Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 1, January-2023, ISSN 2230-7540

Data Integrity and Client Side Data Security Trust Model in Cloud

Deepak Shinde*

Assistant Professor, Madhav Mahavidyalaya, Gwalior, M.P.

Abstract- ***Cloud computing demands multifaceted security solutions for a big, loosely linked system. In cloud computing, applications & databases are housed in remote data centers, where the reliability of data & service management is uncertain. Customers' confidence in a cloud service provider's reliability and security is a key factor in their decision to use that provider for mission-critical data. We describe the threats, vulnerabilities, & risks associated with cloud computing, and we present a cloud computing security development lifecycle model to ensure user safety and facilitate maximum data protection while still reaping the benefits of cloud computing. To prevent unwanted access, alteration, or deletion of both static & dynamic data, an algorithm for validating their integrity is presented.***

Keywords- Cloud Computing, Data Integrity, Cloud Risks, Trust In Cloud, Security

----------X----------

INTRODUCTION

Cloud computing involves the interconnection of several computers across a shared network, either public or private [1]. We now have a highly scalable infrastructure on which to store information and run programs. The advent of this kind of computing has resulted in dramatic reductions in the cost of computer power, web hosting, data, & delivery. Cloud computing has the potential to transform a data center from an expensive, capital-intensive setup to a more flexible, cost-based one. The cloud's unique ability to go beyond internal boundaries is what sets it apart from more traditional ideas of distributed, utility, & grid computing. Providers who manage the platforms and rent out resources like memory, Virtual Machines (VMs), & bandwidth, etc. on a pay-per-use basis are one type of CSP; another type of CSP leases cloud resources from multiple CSPs to end users based on their needs, with no regard for the location or method of delivery of these services [2]. Computing paradigms like the Grid & Cloud, among others, have made commitments to eventually deliver on the promise of Utility Computing.

It is critical for consumers to obtain service delivery assurances from providers, however, since cloud apps may be crucial to the clients' fundamental business activities. SLAs are contracts between service providers and their consumers that give this assurance. Cloud computing service providers have begun launching new datacenters in various parts of the world to provide redundancy & guarantee reliability in the event of site failures. These providers include Amazon, Dimension data, Google, Salesforce, IBM, iWeb, Microsoft, & Sun Microsystems.

Given the dynamic nature of cloud service needs, CSPs must ensure they can swiftly and flexibly provide consumers with the resources they need while still protecting their privacy. Service hardware is becoming able to efficiently run programs inside VMs because to recent developments in microprocessor technology & application software. Virtual machines provide for both hardware and VM separation in the cloud. As a cloud service, providers make available virtual machines (VMs) & programs running on them, enabling customers to deploy their own software. The usage of virtual machines introduces new difficulties, such as the need to intelligently allocate actual cloud resources to balance conflicting user demands.

IaaS services continue to be best by vulnerabilities at many levels of the software stack, also to leakage of information, to collocated malware infected VM instances, despite the rapid development of IaaS techniques like Amazon EC2 1 service, Microsoft Azure 2 service, & services provided by RackSpace 3 and other services. Many times, we have been reminded of the need of having secure cloud storage & cloud computing. In [3], for instance, the author highlights the fact that security concerns are a primary barrier preventing businesses from sending their data & computations to the cloud by citing industry decision makers. Concerns about cloud provider insolvency and subsequent unclearness & recognized processes of data protection and retrieval are among the more general reasons why some people are hesitant to fully embrace cloud computing.

ARCHITECTURE OF CLOUD COMPUTING

Different cloud computing architectural, commercial, & operational models are described here [4][5]. As can be seen in Fig. 1[10], the hardware layer, platform layer, application layer, & infrastructure layer represent the four tiers of cloud computing's layered architecture.

- **The Hardware Layer:** Data & application servers, network routers, connecting switches, power supplies, and cooling systems are all examples of the hardware components that fall within the purview of this layer. In practice, data centers are where the hardware layer is put to use. Thousands of cloud servers are often housed in a data center, organized in racks and linked to one another by network switches, network routers, or other means. Complex and time-consuming tasks at this level include hardware setup, fault tolerance, data traffic management, power consumption, and cooling resource management.

- **The Platform Layer:** The platform layer, the third layer up from the bottom, is where the frameworks for applications & operating system itself live. The platform layer's goal is to facilitate easier application deployment in cloud-hosted VM containers. To implement the storage, database, & business logic of unique web apps, Google App Engine (GAE) operates on this layer.

- **The Application Layer:** The real cloud apps are located in this upper layer of the architecture. To improve performance, availability, & reduce resource use costs, cloud applications may automatically scale in response to changing demand. Traditional cloud hosting infrastructures, such as dedicated data & application server farms, lack the adaptability of cloud computing's architecture. Each layer is only marginally connected to the layers above and below it, which ensures that each layer may develop in isolation. Cloud computing's architecture makes it possible for it to accommodate a wide variety of application needs with cheap administration & maintenance costs.

- **Infrastructure layer:** The cloud infrastructure layer, also known as the virtualization layer, is responsible for separating the real cloud's resources (such as servers) into several smaller virtual ones. Many useful features, such as dynamic resource allocation, are made possible by the infrastructure layer thanks to virtualization technology.

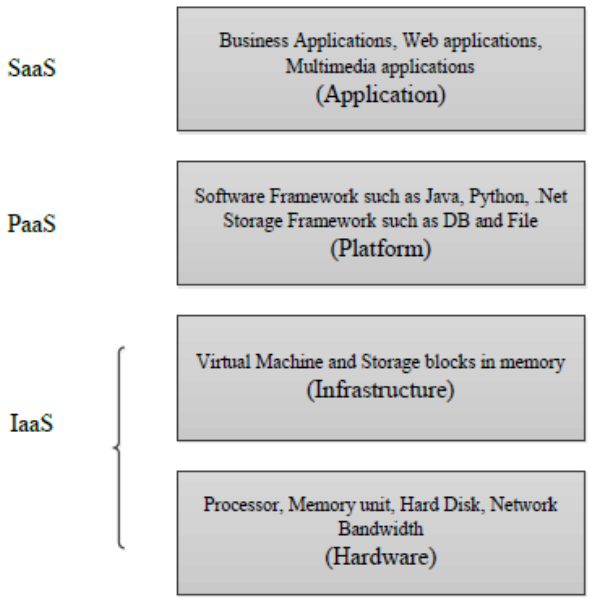

Figure 1: Layered cloud computing model architecture

CLOUD COMPUTING RISKS

Although there are many benefits to using cloud computing, there are also some drawbacks [1] to be aware of. Below, we discuss a few of these potential risks:

- **Security & Privacy:** It's the biggest issue with the cloud right now. When using cloud computing, sensitive data & information are continually at danger due to the third-party nature of data & infrastructure management. Although cloud service providers promise extra-safe password-protected accounts, any signs of security breaches might lead to a drop in users.
- **Lock-In:** Clients have a hard time switching from one CSP to another. Clients are forced into dependency on a single CSP.
- **Isolation Failure:** This risk involves the collapse of isolation mechanism, which isolates tenants' storage, memory, & routing.
- **Management Interface**: A publicly available CSP will have an interface that can be accessed online.
- **Unsafe Deletion of Data:** The user's requested deletion of data may or may not be carried out. This occurs for two reasons: first, the storage disk that was destroyed also included the data of other users, and second, the additional copies of cloud data that were stored but did not really exist.

TRUST IN CLOUD

The three components of trust are Expectancy, belief and willingness to risk. A user's level of trust in a CSP is proportional to the quality of the services they provide. The success of a cloud service & income of its provider are directly tied to the level of trust its

customers have in the service. Some criteria to aid the user in picking a CSP that can be trusted is required.

Trust Semantics

In the literature on Trust in the cloud, "trust" is commonly used interchangeably with "privacy" & "security" [6]. Can you define the word "trust" for me? It's a complex social phenomena with many facets. The following definition is used, which is based on credibility in social science:

- ***Expectancy:*** The trustor expects the trustee party to provide legal substance or effectively implement cooperative processes.
- ***Belief****:* Based on trustee competency, dependability, & helpfulness, the trustor expects the anticipated behavior.
- ***Willingness of taking risk:*** Trustors risk for such belief.

The trustee's ability, capability, &7 integrity determine the trustor's confidence in the trustee's foreseeable behaviors.

The trustee's candor reassures the trustor about their anticipated behavior. Cloud computing has two trust types depending on trustor expectation: Trust in belief is based on the trustee's beliefs, not performance. The performance trustee may be the success trustee's actions or claims. Trust in performance is not transferable, but trust in belief broadcasts it [7,8]. According to the definition, the trustor's belief rests on the trustee's capacity, honesty, & care. This rationally interprets evidence to anticipation. This underpins cloud computing trust.

Types of Trust

Cloud computing trust is categorized as reputation-based, SLA verification-based, policy-based, evidence-based, & societal.

Reputation-based trust estimates public confidence in an entity. An entity that must make a trust decision on a trustee utilizes the trustee's reputation to estimate its trustworthiness. CSPs build & maintain cloud reputation because it influences cloud service choices. Classically, reputation is expressed by a wide score indicating the general view or a few scores on several key performance elements. After establishing preliminary confidence and using a cloud service, SLA verification-based trust requires cloud users to confirm and re-examine the trust value. User-provider SLAs are legal. Thus, cloud computing trust management requires QoS monitoring & SLA verification. Third-party CSPs must offer these services.

Policy-based trust requires "formal". Public Key Infrastructure (PKI) supports key certification, digital signature, & validation using "formal" trust methods. It certifies and validates data attributes. A Certification Authority (CA)'s certificate policies determine trust. Validated public key certificates are sent & stored. Certificate policies determine PKI trust.

Evidence-based trust is built on demonstration of adaptability, helpfulness, & honesty. That expectation is evidence-based trust:

$$believe(c, attrb1(sb, av1)) \wedge \ldots \wedge believe(c, attrbn(sb, avn)) \rightarrow trust\_*(c, sb, x, ct)$$

which states that if a cloud user *c* believes a subject *sb* has attribute *attrb*1 with value av1, ..., attribute *attrbn* with value a*vn*, then *u* trusts (it is either *trust in belief* or *other one*) *sb* w.r.t *x*, the performance of *sb* or information is believed by *sb*, in a particular context *ct*.

Societal trust includes individuals & businesses. Cloud entities must be trusted. Trust between suppliers & clients helps information security service businesses develop.

PROPOSAL CLOUD DATA SECURITY MODEL

Cloud security protects data & infrastructure from attackers through organization-safe rules, layered technologies, & controls. Figure 2 shows a cloud computing system development approach for dependable, well-managed, secure, & patched services. Its goal is to identify all the duties needed to establish & maintain cloud security, with cloud training employees following the following steps.

a. Identifying Cloud Security Domains and Their Subcategories: comprising risk-classed physical & logical infrastructure, hosted applications, and platform services. Data centers and its hardware & components provide services and networks. Virtual or physical operating system instances, routed networks, and unstructured data storage make up the logical infrastructure. Online services use platform services including compute runtimes, DNS, & advanced functionalities. Virtual or physical infrastructure services.

- **Physical Infrastructure Security:** Physically protect servers, routers, storage systems, power supply, and other operational components. Security encompasses managing, regulating, & monitoring physical access, fire, natural catastrophes, burglary, theft, vandalism, & terrorist protection.
- **Network, servers and End Points Security:** protects data center equipment & network connections with many security levels.
- **Data Security:** There is high, medium, and low data sensitivity levels. Static or dynamic data may be delivered virtually. Data may be transferred externally or stored on

removable media. Storage, internal system, & network transfers need encryption.

- **Security of personal information:** with the goal of preventing its improper use, disclosure, or access.
- **Identity & Access Management:** Logical access is granted via role-based access constraints. They meet business needs and are allowed for access. It automates authorization & authentication for cloud resource access security.
- **Application and Process Security:** for cloud computing security

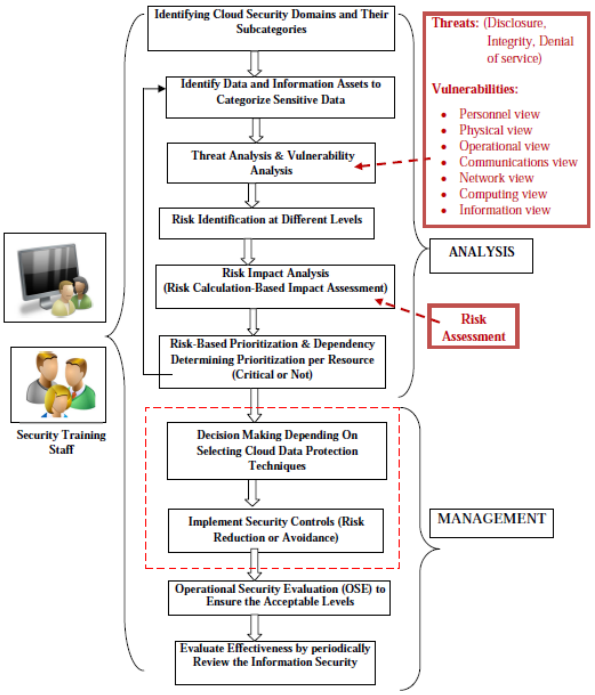

Figure 2: Proposed Cloud Computing Security System Development Model

b. Identify Data & Information Assets to Categorize Sensitive Data: which identify the organization's information assets, their worth, and the risks of losing or misusing them. Cloud technologies decouple information assets from a common physical infrastructure for numerous consumer objects.

Classification determines security restrictions. Defense determines safeguards after classification.

which identify the organization's information assets, their worth, and the risks of losing or misusing them. Cloud technologies decouple information assets from a common physical infrastructure for numerous consumer objects.

Classification determines security restrictions. Defense determines safeguards after classification.

The six concerns to address are [9]:

- Breach notification and data residency
- Data management at rest (being stored).
- Data protection in motion (being processed)
- Encryption key management
- Access controls
- Long-term resiliency of the encryption system

c. Threat Analysis & Vulnerability Analysis: Threat models & vulnerability studies are examined and updated to describe possible attacks & threat modeling.

- **Threats:** (Disclosure, Integrity, Denial of service).
- **Vulnerabilities:** (Personnel view, Physical view, Operational view, Communications view, Network view, Computing view, Information view).

d. Risk Identification/Resources: covers all risks. Risk evaluations occur at many levels. Private clouds & nonprivate clouds have different dangers and needs. Private clouds contain all their resources behind an organization's firewall, whereas public, hybrid, & community clouds have some on a common network.

Three top-level security domains determine risk management. Three information security categories [10]:

i. Logical security: protects data using software such as password access, authentication, and authorization,
ii. Physical security: protects the infrastructure, building and physical access to the data center, and
iii. Administrative or Premises security: protects the people who may have access to data and the property within the data center.

e. Risk Impact Analysis: focuses on disruptive risks based on effect assessment 7 business. Threat 'T', vulnerability 'V', and consequences 'C' effect risk R. C, V, & T determine risk [11].

$$R = f(C,V,T) \quad \textbf{(1)}$$

The multiplicative risk formula is:

$$R = C\,x\,V\,x\,T\,x\,lk \quad \textbf{(2)}$$

The constant k scales R from 0 to 100. The unit of measure for C becomes R when T & V are probabilities. Depending on the statistical approach, each factor is 1–10 or 0–1. Risk cannot be estimated using the multiplicative formula Risk = T x V x C. Thus, additive formulas were formerly utilized.

$$R = aC + bV + cT \quad \textbf{(3)}$$

Constants a, b, & c. The additive formula assumes components aggregate risk. Each organization's policy and other problems affect risk estimation in a

security system. Constants a, b, & c. The additive formula assumes components aggregate risk. Each organization's policy and other problems affect risk estimation in a security system.

f. Risk-Based Prioritization: Assess resource criticality. To test their usefulness, reliability, & cost-effectiveness. It oversees security control development.

g. Decision Making Depending on Selecting Cloud Data Protection Techniques: Security weaknesses must be addressed. Discard solutions that don't combine security & usability to reduce the risk of data theft, loss, or improper access &d empower staff with tools to perform efficiently and safely. Cloud security is limited by data type, location, and company. Security challenges include sensitive data access, data segregation, privacy, error exploitation, data recovery, cloud user authorisation, hostile insiders, management interface security, account control, data encryption & key management, & multi-tenancy.

Anyone may use a CSP & access data. Thus, the following methods are required to mitigate data risks:

- ***Using Secure Hash Function to Check Data Integrity:*** Figure 3 shows cloud data integrity testing using a one-way mathematical procedure to limit a stream of data to a defined size. Digests are data fingerprints. It is almost hard to duplicate the data digest using a new stream of data. Data digests ensure electronic communication integrity [12]. If a third party intercepts sender's message & replaces it with a fresh message and its digest, recipient is still vulnerable.
  If the data owner & cloud user (receiver) share a secret key, a secure hash may construct an HMAC. The cloud stores the hash value and data file.
  Cloud data and HMAC are supplied to the user if requested. Regenerating the HMAC protects against data modifications from any source. Without the secret key, a third party may intercept & change the sender's message, but he cannot construct a valid HMAC [13]
  HMAC works with iterated cryptographic hashes like MD5 & SHA-1. A secret key calculates & verifies message authentication values.
- ***Using a Digital Signature:*** Digital signatures verify data integrity. If the data has changed since the signature, a new digest is issued. Different signature. Thus, invalid data fails validation.
  Digital signatures authenticate systems & applications. Remote server access, network management security, and physical access to restricted areas all benefit from authentication.
- ***Using Security for Infrastructures****:* Sender & receiver must utilize many cryptographic security techniques to establish a broad security domain. For secrecy, they must share symmetric encryption keys. Public key-based key management with a TTP may efficiently distribute symmetric keys. Security services across organizational boundaries need several interlinked TTPs. Complete solution.
  Sender & recipient must exchange public keys and verify identities. A trustworthy third party must distribute public keys and verify the key pair's owner.
- ***Using Cloud Data Tokenization at the field level:*** It keeps sensitive data local while tokens are saved and processed on the cloud. A "lookup" table may restore token values. To avoid DoS, these tables are usually stored in a company's firewall-protected database. Tokens retain their structure & data type.
- ***Using Decrypting inside a Processor:*** Authenticated computer processors must decode sensitive data. If the cloud virtual machine is operating on a trusted platform, the technology will provide businesses confidence in its security.
  Data links need to be inspected and access: ports are essential for protecting the integrity of communication channels.
- ***Using API Standards:*** Tight integration with virtualization management machines requires a standardization of application programming interfaces.
- ***Apply Restrict access to sensitive information:*** To prevent malicious or accidental data access by unauthorized parties, proper security precautions must be taken.
- ***Apply Monitoring Tools:*** File characteristics, directory tracking, and auditable reports are only some of the features that should be included in virtual machine-level integrity monitoring software.
- ***Data Backup:*** It's the best insurance against data loss, whether deliberate or accidental. The most recent backups should also be encrypted for safety.
- ***Apply tiered access control lists (ACLs):*** Clustering of DNS servers allows for a globally redundant internal & external DNS infrastructure, allowing for virtual local area networks (VLANs) & applications to be segregated as required.

h. Implement Security Controls (Risk Reduction or Avoidance): where the proper measures will be taken for protecting information at all stages of its lifecycle (transfer, processing, & storage).

i. Operational Security Evaluation (OSE): comparing the state of the system under evaluation with reference security standards & baselines in terms of its network connections, platform, system

configuration, and monitoring capabilities. The OSR procedure guarantees sufficient & reliable security.

j. Evaluate Effectiveness by periodically review the Information Security: Information security reviews should be conducted on a regular basis to determine how well the security system is working, how far it has progressed, how well it is performing, and what can be changed to increase the system's efficiency.

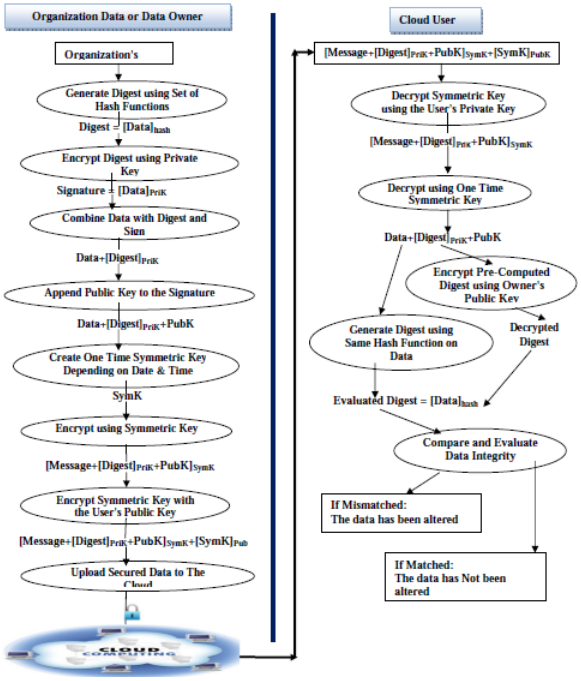

Figure 3: Data Integrity Checking Algorithm

CONCLUSION

The biggest risk in any computer model today is security. To mitigate potential data loss & ensure that users may take full use of cloud computing, we have suggested a cloud computing security development lifecycle model. An explanation of the data integrity checking method is provided, which does away with the need for external audits. Managing data integrity testing and assessment efficiently using a collection of hash functions is one manner in which cloud users may interact with the cloud provider as a third party. When a cloud user requests data, the system retrieves both the data and its associated hash value, and then checks for data modification by producing a new hash value and comparing it to the original.

REFERENCES

1. Cloud Computing Tutorial, [Online], Available: http://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf
2. R. N. Calheiros, R. Ranjan, A. Beloglazov, C.A. De Rose, and R. Buyya., " CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and Experience*, pp.23-50, 2011.
3. R. Buyya, C.S. Yeo, S. Venugopal , J. Broberg, I. Brandic., " Cloud computing and emerging IT platforms: Vision, hype,and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*; pp. 599–616, 2009.
4. Q. Zhang, L. Cheng, and R. Boutaba., "Cloud computing: state-of-the-art and research challenges," *In Journal of internet services and applications*, pp.7-18, 2010.
5. Tanvir Ahmed, "Cloud Computing a Solution for Globalization", International Journal of Education and Management Engineering(IJEME), Vol.6, No.4, pp.30-38, 2016.
6. J. Huang and D.M. Nicol., "Trust mechanisms for cloud computing," .*Journal of Cloud Computing*, pp.1-14, 2013.
7. D. Nicol, J. Huang., "A formal-semantiics-based calculus of trust," In Internet Computer Sytems IEEE, pp. 38–46, 2010.
8. J. Huang, M.S. Fox., "An ontology of trust: formal semantics and transitivity," *In proceedings of the ICEC*, New York, NY, USA, pp. 259–270, 2006.
9. http://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-beforeencrypting-cloud-data.
10. http://www.sans.org/readingroom/whitepapers/cloud/introduction-securingcloud-environment-34052.
11. GRiP – A Flexible Approach for Calculating Risk as a Function of Consequence, Vulnerability, and Threat. Available at: http://www.dis.anl.gov/pubs/69700.pdf.
12. Kuhn R. D. and others, (2001), "Introduction to Public Key Technology and the Federal PKI Infrastructure", U.S. Government publication. http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.
13. Kuhn R. D. and others, (2001), "Introduction to Public Key Technology and the Federal PKI Infrastructure", U.S. Government publication. Available at:http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

Corresponding Author

Deepak Shinde*

Assistant Professor, Madhav Mahavidyalaya, Gwalior, M.P.