Efficient Security Measures to Avoid Data Vulnerabilities in Cloud Using Encryption Techniques

Nomula Manoj Kumar Reddy[1], S Divya[2]
UG Scholar[1], Assistant Professor[2]
Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,Chennai,Tamilnadu,India.
E-mail : manumanoj.mm611@gmail.com , Divyasundar1819@gmail.com

Abstract: The technology of engineering science is growingfaster and its usage isto bootincreasing speedily. The data and its usage has become an important issue in existence. There by the storage of data may be a crucial issue in means of life. For this data storage, Cloud Computing is useful. Cloud computing is that the follow of using a network of remote servers hosted on internet to store, manage and methodology data on demand and pay as per use. It provides access to a pool of shared resources instead of native servers or personal computers. as a result, outfit do not acquire the things physically, it saves managing value and time for organizations. As a result of the sector of cloud computing is spreading the new techniques are developing. This increase in cloud computing setting to boot can increase security challenges for cloud developers. Most of the organizations are an excellent deal concerned regarding the possession of their data.This analysis paper presents a review on the cloud computing concepts yet as security issues inherent at intervals the context of cloud computing and cloud infrastructure. This paper in addition analyses the key analysis and challenges that presents in cloud computing and offers best practices to service suppliers yet as enterprises. The foremost goal is to review different types of attacks and encryption techniques to secure the cloudmodel.

Keywords: Data storage,Cloud Computing, Network, Privacy, Organization, Security Challenges.

1. INTRODUCTION

Cloud Computing could also be a model for facultative ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (such as networks, server, storage, applications and services) which is able to be rapidly provisioned and discharged with smallest management effort or service provided interaction. In Cloud Computing, there are four different types of clouds. they are Public cloud, personal cloud, Community cloud, Hybrid cloud. The term “cloud computing” describes the computation style taking the form of a cloud thatis positively accessible by users on demand. Some vendors associated researchers define cloud computing narrowly as an updated version of utility computing; primarily virtual servers that are on the market on the online right away. Cloud computing first appeared in 2006, once Amazon's Elastic Computing Cloud (EC2.In 2007, holler discharged its version of cloud computing at constant time that IBM's Blue Cloud was introduced. Others like Google's Mapreduce, and Microsoft's Windows Azure followed suit one another. computing will bring several edges to the market and three most important areeffectiveness, security and quality.

Cloud Service suppliers (CSP's) are offering cloud platforms for theircustomers to utilize and create their net services, terribly like internet Service suppliers (ISP's) also offer the costumers high speed broadband to access the internet online. CSPs and ISPs every offer services. The clouds are the new trend among the evolution of the distributed systems. Earlier to Cloud we tend to tend to used Grid. In CloudComputing,including the end user does not want data or expertise to control the infrastructure of clouds; it provides only abstraction. These are usually utilized as a service of the online with high quality, higher product, quality of service and high computing power.

Cloud computing suppliers deliver common on-linebusinessapplicationshas three entirely differentServiceModels: coding system as a Service (SaaS), Platform as a service (PaaS), Infrastructure as a service(IaaS).Software as a Service (SaaS) called a deliverymodel where the pc code and thus the data that associated with is hosted over the cloud setting by third party called cloud service provider, rather like your Gmail account, you utilize that application on someoneelse's system. Platform as a Service (PaaS): throughout this service, you will be able to use Web-based tools to develop applications in order that they run on systems program that's provided by another company, like Google AppEngine.

2. RELATED WORK

Reference1. Sameera Almulla, Chan YeobYeun "Cloud Computing Security Management" ,Source:IEEE Xplore.

Cloud computing has monumental prospects, however with equal range of security threats. one among the most important security worries with the cloud computing model is that the multi-tenancy. during this paper, we have a tendency to 1st mentioned numerous models of cloud computing, security problems and analysis challenges in cloud computing. Multi-tenancy is major issue for Cloud Computing Security. There are unit many alternative security challenges that embody security aspects of network and virtualization.

The infinite prospects of cloud computing cannot be unseen just for the safety problems the never-ending analysis and analysis for strong, regular and integrated security models for cloud computing can be the sole path of inspiration. Based on this undeniable fact that the impact of security problems in cloud computing will be diminished by multi-tenancy design. no matter the character of security problems, it will be doubtless complete that the readying of any style of cloud computing ought to contend with the safety issues adore those of the security crucial systems. We believe that because of the quality of the cloud, it'll be troublesome to attain end-to-end security. New security techniques got to be developed and older security techniques area unit required to be radically tweaked to be able to work with the clouds design. we have a tendency to hope our work can give an improved understanding of the planning challenges of cloud computing, and pave the trail for more analysis during this space.

Reference 2. Salim Hariri "CLUSTER COMPUTING JOURNAL"

Cloud computing is developing apace and is often believed to be the long run of the computation world. during this approach, there are unit major issues like security that require to be addressed completely and full so as to spice up this development. AN analysis of the present situation shows that the safety level of gift solutions isn't at the amount that might attract new enterprises and persuade those already learning the technology to migrate from traditional computation technology to cloud computing.

Different file systems have addressed the safety issue by currently, however they are doing not appear to be a convincing resolution to the matter. Even the main systems, like GFS and HDFS, both already in use by the biggest suppliers like Google, seem to be incomplete. In GFS/HDFS architecture, problems like that the Master server stores all the information related to the chunks and kind of like this, lead the complete system to be prone to attacks and failures. Attackers simply got to access to Master server/node server to realize access to information AN HDFS classification system instance needs one distinctive server, the name node. this can be one purpose of failure for AN HDFS installation. If the name node goes down, the classification system is offline and this reduces the system's accessibility rate.

The author's planned model, the partly Distributed classification system with Parity Chunks, addresses all 3aspects of security, together with Confidentiality, Integrity, and Accessibility (CIA). The model is meant during an approach that's versatile and customizable to suit into any condition and any specific client would like whereas keeping the budget at an optimum level. Saving the budget at constant time it supports inexperienced technology; with optimum range of file servers.

Reference 3. Garima Gupta, P.R.Laxmi and Shubhanjali Sharma "A Survey on Cloud Security issues and Techniques"

Cloud computing as a platform for outsourcing and remote process of application and information is gaining speedy momentum. Security concerns; particularly those around platform, information and access; will convince be hurdles for adoption of public and hybrid clouds. during this paper, we've tried to categorize the key issues and discuss the connected technical implications and analysis problems, together with some advanced security problems specific to cloud. we've additionally mentioned some problems concerning security-related restrictive compliance in cloud. in addition, we've bestowed few high-level steps towards a security assessment framework. we have a tendency to created many observations in current cloud security landscape. Firstly, the safety standardization activities, below aegis of the many customary bodies and business forums like CSA, OGF, W3C, SNIA etc. area unit fragmented. Proliferation of open community based mostly identity management solutions additionally makes cloud identity management and integration troublesome. Second, fast provisioning of the users in cloud and mapping of their roles between enterprise and cloud has become somewhat difficult. Third, information anonymization and privacy conserving techniques can increasing assume larger importance and a lot of thought analysis is needed during this space. Fourth, migrating generic in house software package code to public cloud need thorough understanding of potential security risks. Finally, adherence to the restrictive compliance by the cloud suppliers and higher revealing norms from them is imperative for industrial success of cloud.

Reference 4. Sengupta, Vikrant, Vibhu Sharma "Cloud Computing Security- Trends and analysis Directions"

This paper describes a number of the cloud ideas and demonstrates the cloud properties like measurability, platform freelance, low-cost, physical property and responsibilities. though there are unit numerous security challenges in cloud computing however during this paper, we've mentioned a number of them and additionally the techniques to forestall them, they will be wont to maintain the secure communication and take away the safety issues. This survey is largely done to check all the issues like attacks, information loss and unauthenticated access to information and additionally the ways to get rid of those issues. because the cloud computing is dynamic and sophisticated, the normal security solutions provided by cloud atmosphere don't map well to its virtualized environments. On the opposite hand, we have a tendency to observe the virtualization connected security risks aren't specific to cloud, however risks associated with open source shared application server, sound unit and middleware elements undoubtedly are; and a trustworthy Computing Platform to execute / isolate consumer run-times in cloud will certainly facilitate. we have a tendency to believe that this survey, although short, provides a broad-level summary of necessary current and rising security issues in cloud and delineate main analysis challenges. As a succeeding work, a lot of elaborate survey will be undertaken. we have a tendency to additionally attempt to flesh out the assessment framework more, supported by tools – to help migration of enterprise applications to cloud. Organization like Cloud Security Alliance (CSA) and National Institute of Standards and Technology area unit performing on cloud computing security. during this paper we've mentioned a number of security approaches however many alternative approaches, also there that are within the method. Some standards are given which may be wont to maintain secure communication and security during a cloud as several systems communicate in it and perform operations.

Reference5. International Journal of Advanced research in computer Engineering & Technology (IJARCET) Volume seven, Issue 4,April 2018, ISSN: 2278 – 1323.

Virtualized resources within the cloud lower direct investment and products development prices. However, the low price comes with a trade-off. The on top of analysis suggests that it's too oversimplified to look at the cloud as an inexpensive security. Legitimate yet as illegitimate organizations and entities area unit gaining access to information on the cloud through contraband and quasi-legal means that. The cloud's diffusion which of social media have superimposed onto organizations' speedy digitization during a complicated manner that permits cyber-criminals and cyber-espionage networks to use the cloud's weaknesses.

The on top of analysis therefore indicates that making certain that each technological and behavioral /perceptual factors area unit given equal thought within the style and implementation of a cloud network is therefore crucial.

Existing establishments area unit subject to powerful environmental choice mechanisms (Gilson 2001). Existing establishments area unit seemingly to be exposed and restructured to support a replacement set of beliefs and actions and therefore the rules area unit seemingly to be revised. New establishments and therefore the plan of existing establishments area unit required to confront rising security and privacy issues within the cloud business. there's a sign that existing establishments associated with the cloud area unit thickening. during this regard, the war for the long run of security and privacy problems within the cloud is simply starting. robust analysts of cloud security area unit gaining new quality. as an example, a replacement approach of auditing specifically designed for the cloud business is evolving. Overall, it's truthful to mention that privacy and security problems associated with the cloud business area unit undergoing political, social, and psychological metamorphosis.

3. EXISTING SYSTEM

The model bestowed during this paper additionally has implications for management apply and public policy. Most cloud providers' services go with no assurance or promise of a given level of security and privacy. Cloud suppliers lack policies and practices associated with privacy and security. neither is that their solely drawback. Cloud suppliers have additionally incontestable a bent to cut back their liability by proposing contracts with the service provided "as is" with no warrantee (McCafferty 2010). Perception of impotence or insubordination of cloud suppliers could therefore act as a roadblock to organizations' cloud adoption selections. during this regard, on top of analysis indicates that security and privacy measures designed to cut back perceived risk yet as transparency and clear communication processes would produce a competitive advantage for cloud suppliers. The newness and individuality of the cloud usually mean that purchasers wouldn't apprehend what to elicit in investment selections. an understanding of model would additionally facilitate organizations take technological, activity and perceptual/attitudinal measures. The users of the cloud area unit working on the belief that cloud suppliers take privacy and security problems seriously (Wittow& Buller 2010). However, against the scene of the institutional contexts, this could rather be a convenient however presumably false assumption.

The model also results in helpful queries that require to be asked before creating cloud connected investments. Given the institutional and technological atmosphere, potential adopters ought to raise robust inquiries to the seller concerning certification from auditing and skilled organizations (e.g., AICPA), locations of the vendor's information centers, and background check of the vendor's workers, etc.

The on top of analysis counsel that a 1 size fits all' approach to the cloud cannot work. The model bestowed in Figure one would additionally facilitate in creating strategic selections. as an example, organizations could need to build selections regarding combos of public and personal clouds19. as an example, the general public cloud is effective for a company handling high-transaction/low-security or low information worth (e.g., sales division automation). non-public cloud model, on the opposite hand, could also be acceptable for enterprises that face important risk from info exposure like money establishments and health care supplier or bureau. as an example, for medical-practice firms coping with sensitive patient information, that area unit needed to go with the HIPAA rules, non-public cloud could also be acceptable.

In general, legal systems take while to alter (Dempsey-2008). restrictive establishments are associated with liability and alternative problems within the cloud aren't well developed. Cloud suppliers could feel pressures to get endorsements from skilled societies. AICPA's endorsements have driven the diffusion of cloud applications among some certified public accountant companies.

Now a days, accurately or not, businesses area unit involved regarding problems like the privacy, accessibility, information loss (e.g., motion down of on-line storage sites), information quality and possession (e.g., accessibility of information in usable type if the user discontinues the services) (Martin 2010). Cloud supplier's area unit criticized on the bottom that they are doing not answer queries and fail to grant enough proof to trust them (Brodkin 2010)20,21. during this regard, several of the user issues will be addressed.

Since geographic dispersion of information is a crucial issue related to price and performance of the cloud, a problem that deserves mention relates to restrictive arbitrage. consultants expect that countries update their laws on an individual basis instead of to act during a triangular fashion (TR 2010). Economies worldwide vary greatly in terms of the legal systems associated with the cloud. because of the novelty, territorial arbitrage is higher for the cloud compared to the IT business generally. during this regard critics area unit involved that cloud suppliers could store sensitive info in jurisdictions that have weak laws associated with privacy, protection and accessibility of information.

A final issue that deserves mention relates to the impacts of clouds controlled by the developing world players on security problems with industrial countries. it's tempting for world cloud players to use cheaper hosting services in developing countries. Cybercriminals, however, realize it a lot of enticing to focus on wealthy economies. as an example, the U.S. is the No. one target for cyber-attacks. Since several developing countries area unit high law-breaking sources, security risks related to the diffusion of clouds in these countries could unfold to industrial countries.

Techniques to secure data in cloud:

1. Authentication and Identity Authentication of users and even of communicating systems is performed by numerous ways, however the foremost common is cryptography. Authentication of users takes place in numerous ways that like within the style of passwords that's better-known on an individual basis, within the style of a security token, or within the type a measurable amount like fingerprint. One drawback with exploitation ancient identity approaches during a cloud atmosphere is once the enterprise uses multiple cloud service suppliers (CSPs). In such a use case, synchronizing identity info with the enterprise isn't scalable. alternative issues arise with ancient identity approaches once migrating infrastructure toward a cloud-based resolution.

2 Data Encryption: If you're progressing to store sensitive info on an outsized information store then you would like to use encryption techniques. Having passwords and firewalls is sweet, however folks will bypass them to access your information. once information is encrypted in an extensive type that can't be browse while not an encryption key. the information is completely useless to the unwelcome person. it's a way of translation of information into cipher. If you wish to browse the encrypted information, you must have the key or that's additionally known as coding key.

3 Information Integrity and Privacy: Cloud computing provides info and resources to valid users. Resources will be accessed through net browsers and might even be accessed by malicious attacker. A convenient resolution to the matter of data integrity is to produce mutual trust between supplier and user. Another resolution will be providing correct authentication, authorization and accounting controls that the method of accessing info ought to undergo numerous multi levels of checking to confirm licensed use of resources. Some secured access mechanisms ought to be provided like RSA certificates, SSH based mostly tunnels.

4 Availability of Information: Non accessibility of information or data could be a major issue concerning cloud computing services. Service Level agreement is employed to produce the knowledge regarding whether or not the network resources area unit on the market for users or not. it's a trust bond between client and supplier. And to give accessibility of resources is to possess a backup set up for native resources yet as for many crucial info. this allows the user to possess the knowledge regarding the resources even once their inconvenience.

5 Secure Information Management: It is a way of data security for a set of information into central repository. it is comprised of agents running on systems that area unit to be monitored then sends info to a server that's known as "Security Console". the safety console is managed by admin World Health Organization could be a creature World Health Organization reviews the knowledge and takes actions in response to any alerts. because the cloud user base, dependency stack increase, the cloud security mechanisms to unravel security problems additionally increase, this makes cloud security management way more difficult. it's additionally referred as a Log Management. Cloud suppliers additionally give some security standards like PCI DSS. info Security Management Maturity is another model of data Security Management System.

6 Malware-injection attack resolution: This resolution creates a no. of consumer virtual machines and stores all of them during a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operative systems. the appliance that's pass by a consumer will be found in FAT table. All the instances area unit managed and regular by Hypervisor. IDT (Interrupt Descriptor Table) is employed for integrity checking.

4. PROPOSED SYSTEM:

In this paper we are going to know about the big data security issues and challenges. Some of the issues are:

Vulnerability to fake data generation: Before continuing to all or any the operational security challenges of huge information, we must always mention the issues of pretend information generation. To deliberately undermine the stan- dard of your massive information analysis, cybercriminals will fabricate information and pour it into your information lake. For instance, if your producing company uses detector informationtonoticeoutofwhackproductionprocesses, cybercriminals can penetrate your system and make your sensors show fake results, say, wrong temperatures. This way, you'll be able to fail to note ugly trends and miss the chance to resolve issues before serious harm is caused. Such challenges are often resolved through applying fraud detection approach.

Potential presence of untrusted mappers:

Once your massiveinformationiscollected,itundergoesmultiprocessing. One of the methods used here is MapReduce paradigm. When the data is split into numerous bulks, a mapper processes them and allocates to storage options. If associate outsider has access to your mappers' code, they will modification the settings of the prevailing mappers or add 'alien'ones. This way, your processing are often effectively ruined: cy- bercriminals will build mappers turn out inadequate lists of key/value pairs. Which is why the results stated by the scale back method are faulty. Besides, outsiders can get access to sensitiveinformation.

Troubles of cryptographic protection:
Although cryptography could be a well-known manner of protective sensitive info, it is further on our list of big data security issues. Despite the likelihood to cypher massive information and also the essentials of doing thus, this security measure is often ignored. Sensitive information is mostly hold on within the cloud with none encrypted protection. And the reason for acting so recklessly is simple: constant encryption and decryption of huge data chunks slow things down, which entailsthelossofbigdata'sinitialadvantagespeed.

Possibility of sensitive information mining:
Perimeter-based security is often used for giant information protection. It implies that all 'points of entry and exit' square measure secured. But what IT specialists do within your system remains a mystery. Such a scarcity of management at intervals your massive information resolution could let your corrupt IT specialists or evil business rivals mine unprotected informationandsellitforhisorherownprofit.Yourcompany, in its turn, can incur huge losses, if such information relates to new product/service launch, company's financial operations or users' personalinformation.

Struggles of granular access control:
Sometimes, information things fall into restrictions and much no users will see the key information in them, like, personal info in medical records. But some parts of such items could theoretically be helpful for user s with no access tothe secret parts, say, for medical researchers. All the useful contents arehidden.

Absent security audits:

Big datainformationsecurity auditsfacilitate the corporations gain awareness of their security gaps and though it's suggested to perform them daily, this recommendation met rarely. Working with massive information has enough challenges and issues because it is, and an audit would only add to the list. Besides, the dearth of your time, resources, qualified personnel or clarity in business-side security needs makes such audits even a lot of false.

Data provenancedifficulties:
Data provenance is a broad big data concern. From security perspective, it is crucialbecause:

1. Unauthorized changes in metadata can lead you to the wrong data sets, which will make it difficult to find needed information.
2. Untraceable data sources can be a huge impediment to finding the roots of security breaches and fake data generation cases.

E-Discovery Problems: E-discovery refers to the search of electronic data for use as evidence in a legal proceeding. Court and even the Government can order e-discovery in the form of a hacking activity to aid the search of critical evidence. Electronic evidence is much more easily to be searched and collected. However, it is now more difficult to search for electronic evidence because there are lots and lots of data and that it is difficult to comply with legal restrictions. Furthermore,eDiscoveryisnowmoreexpensivethanever.

Privacy Breach: It refers to the release of otherwise private information to persons who should have no access to it, whether it be done deliberately or mistakenly. Privacy breaches occur may occur when a business In this paper we are going to know about the issues of the big data security. We present various security measures which would improve the security of big data environment. Since the Following security measures should be taken to ensure the security in a bigdata.

- RigorousSystemTestingofMapReduceJobs
- FileEncryption

employs weak security measures. Although the hacker is still primarily liable fortheact,itcouldhavebeenpreventedshouldtherehavebeen stricter tools and protocols that safeguard privacy

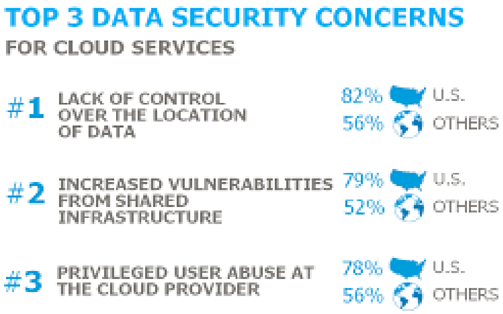
5. PROPOSEDACTIVITIES:

Third Party Secure Data Publication to Cloud and some of the security breaches.Each section performs totally different operations and offers different merchandise for businesses and people round the world. There are unit various security problems for the cloud computing because it encompasses the several technologies which incorporatenetworks, databases, operative systems, virtualization,resourceplanning management, dealingmanagement, concurrency management and memory management. Therefore, security problems for several of those systems and technologies area unit applicable to cloud computing. Information security involves encryptingthe information yet as making certain that acceptable policies area unit implemented for data sharing. The given below area unit the varied security issues during a cloud computing atmosphere.

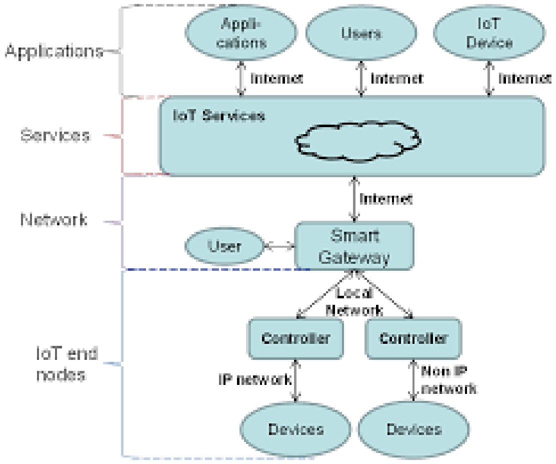
Data Transmission: It is the method of causation digital or analog information over a communication medium one or a lot of computing network. In Cloud atmosphere most of the information isn't encrypted within the intervals. To method information for any application that information should be unencrypted. In similarity coding that permits the information to be processed while not being decrypted. The attack is allotted once the attackers place themselves within the communications path between the users. Here there's the likelihood that they will interrupt and alter communications.

Virtual Machine Security: The term Virtual Machine (VM) describes sharing the resources of single physical laptop into numerous computers at intervals itself. VM’s give gracefulness, flexibility and measurability to the cloud resources by permitting the vendors to repeat, move and manipulate their VM’s. Keeping this in mind, malicious hacker’s area unit finding ways that to urge their hands-on valuable information by manipulating safeguards and breaching the safety layers of cloud environments. The cloud computing situation isn't as clear because it claims to be. The service user has no plan regarding however the information is processed and hold on and can't directly management the flow of information storage and process. Having VM’s would indirectly permits anyone access to the host disk of the VM to require a contraband copy of the complete system.

Information Integrity: Corruption of information will happen at any level of storage. thus, Integrity observation is should in cloud storage. information Integrity during a system is maintained via information constraints & transactions. Transactions ought to follow ACID (atomicity, consistency, isolation, durability). information generated by cloud computing services area unit unbroken within the clouds. Keeping information within the clouds, users could lose management of their information and accept the cloud operators to enforce access management.



Data Location Cloud users aren't tuned in to the precise location of the information center and additionally they don't have any management over the physical access thereto data. Most of the cloud suppliers have data centers round the world. In several countries sure varieties of information cannot leave the country as a result of doubtless sensitive info. Next within the quality chain there are unit distributed systems during which therearea unit multiple databases and multiple applications.



6. REFERENCES:

[1] Sameera Almulla, Chan YeobYeun "Cloud Computing Security Management" ,Source:IEEE Xplore. Proc. 2009 ACM Workshop on Cloud Computing Security (CCSW '09), pp. 85-90, 2009.

[2] Salim Hariri "CLUSTER COMPUTING JOURNAL"] https://cloudsecurityalliance.Org/download/the-notorious-nine-cloud-computing-top -threats-in-2013, Feb. 2013.

3] Garima Gupta, P.R.Laxmi and Shubhanjali Sharma "A Survey on Cloud Security issues and Techniques" Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[4] Sengupta, Vikrant, Vibhu Sharma "Cloud Computing Security- Trends and analysis Directions" Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.

[5] International Journal of Advanced research in computer Engineering & Technology (IJARCET) Volume seven, Issue 4,April 2018, ISSN: 2278 – 1323.

[6] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: Theory and implementa tion,” Cryptology ePrint Archive, Report 2008/175, 2008.

[7] Qian Wang, Cong Wang, KuiRen, Wenjing Lou, and Jin Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", To appear, IEEE Transactions on Parallel and Distributed Systems (TPDS), Vol. 22, No. 5, pp. 847-859, May, 2011.

[8] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www. cloudsecurityalliance.org.

[9] R. C. Merkle, “Protocols for public key cryptosystems,” in Proc. of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.

[10] Y. Zhu, G.J. Ahn, H. Hu, S.S. Yau, H.G. An, and C.J. Hu, “Dynamic Audit Services for Outsourced Storages in Clouds,” IEEE Trans. Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013.