ISSN (Online) 3134-884X

Advanced Research Journal of Computer Science

Received: September 27, 2024 | Accepted: November 02, 2024 | Published: December 04, 2024

Volume 01, Issue 01, Pages 21-26

DOI https://doi.org/10.66590/arjcs2024010105

Research Article

OPEN ACCESS

Check for updates

Big Data Protection Issues in Cloud Computing

Waqas Manzoor[1*] and Muhammad Irfan Sher[2]

[1,2]Department of Computer Science, University of Agriculture, Faisalabad, Pakistan

Abstract | Now-a-days mobile devices like iPhone, android phones, HTC mobiles etc. are not just used for making calls, text messages and for basic operations. Now mobile phones have become smart phones; they can be used to perform almost all the work that can be done on computer. Cloud computing has developed the latest trend regarding development within the quickly building mobile world. In cloud computing information storage and information handling are continued on web as opposed to on a single device. In this research there will be introduction to CC related to mobile devices called mobile cloud computing (MCC), comparison of G Cloud and i Cloud (two platforms providing cloud computing utilities for mobile devices) and in the end take a view of impact of cloud computing on smart phones. The main objective of research is that to understand the concept of "Mobile Cloud Computing" and investigate CC impact on mobile devices, which will help overall students and will be supportive in the upcoming for related application in portable expedient.

Key Words Cloud Computing, Data Security, Systematic Literature Review, IBM and Web Services

Author Designation:

*Corresponding author: Waqas Manzoor (e-mail: waqasmanzoor68@ymail.com).

How to Cite the Article:
Manzoor, Waqas and Muhammad Irfan Sher "Big Data Protection Issues in Cloud Computing." *Advanced Research Journal of Computer Science*, vol. 01, no. 01, December 2024, pp. 21-26. https://doi.org/10.66590/arjcs2024010105

INTRODUCTION

Rapid progress in concept of cloud computing (CC) has been observed in past few years. Via internet a wide range of properties like computational power, computational stages, different applications and loading has been provided CC to users. Google, Amazon, Microsoft, IBM, etc. are major cloud benefactors in current marketed segment of world [1].

Requirement for data protection boosts up in recent time period due Growing number of companies resorting to use cloud resources. A major challenge faced by CC service providers is to secure and protect the most vital property of user which is data.

Data in cloud can be in two forms, which are: transit (when data is travelling along network from cloud and user) and rest (when data is saved at cloud).

Web services and Cloud Computing (CC) both are open to network type attacks as these run on a network. Denial of service is one type of attack faced by both of these, that is if a server has been hijacked by a user, then hacker might halt running services and demand money to make services available. Another attack that might be faced by CC or web is man in middle. It is possible if the SSL (Secure Socket Layer) is configured incorrectly. This makes client and server authentication to behave in un-expected way and lead to main in middle attack [2].

It is vibrant that, issues of data security has played the utmost role in hindering CC to be feast. No doubt, it seems daunting to voluminous user to place data or run software at someone else's disk space and processor.

Some of the eminent security issues faced in CC are phishing, and data loss. These security issues stance stern intimidations to software and data of administrations. [2] Furthermore, shared computing possessions and multi-tenancy model in Cloud computing has announced new-fangled challenges of security that need new methods for confrontation.

Background

What about Cloud Computing?

The CC can be defined by US NIST (National Institute of Standards and Technology) in the form of a model in order to enable the network access on-demand, easy to use, ubiquitous for sharing pool of configurable computing resources (e.g., services, applications, storage, servers and networking) [3]. These can be released and

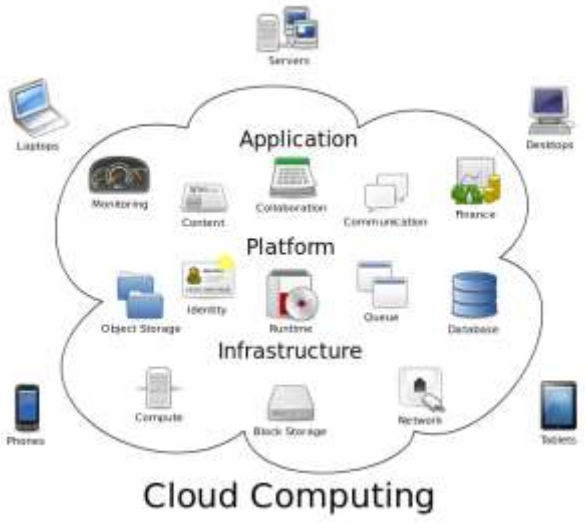

Figure 1: Logical diagram of CC [5]

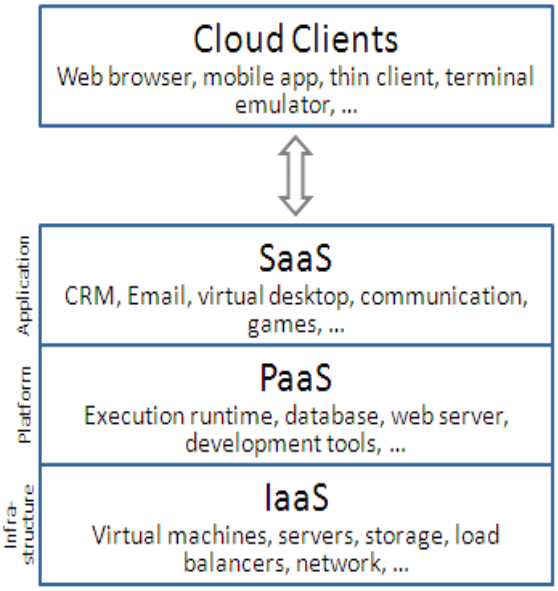

Figure 2: Cloud Service Model Representation [5]

fastly provisioned by applying minimum management efforts and service provider interaction.

CC is use of resources for computation (software and hardware) that are providing as a service over a grid (generally the internet). Generally, hardware and software in data center is named as cloud, that is provided to public on bases of pay-as-you-go manner [4].

A general/logical representation is shown in Figure 1 where a cloud is comprised of different service models (briefly given in next section) such as application, platform and infrastructure and it is made accessible through clients such as laptops, phones, tablets and desktops.

Models of Cloud Service

Cloud Infrastructure as a Service (IaaS): Are these cloud services that delivers provision of loading, networks, processing, and other essential computing possessions to users. This service (or in other terms infrastructure) enables the user to deploy and run any capricious software including both system software (like Windows) and application software (like Microsoft Office).

Cloud Software as a Service (SaaS): SaaS provide different services to user to use the applications performing on a cloud infrastructure, by using internet user use these services anywhere in the world.

Cloud Platform as a Service (PaaS): provides provision to clients to organize consumer-developed or achieved claims created using tools and programming languages maintained by provider [1,3].

A sample representation of cloud service model is shown in Figure 2 where different service models with their example participants are shown in layered form. IaaS is the utmost elementary and each one upper model abstracts from the specifics of the lower models.

Models of Cloud Deployment

Total four models of deployment regardless the services models utilized (IaaS, SaaS or Paas) which are described below. Figure 3 also presents a graphical representation of these deployment models.

Public Cloud: is maintained by a business party which sells its services. Its services or infrastructure is made accessible to public on the basis of pay-as-use.

Private Cloud: its infrastructure or services are made manageable solely for a single organization. Private cloud managed or owned by its organization or through the third party.

Community Cloud: its services or infrastructure is accessible in a specific geographic area or community that has some common interests (e.g. policy, mission, security requirement or compliance considerations).

Hybrid Cloud: Hybrid means grouping of two or more clouds (public, private or community) that persist exclusive objects but are assured together by even knowledge that permits application and data movability [1,3] (Figure 3).

Position of Security in CC

IDC (International Data Corporation) conducted a survey among IT professionals and senior business officials about cloud computing, and its numerical results are shown in figure 1. It clearly states, that security is at top as related to other factors of cloud computing. Microsoft General Counsel Brad Smith also offer data from a Microsoft's custom-made survey which measured attitudes on CC in January 2010. Which says, 86% of senior business leaders and 58% of general population is very agitated about the budding CC and on the other hand more than ninety percent (90%) of these peoples are very much anxious about their data's safety, access and confidentiality, which resides on cloud [5] (Figure 4).

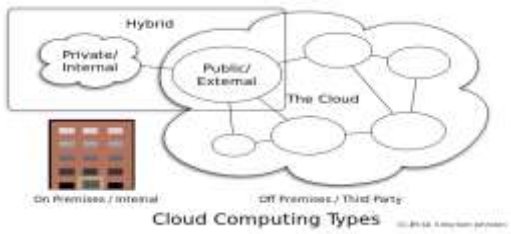

Figure 3: Models of Cloud Computing Deployment [5]

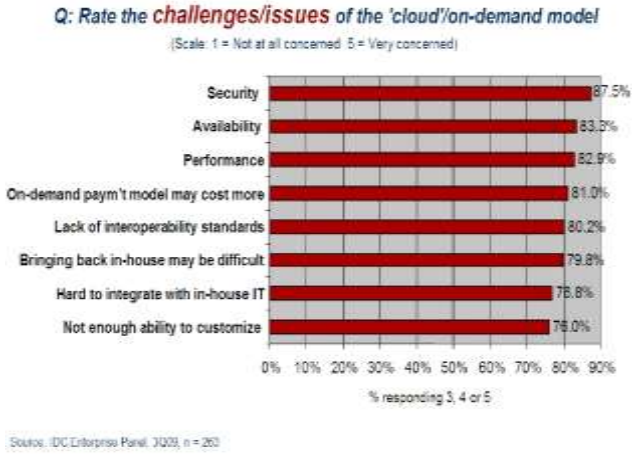

Figure 4: Position of Security in Cloud Computing [10]

Results of surveys (stated above) clearly states that, the parameters which are more affected the growth and performance of CC security is major challenge amongst all the.

MATERIALS AND METHODS

This work reviews the earlier work for concede the present knowledge to answer research questions given in Table 1. Previous work mostly comprised of traditional literature review that is done by non-rigorous and unfair approach therefore considered with low scientific value. Where SLR (Systematic Literature Review) is one of defined characteristics and describe added strong scientific viewpoint [6]. So, this work has commenced SLR as primary research method.

Planning the Review

Planning of SLR is given in subsequent sections

The need for a Systematic Literature Review

We searched databases (such as Science direct, Scopus, Springer link) with following query (Cloud Computing) OR (Cloud security methods) AND (systematic review) OR (methodical literature review). This query string did not return effective results (related to SLR). This clarifies that there is need of SLR for this issue.

Research Questions are Define

Following research questions shown in Table 1 were formed to meet research aims and objectives.

Table 1: Research Questions

Research Queries	Purpose
RQ.1 What are data security challenges in cloud computing environment?	To identify safety trials in CC.
RQ.2 What are presently implemented security measures to protect data that is stored at cloud?	To identify data storage security techniques.
RQ.3 What are currently implemented security techniques that protects data during transmission between clouds and clients?	To identify data transmission security techniques.

Defining Keywords

Research is based on Population Intervention Comparison Outcomes (PICO) criteria which is specified as:

- Population: Picked “Cloud Computing” as population
- Intervention: “Security” is the Intercession for this research.
- Comparison: Nope procedures or technologies are compared in this research work.
- Outcomes: Different data security challenges and techniques should be outcomes.

Selection Criteria and Procedures

Selection criteria is based on guidelines provided by [6]. Table 2 shows the selection procedure on which this research is based.

Conducting the Review

Given lower segment defines the leading of SLR.

Study Selection Criteria

For sake of filtering research papers that appeared against search query inclusion and exclusion criteria is defined as below

Inclusion Criteria

We are including studies or research papers on the basis of following criteria:

- Studies that describe security challenges or issues about security of data (may data is saved on cloud or data is in state of communication)
- Studies describing mitigating techniques against security risks when data is saved in cloud.
- Studies describing mitigating techniques against security risks when data is travelling between cloud and local machine.

Exclusion criteria

We have excluded the research papers on the basis of following points:

- Studies which are in other languages except English.
- Studies in which information is replicated.

Table 2: Selection Standards

Significance	Standards
By Search	Specified in search/query string Publication year (2005 -2012)
Title	Language must be English Must include words Cloud and Security
Abstract	Should show relevance about data security in cloud computing
Full Transcript	Experiential study on safety trials and vindication procedures

This study searches the query string to find out empirical studies in various five databases (i.e. ACM, IEEE Xplore, Springer Link, Scopus and science direct) and between 2005 and March, 3, 2013. Various steps to selection process are shown in Figure 4.

RESULTS AND DISCUSSIONS

SLR Results

The vast amount of research is completed in the area of CC, in recent years. By using SLR process we collected 46 papers related to meet the aims of research which papers are published science the year 2005. The results and analysis of these papers which we get in the process of SLR in this section discuss. In Table 1 and Table 2 A complete description list detail is given to recognized challenges and extenuation techniques in this research. In the earlier years, the research follows the distributed computing and focus on many services in these services include like grid computing. Now in the last decay, there is rapid change in research field focus on standard CC which is the next generation computing field. In the last 7 years, we mainly focused on data security aspects of the CC. During the literature study totally seventy-four papers are salvaged. The papers that we are selected mostly between 2010 to 2012 years. The Figure 5 Shows the last 7 years empirical indication of study on security in CC.

Identified Challenges

From the analysis, we have recognized 31 security trials during the SLR which are discuss below. The comprehensive explanation of these challenges is presented in Table . The list of known contests are WS-security, Phishing attack, Wrapping attack, Injection attack, Denial of service (DoS), IP spoofing, Direct attacking method, Information, Tampering, Repudiation Disclosure, Physical security, Elevation of privilege, WLAN's security, Replay attack, Man-in-the middle attack, Interleaving, Reflection attack, self-adaptive storage resource management, Timeliness attack, Client monitoring, Lack of trust, Weak SLAs, Perceived lack of dependability, Auditing, Back door, Transmission control Protocol hijacking, Completeness, Roll back attack, Fairness, Data leakage, data locality, Data security, Computer network attack, Denial of service (DoS), Data discrimination, Network security, Backup, Data integrity and Data handling. There are some of the CC attributes, which are part of investigation and also become threat to

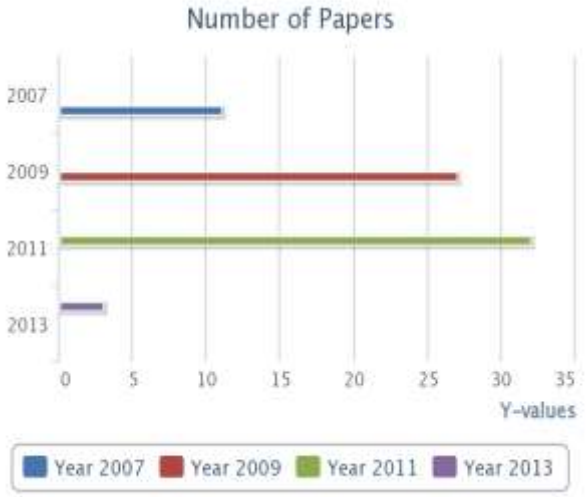

Figure 5: Number of Papers per Year Study

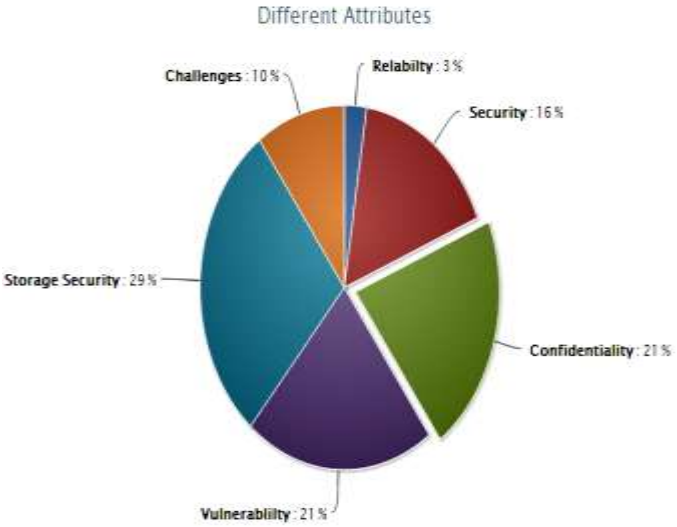

Figure 6: Identified security issues

the Cloud Computing. These cooperated attributes within CC are explained in appendix A. These are dependability, usability, security, accountability, availability, integrity and confidentiality. The most threatening attributes records are explained in Figure 6. The Figure 6 shows that Confidentiality 21%, storage security 29% and recorded most threaten, while associating to others.

CONCLUSIONS

All the mentions methods have strong influence on the Safety, Competence, Performance, Quality of Services, Privacy and Access control of CC. The defined extenuation procedures somehow improve the complete services in CC environment. The result is revealed in Figure 7.

During the SLR from the analysis, we have identified security techniques. The comprehensive explanation of these procedures is offered in Table τ.

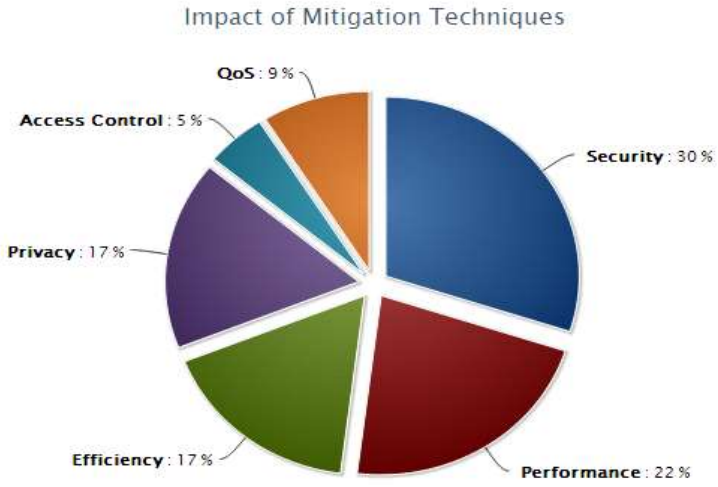

Figure 7: Identified Extenuation Techniques

Table 3: List of Identified CC Security Challenges

Sr. #	Challenge	Short Description	Paper Reference	Compromised attribute(s)
1	Trojan Horses and Malware	Malicious code is hidden by Trojan horses confidential to host program which seems to perform something useful.	[2, 11]	Security
2	Password Guessing	The most widely used technique to validate users is password. It is a common and effective attack to obtain a user password through any way.	[12]	Confidentiality
3	Direct attacking method	Cipher text deciphers directly instead to try to break the Encryption key.	[13, 14]	Confidentiality
4	Social Engineering	These types of attacks use social services to get authentication information such as passwords or pin digits that are used again information system.	[15]	Confidentiality
5	Weak Service Level Agreements (SLAs)	Consumers might face difficulties that arise from vendor lock-in, *insufficient* security measures, data unobtainability, hidden costs, and non- transparent setup.	[8]	Availability Confidentiality
6	Lack of trust	Clients facing challenge to choose most suitable and best cloud service provider as the total of cloud service provider is growing.	[16]	Confidentiality
7	TCP Hijacking	The IP has been substituted by attacking computer for that of trustworthy client. And server computer continues to interchange with awareness that it communicating with trustworthy client	[17]	Confidentiality Integrity
8	Physical security	The hazard of the hardware machineries may be confronted by persons or natural ruins, irrespective of the equal of inner software and policy security.	[10]	Security Availability
9	Auditing	It was examined and reviewed method in order to check either any type of security vulnerability has been occurred or gone to be occurred. It is used to save data in form of log files.	[7]	Security Confidentiality
10	Perceived Lack of Reliability	The hazard of not clear information whether the availability is for a single server where the simulated illustration of specific client resides or for all the servers placed in data centers in different locations of the world.	[9]	Availability
11	Client monitoring and security	The service storage has to be alert of the changed types of consumers and of their contact rights.	[19]	Security
12	Information Disclosure	A file reads from a co- tenant's workflow by cloud user, without authorization	[20]	Confidentiality
13	Self-adaptive storage resource management	All the information which has been observed needs to increase dynamic control on larger level transfer of data-on-data transfer schedule, dedicated circuits, performance estimation of distant storage services, automated management and distributed data scheduling.	[1]	Integrity Confidentiality
14	Completeness	In detail, a user should evade with the data service provider having detailed information she/he is legally in order to access on the behalf of stated permission.	[15]	Security
15	Roll back attack	In which still affords older version to user by malevolent services When the data owner updated the data with a new variety.	[2]	Security
16	Data manipulation	This involves data addition, change and data deletion.	[3]	Availability Integrity
17	Fairness	During the data transmission process, in order to gain certain advantages, malevolent party may trash to answer after receiving the indication from another peer.	[18]	Confidentiality

Table 4: List of Identified Mitigation Techniques

Sr. #	Technique Name	Short description	Paper Reference	Impact
1	IBA	This system splits the sharing users into the very same domain and in this domain trusts on the sharing global master key to exercise common verification.	[9]	Performance Security
2	MTACM	This is planned to insert the security duty parting principle in CC.	[8]	Security Access Control
3	RSA Algorithm	It can be used in order to weighing Data security and Cloud Storage ethodologies by executing digital signature	[4]	Security
4	TLS Handshake	This is designed in order to interchange the sign data dealing, which is used to remove the doubtfulness that is leading towards arguments and denials between the service provider and users.	[3]	Security
5	Message Authentication Codes (MACs)	This involves verifying the integrity by recalculating the Message authentication code of the received data file and comparing it to the locally recomputed value.	[15]	Efficiency
6	Data coloring and software water marking techniques	This lets us isolate user access and protect subtle information from provider access.	[20]	Performance Security
7	Proof Of Retrievability (POR).	POR gives a resilient of data truthfulness in the Cloud which the client can pay to check the correctness of his data in the Cloud.	[18]	Efficiency Performance
8	Diffie-Hellman key exchange	It has been defining the method between Cloud service user and the provider in order to privately sharing a symmetric key for safely data access.	[12]	Security Access Control
9	Self-Cleansing Intrusion Tolerance (C-SCIT)	It defines a tolerance system which is recovery based and leveraging the cloud services from the different sellers.	[13]	Security Performance
10	Application-oriented Remote Verification Trust Model (ARVTM)	The model appraises and informs user belief levels to choose whether access to demanded possessions or services should be official.	[19]	Security

REFERENCES

[1] Armbrust, M. *et al.* "A view of cloud computing." *Communications of the ACM*, vol. 53, no. 4, 2010, pp. 50–58.

[2] Jamil, D. and H. Zaki. "Cloud computing security." *International Journal of Engineering Science and Technology*, vol. 3, no. 4, 2011, pp. 3478–3483.

[3] Mell, P. and T. Grance. *The NIST Definition of Cloud Computing (Draft).* NIST Special Publication 800-145, 2011.

[4] Ahuja, R. *et al.* "SLA based scheduler for cloud for storage & computational services." *Computational Science and Its Applications (ICCSA), 2011 International Conference on*, IEEE, 2011.

[5] Dahbur, K. *et al.* "A survey of risks, threats and vulnerabilities in cloud computing." *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*, ACM, 2011.

[6] Jaatun, M, *et al.* "Special issue on security in cloud computing." *Journal of Cloud Computing*, vol. 1, no. 1, 2012, pp. 1–2.

[7] Almulla, S.A. and C.Y. Yeun. "Cloud computing security management." *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on*, IEEE, 2010.

[8] AlZain, M. *et al.* "A new model to ensure security in cloud computing services." *Journal of Service Science Research*, vol. 4, no. 1, 2012, pp. 49–70.

[9] Boampong, P.A. and L.A. Wahsheh. "Different facets of security in the cloud." *Proceedings of the 15th Communications and Networking Simulation Symposium*, Society for Computer Simulation International, 2012.

[10] Cheng, F. "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm." *Mobile Networks and Applications*, vol. 16, no. 3, 2011, pp. 304–336.