


Proceeding Paper

A Futuristic Approach to Security in Cloud Data Centers Using a Hybrid Algorithm [†]

Dipankar Chatterjee ¹, Mostaque Md. Morshedur Hassan ², Nazrul Islam ^{2,*} , Asmita Ray ²
and Munsifa Firdaus Khan Barbhuyan ²

¹ Department of Information Technology, Techno India University, Kolkata 700091, India; dipankar.calcutta@gmail.com

² Department of Computer Science and Engineering, Assam Down Town University, Guwahati 781026, India; mostaq786@gmail.com (M.M.M.H.); rayasmi.dtu2020@gmail.com (A.R.); munsifa737@gmail.com (M.F.K.B.)

* Correspondence: nazrul87@rediffmail.com

[†] Presented at the International Conference on Recent Advances on Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: All associations use on-premises data focus. An on-premises data focus suggests that an association maintains all locally required IT systems. An on-premises data focus consolidates everything from the servers that support Web and email access to the provision of gear and communicates related data back to the organization to establish features like uninterrupted control. Data focus organization is not confined to ensuring that an establishments and program strategies are helpful. Data focus chiefs are also responsible for the security of their circumstances. Establishing a data community office is a sensible idea. Most do not have outside windows and, by and large, only a few entrances. Security staff surveil the inside of the structure, screening for dubious activity using footage from observation cameras positioned along the perimeter. This integrates the use of strong security measures, like two-factor confirmation, for all clients. It is also suggested to encrypt all data in movement, both inside the data center and between the data community and any external structures. The components of data centers must be safeguarded against physical threats. A data center's physical security controls include a secure location, physical access controls for the building, and monitoring systems. As organizations relocate on-premises IT frameworks to cloud specialist co-ops, cloud information capacity, cloud foundations, and cloud applications, it is vital to comprehend the safety strategies they implement and the service-level arrangements they have set up.

Keywords: cloud data center; cloud parameters; security system; cloud component; security parameters; cloud data stores



Citation: Chatterjee, D.; Hassan, M.M.M.; Islam, N.; Ray, A.; Barbhuyan, M.F.K. A Futuristic Approach to Security in Cloud Data Centers Using a Hybrid Algorithm. *Eng. Proc.* **2023**, *59*, 47. <https://doi.org/10.3390/engproc2023059047>

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

Published: 14 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A cloud data center moves traditional on-prem data. A cloud data focus moves a regular on-prem data focus off-site. Instead of supervising their own system, an association rents an establishment regulated by an outside associate and obtains data focus resources over the Internet [1]. In these circumstances, the cloud benefit provider is aware of required maintenance and updates and obtains an advantage-level understanding of the pieces of the system stack within their direct control. Data focuses comprise parts set up to perform three principal functions. Process resources provide the memory and control required to run applications. Limited resources have undertaking data on a collection of media, counting fortifications [2]. Organizing resources reinforces interchanges between the various parts of the data center and the outside world. Present-day data habitats have superior class structures, causing several difficulties for data focus chiefs and characterizing data communities comprising various gear and PC program game plans from various merchants [3,4]. Data focus chiefs are responsible for conveying, orchestrating, checking, and maintaining systems and their connected licenses, security, and re-designs, and this is just

the beginning when considering various data habitats with moving advancement levels [5]. In Figure 1, a description of hybrid cloud data center features is provided. Data focus chiefs should meet specific SLAs, providing openness, data support, recovery speed, etc., for complex circumstances. Data focus chiefs are expected to maintain consistent contact with organizations and applications regarding closing plans. This involves ensuring that each data center has the resources required and executing changes taken after modifying an organization's underwriting structure. Figure 1 explains hybrid cloud data system features. Data focuses should utilize strict spending plans in which essential and cooling costs are prioritized. These qualities and assets are to be acquired considering the qualities they bring rather how they fit to a data community's requirements and difficulties [6–8]. Data focuses support all endeavors from registration and management to business applications. To the extent that current businesses utilize PCs, the data community is critical. Data focus centers enables associations consider how they control their data, thus prompting associations to focus on IT and data when the preparing the workforce, registering and sorting out network establishment, and determining a plan for office security [9].

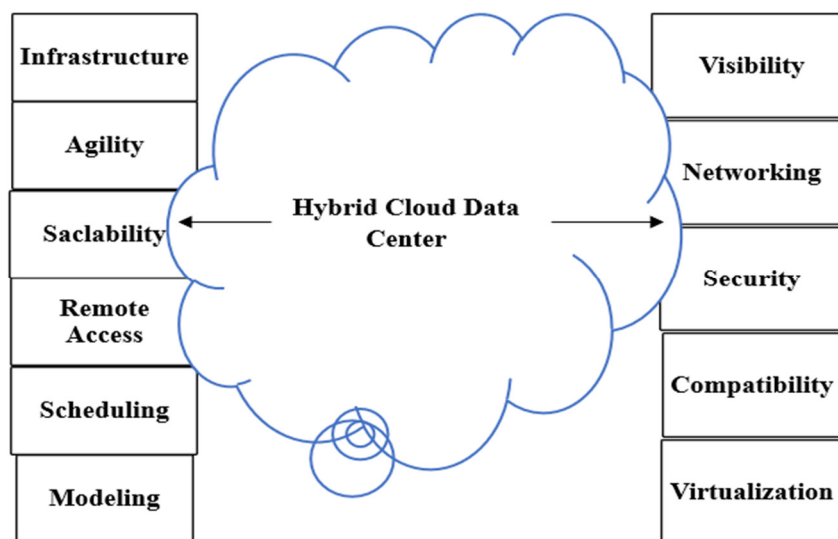


Figure 1. Features of a hybrid cloud data center.

A data community—also known as a data center or data focus—might be an office comprising coordinated PCs, limit structures, and processing establishments that organizations and different associations use to arrange, handle, and store enormous amounts of data, as well as to communicate. Trade consistently relies heavily upon the applications, organizations, and the data inside a data community, making data communities critical issues and fundamental assets for customary tasks [10]. Adventure data focuses on continuously joining distributed computing resources and workplaces to provide and guarantee in-house, local resources. As endeavors logically transition to distributed computing, the limits between cloud suppliers' data habitats and data focuses become less clear. Data focus chiefs must ensure that data habitats can achieve a benefit-level understanding of these resources [7]. This consolidates critical organization in the long term and checking and responding to conditions that might influence a data center's tasks in the present moment [11].

2. Related Work

Data center organizations are expected to handle various distinct subjects connected with the data community. The organization of an actual data center office might integrate commitments connected with the office's veritable inheritance, utilities, reputation, and staff. Data center features integrate equipment assets and program approval and release organization [11–13]. A data center's structural organization lies at the point of intersection

of IT and office organization and is consistently satisfied by paying attention to data focus execution to upgrade essentialness, equipment, and floor use. The data community provides specific organization services to an association and, accordingly, it also provides services to the end clients of the association. Data center organization integrates the everyday structures and organizational systems provided by a data center [14]. Figure 2 explains the service providers working for the data center so that the end users may receive the most appropriate cloud services.

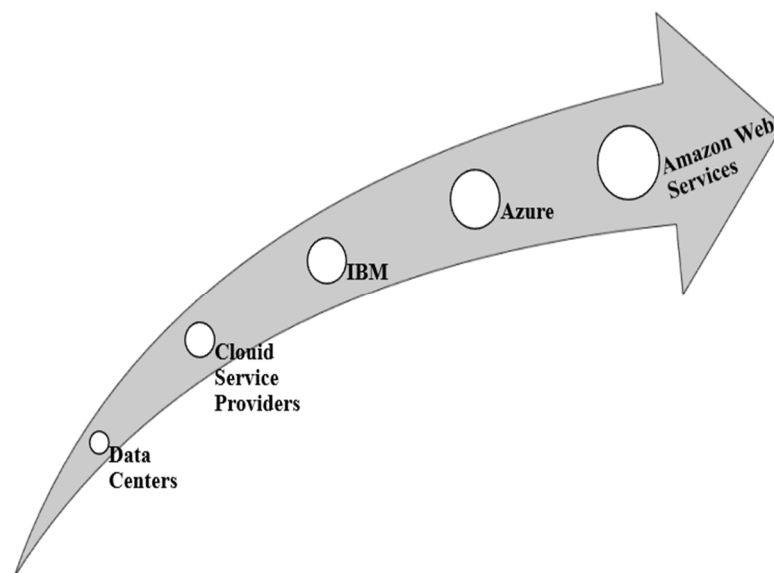


Figure 2. Role of cloud data centers in cloud providers.

Fast, flexible risk disclosure and response are essential to limiting the impact and results a potential security event. Robotization and coordination boost the amplexness of slope security packages by automating normal and scheduled security tasks. Most associations receive hybrid cloud services, distributing their structures among open and confidential cloud services. Hybrid cloud security is essential to avoiding the sidelong growth of risk in an association's current circumstance. Serverless game plans provide various advantages to an association, like extended flexibility and versatility, as well as reduced cost and the organization mentioned above [15,16]. In any case, they additionally require specially designed serverless security plans to supply comprehensive security and quality risk detection and control. Security teams cannot access what they cannot see. Organizing security and quality risk detection—improved with knowledge of risk is fundamental to security teams' ability to distinguish and respond effectively to risks [17].

The growth of virtualization has incorporated one more crucial estimation into data focus structure organization. At present, virtualization supports the pondering of servers, frameworks, and limits, allowing each registering resource to be coordinated into pools regardless of their actual region. Action planning, event limiting, and server virtualization can be executed through a PC program, giving programming-characterized data centers balance. Directors can then choose a course of action, delegate responsibilities, limit events, and to be sure arrange services from these normal resource pools. When chiefs no longer need these resources, they can return them to the pool for reuse [18–20].

3. Cloud Data Center Parameters

The migration from an on-premises data focus to a cloud data focus does not mercifully move everything to the cloud. Various organizations have hybrid cloud data focuses which have a mix of on-premises data focus parts and virtual data place parts [7]. Figure 3 defines the services provided by different cloud services, with several parameters. In the figure below, we can perceive how as-an-administration models are moving the ownership

of data focuses and the parts of these establishments from a completely guaranteed and operated on-premise office to an item benefit show [20].

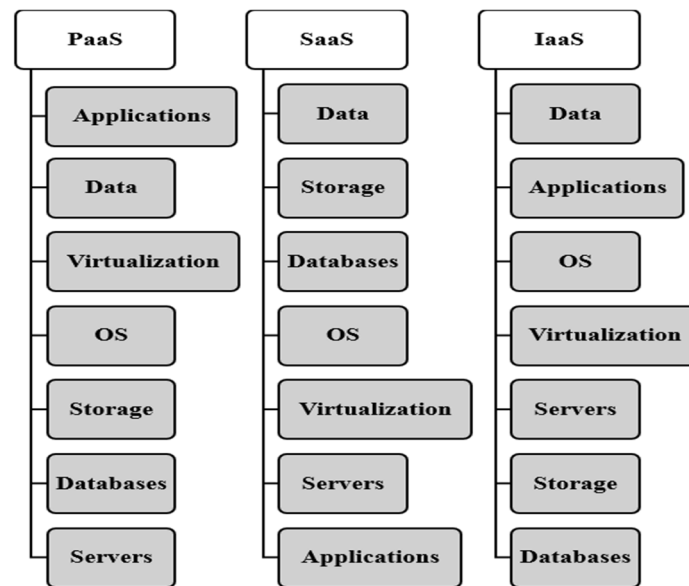


Figure 3. Service managed by cloud data centers.

The transition to the cloud suggests that data community security is more complicated than at any time in recent memory. As data focus managers move systems and organizations to the cloud, they should do so securely while ensuring data focus resources meet the needs of their clients [13]. For a data center, a versatile security strategy is fundamental and should offer flexibility; this is one of the greatest advantages of cloud-based establishments. Hyperscaler-arranged security ensures that security resources can reliably scale to meet solicitation. Data focus requires protection against the latest digital risks. NGFWs provide broad security to an association's on-prem or cloud-based data center [12]. Present-day data communities cause the widespread use of observational and organizational programs. These programs, including DCIM instruments, restricted licensing, and IT, allow data focus chiefs to screen offices and equipment, degrees of execution, recognize dissatisfactions, and realize a wide range of corrective exercises without at any point entering the data center [16].

4. Evaluation System of Cloud Data Centers

A data community could be an actual location that stores registering machines and their associated gear. It contains the foundational equipment that IT structures require, for example, servers, data limit drives, and organizational equipment. The actual office stores any organization's high-level data. In an on-premises data focus, resource flexibility is compelled by the establishment that the organization has procured and conveyed [7]. Inside the cloud, additional resources can be quickly and easily scaled as required. In an on-premises data focus, resource versatility is restricted by the ability to acquire, plan, or update devices. Inside the cloud, a client can scale up or down resources quickly to address trade issues. Keeping an on-prem data focus is more exorbitant than a cloud-based one. On-prem, an association pays the full expense of the entirety of its establishment. Inside the cloud, resources can be shared, and cloud benefit providers can exploit economies of scale [9,10]. In an on-premises data focus, an association has absolute command over its establishment, which can be perfect or horrendous. Inside the cloud, availability is guaranteed by benefit-level assertions, which might provide unrivaled guarantees compared to what an association can offer in-house. Regarding security, inside the cloud, the cloud benefit provider is responsible for obtaining part of an association's establishment stack and is more experienced at doing so. Regardless, a few clients might require additional

security for cloud-based data habitats that are not locally provided by the cloud benefit provider. In an on-prem data focus, the association has absolute command over the systems that it sends and occupies. Inside the cloud, the association is compelled to use what is publicized by the advantage provider.

Data center designs also understand the meaning of imperativeness adequacy. From the clear data shown in Figure 4, the community might expect, figuratively speaking, numerous kilowatts of imperativeness; however, some data focuses may require more than 100 megawatts [16]. At present, green data habitats with reduced environmental effects achieved through low-emissions building materials, exhaust systems, and elective imperativeness advancements are growing in reputation. Data focuses can amplify efficiency through actual arrangements known as hot walkways and cold-aisle designs. The server racks are arranged in subbing segments, with cold air intake on one side and hot exhausts on the other. The outcome is the substitution of hot and cold aisles, with the molding gear forming a hot walkway and the cold air intakes forming a chilly walkway. Exhaust is used to cool molding. Most of the time, this equipment is set up between the server cabinets inside the walkway and scatters the thermal load about once again into the cooling unit [15]. This course of action of examining molding gear is known as in-line cooling. Associations, much of the time, evaluate the proficiency and degree of essentialness of a data focus through its control usage feasibility (PUE), which addresses the extent of the entire control of the data community separated by the control used by IT equipment [2].

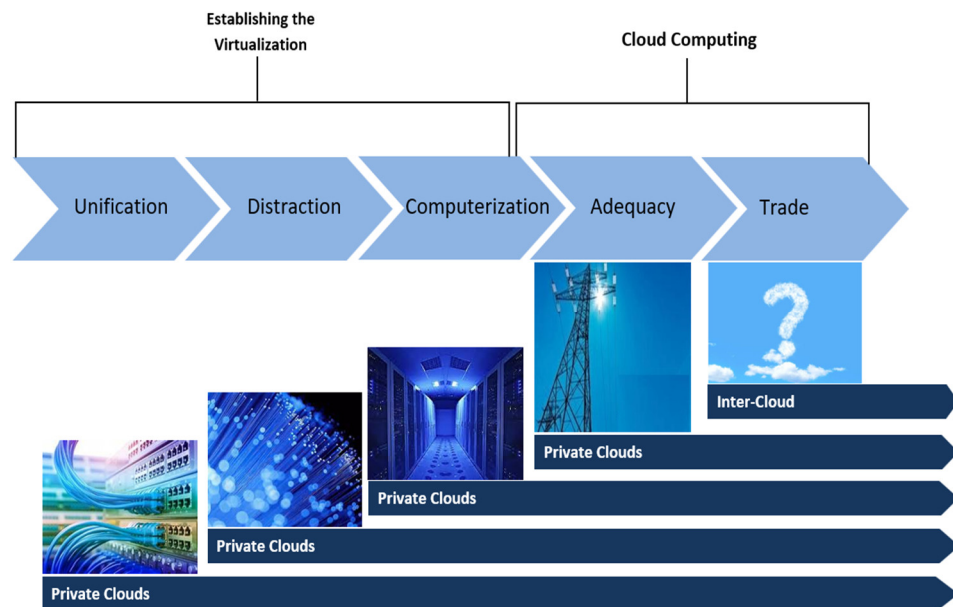


Figure 4. CISCO cloud data centers path.

Nevertheless, the ensuing rise of virtualization has permitted for more beneficial utilization of IT gear, resulting in much higher effectiveness, lower vitality utilization, and diminished vitality costs. Measurements such as PUE are not central to vitality effectiveness objectives. Regardless, organizations can still survey PUE and utilize comprehensive control and cooling examinations to improve it and oversee vitality proficiency [7]. Although nearly any appropriate area can serve as an information center, an information center’s objectives and usage require cautious planning. Aside from the fundamental issues of cost and acquisition, locales are chosen based on a few criteria: geographic area, seismic and meteorological soundness, access to streets and air terminals, the accessibility of vitality and broadcast communications, and, indeed, the prevailing political environment. Once the location is secured, the information center design can be outlined to center on the structure and format of mechanical and electrical frameworks and IT gear. These issues are

guided by the availability and proficiency objectives of the specified information center level [17,18].

5. Proposed Algorithm

The proposed algorithm, Algorithm 1, for securing cloud data centers against the attacks.

Algorithm 1. The proposed hybrid algorithm provides security using RSA and DES.

Input: The parameters of cloud datacenters are counted as the input in the algorithm.

Output: The efficient performing the security to the datacenters.

```

1:      Procedure (Methods)
2:      If (Cloud datacenters) then
3:      {
4: Perform the RSA algorithm checks for the datacenters.
5:      If (the RSA checks datacenters are not secure)
6:      {
7:      Perform the DES algorithm checks for datacenters.
8:      {
9:      If (Service is highly secured) then
10: Step1: The datacenters provided by the cloud service provider (CSP) are 100% secure.
11:      }
12: end if
13: Step2: The datacenters provided by the CSP are 75% secure.
14:      }
15: end if
16: end if
17: end if
18: end procedure

```

6. Conclusions and Future Work

In conclusion, the data center with various locations might choose to establish data communities while decreasing the number of locations to reduce the considerable incurred cost of IT tasks. Association commonly occurs during consolidations and acquisitions when most organizations do not need data focuses managed by a subordinate business. Emphasizing the distinctions between the endeavors of data focuses and distributed computing is needed for the progression of hybrid cloud circumstances. As endeavors continuously rely upon open cloud providers, they should merge networks between their data communities and cloud providers.

Author Contributions: Conceptualization, D.C. and A.R.; methodology, M.M.M.H., N.I., D.C., M.F.K.B. and A.R.; validation, D.C. and A.R.; formal analysis, M.M.M.H., N.I., D.C., M.F.K.B., and A.R.; investigation, D.C. and A.R.; resources, D.C. and A.R.; data curation, D.C. and A.R.; writing—original draft preparation, M.M.M.H., N.I., D.C., M.F.K.B. and A.R.; validation, D.C. and A.R.; writing—review and editing, M.M.M.H., N.I., D.C., M.F.K.B. and A.R.; validation, D.C. and A.R.; visualization, D.C. and A.R.; supervision, D.C. and A.R.; 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. Bilal, K.; Malik, S.U.R.; Khan, S.U.; Zomaya, A.Y. Trends and challenges in cloud datacenters. *IEEE Cloud Comput.* **2014**, *1*, 10–20. [[CrossRef](#)]
2. Randhawa, P.; Shanthagiri, V.; Kumar, A. Recognition of violent activity response using machine learning methods with wearable sensors. *J. Adv. Res. Dyn. Control Syst.* **2019**, *11*, 592–601. [[CrossRef](#)]
3. 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.
4. Subrahmanya, S.V.; Shetty, D.K.; Patil, V.; Hameed, B.M.; Paul, R.; Smriti, K.; Naik, N.; Somani, B.K. The role of Data Science in healthcare advancements: Applications, benefits, and future prospects. *Ir. J. Med. Sci. (1971)* **2021**, *191*, 1473–1483. [[CrossRef](#)] [[PubMed](#)]
5. 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.
6. Shuja, J.; Gani, A.; Shamshirband, S.; Ahmad, R.W.; Bilal, K. Sustainable cloud data centers: A survey of enabling techniques and technologies. *Renew. Sustain. Energy Rev.* **2016**, *62*, 195–214. [[CrossRef](#)]
7. 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](#)]
8. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 64–71. [[CrossRef](#)]
9. Li, X.; Garraghan, P.; Jiang, X.; Wu, Z.; Xu, J. Holistic virtual machine scheduling in cloud datacenters towards minimizing total energy. *IEEE Trans. Parallel Distrib. Syst.* **2017**, *29*, 1317–1331. [[CrossRef](#)]
10. Tiwari, A.; Garg, R. Reservation System for Cloud Computing Resources (RSCC): Immediate Reservation of the Computing Mechanism. *Int. J. Cloud Appl. Comput.* **2022**, *12*, 1–22. [[CrossRef](#)]
11. Kumar, S.; Srivastava, P.K.; Srivastava, G.K.; Singhal, P.; Singh, D.; Goyal, D. Chaos based image encryption security in cloud computing. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 1041–1051. [[CrossRef](#)]
12. Kumar, S.; Kumari, B.; Chawla, H. Security challenges and application for underwater wireless sensor network. *Proc. Int. Conf. Emerg.* **2018**, *2*, 15–21.
13. Nishad, L.S.; Kumar, S.; Bola, S.K.; Beniwal, S.; Pareek, A. Round robin selection of datacenter simulation technique cloudsims and cloud analyt architecture and making it efficient by using load balancing technique. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 2901–2905.
14. Shen, H.; Chen, L. A resource usage intensity aware load balancing method for virtual machine migration in cloud datacenters. *IEEE Trans. Cloud Comput.* **2017**, *8*, 17–31. [[CrossRef](#)]
15. 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.* **2022**, *10*, 1–28. [[CrossRef](#)]
16. Rohinidevi, V.V.; Srivastava, P.K.; Dubey, N.; Tiwari, S.; Tiwari, A. A Taxonomy towards fog computing Resource Allocation. In Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 23–24 December 2022; pp. 1–5.
17. Chouhan, A.; Tiwari, A.; Diwaker, C.; Sharma, A. Efficient Opportunities and Boundaries towards Internet of Things (IoT) Cost Adaptive Model. In Proceedings of the 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 11–13 February 2022; pp. 1–5.
18. Dittmann, L.; Fagertun, A.M.; Kamchevska, V.; Galili, M.; Oxenlove, L.; Ruepp, S.; Berger, M. A roadmap for evolving towards optical intra-data-center networks. In Proceedings of the ECOC 2016, 42nd European Conference on Optical Communication, Dusseldorf, Germany, 8–22 September 2016; pp. 1–3.
19. Rangaiah, Y.V.; Sharma, A.K.; Bhargavi, T.; Chopra, M.; Mahapatra, C.; Tiwari, A. A Taxonomy towards Blockchain based Multimedia content Security. In Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 23–24 December 2022; pp. 1–4.
20. Singh, N.K.; Jain, A.; Arya, S.; Gonzales, W.E.G.; Flores, J.E.A.; Tiwari, A. Attack Detection Taxonomy System in cloud services. In Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 23–24 December 2022; pp. 1–5.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.