the pragmatic case i.e., it needs more memory and conceivably additional time. In GE, decryption takes multiple times bigger the time than encryption.

```
h := 1 /* initialization of the pivot row */
k := 1 /* initialization of the pivot column */
while h ≤ m and k ≤ n
  /* Find the k-th pivot: */
  i_max := argmax (i = h ... m, abs(A[i, k]))
  if A[i_max, k] = 0
    /* No pivot in this column, pass to next column */
    k := k+1
  else
     swap rows(h, i_max)
     /* Do for all rows below pivot: */
     for i = h + 1 ... m:
        f := A[i, k] / A[h, k]
        /* Fill with zeros the lower part of pivot column: */
        A[i, k]  := 0
        /* Do for all remaining elements in current row: */
        for j = k + 1 ... n:
           A[i, j] := A[i, j] - A[k, j] * f
     /* Increase pivot row and column */
     h := h+1
     k := k+1
```

While iterative strategies, Gaussian end calculation can fizzle, or utilize a capricious amount of time. GE has the disadvantage in the functional instance of inadequate grids that it needs way more memory, and possibly additional time. The problem of multi-keyword ranked search over encrypted cloud data(MRSE) while preserving the strict system-wise privacy in cloud computing paradigm [3]. However Among various multi-keyword semantics, we have chosen the efficient principle of “coordinate matching”, i.e., as many matches as possible, to hold and capture the similarity between search query and data documents [3].

V. PROPOSED SYSTEM

V.I. CRYPTOGRAPHIC ALGORITHMS: SYMMETRIC CRYPTOGRAPHIC ALGORITHMS

It is additionally called as symmetric cryptosystem in light of the fact that it comprises of a solitary key. The most broadly utilized symmetric cryptographic calculation is DES (Data Encryption Standard). The Data Encryption Standard (DES) is a symmetric-key calculation forward encryption of electronic information. DES is presently viewed as uncertain for some applications. This is for the most part because of the 56-bit key size being excessively little. The distributed .net and the Electronic Frontier Foundation worked together to openly break a DES key in 22 hours and 15 minutes. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The calculation is accepted to be for all intents and purposes secure as Triple DES, despite the fact that there are hypothetical assaults. This cipher has been supplanted by the Advanced Encryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Standard (AES). Besides, DES has been pulled back as a standard by the National Institute of Standards and Technology. Some documentation makes a refinement between DES as a standard and as a calculation, alluding to the calculation as the DEA (Data Encryption Algorithm).
Advanced Encryption Standard (AES), likewise known by its unique name Rijndael is a determination for the encryption of electronic information set up by the U.S. Rijndael is a group of ciphers with various key and block sizes. For AES, NIST chose three individuals from the Rijndael family, each with a block size of 128 bits, however three distinctive key lengths: 128, 192 and 256 bits. Data Encryption Standard (DES), The algorithm described by AES is a symmetric-key algorithm, which means a similar key is utilized for both scrambling and decoding the information.AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

V.II. ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption. Many protocols like SSH, Open PGP, S/MIME, and SSL/TLS rely on asymmetric cryptography for encryption and digital signature functions. It is also used in software programs, such as browsers, which need to establish a secure connection over an insecure network like the internet orneed to validate a digital signature. Encryption strength is directly tied to key size and doubling key length delivers an exponential increase in strength, although it does impair performance. As computing power increases and more efficient factoring algorithms are discovered, the ability to factor larger and larger numbers also increases. For asymmetric encryption to deliver confidentiality, integrity, authenticity and non-reputability, users and systems need to be certain that a public key is authentic, that it belongs to the person or entity claimed and that it has not been tampered with or replaced by a malicious third party. There is no perfect solution to this public key authentication problem. A public key infrastructure (PKI), where trusted certificate authorities certify ownership of key pairs and certificates, is the most common approach, but encryption products based on the Pretty Good Privacy (PGP) model (including Open PGP), rely on a decentralized authentication model called a web of trust, which relies on individual endorsements of the link between user and public key.

V.III. RSA ALGORITHM

In order to overcome the difficulties in the existing method and to provide the cost effective and user friendly application, our pollution detection algorithm i.e., RSA (Ron Rivest - Adi Shamir - Leonard Adleman) and it is widely used for secure data transmission through key generation. It is an asymmetric cryptographic algorithm, used by modern computers to encrypt and decrypt the data. Therefore it can detect pollution attacks even before the data is recovered (It allows reduced running time). RSA is very fast and simple encryption technique. It is easier to implement. It is very simple to understand. It is widely deployed, and has a better industry support. It provides confidentiality, integrity and data authentication. The proposed algorithm selects highly effective and efficient useful independent features by using the following algorithm steps.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

ALGORITHM: RIVEST - SHAMIR - ADLEMAN ALGORITHM

- RSA algorithm operations :

KEY GENERATION =>

step1: Choose 2 different large random prime numbers p and q , and check that **p!=q**

step2: Calculate modulus n i.e., **n=p*q**

step3: Calculate totient function, phi or ϕ

ϕ (n)= (p-1)(q-1)

step4: Select an integer i.e., public key exponent "e" , **1< e < ϕ (n)** such that **gcd(e,ϕ(n))=1**

step5: calculate an integer i.e., private key exponent "d" , **d=[1+k.ϕ(n)] / e** (acc. to Extended Euclidean theory)

ENCRYPTION => C = $m^e \bmod n$

DECRYPTION => m = $c^d \bmod n$ where, c = cipher text
m = message
e = public key
n = modulus
d = private key .

VI. CONCLUSION

SAAS i.e., (Software as a Service) is a product circulation show in which a specialist organization has applications and makes them accessible to clients over the Intranet or Internet. The contamination discovery calculation will almost certainly detect the nearness of an assault while getting the information from distributed storage amid the transmission. We have demonstrated that rate less codes enable one to plan a straightforward contamination location component that can be utilized to check information honesty amid the typical read activities of a cloud-based capacity framework. In any case, the location component alone isn't sufficient to illuminate the most critical issue, for example to find the noxious stockpiling hubs so as to expel them from the framework. Here we have proposed an algorithmic arrangement that abuses both contamination locations, empowered by rate less codes, and measurable derivation to iteratively distinguish the pernicious hubs. We have given a scientific model to appraise the time required to recognize all polluters in a total distributed storage framework; we likewise broke down the adequacy of our methodology as an element of a few framework parameters. At last, we have recreated a start to finish dispersed distributed storage situation and, by taking genuine circle follows into record, we have demonstrated that the proposed strategy accomplishes the ideal dimension of vigor to polluters amid practical circle use. The eventual fate of distributed computing and security is incredibly encouraging with a gigantic open door for mechanical achievement for the organizations as of now utilizing this innovation today. In our venture, starting at now records sharing should be possible in a steady progression i.e., on the off chance that a document is being shared, at that point rest of the documents will be in hold up period until and except if it finishes its sharing activity. In any case, soon, it tends to be altered to such an extent that beyond what one record can be chosen at once and share it to the particular clients with most extreme security. Before sufficiently long, cloud innovations will bolster working quicker and that's only the tip of the iceberg viably than it is today.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

REFERENCES

[1]. Parihar Vimladevi Mishrilal, Rohini Dattatrey Patil, "Securing coding-based cloud storage against pollution attacks", International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454-132X Impact factor: 4.295, Volume 4, Issue 2,2018.

[2]. C. Anglano,R. Gaeta; M. Grangetto ," Exploiting Rateless Codes in Cloud Storage Systems",IEEE TRANSACTIONSON PARALLEL AND DISTRIBUTED SYSTEMS, 10.1109/TPDS.2014.2321745.

[3]. Pradeep Kumar Vishwakarma, Mritunjay Kumar Chubey, Kerana Henrix D, " Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" , International Journal of Computer Science and Information Technology Research, ISSN 2348-1196 (print), ISSN 2348-120X (online),Vol. 3, Issue 2, pp: (195-198), Month: April - June 2015.

[4]. Shanmugavel. S, Hariharan. J, Daniel Thomas Abraham, Abirami. M, **"**Prevention of Pollution Attack in Cloud", International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887, Volume 6 Issue III, March 2018.

[5]. Matin Chiregi, Nima Jafari Navimipour,"ReviewCloud computing and trust evaluation: A systematic literature reviewof the state-of-the-art mechanisms", ScienceDirect-Journal of Electrical Systems and Information Technology 5 (2018) 608–622.

[6]. Gaurav Pachauri1, Subhash Chand Gupta2,"ENSURING DATA INTEGRITY IN CLOUD DATA STORAGE", IJISET - International journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.

[7]. Raj Priyadarshini. R and Kanchanadevi. P,"Amalgam Attribute Based Encryption Scheme over the Cloud Data for Secure Access in the Hybrid Cloud", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.

[8]. Tinku Abey Koshy, S Prema ,"Third Party Auditor for Secure Cloud storage", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.

[9]. H.PRABHA,C.MENAGA,"A Hidden Vector Encryption Using Query Tokens in Cloud Computing", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.

[10]. Mr. Deepak Goel,Shriniwas singh, Amit asthana "Data Integrity in Cloud Computing", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

[11]. Dhavamani.A ,Dharmalingam.K, Sathyalakshmi.S ,"Reducing Power Consumption And Increasing The Efficiency In Cloud Data Centers", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

[12]. Vinutha N," Classification of Information as datasets and Encrypting them for Privacy Protection in Cloud", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.