SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 10 | October 2022 - Peer Reviewed Journal

RELIABILITY OF DATA SECURITY IN CLOUD COMPUTING

Mayur Nikum
B.Sc. Information Technology, B.K Birla College, Kalyan, Maharashtra, India.

ABSTRACT
This paper discusses the safety of data in cloud computing. It's a study of data in the cloud and aspects related to it concerning security. The paper will enter to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of knowledge in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have a security loophole in it. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of guest OS which could have a security loophole in it. The paper also will provide an insight on data security aspects for Data-in-Transit and Data-at-Rest. The study is predicated on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

KEYWORDS: *Cloud computing, cloud models, decryption, encryption, malicious behaviour, intrusion, secured communication.*

I.INTRODUCTION

Since its inception, the cloud computing paradigm has become widespread in industry and academia [88]. Inexpensive, scalable, convenient, ubiquitous, and on-demand access to shared resources are a number of the characteristics of the cloud that have led to the migration of business processes to the cloud [25], [2]. Cloud computing has attracted the eye of the research community as it has the potential to bring significant benefits to the industry and community [9], [88]. Resources are provided to users and released on demand from a pool of shared resources [4]. On-demand resource provisioning ensures optimal resource allocation and is cost-effective [78]. Consumers (individuals and businesses) not need to invest heavily in information technology (IT) infrastructure [4]. Customers use cloud-provided resources and pay just for what they use. Cloud providers, on the opposite hand, can reuse resources freed by a specific user, leading to better resource utilisation [78]. simple use is another benefit that cloud computing offers. Customers don't need to have special expertise in cloud-specific technologies [5]. Management of technology and services is shifting from the user to the provider of the service [5]. Cloud computing uses various technologies like web services, virtualization, and multi-tenancy to supply virtualized resources to customers. "Cloud services" are provided to customers over the web [25]. Web applications became an important part of cloud computing as they are used to access and manage cloud resources [70]. Customer processes run in virtualized environments, and virtual environments use physical resources [35]. Multiple virtual processes for various users are assigned to the same logically isolated physical machine. This creates a multi-tenant environment within the cloud. Despite the advantages offered, cloud computing isn't without risks, security being the most one [57].

One of the most significant barriers to the adoption of cloud computing is security [28]. Some commercial and research organisations are relying entirely on cloud computing to download digital assets from third-party providers [57]. Traditional IT infrastructure keeps digital activities within an organization's control zone. All processing, movement, and management happen within the organization's administrative domain. On the opposite hand, organisations don't benefit from administrative control over their services and infrastructure in the tube [52]. The presence of an outsized number of unaffiliated users exacerbates the concern [57]. The CSP can trust the users, but it's possible that they will not trust each other. For the explanations stated previously, clients still be uneasy about their digital activities that exist in the cloud, leading to a reluctance to adopt cloud computing [57].

There are various studies within the literature that discuss security issues in cloud computing. The authors of [85], [101] gave a summary of security issues in cloud computing. However, the above research is restricted to discussing security issues, not security solutions. Reference [71] reviewed security issues at various levels of cloud computing. Security solutions also are presented in [71]. However, discussions about the longer term have not yet been comprehensively discussed, and there's no overview of cloud technologies. In [1], the author presented a comprehensive study on his privacy within the cloud, focusing solely on his e-health cloud. Furthermore, the investigation of [1] is restricted to data protection. reference [121] reviewed security and privacy challenges in cloud computing and discussed defence strategies against existing vulnerabilities. However, the discussion of security issues in [121] focuses on confidentiality, integrity, availability, accountability, and privacy, with little discussion of the technologies that cause vulnerabilities. The authors of [74] identified cloud security issues together with approaches that can be used to address vulnerabilities. Nevertheless, this study lacks discussion of future research directions. Similarly, a study in [39] describes security issues in cloud computing intimately, with a quick description of current and modern security solutions. The add [18] examined common security models for cloud computing, including the cube model, the multi-tenancy model, and therefore the risk assessment model. Furthermore, the authors of [18] discussed the safety risks of cloud computing. However, the risks are described from the attitude of various stakeholders, like customers, governments, and repair providers. Security issues from a technical and operational perspective weren't the subject of the above investigation. Strategies for resolving security issues also are discussed, which components and processes have to be protected and evaluated. it's not detailed how the safety goal is achieved in the current study. Similarly, article [104] discusses security issues in cloud computing and related security solutions. However, the discussion focuses on the privacy portion of cloud security.

In addition, we briefly discuss security issues associated with mobile cloud computing and common strategies leading to solutions. The contribution of this study to the above study is shown in Table 1. "" and "" indicate whether the world specified in the column was discussed in the vote.

The rest of the work is organised as follows. Section 2 provides an architectural framework for cloud computing. Section 3 details security issues within the cloud computing paradigm are detailed in Section 4, and existing solutions in contemporary literature are presented in Section 5. Section 5 highlights security concerns in mobile cloud computing (MCC). Section 6 describes the methodology and open-ended questions, and Section 7 concludes the survey.

Common cloud vulnerabilities, threats, and attacks Cloud computing, like all other area of IT, suffers from many security issues that require to be addressed.

Addresses: 8, 11, 12, and 13. These risks relate to policy and organisational risks, technical risks, and legal and other risks.

Risk 9

Vulnerabilities and Open Issues

The cloud may be a set of technologies, processes, people, and commercial structures. Like all other technologies, people, and commercial structures—even the cloud—have vulnerabilities. Below are a number of them.

Cloud vulnerabilities a number of the open issues and threats that require immediate attention are listed below.

470 465-472 in Procedia computing 110 (2017) 00 (2012) 000-000 Author/Procedia Computer Science

a. Vulnerabilities in shared technology—increased resource usage provides attackers with new opportunities.

a point of attack that can deal damage disproportionate to its importance. An example of sharing

The technology is named a hypervisor, or cloud orchestration.

b. Data Breach - because the burden of data protection shifts from cloud consumers to cloud service providers, the risks of accidental, malicious, and intentional data breach increase.

c. Account-of-Service Traffic Hijacking: one among the greatest benefits of the cloud is that it's the Internet, but the danger of account compromise is the same. Losing access to privileged accounts means loss of service.

i.e., Denial of Service (DoS)-A denial of service attack against a cloud provider can affect all policies.

e. Malicious Insiders-Determined insiders can find more ways to attack and conceal their tracks in the cloud scenario.

f. Internet Protocol-Many IP-specific vulnerabilities like IP spoofing, ARP spoofing, DNS, etc.

Addiction may be a real threat.

G. Injection vulnerabilities—SQL injection bugs, OS injection, LDAP vulnerabilities, etc.

Injections within the management plane can cause major problems for multiple cloud consumers.

H. API and Browser Vulnerabilities: Vulnerabilities in cloud provider APIs or interfaces are significant risks related to social engineering or browser-based attacks. The damage is vital.

Me Changing business models: Cloud computing are often a game changer for cloud customers.

type of business. IT departments and businesses must adapt or face the risks.

Conclusion

Cloud computing security evolves with risk, as risks are often discovered too late to stop.

Incident Cloud computing presents challenges thanks to its disruptive nature, complex architecture, and resources used.

Severe risks are inherent to all or any parties involved. it's important that all stakeholders understand the risks and benefits.

Adjust them properly. Security must be built into every layer of a cloud computing platform.

In order to effectively mitigate risk, incorporate best practises and new technologies.

Consumers, vendors, brokers, carriers, accountants, and every one other should take necessary precautions.

The risk of successfully securing a cloud computing platform versus the risk of facing significant, potentially business-critical risk consistent with recent research, the industry recognises that security technology offers the simplest solutions.

practices, methods, techniques, and techniques for developing systems and services designed for security, sustainability, and resilience. it's important to advance this research to provide such best practices.

More applications and use cases. Further research on the system development life cycle (SDLC) is additionally necessary for cloud consumers to integrate various developments and technological advances.
models that radically improve security and container systems like Docker. Besides, there
Research on training and its impact on human safety is extremely limited. I can work to know it.
Challenges, Requirements, and Impacts of Effective Security Training for Consumers and Other Providers

II.METHODOLOGY

The method used for data collection about the reliability and data security opinions in the user of cloud is internet questionnaire.

Questionnaire

1. Do you ever used any of the cloud storage service?
2. Do you think your data is secured in cloud?
3. Is cloud services friendly to you?
4. In your company or in your college, is there any cloud service used?
5. How much cloud service reliable to you?

This are the question we have spread throughout the cloud users to receive their opinions about cloud services

III.MODELING AND ANALYSIS

The responses of the questionaries have been generated and the graphs and pie charts of the responses are as follows

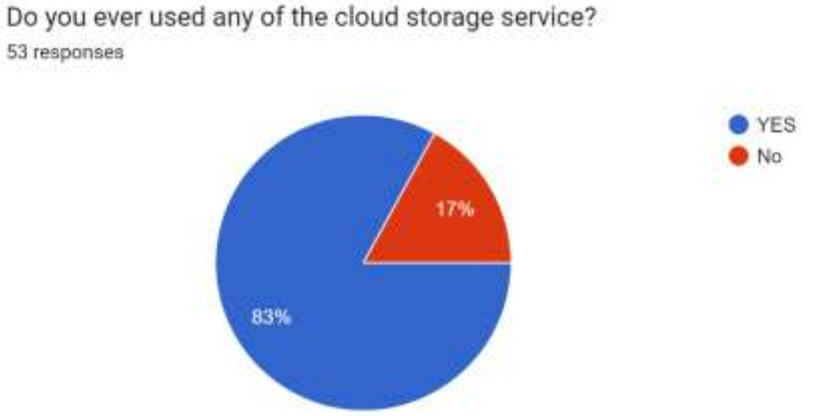

Figure 1

Here the figure one defines that around 83% of the people use the CLOUD STORAGE SERVICES and 17% of them don't use the cloud storage services because of the security concerns. Using the cloud for storage gives you access to your files from anywhere that has an internet connection. In the event of a hard drive failure or other hardware malfunction, you can access your files on the cloud. It acts as a backup solution for your local storage on physical drives.

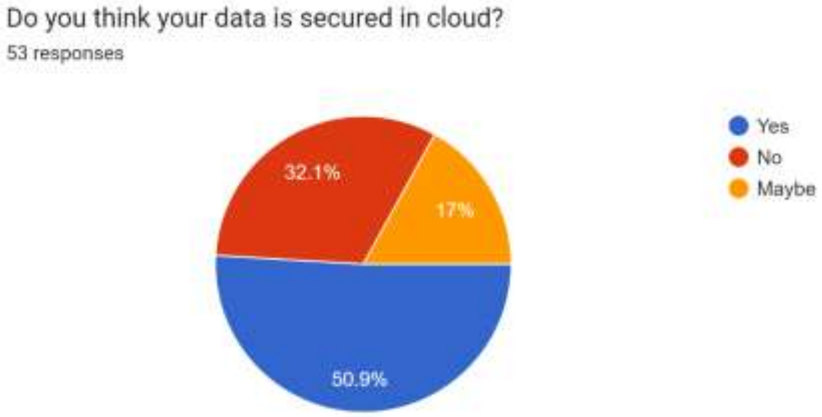

Figure 2

Here the figure defines what people think about their data is secured over the internet cloud or not, as far as the survey is concerned 32% of audience think that their data over the internet is not secured, 17% of the audience thinks that maybe their data is secured over the internet is not, and almost 50% of the data things that their data is secured

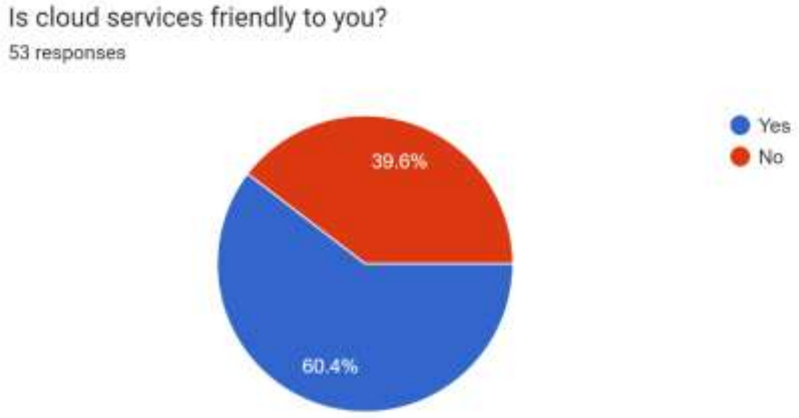

Figure 3

Here the figure defines what people think about their cloud services it is friendly or not, as far as the survey is concerned 39.6% of audience think that their cloud services is not friendly, and almost 60% of the people things that their cloud services if friendly

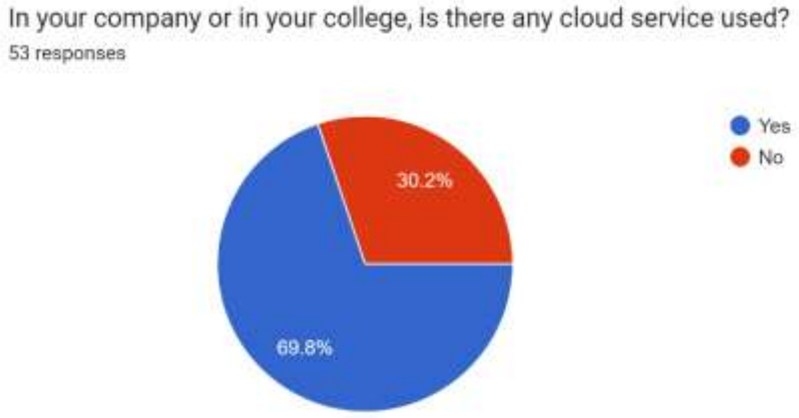

Figure 4

Here the figure defines how many people in their company uses the cloud services or not, as far as the survey is concerned 30.2% of audience not use people use the cloud service in their company, and almost 69.8% of the people use the cloud service in their company

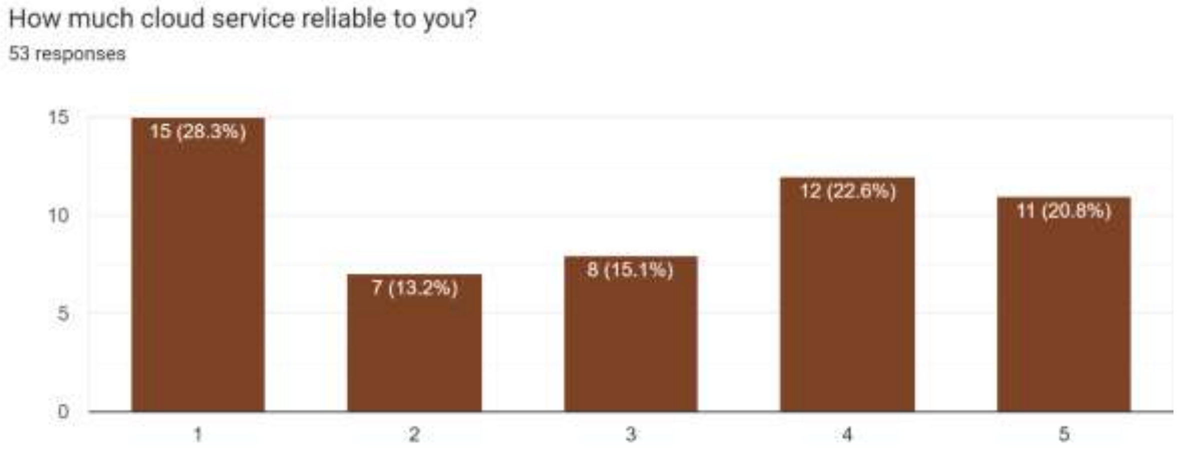

Figure 5

Here the figures define how many people thinks how much cloud service is reliable to them or not, 28% of the people that the cloud service is very poor,13% and 15.1% of the people thinks the cloud reliable service is good, 22% and 20.8% of them tells in the service that the reliability of the cloud service they are using is very good and reliable.

IV.RESULT AND DISCUSSION

The responses of the questionaries have been generated and the graphs and pie charts of the responses are as follows

Here the figure one defines that around 83% of the people use the CLOUD STORAGE SERVICES and 17% of them don't use the cloud storage services because of the security concerns. Using the cloud for storage gives you access to your files from anywhere that has an internet connection. In the event of a hard drive failure or other hardware malfunction, you can access your files on the cloud. It acts as a backup solution for your local storage on physical drives. These figures define how many people thinks how much cloud service is reliable to them or not, 28% of the people that the cloud service is very poor,13% and 15.1% of the people thinks the cloud reliable service is good, 22% and 20.8% of them tells in the service that the reliability of the cloud service they are using is very good and reliable. Figure defines how many people in their company uses the cloud services or not, as far as the survey is concerned 30.2% of audience not use people use the cloud service in their company, and almost 69.8% of the people use the cloud service in their company.

V.CONCLUSION

Despite several advantages offered by the cloud computing, it also fosters security concerns that hamper the fast rate adoption of the cloud computing. All of the users whether individual or organization should be well aware of the security threats existing in the cloud. Comprehending the security threats and counter measures will help organizations to carry out the cost benefit analysis and will urge them to shift to the cloud. As the cloud computing utilizes many traditional along with novel.

ACKNOWLEDGEMENT

I would like to express my gratitude to my advisory Prof. Swapna Nikale who has given me opportunity to publish the research paper as a part of curricular activity. I would also like to thank my fellow friends, my parents and all other supporters who all encouraged me during this research work.

VI.REFERENCE

1. *State of the Cloud Report. (2017). https://www.rightscale.com/lp/state-of-the-cloud (Retrieved 25 May 2017)*
2. *State of Cloud Adoption And Security. (2017). https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoptionand-security/ (Retrieved 25 May 2017)*
3. *Sharma, R. & Trivedi, R. K. (2014). Literature review: Cloud Computing –Security Issues, Solution and Technologies. International Journal of Engineering Research, Vol. 3, Issue 4, pp. 221-225.*
4. *National Institute of Standards and Technology, (2011). NIST Cloud Computing Reference Architecture. https://www.nist.gov/publications/nist-cloud-computing-reference-architecture*
5. *Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Procedia Technology, Vol. 12, pp. 529-534.*

6. *Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, Vol. 63, Issue 2, pp. 561–592.*
7. *Kuyoro S. O., Ibikunle, F., and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), Vol. 3, Issue 5, pp. 247-255*
8. *Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2016). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2016.03.004*
9. *European network and Information Security Agency. (2009). Cloud Computing: Benefits, risks and recommendations for information security. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-andrecommendations-for-information-security/*
10. *Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2012 1:11. DOI: 10.1186/2192-113X-1-11*
11. *Ramachandran, M. (2015). Software security requirements management as an emerging cloud computing service. International Journal of Information Management, Vol. 36, Issue 4, pp. 580-590. 12. Roundup of Cloud Computing Forecasts and Market Estimates, 2015. (2015). http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates2015/#56c0b0f0740c (Retrieved 2 May 2016)*
12. *Wang, C. (2009). Cloud Computing Checklist: How Secure Is Your Cloud? (2009). Forrester Research.*
https://www.forrester.com/report/Cloud+Computing+Checklist+How+Secure+Is+Your+Cloud/-/E-RES55453