Reviewing Trust Issues in Cloud Computing

Amanpreet Singh¹, Amandeep Kaur² and Deepali Gupta³

¹²³Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India

amandeep.bhullar@chitkara.edu.in

Abstract. Cloud computing is a technique to minimize the use of hardware and software infrastructure digitally for the dynamic delivery of services. There are numerous components of current cloud computing models: end-user computers, networks of contacts, access management systems, and infrastructures of applications. Different organizations of cloud computing are providing various policies for handling tasks of cloud vendors and consumers. During task migration, whenever data is transferred over the cloud from one node to another; then the sink node should be trustworthy. It becomes a challenging task to create reliable and trustworthy cloud platforms. As the base from the concept of cloud computing, many authors proposed data privacy, security problems, security challenges, trust models, trust issues, challenges of trust management. In this paper, we highlight some of the trust issues faced by both cloud vendors and cloud customers while using cloud services.

1. Introduction

Cloud computing is a way to access digital services over the internet. Various factors such as low cost, location, and device independence are some of the advantages of cloud computing over traditional computer systems. "The cloud is a computer," explains Buyya [1]. There are many resources using in different fields of the cloud. But apart from all these resources and services provided by the cloud, there are many challenges and issues facing by society as well as by cloud computing platforms like security, resource allocation, lack of resources, load balancing, governance, compliance, migration, performance, build a private cloud and trust issue. The brief description of cloud computing is mentioned below.

1.1. Cloud Computing

Cloud computing is used to limit the cost of applications, equipment, services and networks. Another example is online services, wherein operational cost can be eliminated thereby saving around 30% of the total spending of an organization. Therefore, a cost-effective pay per-use model may be implemented.
As shown in figure 1, from 1940 to 1960, the data used for data center storage. Data was now saved in the cloud and data centers beginning in 2000. Trust building is the key component in the cloud. Several factors like licensing, control and honesty are considered to estimate the trust. One problem with previous research is that the concept of choice involving others is sometimes intermingled with confidence and reciprocity, and there is no explicit single factor derived from the experimental results. Although there is a degree of confidence among the social network members, this dependence in certain circumstances may not be adequate. For instance: storage where consumers risk losing, compromising or corrupting files while providers risk their own environment by hosting unknown files. The authors have defined the risk using the fuzzy belief concept for addressing uncertain risk property.

1.2. Applications of Cloud Computing
Cloud computing applications are endless. From standard software to computer software, any device can run on a cloud computing platform. Some cloud applications are listed as shown in figure 2.
2. Literature Review
Trust issues and challenges in Cloud computing are some of the most important aspects. Many researchers have proposed trust based models. Some of the articles studied for research are:

| Year of Publication | Author Name    | Summary                                                                 |
|---------------------|----------------|-------------------------------------------------------------------------|
| 2020                | Al-Jaser et al.| Authors talked about data privacy [16]                                  |
| 2020                | Devi et al.    | Security issues in cloud computing. [17]                                |
| 2020                | Gupta et al.   | Authors discussed about trust and fault-tolerance problems [18]         |
| 2020                | Tabrizchi et al.| Safety issues in cloud computing [19]                                   |
| 2020                | Kaushik et al. | Security issues handled by trusted third parties [20]                   |
| 2020                | Ali et al.     | Five-phase strategic roadmap [21]                                       |
| 2020                | Liu et al.     | Re-evaluate the issues of trust, integrity and safety in the           |
|                     |                | proposed new model [22]                                                 |
| 2019                | Khan et al.    | Highlighted the issues in the cloud ecosystem [23]                      |
| 2019                | Ruan et al.    | Trustworthiness and confidence [24]                                     |
| 2017                | Xu et al.      | Social trust reward program for allocating tasks of mobile cloud      |
|                     |                | big data [25]                                                          |
| 2017                | Chen et al.    | Proposed a mechanism to facilitate the protection of the              |
|                     |                | trustworthiness of social network [26]                                  |

3. Tools and technologies applied in existing cloud services

3.1. CloudSim
CloudSim is a platform for modeling the effectiveness of delivery policies in a free, repeatable environment provided by cloud developers. CloudSim provides file reading and transfer tracking tools to validate capacity models, load balancing algorithms as the source of the simulation environment. CloudSim allows developers to focus on the specific application architecture issues [27].

3.2. CloudAnalyst
With its graphical representation, usability, and functionality, CloudAnalyst is indeed one of the most common analysis tools in the market for various gateways and environments. [28].

3.3. GreenCloud
GreenCloud is used to manage resource allocation, load scheduling, and load algorithms [29].

3.4. iCanCloud
This tool model details network modeling and simulates a cloud-based simulation platform for applications [30].
3.5. EMUSIM
The purpose of this platform is to simulate the behavior of software applications by using an Integrated Simulation System and CloudSim [30].

4. Trust issues found during survey
The annual State of the Cloud survey was conducted by RightScale in January 2018 on the latest cloud trends. In the survey, it asked about the adoption of cloud infrastructure to 997 technical professionals throughout a broad range of organizations. Its results were clearly about the current challenges of cloud computing. Here various challenges and problems with cloud computing as shown in figure 3.

![Figure 3. Cloud Challenges](image)

4.1. Security
Cloud computing improves productivity by allowing businesses to focus on their core business [9]. Cloud computing is called the “fifth tool,” and, like all other tools available in today’s society, such as power, communications and computing services are accessible when needed [10]. The effectiveness and function of the allocated resources raise special concerns about data privacy and stability. Data and service security contain confidentiality and integrity of resources. In order to effectively address resource planning, including data security and availability, some security issues and constraints must be addressed [8]. The Systematic Literature Review provides a standard move toward the method and an accurate explanation of current data management [11].

| Issues in Security | Service Models | Responsibility Prospective |
|--------------------|----------------|----------------------------|
|                    | IaaS | PaaS | SaaS | Providers | Consumers |
| Security of data   | ✓    | ✓    | ✓    | ✓          |           |
| Security of network| ✓    | ✓    | ✓    | ✓          |           |
| Locality of data   | ✓    | ✓    | ✓    |            |           |
Integrity of data  ✓ ✓ ✓ ✓
Segregation of data  ✓ ✓ ✓ ✓
Retrieval of data  ✓ ✓ ✓ ✓ ✓
Authorization, Authentication  ✓ ✓ ✓ ✓ ✓
Confidentiality of data  ✓ ✓ ✓ ✓
Breaches in data  ✓ ✓ ✓ ✓
Availability of data  ✓ ✓ ✓ ✓ ✓

Table 2 lists the most important security issues in terms of areas of responsibility and possible service models [12].

Table 3. Category, Obstacles in Cloud [13].

| S. No. | Obstacles                     | Category                  | Stackholder Prospective |
|-------|------------------------------|---------------------------|-------------------------|
| 1.    | Service Availability         | Cloud Service Availability| Consumer                |
| 2.    | Data Storage                 | Data, Data Boundaries     | Provider                |
| 3.    | Data Hiding                  | Data, Data Boundaries     | Consumer                |
| 4.    | Data Transfer                | Data, Data Boundaries     | Consumer                |
| 5.    | Performance Uncertainty      | Performance, Scalability  | Consumer                |
| 6.    | Extensible Storage           | Performance, Scalability  | Consumer                |
| 7.    | Error of large scale         | Performance, Scalability  | Provider                |
| 8.    | Quick Scaling                | Performance, Scalability  | Consumer                |
| 9.    | Service Level Agreement (SLA)| Service Policies           | Provider, Consumer      |
| 10.   | Software Licence             | Service Policies           | Provider, Consumer      |

Table 3 lists the 10 big obstacles to cloud computing [13]. Armbrust et al.[13] indicate that for each obstacle consideration differs between stakeholders (consumer and provider). The number one barrier is access to services from all sides. Cloud service providers recommend many services to maximize capacity, but consumer can use multiple services. Therefore, some customers may not be able to use parts of the infrastructure indefinitely. There are several reasons for denial of service, such as system failure, heavy traffic, and server hijacking [14]. Attackers can use publicly available services to gain unauthorized access to resources or perform a number of malicious actions that affect the service. Using fast deployment methods and security monitoring is one way to solve the problem. Cloud scaling technology consists of two types of scaling, horizontal and vertical, and is used to manage cloud resources [15]. Vertical is used to maximize the virtual tools required to restore and boost performance. Service availability is a problem that can be solved if virtual resources are not available. The horizontal way to run a service on a physical resource is to grow. Providing services from a physical location is a matter of quality of service.
The second, third and fourth barriers relate to data boundaries, data confidentiality, and data transfer between networks and data stores. Rest of the obstacles are more technical in terms of how services are built to scale quickly to provide an overview of performance, scalable storage, bug fixes and maintenance costs for large deployment systems maintain. Fast forwarding can make the service inaccessible if you have very high load data that should be considered a security concern. Service policies, service level agreements (SLAs) and software licenses were the ninth and tenth barriers. The question is whether the software is compliant or acceptable, and to ensure that the license cannot be violated [13].

Cost and containment control
All organizations can benefit from the cloud because they don't have to buy new computer hardware. Due to the high demand for cloud services, businesses are using PAYG (Pay-as-You-Go) cloud computing seamlessly.

4.2. Shortage of resources
One of the cloud problems is the lack of resources for business. All cloud and cloud technology in your organization is also varying very quickly, making interoperability of cloud difficult to achieve.

4.3. Governance
Cloud computing faces many problems. The business goal is to follow policies and manage all IT assets according to IT management rules. Also, provide timely service and maintenance for these assets.

4.4. Managing multiple clouds
In recent years, the quality to manage the multiple clouds has increased exponentially. Enterprises are migrating to various types of cloud like public clouds and are led by technology giants like Alibaba and Amazon. According to the survey, 81% of businesses use a multi-cloud strategy. Hybrid enterprises that combine public and private clouds declined by 58 percent to 51 percent in 2017.

5. Word Cloud
A word cloud is a basic method for visualizing what is relevant in a particular document. Trust, security and data keywords are frequently used in the following figure 4.
6. Conclusion

Integrity, security, and trust are important issues that are key obstacles to cloud implementation. The concept of fuzzy belief continues to be used to address uncertain risks. The concern is that many users don't have faith or trust in the storage of cloud data. More critical and classified material is still found in a vast variety of organizations. Another big concern with the cloud is that consumers have control of the lifecycle of data in order to make sure about removal and retrieval of data by a cloud service provider. Still there exist many security issues like the wrapping of Extensible Markup language signature components, browser security, cloud malware attack, flood attacks. Such security systems need to be carefully and thoroughly examined so that any third party cannot access the data without authorization. Addressing problems of trust in current cloud paradigms and highlighting existing vulnerabilities that will be fixed in the future. Several simulations will be performed in a cloud environment to resolve security concerns. However, secure cloud architecture also has some open challenges to address.

Figure 4. Word cloud keywords [31].
References

[1] Arora R and Parashar A 2013 Secure user data in cloud computing using encryption algorithms International journal of engineering research and applications 3 (4) pp 1922-26.

[2] Mathew N, Salgar N, Pretty Varghese and Pawar Y 2014 Application for Intra-College Communication Based on Cloud Computing International Journal of Computer Science and Mobile Computing 3 (3) pp 1012–17.

[3] Teng S, Zheng C, Zhu H, Liu D and Zhang W 2014 A cooperative intrusion detection model for cloud computing networks Int. J. Secur. Appl. 8 (3) pp 107–118.

[4] Chang IC, Liu CC and Guo BR 2014 The financial performance of cloud computing Asian Economic and Financial Review 4 (5) pp 651–54.

[5] Abdullah A 2014 Green Cloud Computing: the need of the hour International Journal of Research 2 (1) pp 316–321.

[6] Avula T, Nela MK, Gudapati R and Velagapudi S 2012 Efficient use of cloud computing in medical science American Journal of Computational Mathematics 2 (3) pp 240–43.

[7] Elragal A and Haddara M 2012 The Future of ERP Systems: look backward before moving forward Procedia Technology 5 pp 21–30.

[8] Sheik A, Munro M and Budgen D 2019 Systematic Literature Review (SLR) of resource scheduling and security in cloud computing International journal of advanced computer science and applications 10 (4) pp 35–44.

[9] Garrison G, Kim S and Wakefield R L 2012 Success factors for deploying cloud computing Communications of the ACM 55 (9) pp 62–68.

[10] Buyya R, Yeo C S, Venugopal S, Broberg J and Brandic I 2009 Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility Future Generation computer systems 25 (6) pp 599–616.

[11] Al-Ruiithe M, Benkelhifa E and Hameed K 2019 A systematic literature review of data governance and cloud data governance Personal and Ubiquitous Computing 23 (5-6) pp 839–59.

[12] Subashini S and Kavitha V 2011 A survey on security issues in service delivery models of cloud computing Journal of network and computer applications 34 (1) pp 1–11.

[13] Fox A, Griffith R, Joseph A, Katz R, et al 2009 Above the clouds: A berkeley view of cloud computing Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS 28 (13) p 2009.

[14] Ramgovind S, Eloff MM and Smith E 2010 The management of security in cloud computing Information Security for South Africa pp 1–7 IEEE.

[15] Patil R and Singh R 2013 Scaling in cloud computing International Journal of Advance Research 1 pp 21–27.

[16] Al-Jaser, NMA 2020 A Survey on Cloud Computing Security–Challenges and Trust Issues International Journal of Computer Science and Information Security 18 (5) pp 7–12.

[17] Devi R K and Thangadkara K 2020 Towards security and privacy issues in cloud computing environment Purakala with ISSN 0971-2143 is an UGC CARE Journal 31 (4) pp 1989–96.

[18] Gupta P and Gupta PK 2020 Trust & Fault in Multi Layered Cloud Computing Architecture Springer pp 77–93.

[19] Tabrizchi H and Rafsanjani M K 2020 A survey on security challenges in cloud computing: issues, threats, and solutions The Journal of Supercomputing 76 (12) pp 9493–9532.

[20] Kaushik S and Gandhi C 2020 Capability Based Outsourced Data Access Control with Assured File Deletion and Efficient Revocation with Trust Factor in Cloud Computing International Journal of Cloud Applications and Computing 10 (1) pp 64–84.

[21] Ali MB, Wood-Harper T and Ramlogan R 2020 A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education Modern Principles, Practices, and Algorithms for Cloud Security pp 162–183 IGI Global.

[22] Liu A, Liu G, Orgun M A and Li Q 2020 Guest editorial: special issue on trust, privacy, and
security in crowdsourcing computing *World Wide Web* 23 (1) pp 389–91.

[23] Khan M S, Warsi M R and Islam S 2019 Trust management issues in cloud computing ecosystems *Proc. of International Conference on Sustainable Computing in Science, Technology and Management, Amity University Rajasthan, Jaipur-India* pp 2233–38.

[24] Ruan Y and Durresi A 2019 A trust management framework for clouds *Computer Communications* 144 pp 124–131.

[25] Xu Q, Su Z, Yu S and Wang Y 2017 Trust based incentive scheme to allocate big data tasks with mobile social cloud *IEEE Transactions on Big Data* pp 1–12.

[26] Chen X and Wang L 2017 A cloud-based trust management framework for vehicular social networks *IEEE Access* 5 pp 2967–80.

[27] Hassan H, El-Desouky Ali Ibrahim, Ibrahim A, El-Kenawy ESM and Arnous R 2020 Enhanced QoS-based model for trust assessment in cloud computing environment *IEEE Access* 8 pp 43752–763.

[28] El Karadawy AI, Mawgoud AA and Rady HM 2020 An empirical analysis on load balancing and service broker techniques using cloud analyst simulator *International Conference on Innovative Trends in Communication and Computer Engineering* pp 27–32 IEEE.

[29] Surana S and Sharma A 2020 Technologies Towards Cloud Computing To Green Cloud Computing. *Science Technology and Development* 9 (6) pp 123–129.

[30] Mansouri N, Ghafari R and Zade BMH 2020 Cloud computing simulators: A comprehensive review *Simulation Modelling Practice and Theory* 104 p 102144.

[31] Horvath III Albert 2015 An Analytical Study Of Consumer Trust In Cloud Computing.