INTELLIGENCE BASED AUTHENTICATION - AUTHORIZATION AND AUDITING FOR SECURED DATA STORAGE

G.Ranjith[1], J.Vijayachandra[2], P.Sagarika[3] and B.Prathusha[4]
[1] HOD & Assistant Professor, [2]Assistant Professor,
Department of Computer Science & Engineering,
Warangal Institute of Technology and Science, Warangal, Telangana, India.
[3,4]M.Tech Student, Department of Computer Science & Engineering,
Warangal Institute of Technology and Science, Warangal, Telangana, India.

ABSTRACT

Cloud computing and Big Data Analytics stores a large quantity of data, which provides scalable computing storage, where user does not have any information where his data is stored but user can access the data which is remotely stored in different data centres all over the world. In this paper we discussed the quality of service for secured cloud system model. We focused on the role of Third Party Auditor (TPA) and Intelligence based security system auditing with CIA Triad and AAA security management to protect data in cloud against exploitations, by providing fault tolerance. Cloud computing has become prominent of its on-demand network access and scalability that is pay as you use. We concentrated on privacy preserving public auditing procedures and algorithms that support regenerating code based data storage which facilitates the auditing scheme that includes setup, audit and repair. We discussed risks, threats and attacks that prevent the auditor from detecting the data losses and corruption. We focus on evaluating the performance based on time and computational complexity using Testing Tools. We proposed public auditing scheme for regenerating code based data storage. The mathematical approach for regenerating code and auditing procedures are given and construction of dynamic data verification system for auditing scheme is generated and proved.

KEYWORDS: *Threats, Auditing, Cloud Storage, Security, Data Recovery& Privacy.*

I. INTRODUCTION

Cloud Computing is a distributed computing paradigm which provides scalable storage resources, where measured services are provided similar to electricity and telephone utilities. The services provided by the Cloud Computing are Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It provides flexible measured service and on-demand data storage services which benefits the cloud user and provides relief from the burden of data storage and management. A number of dynamics such as software interoperability standards, virtualization technologies, high-band width communications, delivery of enterprise applications, data storage centres and web services contributed to the emergence of cloud computing [1].

Cloud Computing attracts an excessive consideration and participation of researchers all over the world to support software industry and business world in securing clouds as most talented and emerging paradigm which provides open and distributed system scalable services over the internet where there are great risks, threats, vulnerabilities and attacks by intruders. Cloud computing offers flexibility which is developing very fast, it facilitates the employees work from where they want, it provides a completeservicewhich contains Infrastructure, Platform and Software. It provides flexibility to employees where they can work outside the office. Elasticity on demand self service is the key elemental feature of cloud computing as it enables the ability to dynamically add or remove virtual machine instances when workload changes. Virtualization is a consolidation of hardware and software where effective virtualized resource management is still one of the most challenging tasks.

Virtualization can optimize resource sharing among applications hosted in different virtual machines to better meet their resource needs. When the workload of a service increases rapidly, the performance decreases, hence monitoring is necessary to check the quality of service of cloud computing [14].
Cloud computing allows more open accessibility from various client devices, which provides easier and improved data sharing. Data is uploaded into a cloud via internet and stored in large data centres, for access by users from the data centre. Security is a major Issue; these mainly deal with Authorisation and secured access control, Authentication and Identification of user, protecting data at rest or transit increases confidentiality, and control management. Cloud storage in cloud environment is different comparing with other architecture where the user data is transferred to huge data centres, which is remotely located, on which user does-not have any control, so cloud provider takes the responsibility for securing of data storage, as it's a difficult task to monitor continuously to protect data from malicious attackers, malwares and stealth viruses. So the responsibility will be handover to a Third Party Auditor [2].
In the Related work we given the description about the security approaches, risks, threats and attacks in cloud computing and the requirement for auditing as the user will not have any idea where his data is stored. The importance of auditing and duties and responsibilities along with the role of third party auditor is discussed. Algorithmic and Mathematical Approach towards the auditing for security of data in cloud storage is given. Finally the Experiment Analysis is given along with the result and discussion.

II. RELATED WORK

Security approaches should be pragmatic in terms of security controls and system functionality. Prevention is ideal but detection is must, however detection without response is useless. The risk is a function of threats as they seek to exploit vulnerabilities, technology is critical and having a robust architecture is a must in order to protect against the threats and in light of counter measures, we apply to protect our assets. Security controls such as CIA Triad and AAA Security management design elements protects the cloud platform and databases [3].
Cloud Malware injection attack is a web based attack, refers to manipulated copy of the victims service instance, uploaded by attacker to cloud, where attacker injects the malicious code. Once the injection is completed, the malicious code is executed where the attacker exploits cloud privileged access capabilities in order to attack the security service domain. SQL injection is the web attack mechanisms used to steal data from cloud by hackers. It is a technique which attempts to pass SQL Commands to connect with back end database. Generally it is used to break the web security in cloud at login page where user name and password will be recognized by the SQL Injection.
XML signature defines XML syntax for digital signature which is a wrapping attack; it is used by various web technologies such as SOAP, SAML and others [4]. The attack is done during the translation of Simple Object Access Protocol (SOAP) message between a legitimate user and the web server which allows programs that run on disparate operating systems to communicate Hyper Text Transfer Protocol (HTTP) and its Extensible Mark-up Language (XML). The attack is done by duplicating the user's account and password in the login period, the hacker embeds a bogus element(the wrapper) into the message structure, moves message with malicious code and then sends the message to the server. Since the original body is still valid, the server will be tricked into authorizing the message that has actually been altered. As a result, the hacker is able to gain unauthorized access to protected resources and process the intended operations.
The major security risks faced by web applications in cloud computing are [5]

- Injection flaws like SQL, OS and LDAP injection
- Cross-site scripting
- Broken Authentication and session management
- Insecure direct object references
- Cross-site request forgery
- Security mis-configuration
- Insecure cryptographic storage
- Failure to restrict URL access
- Insufficient transport layer protection

- Invalidated redirects and forwards

An Information system security policy addresses the critical Issues based on CIA Triad that is Confidentiality, Integrity and Availability where as AAA concept issues are Authentication and Identification, Authorization and Auditing. Confidentiality of data in cloud storage is preventing the un-authorized disclosure of information at rest or transit. The key responsibilities of the Integrity are validating the data origin, Detecting the alteration of data, determining whether the data origin is changed and Recovery from detectable errors and data losses. Availability is concerned with denying illegitimate access to computing resources and preventing external risks, threats and attacks. Authentication is the process of identification it says who u are and the Authorization is the process of verifying, it says what are your permissions to use utilities. Auditing is an inspection, verification or systematic examination regarding storage in cloud computing.

III. THIRD PARTY AUDITOR

The audit in cloud computing is broadly classified into three, they are first party auditor or internal auditor where the cloud user organization audits by its own, it is a self-assessment procedure for intrusion detection and prevention system. Second party auditor is a Cloud Service Provider who has significant resources and experts in building and managing distributed cloud storage servers, owns and operates where an external auditing procedure is used for data security and quality management in cloud services. The Cloud data storage architecture consists of three actors, the cloud user who has large amount of data to be stored and retrieved as per the requirement in the cloud. The cloud service provider who maintains the cloud storage services and provides cloud data storage. To enable privacy preserving public auditing for cloud data storage shown in the model, the protocol we designed should achieve the following prevention, protection and performance guarantees;

1. **Storage accuracy**: To ensure that the users data are indeed stored appropriately and kept all the time in cloud.
2. **Reliable Security:** To ensure that the TPA cannot gain users data from the information collected during the auditing process.
3. **Group auditing**:To enable TPA provide secure and efficient auditing to possible large number of different users simultaneously
4. **Detection and Prevention:** To allow TPA to provide auditing with minimum communication.

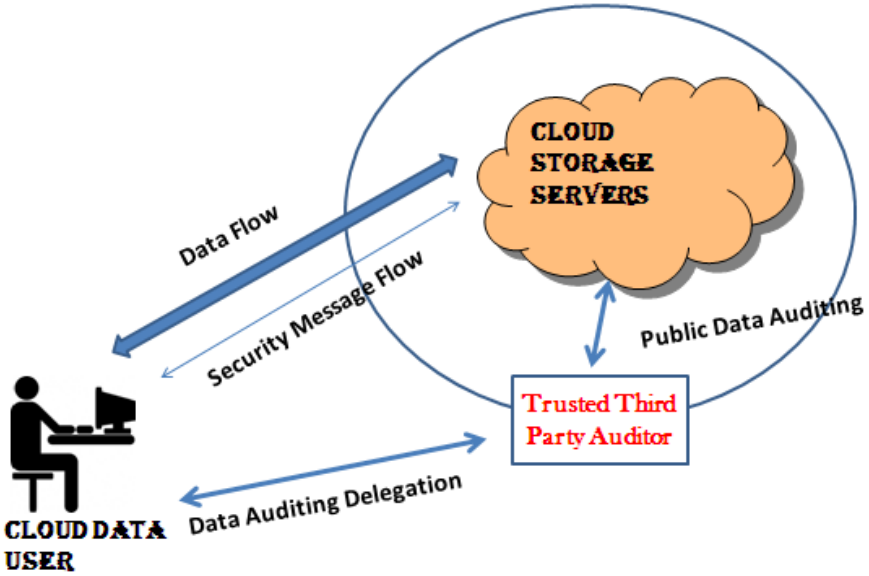

Figure 1: The Architecture of Cloud Data Storage Services

The Trusted Third Party (TTP) is an audit based organization which facilitates secure interactions between two parties that is cloud user and cloud provider, where both of them trust this third party. The Third Party Auditor (TPA) registered security service provider allocated by the cloud service provider with strong Authentication and Authorization. The TPA can perform Multiple Auditing

Tasks for single or multiple clouds in branch manner for better efficiency and security [6]. Public audit-ability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

IV. ALGORITHMIC APPROACH

Authentication, Authorization and Auditing for secure cloud storage is implemented on the basis of the following key points

- Our System Supports an External auditor to audit users outsourced data in the cloud without learning knowledge on the data content.
- The TPA supports scalable on request by cloud service provider for efficient public auditing in the cloud computing
- Auditing is the processes which is done for the cloud to achieve batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA
- The auditing is the intelligence based Dynamic data process for the data and information security in cloud computing
- data integrity algorithm such as Message Authentication Code (MAC code) by means of Hash Based Message Authentication Code (HMAC code) to check the integrity of the data being stored in the cloud.
- By means of MAC code, we enhance the data integrity of the cloud data.

Step 1: Start of an Algorithm
Step 2: Key Generation by **Advanced Encryption Standard (**AES) Algorithm
16-bit Hexa Decimal keys are generated
Step 3: Map the Key to the files
Step 4: Divide the files into the blocks
Step 5: Each Encrypted Block is Associated with Key
Step 6: Store the data blocks to the Cloud Storage Server
Step 7: Simultaneously Intelligent system sends a copy of keys to TPA
Step 8: On request of Cloud Service Provider (CSP) the Auditing processes with be done by TPA
Step 9: Validate the data by signatures and data integrity proofs
Step 10: Successful validation, verification will be done for dynamic auditing by TPA
End of Algorithm.

V. MATHEMATICAL APPROACH

The Auditing procedure for the cloud Service Server (CSS) done by the Third Party Auditor (TPA) where the verification is done to direct, trust worthy and real-timed intelligence based in requirements of cloud user, On request for support to data protection mechanism deployed by the Cloud Service Provider(CSP)[7].

The Audit Process is divided into three phrases Setup, Audit and Repair

Setup:

The audit scheme related parameters are initialized in this procedure.

A) KeyGeneration: Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system,

i. Choose a cryptographic hash function H.In the original DSS, H was always SHA-1, but stronger has h functions from the SHA family are also in use. Sometimes the output of a newer hash function is truncated to the size of an older one for compatibility with existing key pairs.
ii. Decide on a key length L. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024(inclusive). Later, FIPS-186-1, change notice 1 specifies that L should always be 1024.
Later yet, NIST 800-57 recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010(or 2030).
iii. Choose a prime q with the same number of bits as the output of H.
iv. Choose a L-bit prime p such that p-1 is a multiple of q.

v. Choose g, a number whose multiplicative order modulo p is q. This may be done by setting g=h (p-1)/q mod p for some arbitrary h (1< h < p-1) and trying again if the results comes out as 1. Most choice of h will lead to usable g, commonly h=2 is used.

The algorithm parameters (p, q and g) may be shared between different users of the system. The second phase computes private and public keys for a single user.

i. Choose x by some random method, where 0 < x <q.
ii. Calculate $y=g^x$ mod p.
iii. Public key is (p, q, g, y). Private Key is x.

The forthcoming FIPS 186-3 uses SHA-224/256/384/512 as the hash function, q of size 224 and 256 bits and L equal to 2048 and 3072, respectively,

The exist efficient algorithms for computing the modular exponentiations h^a mod p and g^x mod p.

B) Signing:

i. Generate a random per-message value k where 0 < k< q.
ii. Calculate r = (gk mod p) mod q.
iii. Calculates = (k^{-1} (H (m) +x^{*r})) mod q.
iv. Recalculate the signature in the unlikely case that r = 0 or s = 0.
v. The signature is (r, s).

The extended Euclidean algorithm can be used to compute the modular inverse k^{-1} mod q.

Auditing:

i. Reject the signature if either 0 < r < q or 0 < s < q is not satisfied.
ii. Calculatew = $(s)^{-1}$ mod q
iii. Calculateu1 = (H $(m)^*$w)mod q
iv. Calculateu2 = (r*m) mod q
v. Calculatev = ((g^{u1*u2}) mod p) mod q
vi. The signature is valid if v = r.

DSA is similar to the EIGamal signature scheme.

Repair:

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. First, if g = $h^{(p-1)/q}$ mod p it follows that g^q = h^{p-1} =1 (mod p) by Fermat's little theorem. Since g > 1 and q is prime, g must have order q.

The signer Computes,

S = k ^ {-1} (H (m) + xr) \mod {q}

Finally, the correctness of DSA follows from

r = (a ^ k \mod q = (q ^ {u1} v^ {u2} \mod p) \ mod q=v)

VI. EXPERIMENTAL APPROACH

Our Experiment supports an External Auditor for processing the auditing mechanisms that happens between a dedicated Cloud Service Provider and cloud user. The TPA may concurrently handle multiple auditing upon different Cloud Service Providers request. In this Experiment we are using Simulation software which is based on process of real phenomenon with a set of mathematical formulae's. This software provides the simulated environment that is similar to real world environment. Simulation software is designed in a manner so that result should be close to real world. Discrete Event and Continuous simulation are the two categories of simulation package. The Simulation software used in the Experiment is the Cloud Sim Tool Kit for simulation of cloud computing scenarios.

The Cloud Sim Supports for modelling and simulation of large scale cloud computing infrastructure, including data centres on a single physical computing node. It provides availability of virtualization engine, which aids in creation and management of multiple, independent and co-hosted virtualized services on a data centre node. Virtualization technologies with multi-tier architecture are maintained by the virtual machines in cloud data centres [13]. It also provides the basic classes for describing data centres, virtual machines, applications, users, computational resources and policies (e.g., Scheduling and Provisioning). Multiple virtual machines (VM) share the same physical resources (e.g., CPUs, caches, DRAM, and I/O devices), each application should be allocated to an

independently managed VM and isolated from one another. The security vulnerability caused by competition between virtual I/O workloads that is by leveraging the competition for shared resources, an adversary could intentionally slow down the execution of a targeted application in a VM that shares the same hardware [15].

Modelling the Cloud

- **Data Centre**
  - Models the core infrastructure level services (hardware)
  - Composed of set of hosts which is responsible of managing VMs during their life cycles.
- **Host**
  - Components that represents a physical computing node in a cloud
  - Assigned a pre-configured processing capability, memory storage and a scheduling policy for allocating processing cores to virtual machines.
- **Virtual Machine**
  - Models a Virtual machine
  - Host can simultaneously instantiate multiple VMs and allocate cores based on pre-defined processor sharing policies(Space Shared, Time-shared)
- **Cloud Let**
  - Models the cloud based application services which are commonly deployed in the data centres.
  - Every application has a pre-assigned instruction length
  - Speed measured on MIPS (Million Instruction Per Second)
- **Cloud Let Scheduler**
  - Determines how the available CPU resources of virtual machines are divided among cloud lets.
  - Two Types of polices are offered:
    - Space-Shared (Cloud Let Scheduler Space Shared)
    - Time-Shared(Cloud Scheduler Time Shared)
- **Virtual Scheduler**
  - Determines how processing cores of the host are allocated to virtual machines
  - The policy takes into account
    - How many processing cores will be delegated to each Virtual Machine
    - How much of the processing core's capacity will effectively be attributed for a given Virtual Machine.

The Steps Involved in Experiment using Cloud Sim

1. Initialize Cloud Sim Package
2. Creation of Data Centres
3. Creation of a Broker
4. Virtual Machines are Created
5. Cloud Let are Created
6. Auditing Process Starts
7. Setup the Computational Complexity
8. Audit Computational Complexity
9. Repair Computational Complexity
10. End of Auditing Process – The Performance Result is shown.

The Experiment is done using Java Eclipse As the First Module has 4 options where the file can be uploaded for process then it will be split into different parts as per the requirement based on the size using the intelligence system concepts and these parts are considered as tokens and each part of data is encrypted along with the key generation and these keys will be stored to third party auditor so that as per the requirement the auditing process will be completed according to the request of the Cloud Service Provider. The next step is data encryptionand encrypted data is stored in the cloud which is most secured.

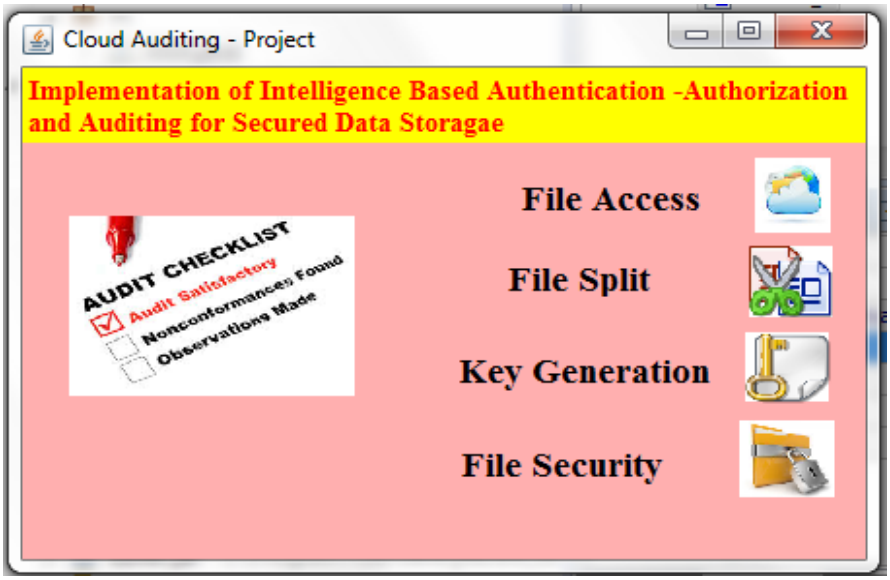

Figure 2: Screen shot of the Cloud Auditing procedure for Secured Cloud Data Storage

In the next module the encrypted data is sent to the cloud server based on the IP Address of the Cloud Storage, and the Keys are sent to the Third Party Auditor for verification and auditing process based on the IP Address of the TPA. Here in this experiment as we are using the simulation process for evaluating the project the IP Address are given as the local host addresses. The Auditing processes will be done by comparing the keys with the TPA and the Encrypted data tokens and keys in the Cloud Storage Server. If the Client was to update or modify the data, the data will be stored in the previous procedure but the unwanted keys and tokens will be removed for the cloud storage and replaced with the new keys and tokens, whereas the same procedure will be followed towards the keys with the Third Party Auditor [12].

VII. RESULT AND DISCUSSION

The Setup phase we mainly measure the time cost of the block and authenticator generation utilizing authenticator generation methods with variable s=60, 80,100,120,180.
Regenerating code based cloud storage with parameters (n, k, l, α, β) where $(\alpha \leq l \leq \beta)$.
The parameters $(n = 20, k= 5, l = 5, \alpha = 1, \beta = 5)$.
As per our experiment the original file is divided into n blocks and encoded into $n\beta$ coded blocks that is 20x5=100.Where n is number of blocks, s is segments in block, K is Key Gen , l is length of block, α and β are parameters.

	Without audit	With audit and recovery
S=60	7966 ms	7994 ms
S=80	10642 ms	10653 ms
S=100	13296 ms	13301 ms
S=120	15022 ms	158807 ms
S=160	21284 ms	21305 ms

The result obtained after the experiment

The final result as per the experiment the Third Party Authenticator can be detect the corrupted data base in cloud server is 99% where the recovery or regenerating the code is 95%.The extensive security and auditing analysis views highly efficient and feasibly integrated regenerating data losses in cloud storage.

VIII. CONCLUSION

To secure clouds from malicious attacks, malwares and stealth viruses a continuous monitoring system and auditing process based on intelligence system is developed [8]. Although cloud computing

is a new phenomenon, it is emerging at a rapid growth, where security issues are becoming challenge. The system we developed is used for auditing process for privacy preserving in cloud storage. For example A and B work together as a group and share a file in the cloud. The shared file is divided into a number of small blocks, which are independently signed by users. Once the block in his shared file is modified by a user, this user needs to sign the new block using his public/private key pair. The TPA monitors all such actions done by A and B [9]. Even the data sharing in cloud computing will be auditing by the TPA. The Advances in the Cloud computing are very much useful to the society and the cloud users where these practical applications need the privacy and authentication as e-commerce and smart gird technologies are improving their quality of service very vastly [10].

IX. FUTURE WORK

Data Redundancy is one of the major problem that the cloud computing is facing. It is known that many storage nodes are filled with the replication of data in cloud computing, more and more data intensive applications are developed in this computing environment. The data-intensive applications devote most of their execution time in disk Input and output for processing a large volume of data. So the Complexity of Time and Space are important to improve the performance of the Cloud storage [11].

REFERENCES

[1]. Peter M. Mell; Timothy Grance, "The NIST Definition of Cloud Computing," *Special Publication (NIST SP)* - 800-145, pp.1-7, September 28, 2011.

[2]. J.Vijaya Chandra, Dr.NarasimhamChalla, Dr.SaiKiranPasupuleti, Dr.K. ThirupathiRao, Dr.V.Krishna Reddy, "Numerical Formulation and Simulation of Social Networks Using Graph Theory on Social Cloud Platform," pp. 1253-1264, *Global Journal of Pure and Applied Mathematics*, Volume 11, Number 2(2015).

[3]. J.Vijaya Chandra, Dr. NarasimhamChalla and Dr.Mohammed Ali Hussain,"Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing", pp.7755-7768,*International Journal of Applied Engineering Research*, Volume 9,Number 20(2014).

[4]. Ahmed Patel, Mona Taghavi, KavehBakhtiyari, JoaquimCelestino Junior, "An Intrusion detection and Prevention System in Cloud Computing: A Systematic review", *Journal of Network and Computer Applications*, Vol. 36(1), pp 25–41, January 2013, ELSEVIER, ISSN: 1084-8045.

[5]. DimitriosZissis, DimitriosLekkas, "Addressing Cloud Computing Security issues", *Future Generation Computer Systems*, Vol. 28(1), PP 583-592, ELSEVIER, 2012, North Holland, ISSN: 0167-739X.

[6]. Jian Liu; Kun Huang; Hong Rong; Huimei Wang; Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol.10, no.7, pp.1513,1528, July 2015.

[7]. Chang Liu; Jinjun Chen; Yang, L.T.; Xuyun Zhang; Chi Yang; Ranjan, R.; Rao, K., "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," *IEEE Transactions onParallel and Distributed Systems*, vol.25, no.9, pp.2234,2244, Sept. 2014.

[8]. Jenn-Wei Lin; Chien-Hung Chen; Chang, J.M., "QoS-Aware Data Replication for Data-Intensive Applications in Cloud Computing Systems," *IEEE Transactions onCloud Computing*, vol.1, no.1, pp.101,115, Jan.-June 2013.

[9]. Boyang Wang; Baochun Li; Hui Li "Oruta: privacy-preserving public auditing for shared data in the cloud", IEEE Transactions onCloud Computing, page(s): 43 - 56 Volume: 2, Issue: 1, Jan.-March 2014.

[10]. Xinyi Huang; Liu, J.K.; Shaohua Tang; Yang Xiang; Kaitai Liang; Li Xu; Jianying Zhou "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", *IEEE Transactions on Computers*, page(s): 971 - 983 Volume: 64, Issue: 4, April 1 2015.

[11]. Gaofeng Zhang; Xiao Liu; Yun Yang "Time-Series Pattern Based Effective Noise Generation for Privacy Protection on Cloud", *IEEE Transactions on Computers*, page(s): 1456 - 1469 Volume: 64, Issue: 5, May 2015.

[12]. Cong Wang; Chow, S.S.M.; Qian Wang; KuiRen; Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Transactions on Computers*, vol.62, no.2, pp.362,375, Feb. 2013.

[13]. Haikun Liu; Bingsheng He, "VMbuddies: Coordinating Live Migration of Multi-Tier Applications in Cloud Environments," IEEE Transactions on Parallel and Distributed Systems, vol.26, no.4, pp.1192,1205, April 1 2015.

[14]. Jinzhao Liu; Yaoxue Zhang; Yuezhi Zhou; Di Zhang; Hao Liu, "Aggressive Resource Provisioning for Ensuring QoS in Virtualized Environments," IEEE Transactions on Cloud Computing, vol.3, no.2, pp.119,131, April-June 1 2015.

[15]. Chiang, R.C.; Rajasekaran, S.; Nan Zhang; Huang, H.H., "Swiper: Exploiting Virtual Machine Vulnerability in Third-Party Clouds with Competition for I/O Resources," IEEE Transactions on Parallel and Distributed Systems, vol.26, no.6, pp.1732,1742, June 1 2015.

AUTHORS

Gyaderla Ranjith is a Post Graduate in Master of Technology from J.N.T University, in Computer Science and Engineering. Having Teaching Experience of 05 years, He is actively involved in teaching Theory of Computation, Computer programming languages, Object oriented concepts and Computer Networks. He published 5 Research papers at International Journals, Member of IACSIT and at present Working as Asst Professor & HOD, Department of Computer Science and Engineering, Warangal Institute of Technology and Science, Oorugonda(V), GudepaduX Roads, Atmakur(M), Warangal-506342.

Jadala Vijaya Chandra, obtained M.TECH in computer science & Engineering from JNTU, Hyderabad and Pursuing Ph.D from K.L. University. His Research Area is Cloud Security. Published 5 Research Papers for International Scopus Indexed Journals and 5 International Conferences& 6 National Level Conferences and attended 10 workshops. He has rich experience of over 14 years in computer operations, maintenance, Project Management, and Computer Education in reputed organizations. At present he is working as Assistant Professor, Warangal Institute of Technological sciences, Affiliated to Kakatiya University.

Pochala Sagarika is M.TECH student CSE(SE) worked as a software engineer at Open Origin IT Solutions , Amplus Solutions, Sholey IT Solutions. Interested areas of research are Network Security and Cloud Security at present Pursuing M.TECH at Warangal Institute of Technology and Science, Oorugonda(V), GudepaduX Roads, Atmakur(M), Warangal-506342.

Bonagani Prathusha is M.TECH student Computer Science and Engineering, specialization at Software Engineering at Warangal Institute of Technology and Science, Oorugonda(V), GudepaduX Roads, Atmakur(M), Warangal, Affiliated to Kakathiya University. Interested research areas are Artificial Intelligence, Data Mining and Data Warehousing and Cloud Computing.