engineering proceedings

MDPI

Proceeding Paper

Multi-Level Cloud Datacenter Security Using Efficient Hybrid Algorithm †

Koushik Chakraborty [1], Amrita Parashar [2], Pawan Bhambu [3], Durga Prasad Tripathi [4], Pratap Patil [5] and Gaurav Kumar Srivastav [6,*]

[1] Office of the Registrar, Adamas University, Kolkata 700126, India; koushik215@gmail.com
[2] Department of Computer Science and Engineering, Vellore Institute of Technology, Bhopal 466114, India; amritaparashar05@gmail.com
[3] Department of Computer Science and Engineering, Vivekananda Global University, Jaipur 303905, India; pawan.bhambu@vgu.ac.in
[4] Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522502, India; tripathi@kluniversity.in
[5] Department of Information Technology and Engineering, Amity University in Tashkent, Tashkent 5300016, Uzbekistan; pratapmcs@gmail.com
[6] Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow 226010, India
* Correspondence: gaurav.bsnl22@gmail.com
† Presented at the International Conference on Recent Advances on Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: Security is currently the main boundary for cloud-based administrations. It is not adequate to just consolidate the cloud by adding a couple of additional controls or component answers for your current organization security programming. Businesses must utilize both virtual and physical information center security frameworks to keep them secure. The objective is to defend it from dangers that may jeopardize the secrecy, judgment, or openness of mental property or commerce data resources. These are the fundamental central focuses of all assigned attacks, and in this way, they require a high degree of security. Hundreds to thousands of physical and virtual servers are partitioned up into information centers agreeing to sort applications, information classification zones, and other criteria. To protect applications, frameworks, information, and clients, information center security takes on the workload over physical information centers and multi-cloud situations. It also applies to open cloud data centers. All server ranches ought to protect their applications and data from a rising number of refined threats and around-the-world ambushes. Each organization is at risk of assault, and numerous organizations have been compromised without being mindful of it. An evaluation of your resources and business necessities is important to improve a spotless way to deal with your way of life and cloud security technique. To deal with a strong mixture of multi-cloud wellbeing program, you should lay out perceivability and control. You can consolidate incredible controls, organize responsibility dispersion, and lay out fantastic gambles on the board with the assistance of safety items and experts.

Keywords: cloud security; security parameters; cloud resources; security techniques; security types

Citation: Chakraborty, K.; Parashar, A.; Bhambu, P.; Tripathi, D.P.; Patil, P.; Srivastav, G.K. Multi-Level Cloud Datacenter Security Using Efficient Hybrid Algorithm *Eng. Proc.* **2023**, *59*, 50. https://doi.org/10.3390/engproc2023059050

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 14 December 2023

1. Introduction

Cloud security is shared by the client and the cloud supplier. Undertakings are fundamentally partitioned into three classes as indicated by the Common Obligation Model: obligations that are generally the supplier's, obligations that are dependably the clients, and obligations that change considering the supplier's model, like the Infrastructure as a Service (IaaS), Data as a Service (DaaS), Network as a Service (NaaS), and Platform as a Service (PaaS), among others [1]. Security obligations that are constantly performed by organizations incorporate the actual framework, as well as admittance to, fixing, and arrangement of

the actual hosts and the actual local area on which the registering frameworks, stockpiling, and different resources live [2]. The administration of clients and their entrance honors, the anticipation of unapproved admittance to cloud accounts, the encryption and security of cloud-based information resources, and the administration of their security pose are generally the client's security obligations [3,4]. As a rule, cloud specialist organizations are largely responsible for creating backends to battle security blemishes. Other than picking a security-conscious provider, clients ought to focus generally on a real assistance plan and safe use penchants. Clients ought to likewise verify that any end-client equipment and organizations are secure [5,6].

2. Security Types

Outsider suppliers offer different sorts of cloud administration as modules for the cloud climate. You might be liable for an alternate level of the help's parts, which is contingent upon the sort. The supplier is accountable for dealing with the actual organization, information capacity, information waiters, and PC virtualization structures in any outsider cloud administration [7,8]. The assistance is virtualized on the supplier's servers and conveyed to clients by means of their inside oversaw network for remote access, as shown in Figure 1. Clients can access their processing necessities from any place with a web network thanks to this offloading of equipment and other foundation costs. The cloud suppliers in the IaaS model do not uncover the framework layer to their clients and have unlimited authority over it. Clients of the cloud every now and again miss the mark on the capacity to precisely recognize, evaluate, or imagine their cloud surroundings [9]. Scale and speed are utilized to arrange and decommission cloud resources progressively. Cloud client jobs are regularly set up in an exceptionally free manner, giving a larger number of honors than are needed or expected [10]. Meetings are presented to security gambles at the application level when keys and honors are not as expected arranged.

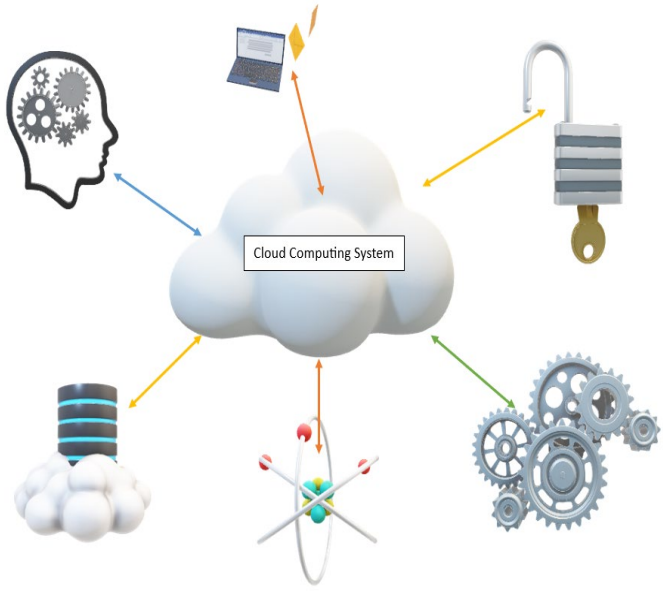

Figure 1. Cloud security resources.

3. Cloud Resource Security

The concentrated perceivability and strategy-based granular control are just given by an incorporated local cloud and outsider security stack. The higher the degree of confirmation, the greater the honors. Furthermore, great IAM cleanliness, for example, authorizing vigorous secret word arrangements and consent breaks, ought not to be disregarded along with the controls across legitimately disconnected organizations and microsegments for zero-trust cloud network security [11].

By wisely cross-referring to accumulated log information with interior information like the resources and arrangement shown in Figure 2 frameworks, weakness scanners, etc., and furthermore, outside information, for example, geolocation data sets and public danger insight, we took care of [12]. Moreover, they offer devices that accelerate episode reaction times and help with picturing and questioning the dangerous scene.

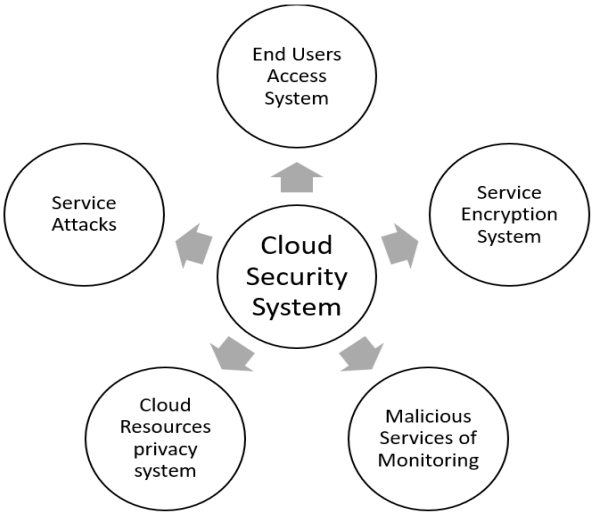

Figure 2. Security applications of cloud resources.

4. Security Parameters

One part of cloud security that deals with the specialized side of danger anticipation is information security. Clients and suppliers can erect boundaries that keep delicate information from being seen or gotten to [13]. Encryption is one of the best of these choices. Your information is mixed during encryption, making it simply open to those with the encryption key. Your information will be successfully mixed up and pointless on the off chance that it is taken or lost. The cloud security parameters are shown in Figure 3. Cloud networks put an accentuation on information travel securities like virtual confidential organizations [14].

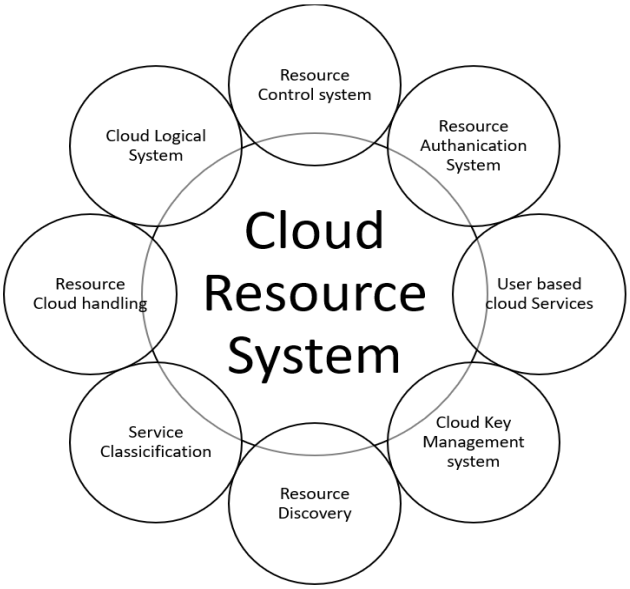

Figure 3. Security parameters of cloud resources.

The entrance privileges conceded to client accounts are the subject of character and access for the executives. This additionally applies to the administration of client account approval and verification. Access controls are fundamental for keeping genuine and vindictive clients from accessing and compromising touchy frameworks and information [15]. IAM covers things like the secret words of the executives and multifaceted verification, in addition to other things. The cloud act forces its own legitimate limitations on cloud suppliers, conceivably to the detriment of client security. US unofficial law at present permits regulatory-level policing demands referencing data from cloud provider servers. While this might make it workable for examinations to continue effectively, it might likewise disregard some security freedoms and lead to the expected maltreatment of force [16]. A solitary, weak gadget or part can contaminate the remainder of an organization. At the point when they provide information capacity or different administrations, cloud suppliers open themselves to dangers from an extensive variety of end clients. To determine most cloud security issues, clients and cloud specialist organizations should stay proactive about their separate jobs in network protection. Specialized and social client security preparation. Eventually, for both cloud specialist organizations and clients to stay safe, straightforwardness and responsibility will be fundamental [5].

5. Hybrid Security System

A part of network protection dedicated to shielding distributed computing frameworks is known as cloud security. This incorporates defending information across online-based stages, applications, and frameworks. Cloud specialist co-ops and the clients who use them, little to medium-sized organizations, and ventures should cooperate to access these frameworks. Through web associations that are dependable, cloud specialist co-ops have administration on their servers [17]. Cloud security strategies are utilized to protect client information privately on the grounds that their business relies upon client trust. In any case, the client is likewise, to some degree, liable for cloud security. Conventional network safety zeroes in on safeguarding the edge. Network protection experts should embrace an information-driven approach because of distributed computing security risks [4]. Networks face difficulties too from interconnectedness. Networks are much of the time penetrated by noxious entertainers utilizing split-the-difference or feeble qualifications. At the point when a developer sorts out some way to make an appearance, they can without a doubt broaden and include ineffectually shielded interfaces in the cloud to find data on different informational indexes or centers. They even have the choice of trading and putting away any taken information on their own personal cloud servers. Security in the cloud should envelop something beyond shielding information access. Access through the web and outsider information stockpiling both present their own dangers [18]. Your information access might be lost, assuming that those administrations are upset under any circumstances. At the point when servers endured equipment harm during a news blackout at an Amazon cloud information office, a few clients lost their information. This fills in as a decent representation of why you should keep nearby reinforcements of, in any event, a portion of your applications and information [19].

6. Proposed Algorithm

The research methodology for cloud security is very strongly proposed in this research article, and the availability of resources is shown in Figure 4. The Algorithm 1 works for the multi-level security system known as the hybrid algorithm. The algorithm consists of two algorithms with their best parameters. In this proposed algorithm, the cloud services available in the datacenters are considered input variables. The cloud services are first checked in terms of the availability zone. If the resources are available, then the resources will be provided under the first check algorithm, i.e., DES. Then, the resources have proper passing with RSA, and then the second check is passed using AES for the double check so that the services are provided in time for the end users.

Algorithm 1: The multilevel proposed hybrid algorithm provide security by using DES and AES.

Input: The cloud datacenters are counted as the input.
Output: The highly efficient security of cloud services between cloud users and datacenters.
1: Procedure (Methods:)
2: If (CD = Available) then
3: {
4: Perform the DES algorithm checks for the Availability Zone.
5: If (the DES checks services are not secure)
6: {
Perform the AES algorithm check for Availability Zone.
7: {
If (Service is highly secured) then
Step1: The Availability Zone. is secure.
8: }
end if
9: Step2: The Availability Zone. is less secure.
}
10: end if
11: end if
12: end procedure

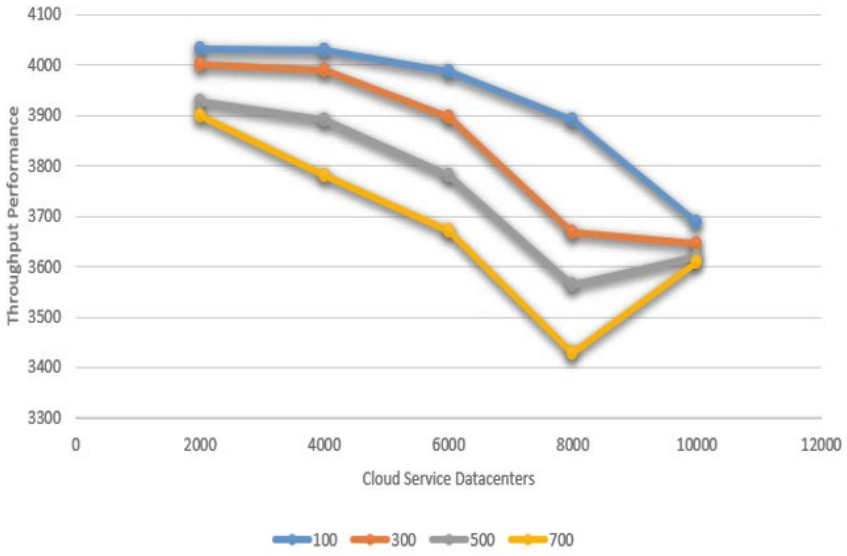

Figure 4. Throughput performance of cloud security.

7. Conclusions and Future Work

The conclusion defines the performance of cloud security for cloud resources. This security system is best when working with hybrid algorithms. In future, our research should be applied to fog computing and IoT services. For security and enterprise customers, hybrid cloud security services may be an excellent option. Because they are typically too complicated for personal use, they are best suited for security and enterprise applications. However, the combination of cloud scale and on-premises control of specific data could be utilized by these organizations. Sadly, malicious actors are increasingly looking for exploits on cloud-based targets as they realize their value. Even though cloud providers take on a lot of clients' security roles, they do not manage everything. This passes on even to non-specialized clients with the obligation to self-teach on cloud security.

Author Contributions: Conceptualization, K.C. and A.P.; methodology, P.B., D.P.T., P.P. and G.K.S.; validation, P.B., D.P.T., P.P. and G.K.S.; formal analysis, K.C. and A.P.; investigation, K.C. and A.P.; resources, P.B., D.P.T., P.P. and G.K.S.; data curation, K.C. and A.P.; writing—original draft preparation,

P.B., D.P.T., P.P. and G.K.S.; validation K.C. and A.P.; writing—review and editing, P.B., D.P.T., P.P. and G.K.S.; validation, K.C. and A.P.; visualization, P.B., D.P.T., P.P. and G.K.S.; supervision, K.C. and A.P.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kumar, S.; Kumari, B.; Chawla, H. Security challenges and application for underwater wireless sensor network. In Proceedings of the International Conference on Emerging Trends in Expert Applications & Security, Jaipur, India, 17–18 February 2018; Volume 2, pp. 15–21.
2. Kumar, S.; Gupta, U.; Singh, A.K.; Singh, A.K. Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. *J. Comput. Mech. Manag.* **2023**, *2*, 31–42. [CrossRef]
3. Koppaiyan, R.S.; Pallivalappil, A.S.; Singh, P.; Tabassum, H.; Tewari, P.; Sweeti, M.; Kumar, S. High-Availability Encryption-Based Cloud Resource Provisioning System. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence, Jaipur, India, 23–24 December 2022; pp. 1–6.
4. Singh, P.; Hailu, N.; Chandran, V. Databases for Cloud Computing: Comparative Study and Review. *Eur. J. Acad. Essays* **2014**, *1*, 12–17.
5. Manikandan, R.; Maurya, R.K.; Rasheed, T.; Bose, S.C.; Arias-Gonzáles, J.L.; Mamodiya, U.; Tiwari, A. Adaptive cloud orchestration resource selection using rough set theory. *J. Interdiscip. Math.* **2023**, *26*, 311–320. [CrossRef]
6. Srivastava, P.K.; Kumar, S.; Tiwari, A.; Goyal, D.; Mamodiya, U. Internet of thing uses in materialistic ameliorate farming through AI. *AIP Conf. Proc.* **2023**, *2782*, 020133.
7. Pain, P.; Sadhu, A.; Das, K.; Kanjilal, M.R. Design and Implementation of Multi-Operative Reversible Gate for Even/Odd Parity Generators in Quantum Based Technologies. *J. Comput. Mech. Manag.* **2023**, *2*, 20–28. [CrossRef]
8. Tiwari, A.; Garg, R. Eagle Techniques In Cloud Computational Formulation. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *1*, 422–429.
9. Khan, H.; Singh, P. Issues and Challenges of Internet of Things: A Survey. *J. Inform. Electr. Electron. Eng. (JIEEE)* **2021**, *2*, 1–8. [CrossRef]
10. Kumar, S.; Kumar, S.; Ranjan, N.; Tiwari, S.; Kumar, T.R.; Goyal, D.; Rafsanjani, M.K. Digital watermarking-based cryptosystem for cloud resource provisioning. *Int. J. Cloud Appl. Comput. (IJCAC)* **2022**, *12*, 1–20. [CrossRef]
11. Tiwari, A.; Garg, R. Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems. *Int. J. Semant. Web Inf. Syst. (IJSWIS)* **2022**, *18*, 1–18. [CrossRef]
12. Dora Pravina, C.T.; Buradkar, M.U.; Jamal, M.K.; Tiwari, A.; Mamodiya, U.; Goyal, D. A Sustainable and Secure Cloud resource provisioning system in Industrial Internet of Things (IIoT) based on Image Encryption. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence, Jaipur, India, 23–24 December 2022; pp. 1–5.
13. Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.* **2009**, *25*, 599–616. [CrossRef]
14. Calheiros, R.N.; Ranjan, R.; Beloglazov, A.; De Rose, C.A.; Buyya, R. CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Softw. Pract. Exp.* **2011**, *41*, 23–50. [CrossRef]
15. Buyya, R.; Abramson, D.; Giddy, J.; Stockinger, H. Economic models for resource management and scheduling in grid computing. *Concurr. Comput. Pract. Exp.* **2002**, *14*, 1507–1542. [CrossRef]
16. Kamble, S.; Saini, D.K.J.; Kumar, V.; Gautam, A.K.; Verma, S.; Tiwari, A.; Goyal, D. Detection and tracking of moving cloud services from video using saliency map model. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 1083–1092. [CrossRef]
17. Tiwari, A.; Garg, R. Orrs Orchestration of a Resource Reservation System Using Fuzzy Theory in High-Performance Computing: Lifeline of the Computing World. *Int. J. Softw. Innov. (IJSI)* **2022**, *10*, 1–28. [CrossRef]
18. Singh, S.; Singh, P.; Tanwar, S. Energy aware resource allocation via MS-SLnO in cloud data center. *Multimed. Tools Appl.* **2023**, *4*, 1–23. [CrossRef]
19. Singh, P. Energy Management in Cloud Through Green Cloud Technologies. *J. Manag. Serv. Sci. (JMSS)* **2022**, *2*, 1–11. [CrossRef]