ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Protection of Outsourced Data Using Remotely Verifying Integrity of Regeneration Codes Approach in Cloud Computing

Srinivasa Rao Vykuntam
M.Tech (Software Engineering),
Department Of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement (sistam), Srikakulam.

Mula.Sudhakar
Assistant Professor,
Department Of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement (sistam), Srikakulam.

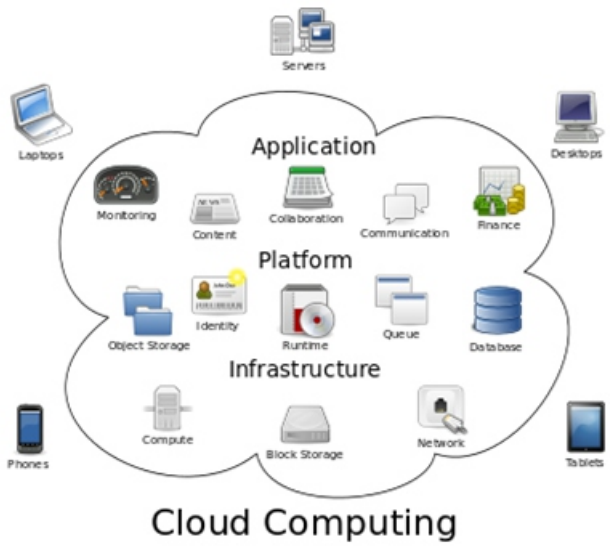
Abstract:

Cloud computing is is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.In cloud service providers there are so many security methods to secure confidentiality, integrity, and authentication of the data and users. In traditional methods the data storing in multiple databases but this process is very complex. Which means retrieving the content from multiple databases are very complex task. It reduces the performance of the system and increases burden to all servers which is storing the data blocks. So we introduced a novel framework which consists of symmetric cryptographic algorithm and a novel verification algorithm. For verification of the data in server we propose error estimation rate technique in bit level.

Keywords: Cloud computing, Communications, Nodes, security, Data Integrity, cryptographic algorithm.

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Broad network access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling:

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity:

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service:

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Data Integrity and security Issues in Cloud computing: The six issues that must be addressed are:

1.Breach notification and data residency.

2.Data management at rest.

3.Data protection in motion.

4.Encryption key management.

5.Access controls.

6.Long-term resiliency of the encryption system.

Breach notification and data residency:

Not all data requires equal protection, so businesses should categorise data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions.

Experts also recommends that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities. The plan should take stakeholders into account, such as legal, contract, business units, security and IT.

Data management at rest:

Businesses should ask specific questions to determine the cloud service provider's (CSP's) data storage life cycle and security policy.

Businesses should find out if:

Multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants. Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions. Storage used for archive and backup is encrypted and if the key management strategy include a strong identity and access management policy to restrict access within certain jurisdictions.Experts recommends that businesses use encryption to implement end-of-life strategies by deleting the keys to digitally shred the data, while ensuring that keys are not compromised or replicated.

Data protection in motion:

As a minimum requirement, Experts recommends that businesses ensure that the CSP will support secure communication protocols such as SSL/TLS for browser access or VPN-based connections for system access for protected access to their services.

The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data is unencrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In IaaS, Experts recommends that businesses favour CSPs that provide network separation among tenants, so that one tenant cannot see another's network traffic.

Encryption key management:

Enterprises should always aim to manage the encryption keys, but if they are managed by acloud encryption provider, Experts says they must ensure access management controls are in place that will satisfy breach notification requirements and data residency.

If keys are managed by the CSP, then businesses should require hardware-based key management systems within a tightly defined and managed set of key management processes.When keys are managed or available in the cloud, Experts says it is imperative that the vendor provides tight control and monitoring of potential snapshots of live workloads to prevent the risk of analyzing the memory contents to obtain the key.

Access controls:

Experts recommends that businesses require the CSP to support IP subnet access restriction policies so that enterprises can restrict end-user access from known ranges of IP addresses and devices.

The enterprise should demand that the encryption provider offer adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network and maintenance.

Businesses should also require:

Logging of all user and administrator access to cloud resources, and provide these logs to the enterprise in a format suitable for log management or security information and event management systems.

The CSP to restrict access to sensitive system management tools that might "snapshot" a live workload, perform data migration, or back up and recover data.That images captured by migration or snapshotting tools are treated with the same security as other sensitive enterprise data.

Longterm resiliency the encryption system:

Experts recommend that businesses understand the impact on applications and database indexing, searching and sorting. They should pay specific attention to advanced searching capabilities, such as substring matching functions and wildcarding such as "contains" or "ends with".

If the encryption vendor offers options for "function preserving encryption" — for example, to preserve sort — regulations may require the use of standardised and approved algorithms or proof of independent certification for the potentially weakened encryption.

Existing System:

We consider the problem of checking the integrity of static data, which is typical in long-term archival storage systems. This problem is first considered under a single serverscenario by Juels and Kaliski and Ateniese et al. giving rise to the similar notions POR and PDP respectively.

A major limitation of the above schemes is that they are designed for a single-server setting. If the server is fully controlled by an adversary, then the above schemes can only provide detection of corrupted data, but cannot recover the original data.

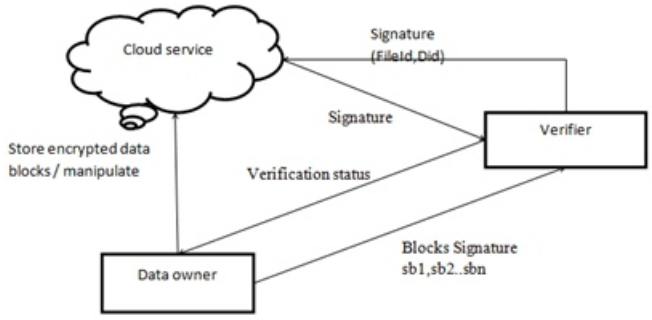
This leads to the design of efficient data checking schemes in a multi-server setting. By striping redundant data across multiple servers, the original files can still be recovered from a subset of servers even if some servers are down or compromised.

Efficient data integrity checking has been proposed for different redundancy schemes, such as replication, erasure coding and regenerating coding.

Proposed System:

Apart from the existing system we designed a new architecture avoiding multiple servers.
The architecture is shown below:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal



In our work data owner store the data in the form of blocks for providing security to data in the cloud service. Data owner encrypts data by using the quad lattice transformation as shown below:

Step 1: A square grid of required size is constructed bytaking the binary data from source file.

Step 2: Now grid transposition is applied by reading dataas various circles starting from the center of thegrid to the bottom left at various levels andwriting it down on columnar basis from top left tobottom right.

Step 3: A secret key that varies with each session ascombination of 0's and 1's is generated based onthe grid size, say 160 – bit for 32 – sized, 384 –bit for 64 – sized etc., to produce decimalsequence. Accordingly columnar transposition isdone on the grid.

Step 4: A new grid is generated after transposition.

Step 5: The new grid is converted into ASCII sequenceand written to another file called encrypted file.

Step 6: Steps 1 to 5 are repeated until the total file isformed into grids and encrypted. Padding witho's is done in grid formation deficiency.

Step 7: Key generated for each file is encrypted with thepublic key of sender using Prenominal Prime number Algorithm. Thistechnique of hiding the key is called keywrapping.

Step 8: The encrypted key is then divided into variousblocks and appended to file.

Hence the new encrypted file with wrapped key isgenerated.

Pre nominal Prime number Algorithm:

1. Assume any two prime numbers P , Q
2. Calculate N = P * Q
3. Calculate Z= Φ(N) = Φ (P * Q)
= Φ (P) * Φ (Q) (According to
modular arithmetic)
= (P-1) * (Q-1)
4. Assume a value 'e' i.e. relatively prime to Z and
e < Z and gcd (e , Z) = 1
5. Calculate d, such that e * d 1 (mod Z) 1
(mod Φ(N))
6. Cipher (C) = (m ^ e) mod N
Plaintext (m) = (C ^d) mod N

Thus our key generated is both complex and secure.

Signature Generation algorithm:

Step1: Given input file F
Step2: F=Binary(F);
Step3: For every binary string of character and we convert that binary into signature as shown below:
Consider the string is 1010111
Replace 1 with +1 and 0 with -1
Then the input string changed to +1-1+1-1+1+1+1
Add these converted string values results 3. In this way convert all binary strings as shown above. Finally some group string is formed as signature.

Data owner sends the encrypted data to cloud and generated signature to auditor. Then the verifier verifies the signature based on the signature received from the data owner, and the cloud. The verifier sends verification status to data owner.

CONCLUSION:

In our work we implemented quad a novel architecture that consists of the secure cryptographic algorithm and secure signature generation algorithm. This method reduces the processing time and the burden to the server.

Instead of regenerating the data from the cloud we designed novel and efficient method to store data instead of maintaining multiple servers. Compared to traditional methods the data will manipulate by the data owner by authenticating the data owner by random code generation method.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

References:

[1] Henry C.H. Chen and Patrick P.C. Lee, Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the-Cloud," Proc. 10th Int'l Conf. Applied Cryptographyand Network Security (ACNS'12), pp. 507-525, June2012. [3] G. Ateniese, R. Di Pietro, L. V. Mancini,and G. Tsudik. Scalable and EfficientProvable Data Possession. In Proc of SecureComm, 2008.

[4] G. Ateniese, S. Kamara, and J. Katz.Proofs of Storage from HomomorphicIdentification Protocols. In Proc. of ASIACRYPT, 2009.

[5] K. Bowers, A. Juels, and A. Oprea. HAIL:A High-Availability and Integrity Layer forCloud Storage. In Proc. of ACM CCS, 2009.

[6] K. Bowers, A. Juels, and A. Oprea. Proofsof Retrievability: Theory and Implementation.In Proc. of ACM CCSW, 2009.

[7] B. Chen, R. Curtmola, G. Ateniese, and R.Burns.Remote Data Checking for NetworkCoding-Based Distributed Storage Systems.InProc. of ACM CCSW, 2010.

[8] R. Curtmola, O. Khan, and R. Burns.Robust remote data checking.In Proc. of ACMStorageSS, 2008.

[9] Y. Dodis, S. Vadhan, and D. Wichs.Proofsof Retrievability via Hardness Amplification.In Proc. of TCC, 2009.

[10] Y. Hu, H. Chen, P. Lee, and Y. Tang.NCCloud: Applying Network Coding for theStorage Repair in a Cloud-of-Clouds. In Proc.of USENIX FAST, 2012.

[11]Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,"Enabling Public auditability and Data Dynamic forStorage Security in Cloud Computing," Proc. 14thEuropean Conf. Research in Computer Security(ESORICS'09), pp. 355-370, 2011.

[12] D. Ford, F. Labelle, F.I. Popovici, M. Stokel, V.-A. Truong, L.Barroso, C. Grimes, and S. Quinlan, "Availability in GloballyDistributed Storage Systems," Proc. Ninth USENIX Symp. Operating Systems Design and Implementation (OSDI '10), Oct. 2010.

[13] O. Goldreich, Foundations of Cryptography: Basic Tools. CambridgeUniv. Press, 2001.

[14] O. Goldreich, Foundations of Cryptography: Basic Applications.Cambridge Univ. Press, 2004.

Authors Details :

Srinivasa Rao Vykuntam
is student in M.Tech(software engineering) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech (CSE) from Gokul Institute Of Technology And Sciences, Vizianagaram. His interesting areas are Data Mining, Networking.

Mula.Sudhakar
is working as a Asst.professor in Sarada Institute of Science,TechnologyAndManagement,Srikakulam,Andhra Pradesh. He received his M.Tech (SE) from Sarada Institute of Science, Technology And Management, Srikakulam. JNTU Kakinada Andhra Pradesh. His research areas include Cloud Computing,Dataminig,Network Security