

Important Impact of Security Issues and typical Challenges In Hybrid Cloud Virtualization

Binay Kumar, Salsoor, Ayub Mohammed

Assistant Professor, AISSMS Institute of Information Technology

Article Information

Received : 10 Feb 2025
Revised : 16 Feb 2025
Accepted : 20 Feb 2025
Published : 23 Feb 2025

Corresponding Author:

Binay Kumar

Abstract— This paper presents Present day's information technology organizations are faced with an increase in the challenge and convolution of improve their IT finances for the best potential shipment of service to inner and outer clients. Decrease infrastructure costs, establish IT management, and raise service shipment. The cloud based more than companies are maintained the ADP earnings work and upload unofficial data regular to the work contributor cloud environs. The hybrid cloud consists where the protect services contributor are responsibility for the infrastructure, security controls and security proficiency recommend by the cloud service. The cloud present provides service new technology to suitable secures the data and approach that occupy on their physical infrastructure. We are proposed in this paper present threats and fire wall of the service to maintain the combined member of staff and contract record with entry in approach control authority guidelines for a cluster and extensive advance in the cloud.

Keywords: cloud, infrastructure, security

Copyright © 2025: Binay Kumar, Salsoor, Ayub Mohammed , This is an open access distribution, and reproduction in any medium, provided Access article distributed under the Creative Commons Attribution License the original work is properly cited License, which permits unrestricted use.

Citation: Binay Kumar, Salsoor, Ayub Mohammed , “Important Impact of Security Issues and typical Challenges In Hybrid Cloud Virtualization”, Journal of Science, Computing and Engineering Research, 8(2), February 2025.

I. INTRODUCTION

work and systems and servers. Two sides of personal subjects of attacks, data theft. The cloud physical servers are opposite and controlled by the companies. The cloud sever provide more than one servers are distributed the different customers. The single customer didn't support cloud client. Generally one or more customers are can do all Mainly identify particular the end points are attacks to cyber – attacks with the objective to steal data. Here can be find out different between single use potential subjects of attacks who may become victims through individual attacks on private cloud servers. Sometimes the company total applied to cyber data crime. It is true or not but attacks are target to particular person are much easier in the on-permission solutions. The cloud servers service support the point view, there is also the security challenge when the one or more than customer it is multi tenancy. The distributing of the resources between more than clients. The design of security issues authorised responsibility maintain to solution provide and the customer own itself. In case the multi customers are facing the security issues apply additional service provided to Third Party Company solve the secure service [10]. Cloud divided to possible the certain secure into different area consists infrastructure as a service, platform and application layer, administration and compliant. The infrastructure area service covers to possible threats in physical layer. The customer has access to the parts in the onpermission solution, but the cloud is managed provide the application

layer present by all applications are provided with in the cloud customer. The area of the problems related compliance to obtain laws and regulations are that maintain in giving area association with cloud computing, data storage, risk assessment, certifications and quality standards in the related state organizations [11].

II. PROPOSED HYBRID CLOUD SOLUTIONS

The main issues from personal experience with customers. Fig:1 . Hybrid cloud source

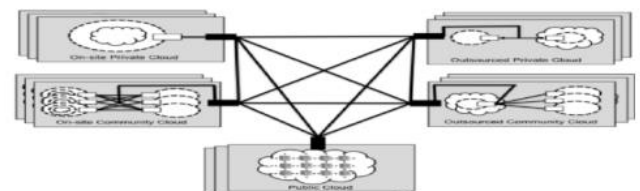


Fig:1 . Hybrid cloud source

1. Relocation of area controllers to the cloud. Support of more dealers is (for ex. When a more number of Desktop Computers) that at least one area controller is reality left as an in- home server (for ex. Un physically operating as a model server). Security should be done over an IPsee VPN channel with in directional faith. Often the authorized authentication is reality clarify with the corporate access within the faith talent of the in particular area [13][14].

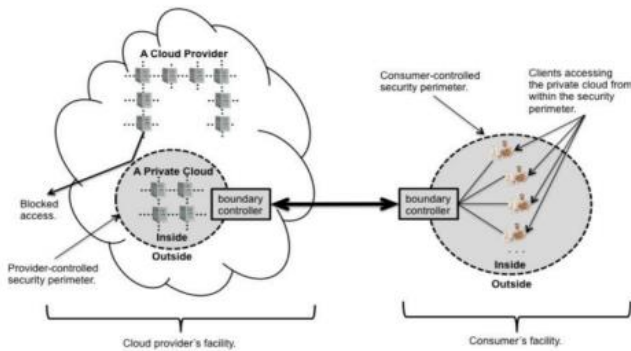


Fig-2.Outsource private cloud, source

Is another burden that customers have when they consider relocation to the cloud (relocation of some services in the cloud). Mostly it is required to manage in union of enterprise systems, more n are beyond mainly with the secure of the network between the public and private cloud servers. The services can authenticate to the area controller based on its location. It require to take into report that the systems, which last in-home infrastructure enclose extra confidential data .

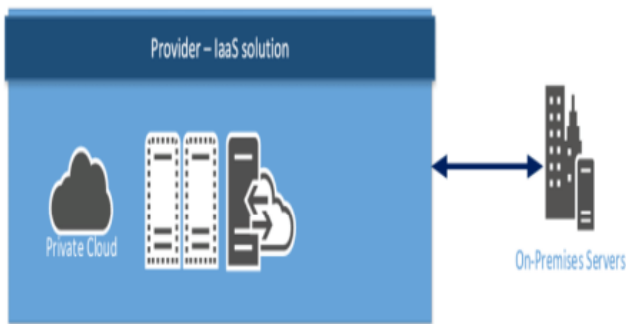


Figure 3 On-Premise Infrastructure connected to IaaS

3. Government wants to clarify the demand of private cloud, but source at a company. The term “Outsource private cloud” is a un sufficient bit false mow ever this plan is workable. Specific location is given by cloud providers for the entire private cloud, which is complete in the text of an remote security boundary. Fig-2.Outsource private cloud, source

III. SOLUTION PROSPECTS

The first option is a position, where a company has its own infrastructure with information systems or virtualization and possibly private cloud- thus provides its employee virtualized applications (eg. App-v) or a full displayed model of an Infrastructure as a Service private cloud design on one of hypervisors (Microsoft, VMWare, Citrix or others). The plan company wants to reduce the usage of infrastructure to change it to the cloud. The company part of the IaaS will continue at the company operating its information system. The second part option will be

reallocated or removed. Then the public cloud will be invest predefine services (mail server), which will be network to the physical servers (onsite) see figure 3)

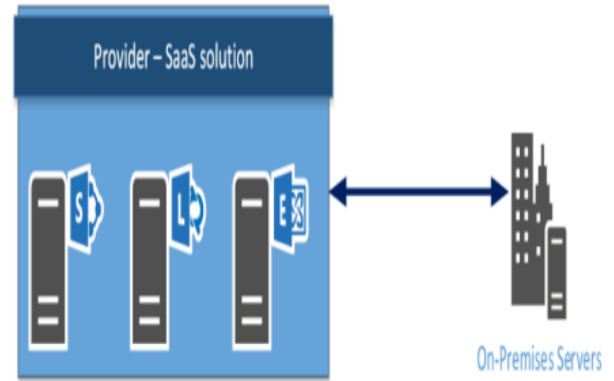


Figure 4 On-Premise Infrastructure connected to SaaS

Figure 3 On-Premise Infrastructure connected to IaaS User authentication is reality clarify each of two over particular accounts (login to cloud services), unite authentication (i.e network area filter company with authentication in the cloud) or possibly even through adding a second option in the form of multi-factor authentication (ex. Cell phone) Figure 4 On-Premise Infrastructure connected to SaaS B. The second option is a schema where a company has the same infrastructure as in the first one, but wants to relocation virtualized servers to the public cloud (IaaS). The advantage of such a schema is mainly a brighten of physical servers, reducing the cost and employees (administrators) etc. Here can be identified the security change in pathway between private and publicIaaS. Government and companies have to clarify serval key points that confuse selecting sure hybrid cloud solutions. Data that is inside the company cannot be change to the cloud, either due to data confidentiality due to requirement to have them in on-premise solutions by the law or other any ISO stands. If the data will be relocation to the public cloud, where it will be physical data stored question asking? Companies often do not want their data to leave the country and search for a cloud provider with data centres in the Czech Republic of this reason [15]

	PRIVATE	PUBLIC	HYBRID	COMMUNITY
SCALABILITY	Limited	Very High	Very High	Limited
SECURITY	Most Secure Options Available	Moderately Secure, Depends Greatly On Service	Very Security	Very Security
PERFORMANCE	Very Good	Low To Medium	Good	Very Good
RELIABILITY	Very High	Medium	Medium To High	Very High
COST	Require More Resources	Pay-As-You-Go-Model	\$\$	\$\$

Figure-5 Overview of parameters regarding to cloud deployment models.

IV. SOLUTION DESIGN

A private cloud outsourcing secure solution provide final customer the company require within the infrastructure to use. The private cloud in the in home private cloud incorporate outsource of limit of additional service if its require provide their own servers and take their infrastructure can be changed to environment to a public cloud. It will provide Software as a Service (SaaS) service takes risk only delicious data. Where there is private cloud that is both hosted/outsourced by a provider- a company with a centre in the republic and placed In- home infrastructure on the another side. The distribution of services and therefore not necessarily wants to have complete redundancy of all the services in private cloud provides in –home infrastructure. The manages provides commit infrastructure with in all security requirements for personal agreements written to administration. This company is internal services and physical servers solve the secure issues. The sharing of hardware along customer support of physical infrastructure and proper communication implemented to hybrid plot done. The authentication wants on-site infrastructure operates to danger systems. Next take immediately to connect the system authentication secure channel with servers that are located at the provider (virtual private network, encrypt, multiple authentication etc.). If any problem facing diving services will be operated with in a private in –home solutions within an internal solution that tend to be service on authentication and identity management, document management for under legislation. If another information system it is not possible to move to a private cloud for n different reasons.

V. CONCLUSIONS

The cloud solutions surely solve specific problems of our time and bring a lot of value in use. In the form of cost saving infrastructure services. Mainly maintains returns of finances. First of all immediately to plan the transition. Then mainly risk problems facing services issues. The services are provides find similar or small less in the cloud environment in –home infrastructure. The highest security risk of the “path or Channel” between the in –home and cloud infrastructure of provide service. It is maintained the quality and security of the customers own infrastructure and the wants to secure the web site connection. Another challenged issue remains centralizing the authentication of personal users, under deployment, and constantly supplemented with new additions to the “simple” authentication. For examples authentication using biometrics and mobile phones, face recognition .etc.

REFERENCES

[1]. P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, Raja Raju, "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN

Model", *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 1955009, 13 pages, 2022. <https://doi.org/10.1155/2022/1955009>.

[2]. D. Sathyanarayanan, T. S. Reddy, A. Sathish, P. Geetha, J. R. Arunkumar and S. P. K. Deepak, "American Sign Language Recognition System for Numerical and Alphabets," 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2023, pp. 1-6, doi: 10.1109/RMKMATE59243.2023.10369455.

[3]. J. R. Arunkumar, Tägele berihun Mengist, 2020" Developing Ethiopian Yirgacheffe Coffee Grading Model using a Deep Learning Classifier" *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, Volume-9 Issue-4, February 2020. DOI: 10.35940/ijitee.D1823.029420.

[4]. Ashwini, S., Arunkumar, J.R., Prabu, R.T. et al. Diagnosis and multi-classification of lung diseases in CXR images using optimized deep convolutional neural network. *Soft Comput* (2023). <https://doi.org/10.1007/s00500-023-09480-3>

[5]. J.R.Arunkumar, Dr.E.Muthukumar," A Novel Method to Improve AODV Protocol for WSN" in *Journal of Engineering Sciences*" ISSN NO: 0377-9254Volume 3, Issue 1, Jul 2012.

[6]. R. K. A. Shameem, P. Biswas, B. T. Geetha, J. R. Arunkumar and P. K. Lakineni, "Supply Chain Management Using Blockchain: Opportunities, Challenges, and Future Directions," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421633.

[7]. Arunkumar, J. R. "Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies." *Journal of Science, Computing and Engineering Research* 6.8 (2023): 06-10.

[8]. J. R. Arunkumar, R. Raman, S. Sivakumar and R. Pavithra, "Wearable Devices for Patient Monitoring System using IoT," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 381-385, doi: 10.1109/ICCES57224.2023.10192741.

[9]. S. Sugumaran, C. Geetha, S. S, P. C. Bharath Kumar, T. D. Subha and J. R. Arunkumar, "Energy Efficient Routing Algorithm with Mobile Sink Assistance in Wireless Sensor Networks," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10201142.

[10]. R. S. Vignesh, V. Chinnammal, Gururaj.D, A. K. Kumar, K. V. Karthikeyan and J. R. Arunkumar, "Secured Data Access and Control Abilities Management over Cloud Environment using Novel Cryptographic Principles," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199616.

[11]. Syamala, M., Anusuya, R., Sonkar, S.K. et al. Big data analytics for dynamic network slicing in 5G and beyond with dynamic user preferences. *Opt Quant Electron* 56, 61 (2024). <https://doi.org/10.1007/s11082-023-05663-2>

[12]. Krishna Veni, S. R., and R. Anusuya. "Design and Study Analysis Automated Recognition system of Fake Currency

- Notes." *Journal of Science, Computing and Engineering Research* 6.6 (2023): 16-20.
- [13]. V. RamKumar, S. Shanthi, K. S. Kumar, S. Kanageswari, S. Mahalakshmi and R. Anusuya, "Internet of Things Assisted Remote Health and Safety Monitoring Scheme Using Intelligent Sensors," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199766.
- [14]. R. S. Vignesh, R. Sankar, A. Balaji, K. S. Kumar, V. Sharmila Bhargavi and R. Anusuya, "IoT Assisted Drunk and Drive People Identification to Avoid Accidents and Ensure Road Safety Measures," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10200809.
- [15]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.
- [16]. G. Karthikeyan, D. T. G, R. Anusuya, K. K. G, J. T and R. T. Prabu, "Real-Time Sidewalk Crack Identification and Classification based on Convolutional Neural Network using Thermal Images," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1266-1274, doi: 10.1109/ICACRS55517.2022.10029202.
- [17]. R. Meena, T. Kavitha, A. K. S, D. M. Mathew, R. Anusuya and G. Karthik, "Extracting Behavioral Characteristics of College Students Using Data Mining on Big Data," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10084276.
- [18]. S. Bharathi, A. Balaji, D. Irene, J. C. Kalaivanan and R. Anusuya, "An Efficient Liver Disease Prediction based on Deep Convolutional Neural Network using Biopsy Images," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1141-1147, doi: 10.1109/ICOSEC54921.2022.9951870.
- [19]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.
- [20]. Revathi, S., et al. "Developing an Infant Monitoring System using IoT (INMOS)." *International Scientific Journal of Contemporary Research in Engineering Science and Management* 6.1 (2021): 111-115.
- [21]. R. K, A. Shameem, P. Biswas, B. T. Geetha, J. R. Arunkumar and P. K. Lakineni, "Supply Chain Management Using Blockchain: Opportunities, Challenges, and Future Directions," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421633.
- [22]. J. R. Arunkumar. "Comprehensive Analysis of Security Issues in Cloud Computing Technologies", *Journal of Science, Computing and Engineering Research*, 6(5), 06-10, June 2023.
- [23]. S. Sugumaran, C. Geetha, S. S, P. C. Bharath Kumar, T. D. Subha and J. R. Arunkumar, "Energy Efficient Routing Algorithm with Mobile Sink Assistance in Wireless Sensor Networks," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10201142.
- [24]. I. Chandra, K. V. Karthikeyan, R. V, S. K, M. Tamilselvi and J. R. Arunkumar, "A Robust and Efficient Computational Offloading and Task Scheduling Model in Mobile Cloud Computing," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICECONF57129.2023.10084293.
- [25]. R. S. Vignesh, A. Kumar S, T. M. Amirthalakshmi, P. Delphy, J. R. Arunkumar and S. Kamatchi, "An Efficient and Intelligent Systems for Internet of Things Based Health Observance System for Covid 19 Patients," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICECONF57129.2023.10084066.
- [26]. DC Jullie Josephine, J. Sudhakar, T. Helan Vidhya, R. Anusuya, G. Ramkumar, "An Improved Multi class Breast cancer classification and Abnormality Detection based on Modified Deep Learning Neural Network Principles", *Deep Learning in Biomedical Signal and Medical Imaging*, CRC Press, Taylor and Francis, 2024.
- [27]. R. Anusuya, Pragya Vashishtha, "Real Automatic Number Plate Image Detection With Yolo Algorithms", *Journal of Science, Computing and Engineering Research*, 7(7), July 2024.