ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 09, Issue 10, pp.8078-8082, October, 2022

RESEARCH ARTICLE

A REVIEW OF LEGACY AND PRIVACY ISSUES IN DISTRIBUTED CLOUD COMPUTING

***Sandesh Achar**

Director of Cloud Engineering, Erie Cir, Milpitas, California, 95025,

ARTICLE INFO

Article History:
Received 28th July, 2022
Received in revised form
29th August, 2022
Accepted 17th September, 2022
Published online 30th October, 2022

Keywords:

Condensate, Gas, Water, Isotherms, Fitting, Bottom-Hole , Depression, Measurement Echometry, Dynamometry.

ABSTRACT

Cloud computing enhances IT consumption and administration by reducing costs, accelerating innovation, reducing time-to-market, and allowing on-demand program development. [1] While the hype began in 2008 and has remained since, there is a definite movement toward cloud computing, and the advantages may be enormous, especially in an age when enterprises want remote access to resources. [1] Legal/contractual, economic, service quality, interoperability, security, and privacy challenges exist despite cloud computing's fast growth. In this chapter, I'll discuss cloud computing's legacy services and its biggest obstacles. We focus on cloud computing's regulations, security, and privacy. This essay offers answers to these problems and reviews upcoming cloud computing developments.

INTRODUCTION

Cloud computing is "a concept for offering simple, on-demand network access to a shared pool of customizable computing resources (such as networks, servers, storage, applications, and services)" [Basu, 2018] Many of us will see this IT paradigm change. Customers love the flexibility to reduce capital costs, delegate infrastructure administration, and rely on on-demand computing supply. Before cloud computing is extensively adopted, there are concerns and barriers. Cloud computing includes Internet-based applications and datacenter infrastructure and software. Who offers cloud services determines NIST's four cloud delivery models? Agencies may utilize one or more models to maximize app and business service delivery.

The four delivery models are as follows:

- Private cloud, in which cloud services are exclusively available to and managed by a company or a third party. These services might be provided elsewhere.
- Public cloud, in which cloud services are available to the general public and are owned by a cloud service provider, such as Amazon's cloud service.
- Community cloud, in which several businesses employ cloud services to assist a specific community with similar issues (e.g., mission, security requirements, policy, and compliance considerations) [Namasudra, 2018]

Corresponding author:** ***Sandesh Achar,
Director of Cloud Engineering, Erie Cir, Milpitas, California, 95025.

These services may be managed by the organization or by a third party and may be available remotely. Government cloud, often known as G-Cloud, is an excellent example of community cloud. This type of cloud computing is provided by one or more government agencies (as a service provider) for use by all or the great majority of government agencies (user role).

- Hybrid cloud, which is made up of many cloud computing infrastructures (public, private or community). A hybrid cloud is data kept in a travel agency's private cloud that is transformed by software running in the public cloud [Odun-Ayo, 2018]
- NIST has identified three major kinds of cloud service offerings in terms of service delivery. These are some examples:
- Software as a service (SaaS) is a business model in which program functionality is rented from a service provider rather than purchased, installed, and operated by the user. [Moravcik, 2018]
- Platform as a service (PaaS), which provides a cloud-based platform for the creation and execution of applications.
- Infrastructure as a service (IaaS) refers to the provision of computing power and storage space on demand [Moravcik, 2015]

Despite cloud computing's benefits, it must first overcome various hurdles. First, cloud computing may limit the user's control over data, programs, procedures, and policies. Different cloud locations may affect program performance. Compliance with rules can be problematic, especially with cross-border issues; cloud computing policy is continually developing. Internet-connected PCs are harder to maintain.

Second, cloud customers that must utilize proprietary formats risk losing data and control if monitoring tools are unavailable. Implementations may lose data. SLAs may be challenging to customize. SLAs may not cover downtime damages and repay little. Cloud computing can reduce internal uptime costs. Sometimes savings lose money. Tax penalties may be imposed on companies with little capital expenditures. Cloud computing standards are immature and outdated. Apps don't work in the cloud. Internet and network cables cause latency and performance issues.

Security Issues in Cloud Computing: Cloud security uses third-party controls and assurance, like traditional outsourcing. Lack of a cloud security standard creates fresh issues. Many cloud providers utilize unique security standards, methods, and models that must be reviewed individually.[6] Adopting client organizations in a vendor cloud model must ensure cloud security meets their own standards through requirements collecting, provider risk assessments, and assurance operations.

Organizations wanting to embrace cloud services face similar security problems as firms with in-house management. Internal and external hazards require risk minimization or acceptance. Following is an overview of the information security challenges adopting firms must face, either through vendor or public cloud provider assurance efforts, or by developing and implementing security measures in a privately held cloud. We examine these issues:

- The restrictions apply to information assets in cloud computing settings.
- The many types of opponents and their cloud-attacking skills.
- Cloud security issues, including considerations for attacks and countermeasures where relevant.
- New threats to cloud security
- Examples of cloud security incidents

Cloud Computing Security Issues Are Classified. There are three primary areas of cloud computing security challenges:

- Traditional safety concerns
- Issues with accessibility
- Concerns about third-party data control

Safety issues: Cloud migration increases the likelihood of computer and network breaches or assaults. Cloud service companies say their security systems and processes are more mature and well-tested than traditional organizations' [Pandey, 2021] If firms are worried about insider threats, it may be easier to preserve information if it's handled by a third party. Contracts with ISPs may be easier to enforce than internal controls."

This category includes: VM attacks VM attacks: Multi Tenant systems may be vulnerable to cloud service providers' hypervisor or virtual machine (VM) technologies. VMWare, Xen, and Microsoft's Virtual PC and Virtual Server have problems (Microsoft Security Bulletin MS07-049). Third Brigade monitors and firewalls possible VM vulnerabilities. Cloud vulnerabilities: SQL injection or cross-site scripting are platform-level issues. Recent Google Docs vulnerabilities (Microsoft Security Bulletin MS07-049). IBM's online service vulnerability scanning tool Rational App Scan is now a cloud service (IBM Blue Cloud Initiative) [Goyal, 2020] Phishers and social engineers are turning to cloud provider phishing (Salesforce.Com Warns Customers). Cloud users must defend the infrastructure needed to connect to and interact with the cloud, a process made more difficult by the cloud's location outside the firewall. Cloud attacks on networked machines are discussed in (Security Evaluation of Grid). The corporate authentication and authorization system isn't cloud-based by default. How does a corporation incorporate cloud resources? How can a corporation integrate cloud security data with its own measurements and policies?

Potential Risks: Smartphone use increases mobile device dangers, and cloud access is no longer restricted to PCs and workstations. Emerging mobile-device-specific attacks rely on laptop and desktop properties including rich APIs that permit network connections and background services, always-on wireless Internet, and large local data storage capacity. Internet-based viruses, worms, and even physical attacks may become increasingly widespread since mobile devices provide an attacker seeking anonymity a less dangerous target. Most mobile devices lack security measures. Smart phones lack antimalware, antivirus, and full-disk encryption.

Cloud service providers hold credit card, bank, and personal data. Thieves can use this information from several customers. Insiders may be employed by external attackers to access client data and explore systems. Customers should ensure cloud service providers are aware of this risk and implement identity validation and security screening. Cloud computing has led to huge data collection for advertising and other uses. Google's cloud infrastructure collects and analyzes advertising client data. Even tiny organizations may now examine data. Data accessibility and low-cost data mining affect consumer privacy. The attackers have consolidated databases and computer mining capabilities. Cloud-based businesses must anonymize data for privacy reasons. EPIC asked Google to shut down Gmail, Google Docs, and other web products until privacy was addressed (FTC Questions Cloud Computing Security). Google and Yahoo! will erase IP addresses and cookies from search data in 18 months. Testing algorithms on anonymized data. Anonymize data for analysis or subcontracting (Netflix Prize). Complex anonymization methods are needed as cloud app deployment expands. A sabotaging adversary must analyze availability. As political conflict moves online, such opponents become more plausible, as Lithuania's recent cyberattacks show (Lithuania Weathers Cyber Attack). Damages undermine system trust and enhance backup costs. Enhanced authentication may allow thin clients as cloud computing grows. Cloud users must login instead of buying and installing software. This reduces software piracy and enables central monitoring. Low-trust consumers may not get important knowledge. This design permits user mobility but requires stronger authentication. More cloud data and applications might boost phishing and identity theft. More services will mashup data as cloud computing increases. This innovation might boost data breaches and consumer sources. Restriction. In such situations, a centralized access control system may not work. Facebook shows. Facebook users exchange private and public information.

This data informs Facebook and third-party apps. Facebook seldom tests apps, so cloud-based programs may steal data.

Security measures in Cloud: This section discusses cloud computing security and privacy. Cloud computing enhances security vulnerabilities since it encompasses networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control, and memory management. Cloud computing security issues affect many of these systems and technologies. The cloud's network must be secure. Cloud virtualization brings new security concerns. Virtual computers must be securely mapped to real equipment. Data security involves encrypting data and following data-sharing rules. Resource allocation and memory management must be secure. Finally, data mining may be employed for cloud-based malware detection by intrusion detection systems (IDS).

As seen in Figure 1, there are six key parts of the cloud computing ecosystem where equipment and software require careful attention for security. These six components are: (1) data security at rest, (2) data security in transit, (3) user/application/process authentication, (4) strong separation of customer data, (5) cloud legal and regulatory difficulties, and (6) incident response.

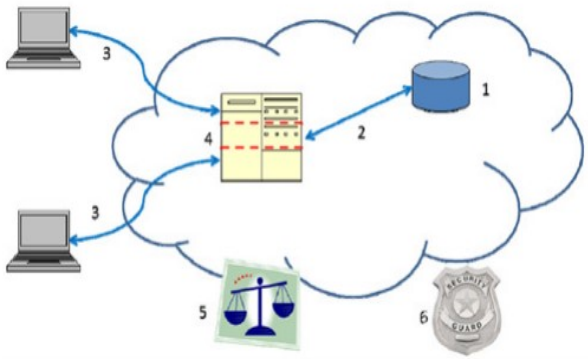

Figure 1. Areas for security concerns in cloud computing

Cryptographic encryption technologies secure data at rest best. Self-encrypting hard drives fulfill the trustworthy computing group's trusted storage requirements. Self-encrypting disks provide automatic encryption at the lowest cost and performance effect. Software encryption may also be used to safeguard data, but it's less secure since an attacker can steal the encryption key without being discovered. Encryption protects data in transit. Authentication and integrity controls ensure data is only delivered to the client's destination and not modified en route. Cloud solutions require strong authentication. User authentication underpins access control. Cloud authentication and access control are more crucial than ever since the cloud and its data are available online. TCG's IF-MAP standard allows cloud service providers and clients to communicate in real time about authorized users and other security issues. When a user's cloud access is updated or revoked, the customer's identity management system tells the cloud provider in real time. Separating a cloud provider's users (competing companies or hackers) to avoid accidental or purposeful access to sensitive data is a major cloud difficulty. A cloud provider divides customers using VMs and a hypervisor.

Existing technologies may increase virtual machine security and isolation. The trusted platform module (TPM) may verify hypervisor and VM integrity, ensuring network isolation and security [Yang, 2018]. Cloud computing raises legal and security challenges. Each client's legal and regulatory professionals must audit the cloud provider's policies and procedures to verify they meet legal and regulatory standards. Data export, compliance, audits, data retention and deletion, and legal discovery must be addressed. Trusted storage and platform module access solutions can control access to sensitive data under data retention and erasure settings. Clients must plan for security breaches and user misconduct. An automatic response or notification is preferable for this. The TCG IF-MAP (Metadata Access protocol) specification supports several security systems and delivers real-time event and user misbehavior notifications [Yang, 2018].

Cloud security and privacy trends: Cloud environments have security, privacy, trust, interfaces, protocols, and semantics. This domain may be services, infrastructure, or applications. Through service creation and orchestration, SOAs enable multi domain. Use multi domain policy integration and safe service composition for a holistic policy-based cloud management architecture. Security and privacy problems must be resolved for broad cloud adoption.

Authentication/ management: Cloud services let customers exchange personal data with Internet-based businesses. IDMs authenticate users and services using credentials and characteristics. Multiple identity tokens and identity negotiation processes generate interoperability issues in cloud IDM. Password-based logins are insecure. IDM protects individuals and processes data. Identity confidentiality in multi tenant cloud systems is unknown. Many jurisdictions can obstruct protection. Front-end services may need to protect user identities from other services. Multi Tenant cloud providers must segregate ID and auth data.[10] Authentication and IDM should relate to security components. Cloud computing needs managing identities.

The diversity and complexity of cloud services and domains require fine-grained access control mechanisms. Dynamic, context-, attribute-, or credential-based access demands must be managed by access control services. Access restriction may be required by privacy laws. Cloud-based access control solutions must handle privileges. Cloud delivery models should contain generic access control interfaces for interoperability, necessitating a policy-neutral design and enforcement framework for cross-domain access. Researchers must use privacy-aware, auditable access control and accounting services. Many service providers use the cloud; however, their security and privacy requirements may differ. Their policies are various. Cloud companies may combine services to offer bigger apps. Interoperability requires procedures to manage dynamic collaboration and detect security breaches. Despite checking domain rules, integration may introduce security weaknesses, research shows. To prevent policy integration-related security breaches, providers must maintain access control rules. Cloud service domains interact dynamically, transitorily, and according to service demands.[9] A trust framework should encompass trust-building and interaction/sharing needs. Integrating cloud policies must handle semantic heterogeneity, secure interoperability, and

policy change. Because consumer behavior can change quickly, a trust-based, secure interoperation architecture is essential for adaptive policy integration. Wireless and peer-to-peer trust management models have been studied. Trust mechanisms for cloud computing are needed immediately. Interoperability difficulties and global cloud installations complicate this matter.

Algorithm of Cloud Services: Clients get cloud services from suppliers and integrators. The service integrator coordinates and interoperates services to suit consumer security demands. WSDL is used by many cloud providers, although it can't define all services. Searching and constructing cloud services requires quality, cost, and SLAs. Characterize services and deliver their advantages, discover the best interoperable solutions, integrate them without exceeding service owner limits, and ensure SLA compliance. A security and privacy-aware framework for autonomous and systematic service provision and composition is needed. Privacy is a major problem in cloud computing, including safeguarding identifying data, policy components, and transaction histories. Many companies fear hosting data and apps off-site. Sharing workloads raises the risk of unauthorized client data access [Chenthara, 2019] Openness and privacy are musts for cloud providers. Secure cloud privacy. Who created and modified data, and how, must be known. Traceability, auditing, and history-based access control use provenance data. Without physical boundaries, cloud systems can't integrate data provenance and privacy. Research is hampered.

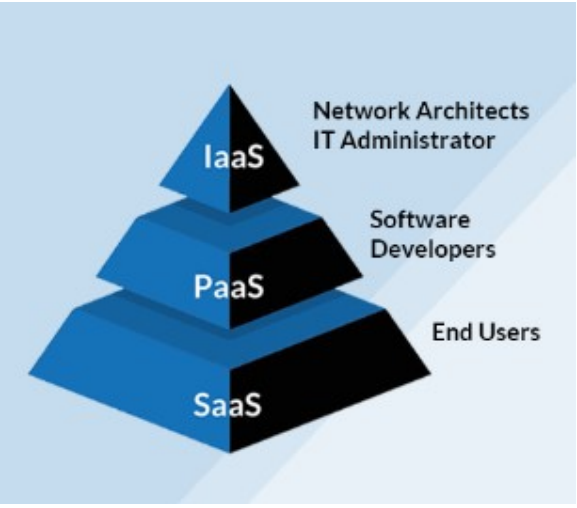

Figure 3. Cloud Services

Cloud computing affects security lifecycle paradigms. Unaddressed shared governance might be problematic. Cloud computing's benefits may diminish client-organization collaboration. Dependence on external entities can slow response to security risks, business continuity, and catastrophe recovery. Risk and cost-benefit analyses must include stakeholders. Customers must address data leakage in multi-tenant clouds, economic volatility, and natural disasters in a perimeter-less environment. Moving to the cloud increases insider threat. Well-targeted assaults can harm other renters in multi tenant settings. Cloud computing users must review life-cycle models, risk analysis and management methods, penetration testing, and service attestation. Information security challenges include creating reliable, realistic security metrics to improve risk assessment. Safe clouds require best practices and rules. Cloud computing's worldwide nature necessitates well-organized cyber insurance. Cloud computing growth, future service designs, and innovations will be impacted by IT trends. In recent years, laptop sales have surpassed desktop sales, and this trend is expected to continue as more notebooks, PDAs, and mobile phones integrate desktop-based PC capabilities, such as Internet access and bespoke application capability. The cloud will handle more complicated configurations with improved performance as processor speed and memory capacity increase.

Conclusion

Today, cloud computing is defined and addressed in several ICT contexts. A server corporation hosts services for network-connected clients in cloud computing. Computer, communication, and networking technology have made this possible. Cloud computing requires a reliable connection. Cloud computing's cheap cost and scalability make it an attractive industry. Despite increased activity and interest, there are major, persisting worries about cloud computing that are limiting development and may undermine cloud computing as a new IT procurement paradigm. Despite the financial and technological benefits of cloud computing, many potential customers have yet to join, and most significant organizations that use it retain fewer sensitive data there. Cloud implementation is pointless without control and transparency, which violates cloud computing's promise. Transparency helps with regulatory compliance and data breaches. Due to a lack of control, larger firms are testing smaller initiatives and less sensitive data. Cloud's promise hasn't been fulfilled. Many of the impediments to cloud computing adoption are old problems in a new context, but worse. Commercial partnerships and offshore outsourcing share regulatory and trust difficulties. Open source software helps IT departments to quickly design and deploy apps, but at the cost of control and monitoring. Before cloud computing, virtual machine and web service attacks existed. Many of these cloud computing difficulties have been studied for a long time, and the foundations for answers already exist. The progress of technology and, by extension, the global economy depend on the success of this new computing paradigm.

REFERENCES

Sunyaev, A. 2020. Cloud computing. In *Internet computing* (pp. 195-236). Springer, Cham.

Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., .. & Sarkar, P. 2018. Cloud computing security challenges & solutions-A survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 347-356). IEEE.

Namasudra, S. 2018. Cloud computing: A new era. *Journal of Fundamental and Applied Sciences*, *10*(2).

Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. 2018. Cloud computing architecture: A critical analysis. In *2018 18th international conference on computational science and applications (ICCSA)* (pp. 1-7). IEEE.

Moravcik, M., Segec, P., & Kontsek, M. 2018. Overview of cloud computing standards. In *2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA)* (pp. 395-402). IEEE.

Hon, W. K., Millard, C., & Singh, J. 2022. Cloud Computing Demystified (Part 2): Control, Security, and Risk in the Cloud. *Security, and Risk in the Cloud (February 2022)*.

Pandey, P. 2021. Security attacks in cloud computing.

Goyal, D., & Rajput, R. S. 2020. Cloud Computing and Security. In *The Evolution of Business in the Cyber Age* (pp. 293-319). Apple Academic Press.

Yang, M., Jiang, R., Gao, T., Xie, W., & Wang, J. 2018. Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain. *Int. J. Netw. Secur.*, *20*(4), 664-673.

Omotosho, O. I. 2019. A review on cloud computing security. *International Journal of Computer Science and Mobile Computing, IJCSMC*, *8*(9), 245-257.

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

****