# Cloud Computing Security Issues and Possibilities

**Robbi Rahim, Edmond Febrinicko Armay, Daniel Susilo, Rustono Farady Marta, Alde alanda**

***Abstract— for organizations green cloud computing is a new computational architecture which provides a business model; organization can acquire it without paying upfront investments. Cloud computing provide the potential gain but providing security in cloud computing is very necessary. Under the cloud model, security issue is become more complicated as new dimensions entered into the security scenario.***

***Keywords-agile; software development; sweet spot; large project.***

## I. INTRODUCTION

In the field of cloud computing there are many security challenges and issues are existing. As data and information are stored in the cloud by third party in the cloud and in can be accessed through the internet, the control and visibility is limited. There is major task is to secure the data. It is necessary to work properly and play its role efficiently to achieve the security [2].

In the last few years the cloud computing uses are increasing day by day and researches give attentions to improve the approaches in both industries and scientific applications. The Gartner [3] described that cloud computing consider in top 10 most promising technologies that provide a better prospect in growth of organizations and companies.

To share the usual pool of customizable registering assets like server, application, systems, administrations and storage the cloud computing empowers helpful, universal, on-request system access that can quickly released and provisioned with negligible establishment exertion or specialiser organization communication.

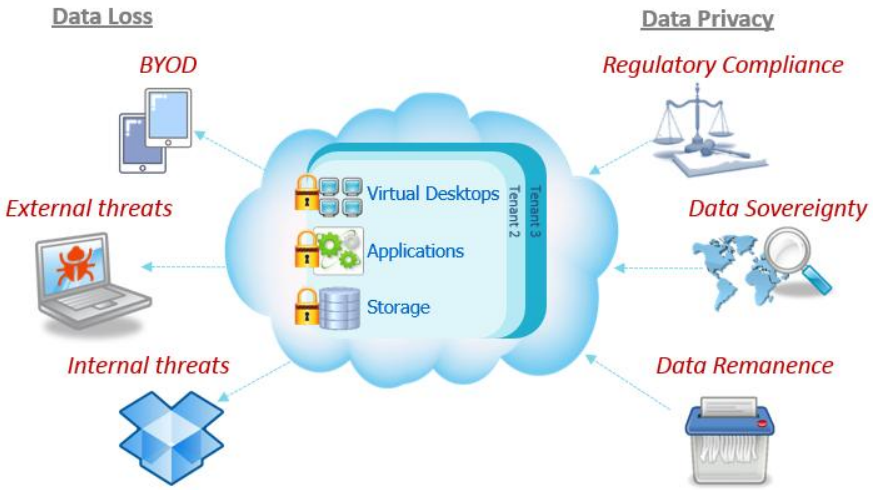


Figure 1: securing cloud computing data

The main task of cloud computing is to give quick, protective and helpful information to services of net computing and storage services. All computing resources imagined as administrations and conveyed over the Internet [4, 5]. Cloud computing shows up as a computational worldview just as a circulation engineering. The cloud can increase the versatility, readiness, capacity to adjust to changes as indicated by interest, effort, accessibility, quicken advancement work and give cost decrease through efficient and streamlined computing [6, 7, 8, 9].

Cloud computing is consider as the combination of several methodology, methods and computing concept like virtualization, Service Oriented Architecture (SOA), Web 2.0 and different advances with dependence on the web, and fulfill the registering needs of clients, it provide normal business applications online through internet browsers[8].

There are several benefits of using the cloud computing but while adopting the cloud computing there are certain obstructions to selection. One of the major issues is the security that is related to legal matters, privacy and compliance [10]. As cloud computing is the new trend in computing technology there is uncertainty at all the level of model, and how the applications get security on that level [11][12].

**Revised Manuscript Received on July 22, 2019.**

**Robbi Rahim**, Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia.
**Edmond Febrinicko Armay**, Department of Physics. Lund University. Lund, Sweden.
**Daniel Susilo**, Dr Soetomo University, Indonesia.
**Rustono Farady Marta**, Universitas Bunda Mulia, Indonesia.
**Alde alanda**, Politeknik Negeri Padang, Indonesia.

## II. LITERATURE REVIEW

Hasan Tabaki et al. [13] shows the one of a kind issues of security and protection challenges with cloud while Minqi Zhou et al. [14] analyzed cloud security and protection issues as far as the uncommon connection between the specialist co-ops and the clients in a cloud. Both the works are without uncovering the need and significance of virtualization security.

Kresimir Popovic et al. [15], in their exploration work have given a conventional outline of the security issues, the necessities and the difficulties that many cloud specialist organizations' experience. In 2011, S. Subashini et al. [16] overviewed SQL infusion imperfections, its cross-site scripting, nonsecure capacity and negate diverts or advances. None of the investigation demonstrates any dangers of the distributed computing security regarding organization models of mists. Kui Ren et al. [17] have examined different security challenges for the open cloud without thinking about the dangers in administration models. Be that as it may, the majority of the current research examines cloud security from a nonspecific perspective outside a cloud. None of these works talk about the risk levels in various administration models (SaaS, PaaS, IaaS) from the point of view of virtualization advancements. Despite the fact that, Hsin-Yi Tsai et al. [18] have inspected different dangers and security issues with virtualization including administration models IaaS, PaaS and SaaS, they have not referenced the effect of virtualization on cloud security with Database as a Service (DaaS). As, on the grounds that virtualization is an extremely basic innovation to distributed computing, one must record its security dangers and accordingly create suitable measures and activities. In addition, there exists much work on dangers identified with either administration or sending models. Yet, as distributed computing innovation thoroughly relies upon system and web, different dangers identified with system security have been accounted in this overview

## III. CLOUD ARCHITECTURE

Architecture of cloud computing include many parts of clouds. These clouds ate loosely coupled to each other. The structure of cloud computing basically divided in 2 parts:

- Front End
- Back End

Both front end and back end connected through internet with each other. The figure shows the cloud computing structure:

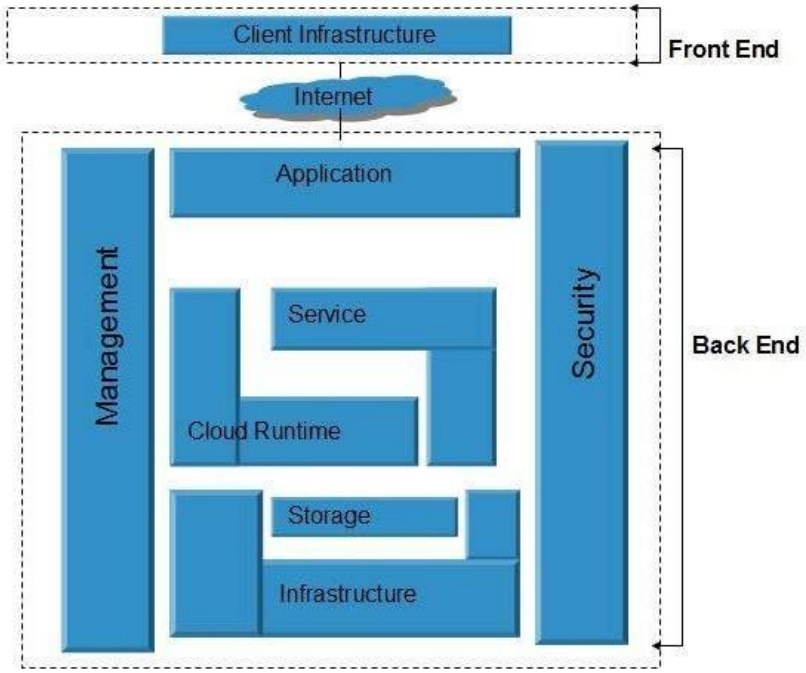


Figure 2: cloud computing architecture

**Front End**

The client section of cloud computing is known as the front end side. The applications and interfaces that are necessary to get the platform of cloud computing are consider as the part of the front end. For example web browser.

**Back End**

The cloud itself consider as the back end in the network. All the resources that needed to assign the cloud computing are consider in this part. It consist of virtual machine, services, servers, large data storage, security mechanism, deployment models etc.
The servers, networks, management of clouds software, platform virtualization and storage devices combine the cloud infrastructure

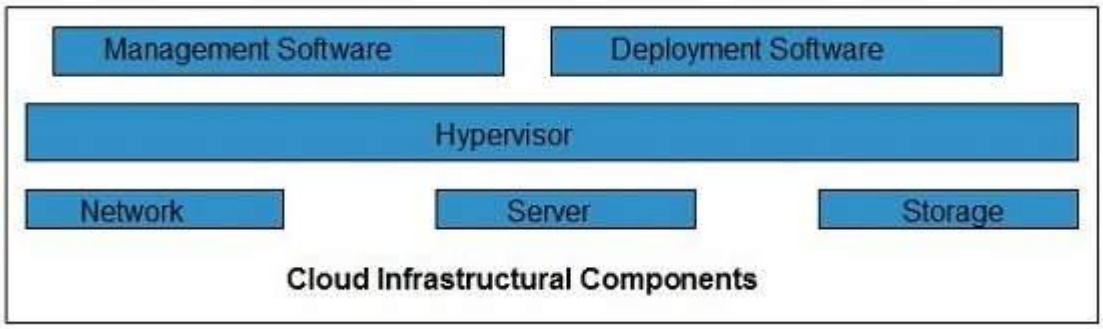


Figure 3: Cloud Infrastructure

There is term called public cloud provide the cloud for everyone. As the name implies they permit general public to access services and system to be easily accessible. Some service provider like Microsoft, Amazon, Google provide cloud services through internet. The model of public cloud is shown in figure given below:

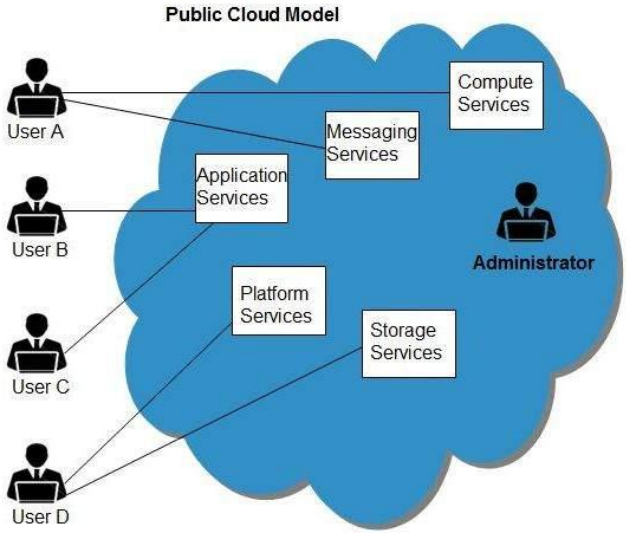


Figure 4: Public cloud model

## IV. THE CLOUD MODEL SERVICES

Three types of services that are provided by clouds are given below:

1. **SaaS**. It is known as Software as a Service. By using this type of services, the client can use the application of the provider that running on the infrastructure of cloud. This type of services can access through several users, from a interface of thin client like web browser.

2. **PaaS**. It is known as Platform as a Service. This type of services allow user to deploy his application on cloud. And there is no need to install any tool or platform on its local machine. To build a higher level service the Paas provide platform layer resources that include software development framework and operating system.

3. **IaaS**. It is known as Infrastructure as a Service. This type of services provides storage, network, fundamental resources and provision processing to customer. The client can run and deploy the software that include applications and other software.

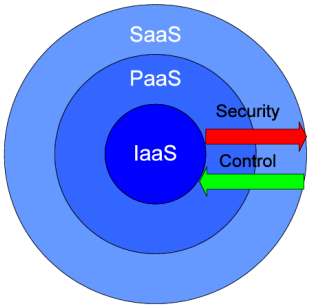


Figure 5: Cloud computing services

## V. CLOUD COMPUTING SECURITY THREATS

There are many security threats in cloud computing. They are describe below:

1. Data ruptures. The danger of an information break isn't one of a kind to distributed computing, however it reliably positions as a top worry for cloud clients.
2. Human blunder. As indicated by Jay Heiser, inquire about VP at Gartner, "Through 2020, 95% of cloud security disappointments will be the client's issue."

3. Data misfortune with no reinforcement. A mishap or disaster can prompt the perpetual loss of client information except if there are measures set up to back up that information.
4. Insider dangers. An ongoing examination report noted, "53% of associations reviewed affirmed insider assaults against their association."
5. DDoS assaults. Conveyed forswearing of-administration assaults present critical dangers to cloud clients and suppliers, including protracted administration blackouts, reputational harm, and introduction of client information.
6. Insecure APIs. As the open "front entryway" to your application, an API is probably going to be the underlying section point for aggressors. Use pen testing to reveal security shortcomings in the APIs you use.
7. Exploits. The multitenancy idea of the cloud (where clients offer registering assets) implies shared memory and assets may make new assault surfaces for vindictive on-screen characters.
8. Account capturing. Utilizing stolen accreditations, assailants may access basic zones of distributed computing administrations, trading off the secrecy, uprightness, and accessibility of those administrations.
9. Advanced tireless dangers. Many progressed tireless risk bunches target cloud conditions as well as utilize open cloud administrations to direct their assaults.
10. Spectre and Meltdown. Assailants can misuse Meltdown to see information on virtual servers facilitated on similar equipment, conceivably grievous for distributed computing has. Ghost is surprisingly more.

## VI. TECHNIQUES USED TO SOLVE SECURITY ISSUES

There are many techniques used in the cloud computing to solve the security issues. Some of them are described below:

1. Authentication and identity

To view the data of a user, the user can set the access right, this is called authentication. The most widely used authentication technique is cryptography [19]. This technique provides the data accessing permission by the use of security tokens and password. This is the solution of confidentiality and privacy issues.

2. Data encryption

In data encryption data or information is converted in a non readable text or we can say in a code that is called cipher text [19]. And the receiver's end that is decrypted in the normal text. To encrypt and decrypt the text an encrypt key is used. There are several encryption algorithm are used some of them are MDS, RSA, AES etc. This technique provides the solution of malicious attack, confidentiality and privacy issues.

3. Service Level Agreement (SLA)

Service level agreement known as an agreement between customer and the user. In this agreement it is shown that when user need the resources that it will be available or not [19]. This is the solution of problem of availability of resources. It is the way through which it can possible to take a backup of local resources.

4. Backing up of data

In cloud network backing up the data provide data security and accessibility of information securely. If the data is lost then the data can recover easily as backup is there. So it reduce the data loss and provide security.

## VII. THE CLOUD COMPUTING ARCHITECTURE AND SECURITY IMPLICATIONS

There are mainly three deployment models and three service delivery models in cloud computing exists [20-24].

The deployment models are:

(1) Private cloud: as the name implies the private cloud only available for specific applications and organizations .

(2) Public cloud: the cloud that is available for general public is considered as public cloud.

(3) Hybrid cloud: This is the combination of public and private cloud. A private cloud allow to use the in public clouds

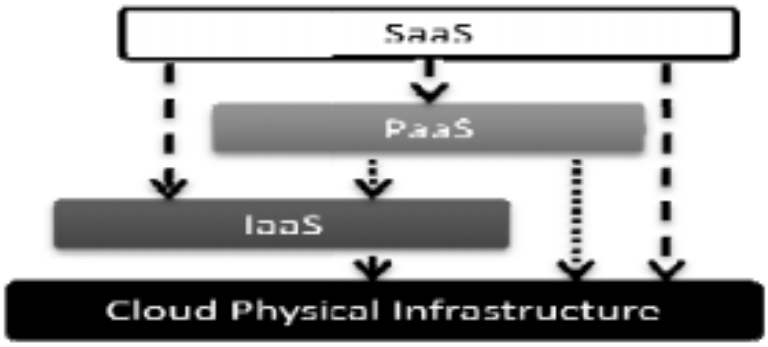


Figure 6: cloud service delivery models

## VIII. CONCLUSION

Cloud computing is the most emerging topic for research. It made user both edgy and excited. Cloud computing provide several services and applications. Security in cloud computing is the major question and there is need to solve all the security related problems. It should provide a secure and safe environment to get the data. This study analyzes the various techniques and methods to provide the data in a secure manner.

## REFERENCES

1. Almorsy, Mohamed & Grundy, John & Müller, Ingo. (2016). An Analysis of the Cloud Computing Security Problem.
2. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing",Journal of Internet Services and Applications, 2013, Volume 4, Number 1, Page 1.

3. Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011 http://www.gartner.com/it/page.jsp?id=1454221 Online.
4. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.
5. Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.
6. Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011.
7. Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.
8. Centre for the Protection of National Infrastructure: Information Security Briefing 01/2010 Cloud Computing. 2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
9. Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10) 2010, 278–281.
10. KPMG: From hype to future: KPMG's 2010 Cloud Computing survey.. 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291
11. Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.
12. Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009.
13. Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail – Joon and Ahn Arizona State University, "Security and Privacy Challenges in Cloud Computing Environments", IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31.
14. Mingi Zhou et al., "Security and Privacy in Cloud Computing: A Survey," Proc. 6th Int'l Conf. Semantics, Knowledge and Grids, IEEE Press, 2010, pp. 105–112.
15. KrS. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal: Network and Computer Applications, vol. 34, 2010, no. 1, pp. 1– 11.
16. simir Popovic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges," Proc. 33rd Int'l Convention on Information and Comm. Technology, Electronics and Microelectronics (MIPRO 10), IEEE Press, 2010, pp. 344–349.
17. Kui Ren, Cong Wang, and Qian Wang, llinois Institute of Technology, "Security Challenges for the Public Cloud", IEEE Press, 2012, pp. 69 – 73.
18. Hsin-Yi Tsai, Melanie Siebenhaar and André Miede, Yu-Lun Huang, Ralf Steinmetz, "Threat as a Service? Virtualization's impact on Cloud Security", IEEE, IT Pro, 2012, pp: 32- 37.
19. Garima Gupta, P.R.Laxmi and Shubhanjali Sharma," A Survey on Cloud Security Issues and Techniques".
20. S. Subashini, ,Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.
21. Susilo, D., Christantyawati, N., Prasetyo, I. J., & Juraman, S. R. (2019, March). Content analysis of LINE application user: intersecting technology and social needed. In *Journal of Physics: Conference Series* (Vol. 1175, No. 1, p. 012224). IOP Publishing.
22. De Leon, M. V. (2019). Factors influencing behavioural intention to use mobile banking among retail banking clients. *Jurnal Studi Komunikasi*, *3*(2), 118-137.
23. D. A. P. Sari, S. Innaqa, and Safrilah, "Hazard, Vulnerability and Capacity Mapping for Landslides Risk Analysis using Geographic Information System (GIS)," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 209, no. 1, p. 012106, Jun. 2017.
24. R. Rahim *et al.*, "HASHING VARIABLE LENGTH APPLICATION FOR MESSAGE SECURITY COMMUNICATION," *ARPN J. Eng. Appl. Sci.*, vol. 14, no. 1, pp. 259–264, 2019.