

An Energy Efficient based Optical Network using Cloud Computing Techniques under an Improved Layer of Honeypots for Security

Anand Kumar Mishra

NIIT University Neemrana, Rajasthan

Amit Kumar Tyagi

National Institute of Fashion Technology New Delhi

Shrikant Tiwari

shrikanttiwari15@gmail.com

Galgotias University, Greater Noida

Research Article

Keywords: Cryptography, Cloud Computing, Energy efficiency, Heuristic optimization, Honeypots, Optical Networks

Posted Date: March 26th, 2024

DOI: <https://doi.org/10.21203/rs.3.rs-4156488/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare potential competing interests as follows: I confirm that the information provided above is complete and accurate to the best of my knowledge. In the event of any changes in my circumstances, I will promptly update this declaration. There is no conflict of interest. I understand the importance of transparency and am committed to ensuring that any potential conflicts of interest do not compromise the integrity of publication of my manuscript in your journal.

An Energy Efficient based Optical Network using Cloud Computing Techniques under an Improved Layer of Honeypots for Security

Anand Kumar Mishra¹, Amit Kumar Tyagi², Shrikant Tiwari³

¹Computer Science and Engineering, NIIT University, Neemrana, Rajasthan

²Department of Fashion Technology, National Institute of Fashion Technology, New Delhi, Delhi India

³School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh-203201, India

anandr.mishra13@gmail.com

amitkrtyagi025@gmail.com

shrikanttiwari15@gmail.com

Abstract: Energy proficiency is significant for optical organizations regarding versatility, minimal expense activity, and maintainability. Understanding energy with regards to optical organizations starts with a comprehension of the constituent parts and gear that make up an optical organization and how their energy use is advancing after some time. The organization design, depicting how these parts are assembled and worked, will likewise extensively affect the energy proficiency of optical organizations. Likewise, the level of security in optical organizations isn't been much explored in the research field. Thereby this paper brings an effective method for optimizing energy and also increasing security in an optical network using hybrid cloud computing techniques like heuristics optimization and FA algorithm. The author also carries a novelty in analysing and improving the security in optical networks using the Honeyspot algorithm. The results carried are shown a greater impact of the proposed system (EEFAHA-HONEYSPOT) over various measures.

Keywords: Cryptography, Cloud Computing, Energy efficiency, Heuristic optimization, Honeypots, Optical Networks

1. Introduction

For data-intensive processes and on-demand data-intensive services (such as online searches, streaming video, etc.), the cloud computing model [1] can offer a flexible and dependable service over the Internet such as weather prediction, stock transactions data analysis etc. Cloud computing will soon be the standard method for both service providers and clients to receive Internet services because of its "pay-as-you-go" and "elastic service" qualities. Distributed cloud services are often made up of many connected, dispersed data centres that work together to provide computing and storage resources for each on-demand request. A high-capacity and adaptable networks must be designed to connect data centres due to the enormous traffic demands of today's bandwidth-intensive applications, like IPTV. In today's digital age, many processes and services require a significant amount of data processing and storage. These data-intensive processes and on-demand services, such as online searches, streaming video, weather forecasting, stock transactions data analysis, etc., require a flexible and dependable infrastructure to handle the ever-increasing volume of data. The cloud computing model offers such an infrastructure. Users can access computing resources like storage, databases, servers, and software via the Internet on a pay-as-you-go model. Cloud computing providers manage the infrastructure, enabling clients to access resources without owning hardware. Distributed cloud services consist of interconnected data centers that collaborate to offer computing and storage resources for on-demand requests. This distributed architecture ensures that resources are available on-demand, making it possible for cloud computing to offer elastic services. To provide cloud computing services, high-capacity and adaptable networks must be designed to connect data centres. The networks must handle the enormous traffic demands of today's bandwidth-intensive applications, like IPTV. Such networks must provide low-latency connections, high bandwidth, and high availability to ensure that users can access computing resources quickly and reliably. cloud computing is the standard method for both service providers and clients to receive Internet services. It offers a flexible and dependable service over the Internet, and distributed cloud services are made up of many connected, dispersed data centres that work together to offer computing and storage resources for each on-demand request. High-capacity and adaptable

networks must be designed to connect data centres due to the enormous traffic demands of today's bandwidth-intensive applications.

Since IP control protocols are adaptable and flexible, and optical networks have features like, low latency, low bit error rate, high bandwidth provisioning etc., IP-over-WDM networking is viewed as a viable network design for next-generation core networks [2]. By using Wavelength Division Multiplexing (WDM) technologies, a fiber's capacity is split up into many wavelength channels, each of which possesses its own independent data transmission capability and does not overlap. The optical connections' lightpaths are made up of these wavelength channels, some of which may cross multiple fiber cables. Because of existing commercial techniques, each lightpath may operate independently at 100 Gbps data rates [3]. It's possible that traffic on a lightpath between two nodes won't be able to use all of its capacity. A lightpath can be shared by many distinct traffic streams to effectively use the available bandwidth. This is referred to as traffic grooming [4]. Although traffic grooming can increase throughput, it also has the potential to lower energy use, though this is not always the case. In this investigation, the backbone networks for moving people and goods between scattered data centres for cloud computing are considered to be IP-over-WDM networking. Since data centres are located on IP-over-WDM system core nodes, cloud technology necessitates an integrated cloud provisioning infrastructure.

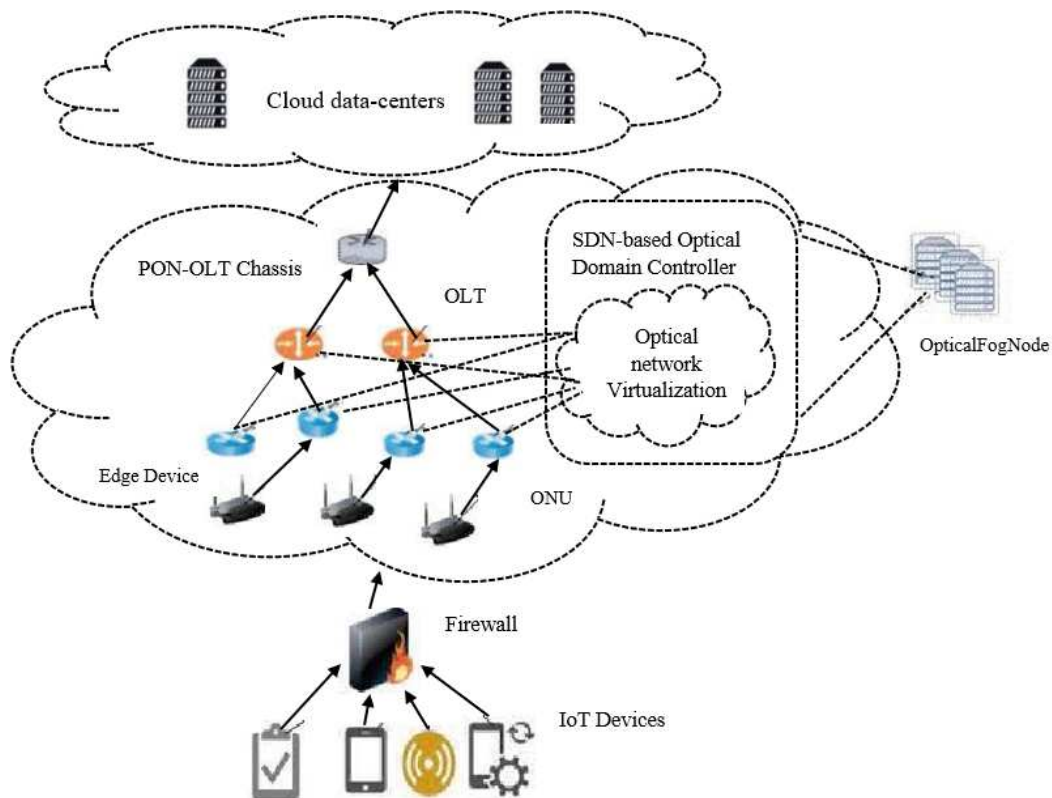


Figure 1. Cloud computing over an optimal network

A significant difficulty in cloud platforms is energy management [5]. The primary operational IT facility for cloud computing in terms of information transmission, storage, etc. is the datacenter, which uses the most energy. According to Bush a typical 500m² datacenter may utilize 38 MW hours of electricity each day, which is more than 3500 EU families could have used in a day. With rising traffic demand and subsequently rising power consumption, it is anticipated that datacenter size would also rise [6]. According to Cisco research datacenter traffic reached 3.4 Zettabytes in 2014, and it is anticipated that this amount would triple in 2019 [7]. The energy use of telecommunications systems, meantime, must not be disregarded. Thus according to Lambert et al., there was a 10.8% annual growth in the amount of electricity used in networks specifically for telecom operator services ranges 150-250 TWh from 2007-2013 [8]. Furthermore, in 2012, 250 TWh, or nearly 2.5% of the world's electricity consumption, was used. Also, according to Lorincz et al., fixed access wired networks, which also include core networks, metro/edge architectures, and contents distribution systems, should have an average 10% annual rise in electricity

efficiency from 2012 to 2030 compared to the anticipated situations [9]. High electricity costs and severe environmental degradation are both results of the enormous quantity of energy that cloud computing infrastructures use (e.g., carbon dioxide emissions.). These worries have made addressing the issue of cloud network energy efficiency a top priority.

1.1 Key Objectives

This work focuses on bringing an effective energy-efficient optical network with the following objectives:

- Provide a novel joint optimization methodology that can take into account both the cloud network's energy efficiency and the placement of data centres throughout the world. Our approach effectively captures the relationship between link energy usage and dynamic workloads, maintaining optimal link utilization ratios within latency and bandwidth constraints.
- Examine two scheduling and routing strategies. The first solution simultaneously maximizes networking and IT infrastructure consumption while using an integrated scheduling scheme to discover the destination location and the route there in a single pass. This technique is Full Anycast (FA) from now on. A different strategy is to choose the location of the request processing first, and then choose the best route to take to get there.
- The Intelligent Optimization-based Energy-efficient Networking (IOEN), heuristic algorithm, combines random depth-first search and a specialized genetic algorithm to determine the best forwarding path for dynamic requests among information centers and between data centers and consumers. An iterative approach can be used to find the optimum solution for this strategy.
- Finally, to improve the security of the optical networks, higher security-based cryptographic methods are used for securing the outer layer from potential attacks.

2. Literature Review

According to Butt et al. (2022), an accurate energy consumption model of the CSP operation is essential for analyzing energy efficiency in various traffic scenarios (Traffic aware cyclic sleep-based power consumption models for a passive optical network) [10]. The method is less accurate because it ignores the ONU's inactivity during the sleeping and sleep-conscious stages. This is particularly true of the current CSP power consumption methods, which fall short in their ability to explain the CSP operations. These gaps are filled by the proposed Inactivity-Aware Model (IAM), which is demonstrated by the results, which are far more precise than those of earlier models and very comparable to those of previously published simulations. The system is also tested using a simulation-based analysis, and it is found that there is only a 5% difference between the simulation findings and the model outcomes.

To address these difficulties, Selvan et al. (2022) propose crucial standards for Energy-efficient resource allocation . From a technical point of view, it offers a answer to the construction of secure data centres using cloud computing infrastructure [11]. To encourage creativity, invention, learning, and enterprise, it is required to build a private information centre and implement cloud computing to connect the operations of diverse research groups. Finally, to bridge the gap between private cloud users and a complete image of offerings, service providers should provide transparent and user-friendly interfaces for users to monitor and manage their resource usage. This can include dashboards that provide real-time information on resource utilization and energy consumption, as well as self-service portals that enable users to provision and manage their own resources. By providing these tools, private cloud service providers can empower users to make informed decisions about resource allocation and energy efficiency.

The research by Das et al. (2022) appears to be relevant for addressing the challenges of supporting C-RAN and MEC deployment over virtualized PONs, and their proposed optimal slicing technique may provide a useful solution for network operators and service providers looking to deploy these technologies at scale [12]. They employ a combined analytical-iterative approach to determine the best distribution of virtual PON slices to utilize MEC node resources as little as possible while still satisfying a goal latency threshold (in our case, 100 s). It sounds like a specific approach or technology that has been developed for allocating virtual PON (Passive Optical Network) slices in real-time or nearly real-time activities.

Taubenblat and colleagues (2022) center their discussion on two primary themes: the advantages of a more streamlined network infrastructure, made feasible by switches equipped with co-packaged optics, and the potential for enhancing utilization through composable, or disaggregated, processes. Their paper, "Optics Facilitated Networks

and Architectures for Data Centre Cost and Power Efficiency," also touches on optical circuit switching, specialized hardware, and networks, albeit briefly.

Yang et al. (2022) use Self-Organizing Feature Mapping (SOFM) to process multi-dimensional information in the context of multi-core elastic optical networks [14]. SOFM is an unsupervised learning algorithm typically used for dimensionality reduction and clustering in machine learning. The positioning of the winning neuron is determined, which establishes the transmission rate of each core, by evaluating the similarities between the competitive layers neuron and the patterns vectors. Finally, the core and spectrum allocation strategy can be implemented to ensure that each core is assigned the appropriate amount of bandwidth and spectrum resources to support its traffic demands. This will involve continuous monitoring of network conditions and adjusting resource allocation as needed to ensure that all nodes can communicate effectively and efficiently. Findings show that the plan can lessen the likelihood of blocking and resource fragmentation.

3. Proposed Methodology

The structure of the suggested methodology is represented in Figure 2.

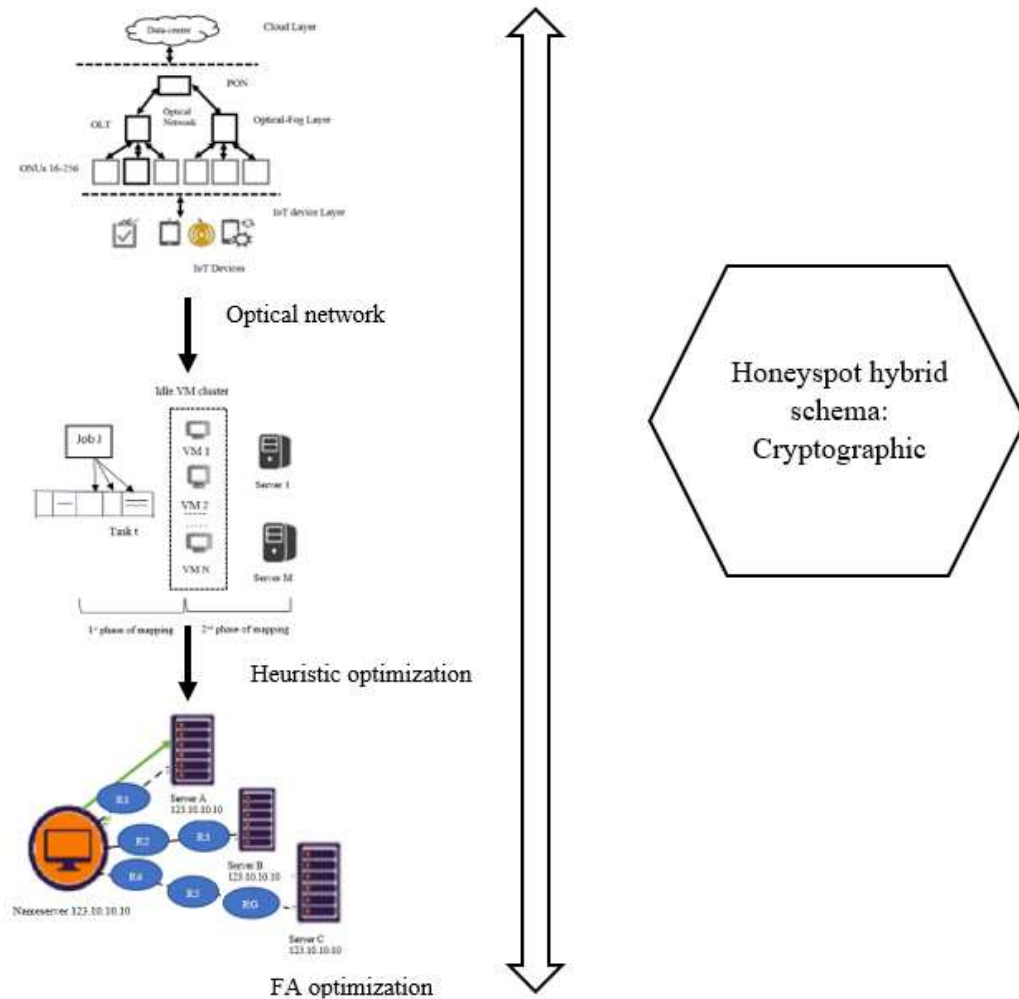


Figure 2. The o architecture of the proposed framework

A bidirectional graph $G(S; C; E)$ is used to represent the optical network, where S represents the group of source nodes, which are made up of optical cross-connects that produce requests. The grouping of core OXCs known as C can be completely disabled, in contrast to source OXCs. A system of optical fibre lines known as E links all OXCs SUC . W wavelengths are assumed for every fiber. The topologies that we used in our study are shown in Figure 3. Furthermore, we describe $D \subseteq S$ as the group of OXCs linked to the data centre by $d \in D$, or the destination sites. The data-centre

objects and d D must be connected by auxiliary connections, also known as virtual links because they don't actually reflect physical ties. While all paths converge at these points, all fiber lines that are incident to d D have $2W$ wavelengths because additional capacity is essential for avoiding network congestion there. We assume that all data centres are the same, with n racks and s servers in each and that idle and peak power features have been created and are being maintained in accordance with [15].

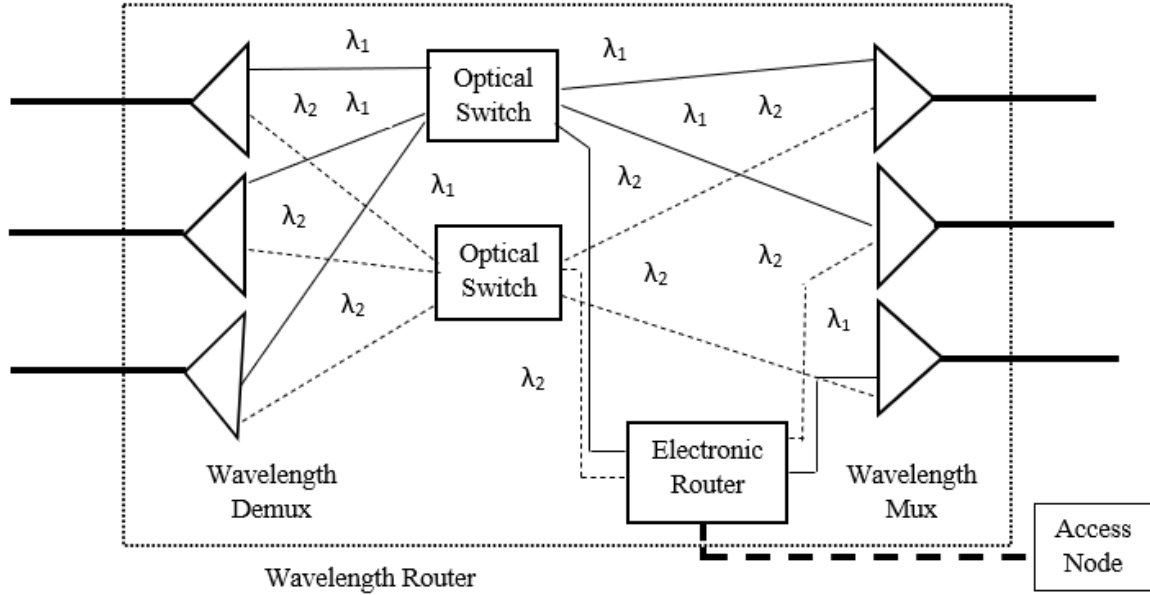


Figure 3. Optical network overall structure topology

3.1 Network Modelling

OXC's are believed to rely on a photonic switching matrix enabled by 3D MEMS, featuring a specific number of input and output fiber ports, each capable of handling up to W wavelengths [16]. Any source-destination combo can establish a light channel as long there's a free port because each OXC is expected to include wavelength converters at the outputs to prevent wavelength blocking (a wavelength route along with all utilized wavelength links from source to destination). The elements that make up Optical Cross-Connect (OXC) systems, are equipment used in optical networks to route data traffic. The switch matrix, EDFA, and transmitters/receivers are all active components that enable the OXC to perform wavelength conversion and amplify optical signals. The no. of input fibers and the wavelength capacity of the fiber, define the number of through ports.

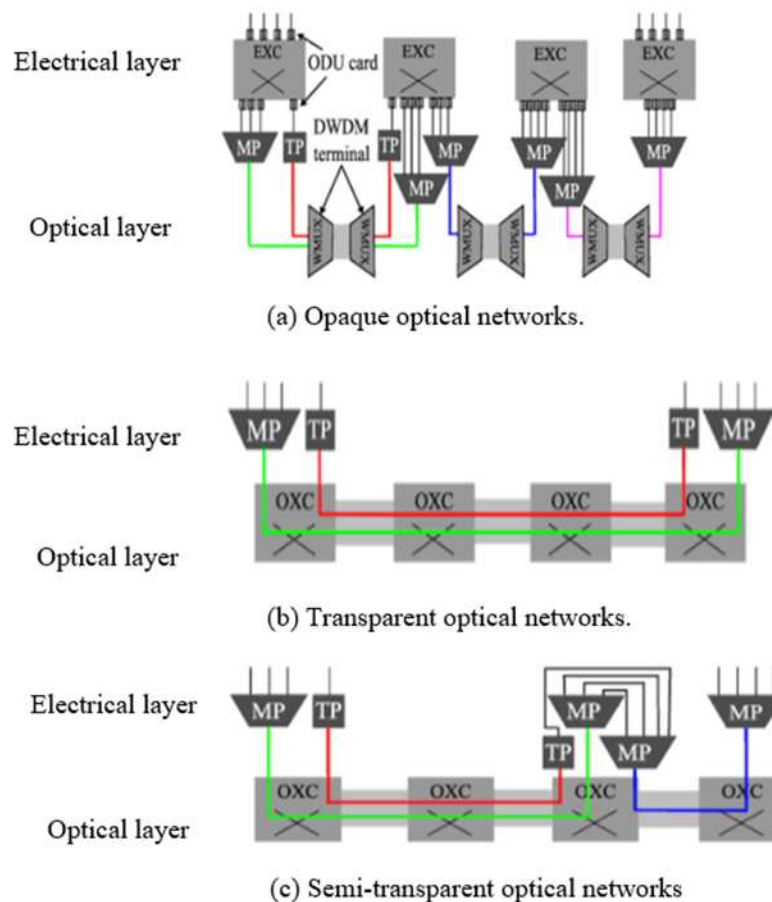


Figure 4. Types of Optical Networks: a) Opaque network, b) Transparent network, c) Semi-transparent network schemas

Optical networks are high-speed communication networks that use optical fiber as the primary transmission medium. Compared to traditional copper-based networks, optical networks provide benefits such as increased bandwidth, extended transmission ranges, and reduced signal attenuation. Here are some key features and benefits of optical networks:

- **High bandwidth:** Optical networks can transmit data at very high speeds, typically ranging from 10 Gbps to several terabits per second. Optical networks are well-suited for tasks demanding high-bandwidth connections, like video streaming, cloud computing, and scientific research.
- **Long-distance transmission:** Optical fiber can transmit data over much longer distances than copper-based cables. Optical networks can transmit data over thousands of kilometers without the need for signal amplification or regeneration, making them ideal for long-distance communication applications.
- **Low signal loss:** Optical fiber exhibits reduced signal loss compared to copper cables, enabling signals to travel longer distances without requiring regeneration. This reduces the need for expensive repeaters and amplifiers, and also improves the signal quality.
- **Security:** Optical networks are more secure than traditional copper-based networks because they are difficult to tap or intercept. Optical signals are transmitted as light pulses through the fiber, and cannot be easily intercepted or tapped without physically accessing the fiber.
- **Scalability:** Optical networks are highly scalable and can be easily upgraded to meet growing bandwidth requirements. This makes optical networks ideal for applications that require scalable and flexible network infrastructure.

Overall, optical networks are an essential component of modern communication systems, providing high-speed, high-bandwidth, and secure connectivity for a wide range of applications.

Types of Optical Networks

Type of optical network are:

- **Opaque Network:** An opaque network is also known as a wavelength switched network. In this type of network, the optical signals are converted to electrical signals at each intermediate node, and then reconverted to optical signals for transmission to the next node. Opaque networks are used in applications where the optical signals need to be processed or manipulated at each intermediate node, such as in wavelength routing or wavelength conversion.
- **Transparent Network:** In a transparent network, the optical signals are transmitted without being converted to electrical signals at each intermediate node. This means that the signal remains in its optical form throughout the network, with no processing or manipulation at the intermediate nodes. Transparent networks are used in applications where the optical signals need to be transmitted over long distances with minimal signal loss or degradation, such as in long-haul or submarine communication systems.
- **Semi-transparent Network:** A semi-transparent network is a hybrid of the opaque and transparent architectures. In this type of network, the optical signals are converted to electrical signals at some intermediate nodes, but remain in their optical form at other nodes. Semi-transparent networks are used in applications where the network requires some level of processing or manipulation, but also needs to maintain signal transparency over long distances.

In conclusion, the selection of network architecture is contingent upon particular application needs, including transmission distance, bandwidth demands, signal integrity, and the necessity for intermediate optical signal processing or manipulation.

Ports a/d are designated for add/drop functions, like managing traffic to and from adjacent data centers. The incoming and outgoing active fibers are characterized as f_{in} and f_{out} , respectively. The power usage of each OXC and each optical fiber link totally determines the network power. The constant power consumption of an OXC's are " 1) switch fabric (P_{sf}), 2) receivers and transmitters (P_{transc}), 3) wavelength converters (P_{conv}), 4) optical amplifiers (P_{ampl}), and 5) the OXC's controller power ($P_{control}$) all affect the OXC's power expenditure (P_{OXC}) ". The total power consumption models of the OXC incorporate these parameters as depicted in Equation (1), while Table 1 outlines typical values for each of these variables.

$$P_{OXC} = P_{control} + P_{sf} + P_{transc} + P_{conv} + P_{ampl}, \quad (1)$$

$$P_{transc} = ports_{a/d} * P_{Tx/Rx}, \quad (2)$$

$$P_{conv} = ports_{through} * P_{transponder} \quad (3)$$

$$P_{ampl} = (f_{in} + f_{out}) * P_{edfa}. \quad (4)$$

In many optical networks, the standard span length is assumed to be around 80 km. However, this can fluctuate based on various factors such as the optical fiber type, network bandwidth needs, and network design specifics. The power consumption (P_l) of a fiber link, which can be managed by the EDFA at the fiber output port of the OXC for the first span, is contingent on its length ($|j-l|$) and can be calculated as described in Equation (2).

$$P_{link}(l) = \left(\frac{|l|}{span-1} \right) * P_{edfa}. \quad (5)$$

That statement accurately summarizes the argument made by the authors. They suggest that while the PUE factor can be used as a simple approximation to account for cooling and power delivery in data centres, a more accurate power-cooling model would be needed for OXCs. They also argue that the impact of cooling and power delivery on energy consumption is more significant for data centres than for OXCs. The PUE factor of 2 implies that for every unit of energy consumed by the network resources, an additional unit of energy is needed for cooling and power delivery.

$$P_{network} = PUE * \left(\sum_{n \in SUC} P_{OXC} + \sum_{l \in E} P_{link}(l) \right). \quad (6)$$

Table 1. Optical network modelling parameters and description

S	Set of request-generating source nodes
C	Set of core nodes. These are entirely deactivable and do not produce any requests.
E	Series of links that are bidirectional
D	A set of OXCs linked to a data centre
W	Wavelength Amount per fibre link
n	No. of servers/rack
π	No. of racks/data center
κ	No. of free coolers
P _{max}	Power used by a server at full load
P _{min}	Server power use when not in use
P _{inrowidle}	Power consumption of in-row cooler when unused (AR)
P _{inrowmax}	Power use of the in-row cooler while all of the servers are operating at full capacity (AR)
P _{pumps}	The pumps for the cooling water's average power consumption (AR)
P _{cooler}	Typical power usage of the cooling (AR)
P _{UPS}	The typical power usage of UPS (AR)
P _{transponder O/E/O}	A line-side WDM transponder's power usage (10 Gbits/s)
P _{control}	Power usage by a controller
P _{sf}	The switching fabric's energy usage
P _{Tx/Rx E/O, O/E}	: The amount of power used by either a transmitter or a receiver.
P _{edfa}	Power requirements for an EDFA
span	span length of amplifier

3.2 Provisioning Optical Networks

Two different approaches are being discussed for handling network traffic routing and IT infrastructure optimization. The first strategy is known as full anycast, and it involves choosing the destination site and the best path to get there in one step. This strategy aims to maximize both network and IT infrastructure utilisation simultaneously, leading to more effective resource allocation. In the second method, a heuristic optimization technique is used to first determine where to handle the request depending on IT architecture optimisation, and then to determine the best feasible routing to that location[17]. This approach is also aimed at optimizing IT infrastructure utilization but focuses more on finding the best possible routing once the destination site has been determined. This approach involves two separate calculations for scheduling a request.

3.2.1 First approach: Handling requests using FA

Handling requests using a Finite Automaton (FA) involves designing a machine that can recognize a language by reading an input string and transitioning between states based on the symbols it reads. Here are the general steps to handle requests using FA:

Design the FA: This involves specifying the set of states, the evolution function, the initial state, and the set of accepting states. **Read the input string:** Start in the initial state and read each symbol in the input string, transitioning to a new state according to the transition function. **Check the final state:** If the final state is an accepting state, then the input string is accepted. Otherwise, it is rejected.

In terms of handling requests, an FA can be used to recognize a language of valid requests, which can be defined by a regular expression. For example, an FA can be designed to recognize HTTP GET requests of the form "GET /path HTTP/1.1", where "path" is any valid path. The FA would transition from the initial state to a state representing the "GET" method, then transition to a state representing the path, and finally transition to a state representing the HTTP version. If the final state is an accepting state, then the request is valid.

Cryptographic techniques can be used to secure requests, such as by encrypting the input string before it is sent to the FA. This can help to protect sensitive information, such as passwords or credit card numbers, from being intercepted and read by an attacker. Additionally, a hybrid schema can be used to combine different cryptographic techniques, such as using both symmetric and asymmetric encryption, to provide a more robust security solution.

The FA routing algorithm assigns link weights to link l when scheduling request rr using the function $PFA : E \times N \rightarrow R$ as defined in Equation (7) (expanded in Equations 7(a), (b), (c), and (d)). It then employs Dijkstra's algorithm to determine the shortest path based on these weights. The requested IT capacity is denoted as $\phi \in N$. In Equation (7b), adding 1 to the total accounts for the EDFAs at the source and destination OXC of connection l . Pnode l calculates the base power for an OXC or the additional power needed to switch a route, whichever is higher. PDC l ; ϕ is specific to virtual links, connecting an OXC to a data center.

$$P^{FA}(l, \phi) = \alpha \cdot P_{link}(l) + \beta \cdot P_{node}(l) + \gamma \cdot P_{DC}(l, \phi). \quad (7)$$

$$P_{link}(l) = \begin{cases} 0 & \text{if link } l \text{ is in use} \\ \left(\left\lceil \frac{|l|}{span} \right\rceil + 1 \right) \cdot P_{edfa} & \text{otherwise} \end{cases} \quad (8)$$

$$P_{DC}(l, \phi) = \begin{cases} P_{base}(\phi) + P_{DC}(\phi) & \text{if adjacent DC of } l \text{ is inactive} \\ P_{DC}(\phi) & \text{otherwise} \end{cases} \quad (9)$$

We make mention of this $\alpha \beta \gamma$ 1, when PFA l ; ϕ assigns each link with the additional power needed if it were to be used to process request r , whether it be virtual or actual. The relative relevance of the power contributions made by connections, OXCs, or data centres can be changed by varying the values α , β , and γ , which have been demonstrated to affect the QoS. (e.g., blocking [36]). This could be favourable since the recently active IT resources (immediately requiring more energy than necessary) can be employed again to meet future requirements, decreasing the short-term energy cost in the future (see Subsection V.A.2). By adjusting the values for α , β , and γ in performance assessment, how energy use and service quality are related. In this study, a parameter set shall be denoted by the symbols α ; β ; γ .

3.2.2 Second approach: energy efficient routing using heuristic optimization

Energy-efficient routing through heuristic optimization is a method to optimize data packet routing in a wireless sensor network (WSN) with the goal of minimizing energy consumption. In WSNs, nodes are often powered by batteries, and energy is a finite resource that must be conserved to prolong network lifespan.

Heuristic optimization is a technique that involves finding a near-optimal solution to a problem by using an algorithm that searches through a set of possible solutions. Heuristic optimization algorithms can be used to solve routing problems in WSNs by finding a route that minimizes the energy consumed by the nodes. Various heuristic optimization algorithms, such as genetic algorithms, ant colony optimization, and particle swarm optimization, are applicable for energy-efficient routing in WSNs. These algorithms iteratively enhance candidate solutions until a near-optimal solution is achieved. The aim in energy-efficient routing with heuristic optimization is to discover a path

that minimizes overall energy consumption by the nodes. This process involves factors like inter-node distances, transmission power requirements, and wireless link quality. Optimizing data packet routing conserves energy, prolongs network lifespan, enhances WSN performance and reliability, and reduces maintenance expenses. Nonetheless, it's crucial to acknowledge that heuristic optimization algorithms may not always yield the optimal solution; the solution quality depends on the algorithm, problem specifics, and chosen parameters. Hence, thorough evaluation of different algorithms and parameters is essential for each problem instance.

This paper defines the niche as a specific environment of an organizational structure, and the optimization method utilizes this concept to divide individuals in a population into several categories based on their fitness values. A new population is formed by choosing the fittest people to represent each classification. To finish a task, the optimization technique makes use of sharing, exclusion, and/or preliminary selection procedures. This strategy attempts to boost the platform's performance in terms of energy consumption and managing massive multimedia data while also increasing the efficiency of the optimization procedure. Having a contingency plan is advisable in case the primary backup option fails. The goal is to prevent the algorithm from accelerating toward local optima by encouraging it to explore various areas of the solution space. Each niche is defined by a niche radius, and solutions that are close to each other in the solution space are penalized to avoid redundancy.

Algorithm 1: Energy Efficient algorithm	
<pre> 1 Input: node/server set S in data centers and the cloud computing network, L(link matrix denoting the connectives among nodes), M (traffic request matrix denoting the request demands of multimedia Data from all source nodes/servers to all destination nodes/servers), C(link capacity matrix denoting the maximum achievable capacity of each link in the network), parameter β, utilization threshold factor α of links in the cloud computing network, path selection operator sel which is a real constant between 0 and 1, population size ps; 2 Output: path populations $pathPop$, which denotes the population of all path sets from all source nodes to all destination nodes; 3 $vSourceNodeVector \leftarrow getSourceNodeVector(S)$; 4 $vDestinationNodeVector \leftarrow getDestinationNodeVector(S)$; 5 $numSourceNode \leftarrow getNumofSourceNode(vSourceNodeVector)$; 6 $numDestinationNode \leftarrow getNumofDestinationNode$ ($vSourceNodeVector$); 7 for $ns \leftarrow 1$ to $numSourceNode$ do 8 $nSourceNodeIndex = vSourceNodeVector[ns]$; 9 for $nd \leftarrow 1$ to $numDestinationNode$ do 10 $nDestinationNodeIndex = vDestinationNodeVector[nd]$; 11 $pathsetFromSrcToDest = getRdfsPathset(nSourceNodeIndex,$ $nDestinationNodeIndex, L, M)$; 12 $pathset[ns, nd] = pathsetFromSrcToDest$; 13 end 14 end 15 $numPathset \leftarrow getPathsetNum(pathset)$; 16 for $np \leftarrow 1$ to $numPathset$ do 17 $[currentPathset, srcNode, destNode] = getCurPath(pathset, np)$; 18 $isMaxhop \leftarrow getMaxhop(currentPathset)$; </pre>	<pre> 19 if $isMaxhop \neq TRUE$ do 20 $isMaxcapacity \leftarrow getMaxcapacity(currentPathset)$; 21 if $isMaxcapacity \neq TRUE$ do 22 $s2dpathset[srcNode, destNode] = currentPathset$; 23 end 24 end 25 end 26 for $ns \leftarrow 1$ to $numSourceNode$ do 27 $nSourceNodeIndex = vSourceNodeVector[ns]$; 28 for $nd \leftarrow 1$ to $numDestinationNode$ do 29 $nDestinationNodeIndex = vDestinationNodeVector[nd]$; 30 $sels2dpathset = s2dpathset[nSourceNodeIndex,$ $nDestinationNodeIndex]$; 31 $numselPathset \leftarrow getPathsetNum(sels2dpathset)$; 32 $np = 0$; $nz = ps / numselPathset$; $ii = 1$; 33 while $np > ps$ do 34 $valrand = getRandValue()$; 35 if $valrand > sel$ do 36 $pathPop[ns, nd, :] = getCurS2DpathPopulation$ 37 ($np = np + nz$); 38 end 39 $ii = ii + 1$; 40 if $ii > numselPathset$ do 41 $ii = 1$; 42 end 43 end 44 end </pre>

In simple terms, algorithm 1 can be disuccsed as:

Algorithm 1: Energy Efficient algorithm
Steps: 1. Input the network topology, including nodes and links, along with their capacities and distances. 2. Initialize the energy consumption variables for each node and link to zero. 3. Calculate the shortest path between each source-destination pair using a suitable routing algorithm (e.g., Dijkstra's algorithm). 4. For each source-destination pair, perform the following steps: a. Iterate through each link in the shortest path.

- b. Calculate the energy consumption for each link based on its distance and capacity.
- c. Update the energy consumption variables for the link and its adjacent nodes.
5. Select the path with the minimum total energy consumption for each source-destination pair.
6. Output the selected paths for all source-destination pairs as the energy-efficient routing solution.

This algorithm aims to find paths that minimize the overall energy consumption in the optical network while satisfying the capacity constraints. By considering the energy consumption and capacities of links, it provides a solution that optimizes the energy efficiency of data transmission in the network.

The actual implementation may require additional details and considerations specific to the optical network technology being used, such as wavelength assignment, modulation formats, and signal quality constraints.

3.3 Initial Population

We create the plan set for each phase of the search following the constraints in Equations (7) through (11) using the necessary population sizes (11). Here, one can construct the initial population of paths linking the source node/server to the destination node/server. A crucial indicator for assessing how well members of the population operate is their fitness value. The effectiveness of the genetic algorithm is directly impacted by this. So, the fitness function must be properly created based on the problem alone. We create the plans group with the stated size of populations for each search stage in this research following the restrictions in Equations (7)–(11). This lowers the energy requirements of networks and boosts their energy effectiveness. Such a scenario allows for the formation of the first population set of pathways between the source node/server and the destination node/server [18]. A crucial indicator for assessing how well members of the population operate is their fitness value. The effectiveness of the genetic algorithm is directly impacted by this. So, the fitness function must be properly created based on the problem alone. The objective functions in Equation (11) are used in this paper to build the corresponding fitness function, which seeks to decrease network energy consumption and increase networking energy efficiency.

$$P_{fitness}(P_{z'}) = \left(\frac{\sum_{\forall p_{z'}(i,j) \in E} F(x_{ij})}{\sum_{\forall p_{z'}(i,j) \in E} x_{ij}} \right) + \left(\frac{E_{sys}}{\sum_{\forall p_{z'}, i=0}^{n-1} \sum_{\forall p_{z'}, j=0}^{num} r_{dc_{ij}}} \right) \quad (10)$$

3.4 Selection Criteria

The fitness value of individual i is $f(p_i)$ for a given population path $Pop \{p_1, p_2, p_3, \dots, p_n\}$ of size n , without losing generality. The following can be used to express the likelihood that individual i is chosen:

$$P_{select}(p_i) = \frac{f(p_i)}{\sum_{i=1}^n f(p_i)}, \quad i = 1, 2, \dots, n \quad (11)$$

Equation (13), on the other hand, predicts that people with high fitness values be passed on straight to the next generation whereas those with poor fitness values reproduce less or not at all. In our selection strategy, we use the main proportional choosing techniques that are fitness value centred to compute the cumulative possibilities to apply the selection probability $P_{select}(p_i)$ of each individual i . If k people in the population have a cumulative probability, then

$$P_{cdf}(k) = \sum_{i=1}^k P_{select}(p_i), \text{ then } P_{cdf}(k) \quad (12)$$

If individual k is chosen, then $P_{cdf}(k)$ is used to make the decision. Following is the decision-making procedure. First, a number between 0 and 1 is chosen at random. Second, λ is put up against $P_{cdf}(k-1)$ and $P_{cdf}(k)$.

results. The choice of individual k is made if $P_{cdf}(k-1) < \lambda < P_{cdf}(k)$. As a result, the same process is used to produce the individuals in the following generation n times.

3.5 Crossover

A genetic recombination technique similar to sexual reproduction in nature is the crossover activity of the path populations. This method will enable the development of new people with more complex genetic make-ups and pass on beneficial genes to the next generation. Crossover tactics include discrete recombination, intermediary recombination, and linear recombination, which are actual crossovers, and binary crossovers. In this study, we offer a novel crossover technique for bringing on new hires [19]. In genetic algorithms, the crossover is typically performed by selecting a crossover point along the chromosome and swapping genetic material between two parent individuals to create one or more offspring individuals. It sounds like, in your crossover method, you are swapping the values of individual genes instead of swapping segments of the chromosome.

Additional operators found in genetic algorithms are mutations. By randomly altering the values of certain genes on chromosomes, mutation aims to increase population diversity. The described uniform mutation operator substitutes gene values in a person's coding string with a uniformly distributed random number falling inside a specific range. Both crossover and mutation are essential operators in a genetic algorithm, and the specific implementation of these operators can have a significant impact on the algorithm's performance.

3.6 Energy Efficient path

The niche strategy initially assesses the size of the population by comparing the hamming distance (d) between the two population members.

$$d = \|x_i - x_j\| = \sum_{k=1}^p (x_{ik} - x_{jk})^2$$

where $i \in [1, n_p + N - 1]$, $j \in [i + 1, n_p + N]$, $N = n_p/2$, and (13)

When two people are separated by a distance $\hat{d}$ that is less than a predetermined distance d , we compare their fitness values and apply a harsher penalty value, $f_{max}(x_i, x_j) = V_{penalty}$, to the one who has the higher fitness value. By doing the niche strategy method, the person with the higher fitness value will have a greater fitness value for both individuals within the specific distance $\hat{d}$. Hence, there is a higher chance that this person will be eliminated in subsequent operations. This helps maintain people at a set distance from one another. The population's diversity is thus successfully preserved in this situation.

3.7 Security layer: Honeypots

The Advanced Encryption Standard (AES) algorithm is a widely adopted symmetric-key encryption method utilized for file encryption and decryption. It employs a secret key for data encryption and decryption, offering high security [20]. The Enhanced Honeypot Algorithm is a security technology that deploys deceptive "honeypot" resources in a network to lure potential attackers. By monitoring these honeypots, network administrators can gather insights into possible attacks and implement preventive measures [21]. The Secure Hash Algorithm 3 (SHA-3) is a cryptographic hashing algorithm used for secure data storage and transmission. It generates a fixed-size hash value unique to the input data, ensuring data integrity verification [22]. One-Time Password (OTP) is an authentication method that generates a unique password valid for a single login session or transaction. The paper suggests that a honeypot-based prediction system could be a useful tool in improving the ability of intrusion detection systems to identify and prevent attacks. However, the specific details of the proposed method would need to be evaluated and tested to determine its efficacy in real-world scenarios.

A honeypot is a security mechanism used to detect and deflect potential attackers or intruders [23]. It is designed to simulate a vulnerable system or network and attract attackers, allowing security professionals to monitor and analyze their behaviour and techniques. Honeypots are used in various fields, including Intrusion Detection Systems (IDS), where they can provide an additional layer of security. By deploying honeypots on a network, organizations can gain

insight into potential vulnerabilities and threats and take steps to mitigate them before they can be exploited. The use of Honeypots in the prediction approach is interesting as it involves deploying a decoy system that mimics a real system to lure attackers and collect information about their tactics and techniques. The interaction level of the Honeypots can then be used to identify potential intrusions in the network. Overall, the proposed work appears to be a promising approach to predicting network intrusions using a combination of feature extraction, clustering, and Honeypot-based detection. However, the effectiveness of the approach would need to be validated through rigorous testing and evaluation.

The three levels of interaction mentioned are High-interaction, Less-interaction, and Medium-interaction [24]. At the High-interaction level, the honeypot offers a complete operating system or utilizes an actual installation of an operating system, along with a monitoring system. This allows the honeypot to handle requests from intruders and even permits malicious schemes to interact with the system while still maintaining control over the process. Furthermore, the text suggests that some high-interaction honeypots also allow limited peripheral connections, making the service appear fully functional in DoS attacks while preventing it from receiving parts that cause massive traffic and losses in the network. Less-interaction honeypots are often implemented as a single physical host that mimics the behaviour of a real system or network service. The honeypot can be configured to appear vulnerable to specific types of attacks, and any attempts to exploit the honeypot can be logged and analyzed. However, unlike high-interaction honeypots, less-interaction honeypots do not involve the full operating system and application layer, which can make them easier to deploy and manage.

Honeypot is a security mechanism that simulates a vulnerable system or network to attract and detect unauthorized access attempts or other malicious activities. The honeypot is designed to be attractive to attackers, but it is isolated from the production network and contains no real data or resources [25]. Therefore, any activity detected on the honeypot is likely to be suspicious and can be further analyzed to identify the attacker's tactics, techniques, and procedures (TTPs). By using honeypots, organizations can gain valuable insights into the current threat landscape and enhance their overall security posture.

Attacker actions are either permitted by the honeypot or blocked by it. Honeypot deletes the Associate's Position, AP(Q_m), for each Q_m that appears in Curr O to pick the response to the attacker. The word for AP(Q_m) is as follows: Attacker actions are either permitted by the honeypot or blocked by it. Honeypot deletes the Associate's Position, AP(Q_m), for each Q_m that appears in Curr O in order to pick the response to the attacker. The word for AP(Q_m) is as follows:

$$AP(Q_m) = \{O_i/O_i \in O/O_r \ \& \ \{O_i O_r\} \in \Phi(T_i)\} \quad (14)$$

The collection of findings known as AP(Q_m), which reasons any hint of T_i when it occurs in conjunction with O_r, is the Associate's Position of O_r. Honeypot responds to each O_j in AS(Ok). Honeypot either never allows the process to expand further or responds with the next message in succession as specified by the protocol requirements.

4. Performance Analysis

The proposed model is implemented using Simulink NS2 and hardware specifications such as Ryzen 5/6 series CPU, NV GTX, 1 TB HDD, and Windows 10 OS. To evaluate the model's performance, metrics like "Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Network Latency (NL), Edge-to-Edge Delay (EED), Network Throughput (NT), Energy Consumption (EC), and Energy Remaining (ER)" are employed. Packet Delivery Ratio (PDR) is the percentage of packets sent by a source node that are successfully received by the destination node. Packet Loss Ratio (PLR) is the percentage of packets that are lost during transmission from the source node to the destination node:

- Network Latency (NL): It refers to the time delay that occurs in data transmission among the source and destination nodes. It is typically measured as the time taken for a package to travel from the source to the destination node and back again.
- Edge-to-Edge Delay (EED): It refers to the time delay that occurs between two nodes in a network. It is the duration it takes for a packet to move between two nodes.
- Network Throughput (NT): It denotes the volume of data that can be transmitted over a network within a specific time frame. It is commonly quantified in bits per second (bps) or packets per second (pps). EC is the amount of energy consumed by a device or network during operation.

- **Energy Remaining (ER):** It refers to the amount of energy that is left in a device or network after it has been used for a certain period of time. This is often used as a metric for evaluating the performance and efficiency of a network.

Table 2 PDR measure, which would be described as the ratio of messages accepted by the liquidator to total messages sent by the sender, compares several models (including the state-of-the-art models marked as L) with the suggested model (EEFAHA-Honeyspot). Figure 5 shows a graphical representation of various models under PDR.

Table 2. Overall comparison of PDR

No. Of nodes	L1	L2	L3	L4	L5	EEFAHA-Honeyspot
10	34	36	44	50	62	78
20	38	40	48	53	66	83
30	43	45	54	62	72	87
60	47	49	59	69	78	90
80	51	53	63	73	82	92
100	55	57	67	76	83	93

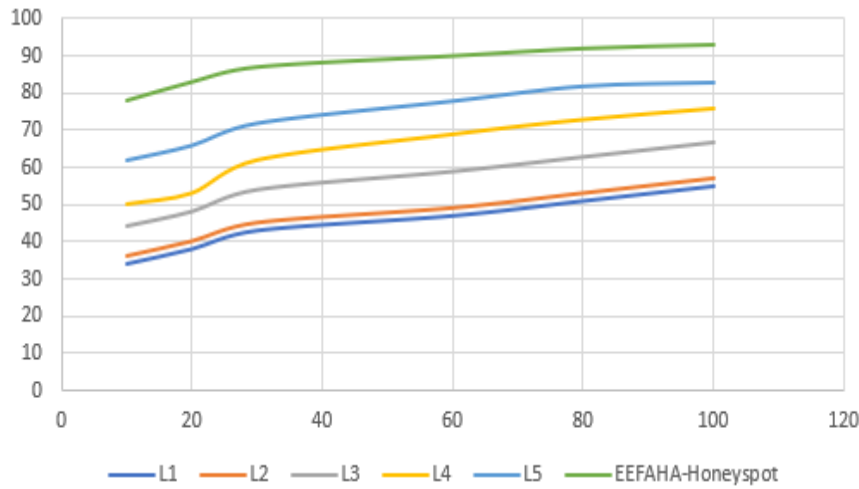


Figure 5. Models vs PDR analysis for optical network

Table 3 compares multiple models based on Packet Loss Ratio (PLR), which is determined by packet loss during transmission and response from source to destination. PLR is described as the proportion of forwarded message losses to the total number of messages sent. During testing, it was observed that the proposed protocol, when related to existing methods, results in a lower packet loss ratio for all numbers of nodes. Figure 6 illustrates the graphical representation of various models compared to the proposed method.

Table 3. Overall comparison under PLR

No. Of nodes	L1	L2	L3	L4	L5	EEFAHA-HONEYSLOT
20	87	84	80	78	74	66
30	83	80	75	71	68	61
60	78	74	70	66	61	57
80	75	71	64	60	55	51
100	70	68	60	57	50	47

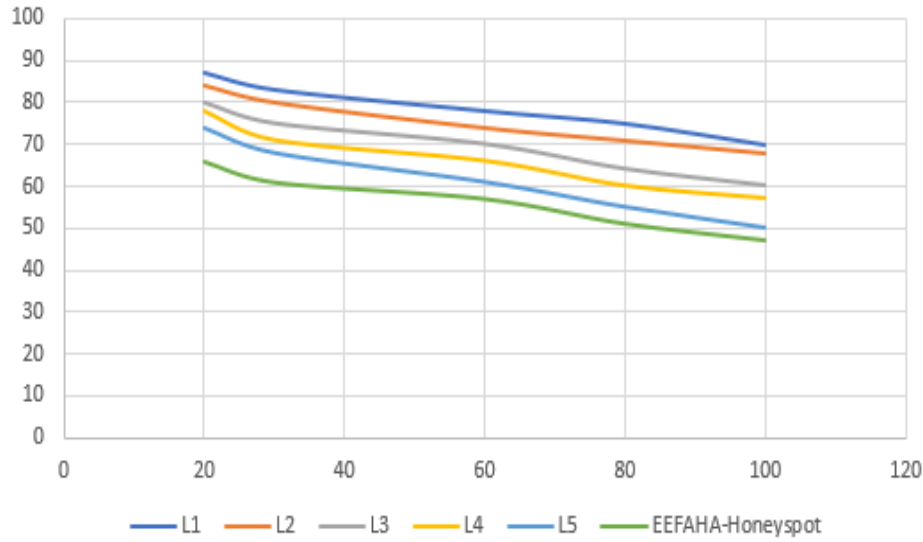


Figure 6. Models vs PLR over optical network analysis

The total assessment under NL, which refers to the amount of time needed to send a data packet across the networks from 1 origin node to another end node, is displayed in Table 4. Network Latency (NL) is comparable to a journey time. According to the results of the investigation, the proposed framework has the lowest latencies, with a time of fifty-three seconds for a total of one hundred nodes. Current models are taking almost 55 and 65 seconds to execute. The proposed model has the lowest delay, according to our analysis of various protocols. Figure 7 shows the overall graphical representation of various models compared to state-of-the-art models.

Table 4. Comparison analysis under NL

No. of nodes	L1	L2	L3	L4	L5	EEFAHA-Honeyspot
20	48	46	44	41	40	33
30	55	57	54	49	45	39
60	64	69	60	52	50	41
80	71	74	69	60	59	43
100	78	80	72	66	57	47

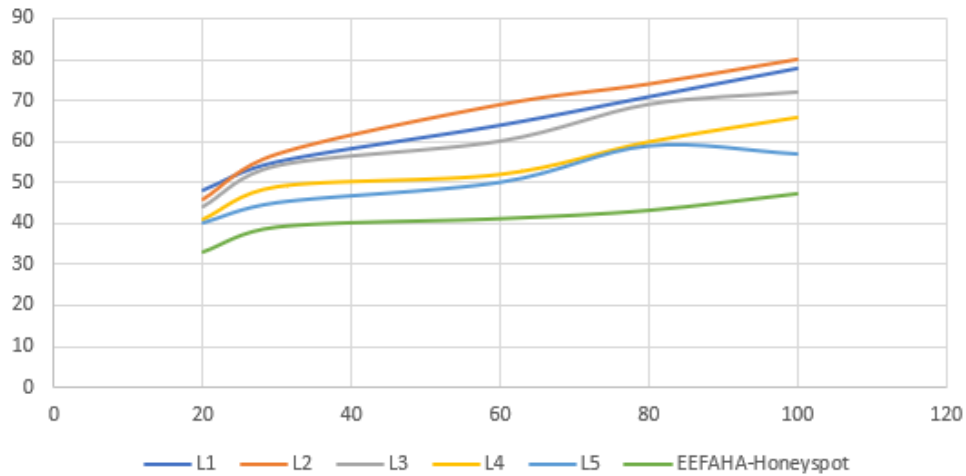


Figure 7. Models vs NL over optical network analysis

The comparative assessment for Edge-to-Edge Delay (EED), which signifies the total hours required to transfer a packet from one of the initial nodes to another of the final nodes within a network, is presented in Table 5.

Table 5. Comparison analysis of EED

No. Of nodes	L1	L2	L3	L4	L5	EEFAHA-Honeyspot
20	6.7	7.4	6.8	5	4.6	3.6
30	5.5	6.2	4.3	4.7	4.1	3
60	4.6	4.3	3.7	4	3.3	2.1
80	7.7	3.8	3.2	3.3	3	1.7
100	8.1	2	3	3	2.7	1.5

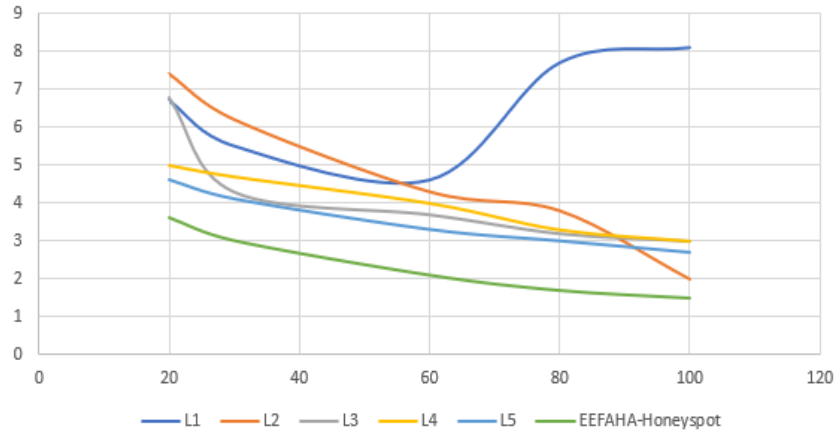


Figure 8. Models vs EED analysis on optical network

The total amount of positive messages is calculated as the sum of all positive messages sent over the networks in a given time frame, according to Table 6. The NT is required to assess the message sent in the interval. The platform's throughput increases as the no. of nodes increases. According to the data, the newly developed proposed system has a throughput of sixty packets per sec, whereas alternative techniques using 100 nodes have lesser throughputs (refer Figure 9).

Table 6. Comparison analysis under NT

No. Of nodes	L1	L2	L3	L4	L5	EEFAHA-Honeyspot
20	30	36	43	47	50	33
30	45	48	54	55	56	53
60	51	56	67	61	74	77
80	59	65	74	67	82	87
100	67	70	79	80	85	89

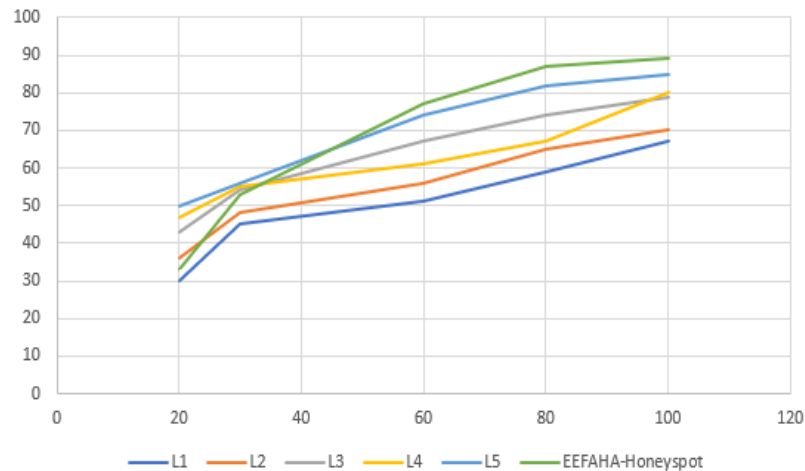


Figure 9. Models vs NT over optical analysis network

The efficiency of the network and data transmission are both reportedly impacted by the node's use of battery power (energy), as is seen in Table 7's comparison study of EC. Node interference during data transmission results from inefficiencies in information transfer. The system's power consumption is quantified as P_{elec} . The battery power loss is denoted as l^2 , and the distance between the nodes in the group is represented by D . Data is transmitted from the transmission amplifier to the forwarding node at a rate of T_{amp} . A transmission amplifier's T_{amp} is the amount of power it uses to transfer data to a forwarding node. Power losses happen when m -bit data is transmitted over the radio channel since the probabilistic model relies on radio signal transmissions to transfer information. The formula below is used to determine the energies (Figure 10).

$$P_{TX}(m, D) = P_{elec} * m + T_{amp} * m * l^2 \quad (15)$$

or when a specific message is transmitted, the radio signal develops

$$P_{RX}(m) = P_{elec} * m. \quad (16)$$

In these conditions, sending and receiving a message is not more affordable. As a result, the whole energy usage may be described in

$$P_{Total} = P_{elec} * m + T_{amp} * m * l^2 + \{P_{elec} * m\} \quad (17)$$

Table 7. Comparison analysis under EC

No. Of nodes	L1	L2	L3	L4	L5	EEFAHA-Honeyspot
20	42	45	43	55	50	33
30	55	57	65	72	56	41
60	67	69	77	77	74	49
80	73	76	79	81	82	52
100	85	82	81	86	85	59

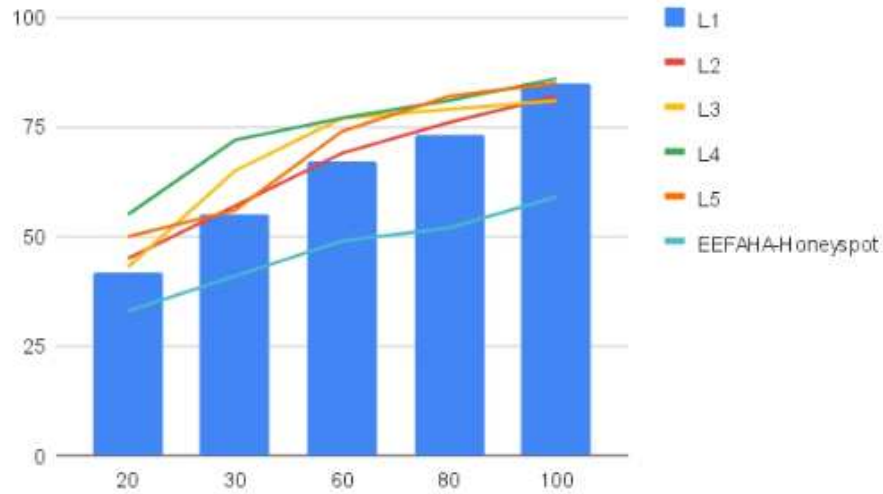


Figure 10. Models vs EC over an optical network

5. Conclusion

This paper concentrates on the issue of energy-productive organizing in cloud administrations with geologically conveyed server farms for interactive media enormous information applications. In particular, we suggest a multiple-

limitation improvement strategy for streamlining energy productivity in distributed computing administrations, which also streamlines energy efficiency in server farms and cloud organizations. They also offer ingenious heuristics calculations that mix the specialized hereditary calculations with irregular profundity first search to address these models for dynamic solicitation requests between various server farms and between server farms and customers. Reproductive outcomes demonstrate the potential of our method.

6. Compliance with Ethical Standards

A. Disclosure of Potential Conflicts of Interest

We confirm that this work is original and has not been published elsewhere, nor is it currently under consideration for publication elsewhere. We declare that we have no financial or personal relationship with other people or organizations that could inappropriately influence our work. There is no conflict of interest to report for any author. We affirm that the all authors have seen and agreed to the submitted version of the paper and their inclusion of names as co-authors.

B. Research Involving Human Participants and/ or Animals

No research involving human participants and/or animals is conducted in this capacity.

C. Informed Consent

No research involving human participants and/or animals is conducted in the scope of this study or project, for which informed consent is to be applied.

The authors have declared that they do not have any conflict of interest regarding publication of this work.

Reference

- [1] Wei, Jia, Mo Chen, Longxiang Wang, Pei Ren, Yujia Lei, Yuqi Qu, Qiyu Jiang et al. "Status, challenges and trends of data-intensive supercomputing." CCF Transactions on High Performance Computing 4, no. 2 (2022): 211-230.
- [2] Hall, Matthew Nance, Klaus-Tycho Foerster, Stefan Schmid, and Ramakrishnan Durairajan. "A survey of reconfigurable optical networks." Optical Switching and Networking 41 (2021): 100621.
- [3] Keiser, Gerd, and Gerd Keiser. Fiber optic communication networks. Springer Singapore, 2021.
- [4] Oluwatoyin, Kadiri Kamoru, Alimi Maryam Odunola, and Ajisafe Yusuph. "Grooming Telecommunications Network: Optimization Replicas and Techniques." Journal of Scientific Research and Reports (2019): 1-8.
- [5] Helali, Leila, and Mohamed Nazih Omri. "A survey of data center consolidation in cloud computing systems." Computer Science Review 39 (2021): 100366.
- [6] Bush, Martin J., and Martin J. Bush. "Coming Clean." Climate Change and Renewable Energy: How to End the Climate Crisis (2020): 213-269.
- [7] Dambhare, Sanket Anil, Rutvik Rajesh Walde, Sahil Ramrao Bhogekar, Saikat Ranajit, Ritik Shriniwas Kotgiriwar, and Sakshi Sudhakar Langde. "Design and Implementation of Encryption Tool using Advanced Encryption Standard (AES)." In 2022 International Conference on Electronics and Renewable Systems (ICEARS), pp. 870-874. IEEE, 2022.
- [8] S. Lambert and W. Van Heddeghem, "Worldwide electricity consumption of communication networks," Optics Express, vol. 20, no. 26, pp. B513–B524, 2012
- [9] Lorincz, Josip, Antonio Capone, and Jinsong Wu. "Greener, energy-efficient and sustainable networks: State-of-the-art and new trends." Sensors 19, no. 22 (2019): 4864.
- [10] Butt, R.A.; Idrus, S.M.; Qureshi, K.N.; Shah, P.M.A.; Zulkifli, N. An energy efficient cyclic sleep control framework for ITU PONs. Opt. Switch. Netw. 2018, 27, 7–17.
- [11] Sharma Tripti, Singh, Senthamil Selvan, and Daniel Krah. "Energy-efficient resource allocation and migration in private cloud data centre." Wireless Communications and Mobile Computing 2022 (2022).
- [12] Das, Sandip, Frank Slyne, and Marco Ruffini. "Optimal Slicing of Virtualized Passive Optical Networks to Support Dense Deployment of Cloud-RAN and Multi-Access Edge Computing." IEEE Network 36, no. 2 (2022): 131-138.
- [13] Taubenblatt, Marc, Pavlos Maniotis, and Asser Tantawi. "Optics enabled networks and architectures for data center cost and power efficiency." Journal of Optical Communications and Networking 14, no. 1 (2022): A41-A49.

- [14] Yang, Hui, Qiuyan Yao, Bowen Bao, Ao Yu, Jie Zhang, and Athanasios V. Vasilakos. "Multi-associated parameters aggregation-based routing and resources allocation in multi-core elastic optical networks." *IEEE/ACM Transactions on Networking* 30, no. 5 (2022): 2145-2157.
- [15] Song, MengXuan, and Kai Chen. "Numerical study on the optimal power distribution of server racks in a data center." In *Building Simulation*, pp. 1-13. Beijing: Tsinghua University Press, 2023.
- [16] Zhu, Ziyi. *High Performance Silicon Photonic Interconnected Systems*. Columbia University, 2022.
- [17] Bešinović, Nikola, Raphael Ferrari Nassar, and Christopher Szymula. "Resilience assessment of railway networks: Combining infrastructure restoration and transport management." *Reliability Engineering & System Safety* 224 (2022): 108538.
- [18] Hajiali, Ismail, Andi Muhammad Fara Kessi, B. Budiandriani, Etik Prihatin, and Muhammad Mukhlis Sufri. "Determination of Work Motivation, Leadership Style, Employee Competence on Job Satisfaction and Employee Performance." *Golden Ratio of Human Resource Management* 2, no. 1 (2022): 57-69.
- [19] Szymanska-Lejman, Maja, Wojciech Dziegielewski, Julia Dłuzewska, Nadia Kbiri, Anna Bieluszewska, R. Scott Poethig, and Piotr A. Ziolkowski. "The effect of DNA polymorphisms and natural variation on crossover hotspot activity in *Arabidopsis* hybrids." *Nature Communications* 14, no. 1 (2023): 33.
- [20] Migirditch, Samuel, John Asplund, and William Curran. "Chaos engineering: stress-testing algorithms to facilitate resilient strategic military planning." In *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, pp. 2160-2167. 2022.
- [21] Hussein, Nehad H. "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3." In *2019 2nd Scientific Conference of Computer Sciences (SCCS)*, pp. 109-115. IEEE, 2019.
- [22] Khater, Sara El-Sayed, Basheer Abd Elfattah Youssef, and Salwa El-Gamal. "Internet of Things (IoT) Authentication and Integrity Model using MBTSKHF One Time Password (OTP)." In *2022 11th International Conference on Software and Information Engineering*, pp. 97-103. 2022.
- [23] Lokman, Siti-Farhana, Abu Talib Othman, and Muhammad-Husaini Abu-Bakar. "Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review." *EURASIP Journal on Wireless Communications and Networking* 2019 (2019): 1-17.
- [24] Cavazos, Jenel T., Mackenzie R. Riegenbach, and Khandis Brewer. "Making large classes feel small: An examination of student interactions with undergraduate teaching assistants." *Scholarship of Teaching and Learning in Psychology* 7, no. 4 (2021): 263.
- [25] Jadhav, Yogesh C., Arjun Sable, Maithri Suresh, and Manjesh K. Hanawal. "Securing Containers: Honeypots for Analysing Container Attacks." In *2023 15th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 225-227. IEEE, 2023.