2023 Global Conference on Information Technologies and Communications (GCITC)
Karnataka, India. Dec 1-3, 2023

A Comprehensive Analysis of Protocols and Models for Improving Energy Efficiency and Security in Cloud Computing

Sachin Patel
Devang Patel Institute of Advance Technology and Research
Charotar University of Science and Technology,
Changa, Gujarat
sachinpatel.dit@charusat.ac.in,
21drdce002@charusat.edu.in

Dr. Amit Nayak
(Principal) Devang Patel Institute of Advance Technology and Research
Charotar University of Science and Technology,
Changa, Gujarat
principal.depstar@charusat.ac.in

2023 Global Conference on Information Technologies and Communications (GCITC) | 979-8-3503-0816-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/GCITC60406.2023.10426325

***Abstract*— Green cloud computing is a current hot issue that is altering how people view data centers. Green Cloud Computing is a method for maximizing the use of computing resources. Users of cloud computing can modify their resource utilization in accordance with their demands. By enabling users to access resources from any location at any time, cloud computing has completely transformed the IT industry as a whole. Numerous data centers have been built as a result of the rising demand for cloud computing. These data centers are made up of various resource types, each with a different power usage pattern. Two major problem with cloud data centers is their high-power usage and security. Virtual machine migration and load balancing are just two of the issues that have been addressed via the development of numerous strategies and practices. This review papers will discuss problems and protocols for energy consumption, also several security models will be reviewed for cloud computing.**

Keywords*— *Data centers, Power usage, Security, Energy consumption, IT industry, Cloud computing

I. INTRODUCTION

Cloud computing is a popular approach that allows users to access third-party computer resources on a pay-as-you-go basis. It integrates various resources such as processing, storage, applications, and data collection through multi-level virtualization and abstraction. The concept emerged from technologies like Grid computing, distributed computing, and virtualization[1].

However, the rapid growth of data centers and increased energy consumption has raised environmental concerns. To address this, the concept of green computing has emerged, aiming to make the IT infrastructure energy-efficient and resource-efficient. Data centres frequently have poor average occupancy and waste a lot of energy on unused resources, based on studies[2].

By dynamically altering the number of active computers according to resource requirements, dynamic virtual machine (VM) consolidation is one potential method for lowering energy use. By hosting numerous VM instances on a single physical server, virtualization technology is essential for optimising resource usage[3].

Another method for distributing workloads evenly among active nodes and ensuring optimal resource utilisation and speedy execution is load balancing. On-demand service provision, network accessibility, resource planning, quick elasticity, and service measurement are characteristics of cloud computing[5].Overall, cloud computing and its related technologies provide scalable and cost-effective solutions, but efforts are being made to improve energy efficiency and resource utilization for a green computing environment[1,2].

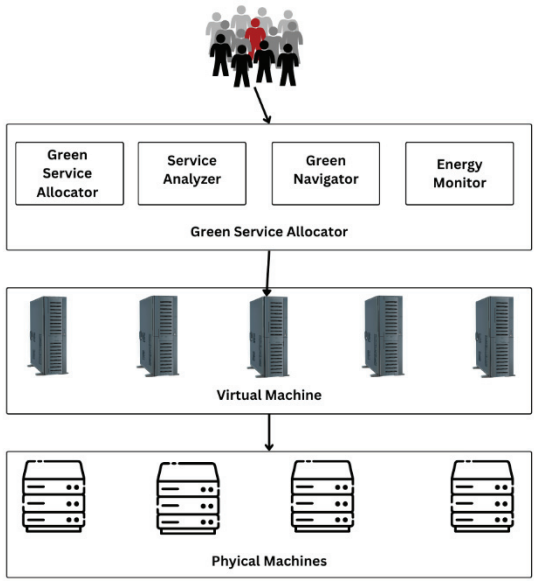

Fig. 1. Architecture of Green Cloud

II. LITRATURE REVIEW

A. Virtual Machine Consolidation

By moving and combining virtual machines (VMs) onto fewer physical computers, VM consolidation is a technique for lowering the number of active physical machines (PMs). VM placement and VM migration are the two methods for VM consolidation[4].VM placement involves determining the right host for a specific VM. It can be power-based, aiming to save energy by shutting down servers, or application-based, which increases resource usage and improves Quality of Service (QoS) [1].

The act of shifting running virtual machines (VMs) from one PM to another reduces the number of running physical machines. The migration process involves selecting overloaded or underloaded PMs, choosing VMs to be migrated, selecting a target PM, and transferring the VM [4]. Incorrect host selection can lead to increased migration, resource waste, and energy usage.

B. Energy Usage Measurement

Measuring precise energy usage in data centers can be challenging, but it is crucial for cost savings. Data centers consume significant electricity, and even simple efficiency improvements can result in substantial savings [5]. While deploying an energy metering and reporting system requires a capital investment, it can provide long-term cost savings. Energy consumption can be monitored to determine peak and low energy needs, and meters can break down power consumption to the component level. Having an energy conservation plan, evaluating it regularly, and taking corrective action to address deficiencies can encourage energy savings [5].

C. Virtual Machine Migration

Virtual machine migration involves moving an active VM from one physical computer to another while ensuring the guest operating system, applications, and remote clients are unaffected. The migration process consists of addressing CPU, motherboard, networking and storage adapters, graphics adapters, and other external connections. The goal is to minimize the noticeable lag during migration and potentially improve performance by moving VMs to machines with larger resources [6].

D. Meta-Heuristic Algorithms for Load Balancing

Meta-heuristic algorithms, such as Particle Swarm Optimization (PSO) and Firefly Algorithm (FA), have shown effectiveness in solving NP-complete problems, including load balancing. PSO has been used to allocate VM resources based on expected user demands, efficiently spreading the load across available machines. FA is inspired by the behaviour of fireflies and utilizes brightness magnitude to represent load levels. By distributing the load evenly among the nodes, it hopes to avoid overloading or underutilization [7].

E. Optimization in Cloud Computing

In order to reduce energy consumption in cloud computing, jobs must be scheduled and resource usage must be optimised. Tasks are scheduled on cloud computing nodes based on their resource utilisation using the idea of task tolerance (ECCT). By maximising resource utilisation per unit of time, the objective is to maximise task parallelism and optimise energy consumption [5]

TABLE I. YEAR-WISE IMPROVEMENT ON MODEL

Model	Description	Changes Observed	Year Introduced
Virtualization-based Security [3]	Infrastructure and virtual machine instances that are secure	Improved isolation, enhanced security controls, flexibility, and resource allocation	2007
Energy-Aware Authentication [14]	Access control and identification that uses little energy	Reduced energy consumption, adaptive authentication mechanisms	2009
Energy-Efficient Encryption [14]	Energy-saving encryption methods	Reduced energy consumption, optimized cryptographic algorithms	2010
Energy-Aware Data Storage [8]	Efficient in terms of energy data management and storage	Reduced energy consumption, optimized data placement strategies	2013
Green Compliance [9]	Green and sustainable cloud computing standards	Guidelines for energy-efficient and sustainable practices	2014
Green Cryptography [10]	Methods for cryptography that use little energy	Reduced energy consumption, lightweight algorithms	2015
Energy-Aware Key Management [11]	Energy-efficient key management	Reduced energy consumption, efficient key distribution	2016
Green Security Monitoring [12]	Monitoring security with minimal energy use	Reduced energy consumption, intelligent event correlation	2017
Energy-Aware Security Assessment [10]	Energy-conscious security evaluation and testing	Integration of energy efficiency considerations	2018
Green Incident Response [9]	Energy-efficient incident response	Reduced energy consumption, efficient incident handling	2018
Secure Virtual Machine Migration [6,8]	Secure migration of virtual machines	Enhanced security controls, secure transmission	2019
Green Security Governance [13]	Integration of security and green practices	Inclusion of energy-related risk factors	2020
Energy-Aware Secure Communication [14]	Energy-efficient secure communication	Reduced energy consumption, optimized protocols	2021
Energy-Efficient Security Incident [14]	Energy-aware incident response	Reduced energy consumption, efficient incident handling	2022
Dynamic Resource Allocation [11]	Dynamic resource allocation for security	Optimized resource allocation, improved cost-effectiveness	2022
Green Cloud Service Level Agreements [13]	Energy-efficient SLAs	Inclusion of energy-related performance metrics	2022
Secure and Green Cloud Architecture [13]	Secure and energy-efficient cloud architecture	Optimization of architectural components, promotion of sustainability	2023

III. DIFFERENT SOLUTIONS GIVEN BY SEVERAL ORGANISATION

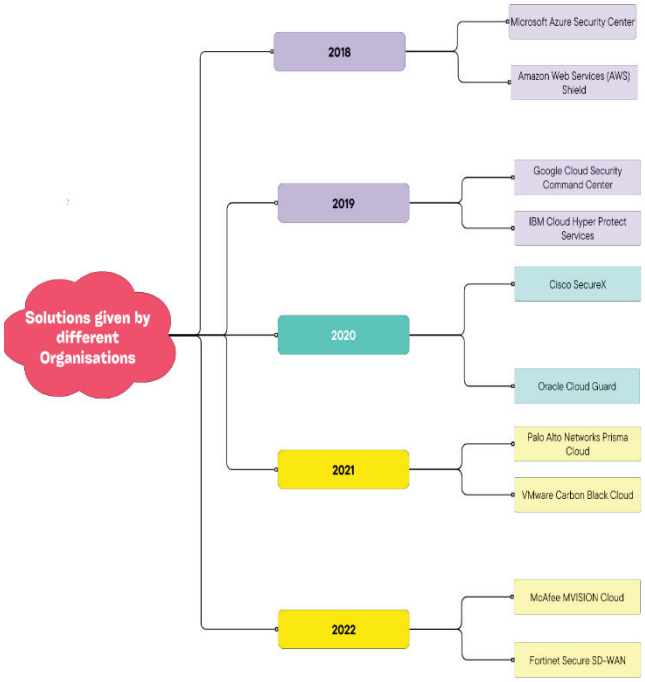

Fig. 2. Solutions provided by different organisations

A. Microsoft Azure Security Center:

Threat Detection:

Azure Security Center provided advanced threat detection capabilities, leveraging machine learning and analytics to identify and alert users about potential security incidents[15].

Vulnerability Assessment:

It offered continuous monitoring of cloud resources to identify vulnerabilities and misconfigurations, along with recommendations for remediation[15].

Security Policy Management:

Azure Security Center enabled users to define and enforce security policies across their cloud environment, ensuring compliance with industry standards and best practices[15].

B. AWS Shield:

Managed DDoS Protection:

AWS Shield provided a managed service to protect cloud applications and data from Distributed Denial of Service (DDoS) attacks. It automatically detected and mitigated large-scale attacks, helping to maintain application availability and performance[15].

C. Google Cloud Security Command Center:

Centralized Visibility:

A centralised dashboard offering visibility into an organization's cloud assets, vulnerabilities, and threats across Google Cloud Platform (GCP) was provided by the Security Command Centre. It made it possible for users to efficiently manage and monitor security posture[15].

Data Risk Assessment:

To help detect and classify sensitive data and ensure compliance with data security requirements, it has built-in data risk assessment capabilities[15].

D. IBM Cloud Hyper Protect Services:

Encryption Technology:

IBM Cloud Hyper Protect Services utilized cryptographic technologies, such as secure enclaves and tamper-resistant hardware, to protect sensitive data and workloads in the cloud. It provided a high level of security assurance for critical applications[15].

E. Cisco SecureX:

Unified Security Platform:

SecureX unified security operations across networks, endpoints, and the cloud into a single platform. It allowed organizations to gain holistic visibility, detect threats more effectively, and respond to incidents promptly[15].

Integrated Security Workflows:

It integrated with various Cisco security products and third-party solutions, streamlining security workflows and enabling seamless collaboration between different security teams[15].

F. Oracle Cloud Guard:

Automated Security Monitoring:

Cloud Guard provided continuous security monitoring of Oracle Cloud Infrastructure (OCI) resources, detecting misconfigurations, vulnerabilities, and threats. It offered automated remediation suggestions and enforced security best practices[16].

Real-time Threat Response:

It enabled real-time response to security incidents by integrating with Oracle's Security Operations Center (SOC) and other incident response tools, facilitating prompt action against potential threats[16].

G. Palo Alto Networks Prisma Cloud:

Comprehensive Cloud Security:

Prisma Cloud provided a comprehensive platform for multi-cloud security, including visibility, compliance, and threat prevention. Workload protection, container security, cloud network security, and data governance were all discussed. [16].

Continuous Compliance Monitoring:

It enabled enterprises to conform to regulatory requirements and industry standards by providing continuous monitoring and enforcement of compliance rules across cloud resources. [16].

H. VMware Carbon Black Cloud:

Cloud-native Endpoint Protection:

Carbon Black Cloud offered improved endpoints security features tailored to cloud settings. It offered real-time threat detection, behavioural analysis, and response capabilities to safeguard cloud workloads effectively[17].

Compliance and Remediation:

It provided compliance and vulnerability management tools, allowing organisations to examine the defensive

alignment of their cloud infrastructure, detect holes, and prioritise corrective steps. [17].

I. McAfee MVISION Cloud:

Cloud Access Security Broker (CASB):

MVISION Cloud acted as a cloud application security broker (CASB), providing full data protection, threat prevention, and compliance capabilities for cloud applications and services. It provided granular visibility and control over data in cloud environments[19].

Cloud-native Security:

It offered cloud-native security features that seamlessly integrated with various cloud providers and applications, ensuring consistent protection across multi-cloud environments[19].

J. Fortinet Secure SD-WAN:

Secure SD-WAN Integration:

Fortinet Secure SD-WAN combined SD-WAN capabilities with advanced security features, offering integrated protection for cloud environments and branch offices. It enabled secure connectivity, application optimization, and threat prevention in a single solution[20].

Centralized Management:

It provided centralized management and orchestration of security policies, allowing organizations to enforce consistent security across their network and cloud infrastructure[20].

IV. FUTURE SCOPE

A. Secure Resource Allocation

The technique of allocating computing resources in a cloud computing environment in a secure and controlled manner is referred to as "secure resource allocation." It entails allocating and allocating resources like network bandwidth, storage, and processing power among many users or applications while maintaining the confidentiality, integrity, and availability of the resources[11].

Secure resource allocation's main goal is to stop unauthorised access, data breaches, and resource abuse. To make sure that only authorised entities have access to particular resources, it entails installing robust authentication systems, access controls, and resource isolation techniques[11].

B. Identify the Headings

Secure virtual machine migration is the process of moving an active virtual machine (VM) within a cloud architecture from one physical host to another without interfering with the services that the VM is using. It makes load balancing, resource management, and maintenance tasks efficient[6].

Security precautions must be taken during VM migration to safeguard the data's confidentiality and integrity and guarantee continuous service availability. Secure VM migration entails safely moving the memory, storage, and state of the VM between hosts while protecting data privacy and limiting unauthorised access[3].

C. Green Security Governance

Green security governance describes how security procedures and guidelines are incorporated into cloud computing settings along with environmentally friendly procedures. When creating and putting into practice security measures, it requires taking energy efficiency, resource optimization, and environmental impact into account [10].

Green security governance aims to balance the need for robust security with the goal of reducing energy consumption and minimizing the carbon footprint of cloud infrastructures. It involves adopting energy-efficient hardware, optimizing resource utilization, implementing power management techniques, and promoting sustainable practices in security operations [10].

D. Energy-Aware Compliance and Auditing:

Energy-aware compliance and auditing involve evaluating and monitoring the energy efficiency and environmental impact of cloud computing systems to ensure compliance with energy-related regulations and standards. It includes assessing and optimizing energy consumption, tracking carbon emissions, and measuring the effectiveness of energy-saving initiatives [9].

Energy-aware compliance and auditing practices help organizations identify areas for improvement, implement energy-efficient measures, and demonstrate environmental responsibility. It involves regular monitoring, reporting, and analysis of energy usage data, as well as implementing energy-efficient technologies and practices in compliance with industry standards and regulations [14]

E. Energy-Aware Compliance and Auditing:

Energy-aware compliance and auditing involve evaluating and monitoring the energy efficiency and environmental impact of cloud computing systems to ensure compliance with energy-related regulations and standards. It includes assessing and optimizing energy consumption, tracking carbon emissions, and measuring the effectiveness of energy-saving initiatives[9].

Energy-aware compliance and auditing practices help organizations identify areas for improvement, implement energy-efficient measures, and demonstrate environmental responsibility. It involves regular monitoring, reporting, and analysis of energy usage data, as well as implementing energy-efficient technologies and practices in compliance with industry standards and regulations[14]

V. CONCLUSION

Cloud services have grown so quickly that practically every company now uses it. There has been a significant technological advancement in the subject since its inception. Building a technology that can benefit both consumers and service providers necessitates a significant amount of effort[1]t. We are dealing with energy as a field challenge because, due to the rapid increase in demand, hardware infrastructure is being implemented at a rapid rate. Formulating solutions to reduce power consumption, as well as improved work allocation procedures in the future for better resource use, should be kept in mind [2].

REFERENCES

[1] Upadhyaya J, Ahuja NJ, “Quality of service in cloud computing in higher education: A critical survey and innovative model”, In I-

SMAC (IoT in Social Mobile , analytics and Cloud) (I-SMAC), 2017 International Conference on IEEE, pp 137-140, 2017

[2] Zeng Y. Comprehensive Review of Server Power Saving and Energy Efficiency Evaluation Technologies[J]. Information Technology &Standardization, 2008.

[3] Beloglazov A, Buyya R. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in Cloud data centers[J]. Concurrency & Computation Practice & Experience, 2012, 24(13):1397–1420.

[4] [Ye KJ. Power Management of Virtualized Cloud Computing Platform[J]. Chinese Journal of Computers, 2012, 35(6).

[5] Gai K, Qiu M, Zhao H, et al. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing[J]. Journal of Network & Computer Applications, 2016, 59(C):46-54.

[6] S. Akoush, R. Sohan, A. Rice, A. W. Moore, and A. Hopper, “Predicting the Performance of Virtual Machine Migration,” 2010 IEEE Int. Symp. Model. Anal. Simul. Comput. Telec ommun. Syst., pp. 37–46, 2010.

[7] T. Keskinturk and M. B. Yildirim, "A genetic algorithm metaheuristic for bakery distribution vehicle routing problem with load balancing," 2011 International Symposium on Innovations in Intelligent Systems and Applications, Istanbul, Turkey, 2011, pp. 287-291, doi: 10.1109/INISTA.2011.5946077.

[8] M. Pirahandeh and D. -H. Kim, "EGE: A New Energy-Aware GPU Based Erasure Coding Scheduler for Cloud Storage Systems," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 2018, pp. 619-621, doi: 10.1109/ICUFN.2018.8436594.

[9] V. Sklyar, V. Kharchenko and N. G. Bardis, "Assurance Case for Green IT Applications: Proof of Compliance with Power Consumption Claims," 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), Corfu, Greece, 2017, pp. 124-127, doi: 10.1109/MCSI.2017.29.

[10] J. Troutman and V. Rijmen, "Green Cryptography: Cleaner Engineering through Recycling, Part 2," in IEEE Ity & Privacy, vol. 7, no. 5, pp. 64-65, Sept.-Oct. 2009, doi: 10.1109/MSP.2009.120.

[11] D. Wu, Q. Wu, Y. Xu and Y. -C. Liang, "QoE and Energy Aware Resource Allocation in Small Cell Networks With Power Selection, Load Management, and Channel Allocation," in IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7461-7473, Aug. 2017, doi: 10.1109/TVT.2017.2650949.

[12] [Z. S. Zaghloul, N. Elsayed, C. Li and M. Bayoumi, "Green IoT System Architecture for Applied Autonomous Network Cybersecurity Monitoring," 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2021, pp. 628-632, doi: 10.1109/WF-IoT51360.2021.9595142.

[13] Geetanjali and S. J. Quraishi, "Energy Savings using Green Cloud Computing," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 1496-1500, doi: 10.1109/ICICICT54557.2022.9917654.

[14] [Y. Wang, T. Zhang, W. Yang, H. Yin, Y. Shen and H. Zhu, "Secure Communication via Multiple RF-EH Untrusted Relays With Finite Energy Storage," in IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1476-1487, Feb. 2020, doi: 10.1109/JIOT.2019.2955743.

[15] Diogenes, Yuri, and Tom Shinder. Microsoft Azure Security Center. Microsoft Press, 2019.

[16] Gunay, Osman, et al. "Entropy-functional-based online adaptive decision fusion framework with application to wildfire detection in video." IEEE Transactions on Image Processing 21.5 (2012): 2853-2865.

[17] Ali, Md Iman, et al. "Security challenges and cyber forensic ecosystem in IOT driven BYOD environment." IEEE Access 8 (2020): 172770-172782.

[18] MacDonald, Neil, and Tom Croll. "Market guide for cloud workload protection platforms." Gartner, Stamford, CT, USA, Rep. G 716192 (2020).

[19] Riley, Analysts Steve, and Craig Lawson. "Magic quadrant for cloud access security brokers." November, Skyhigh Networks, available at: https://info. skyhighnetworks. com/WPGartnerMQ2018_BannerCloud-MFE. html (2017).

[20] Segeč, P., et al. "SD-WAN-architecture, functions and benefits." 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA). IEEE, 2020.