International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2093
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Multipath Routing in Cloud Computing using Fuzzy based Multi-Objective Optimization System in Autonomous Networks

Dr. Gaurav Pathak
Auckland University of Technology, Auckland
New Zealand
E-Mail ID: gauravpathak91@gmail.com

Dr. Mohit Angurala
Assistant Professor & Head of the Department,
Department of Computer Science and
Engineering,
Khalsa College of Engineering and Technology,
Amritsar, Punjab, India
https://orcid.org/0000-0002-9506-5864

Abstract:
Intelligent houses and buildings, autonomous automobiles, drones, robots, and other items that are successfully incorporated into daily life are examples of autonomous systems and the Internet of Things (IoT) that have advanced as research areas. Secured data transfer in untrusted cloud applications has been one of the most significant requirements in the cloud in recent times. In order to safeguard user data from unauthorised users, encrypted data is stored on cloud servers. Existing techniques offer either security or efficiency for data transformation. They fail to retain complete security while undergoing significant changes. This research proposes novel technique in multipath routing based energy optimization of autonomous networks. The main goal of this research is to enhance the secure data transmission in cloud computing with network energy optimization. The secure data transmission is carried out using multi-authentication attribute based encryption with multipath routing protocol. Then the network energy has been optimized using multi-objective fuzzy based reinforcement learning. The experimental analysis has been carried out based on secure data transmission and energy optimization of the network. The parameters analysed in terms of scalability of 79%, QoS of 75%, encryption time of 42%, latency of 96%, energy efficiency of 98%, end-end delay of 45%.

Keywords: Autonomous systems, energy optimization, secure data transmission, cloud computing, network energy optimization

1. Introduction:

A technical development known as cloud computing (CC) involves streamlining the storage and processing of data to increase the capability of IT systems. It enhances access to private data stored in the cloud and enables users to access requests without first authenticating them [1]. Additionally, CC has a lower cost need for building IT infrastructures and acquiring cutting-edge assets. By maintaining a single application, the computers utilised in CC services gain the benefit of multitenant structure. It depends on the ability to access computer resources through mobile devices. Similar to how regular desktop computers traditionally complete tasks, mobile computing does the same. Mobile computing is typically supported by key concepts such software, hardware, and communication. Devices that are typically used as personal devices, such as PCs, tablets, and smartphones, are considered hardware. Software is made up of the programmes that are modelled after and created for mobile platforms. Communication encompasses networks and protocols that comprise concepts relevant to communication techniques, to sum up [2]. The following are elements of the mobile computing strategy. The first component is mobility, which enables fixed or mobile nodes to link with nodes of other devices in a mobile computing environment utilising a mobile support station (MSS). Diversity of access network types is the next factor that enables communication between mobile and MSS nodes despite the presence of various access networks with differing bandwidths and overhead. Third, frequent network disconnects suggest that the mobile nodes lack the capacity to establish dependable connections because of their constrained resources, such as battery power and communication bandwidth. Finally, the signals of mobile nodes are vulnerable to interference in mobile networks because of the issue of poor consistency and safety [3]. The majority of outsourcing models for computing and hosting resources are included in the CC model. CC as defined by NIST, is the process of gaining effective access to network resources with less effort and wait time. When building the security measure, these factors are given more weight for optimal protection. Internet security relies on certain tools and guidelines, such as encryption, firewalls [4], which block superfluous traffic, anti-malware, anti-spyware, and anti-virus software, to protect data communicated over the internet. Although CC is frequently used to deliver a variety of services, it faces a number of difficult problems with resource management, power usage, security, service quality, and big data. The common drawbacks of data centres are their comparatively high running costs and excessive power consumption, which have significant negative effects on the environment. Due to this weakness, offering energy-efficient solutions has risen in importance as a result of the rising energy demand and desire for powerful computing [5].

The contribution of this research are as follows:

- To propose novel technique in multipath routing based energy optimization of autonomous networks
- Secure data transmission is carried out using multi-authentication attribute based encryption with multipath routing protocol
- Network energy has been optimized using multi-objective fuzzy based reinforcement learning

2. Related works:

Method of distributing computing services through software, infrastructure, and other means has changed as a result of the needs and requirements of the customer in the cloud environment. The providing of services and resources via the cloud environment has a huge impact on changing how various sectors operate. Collaborative Security Detection Method (CSD), a framework for game theoretical analysis, was introduced in [6] using the consensus protocol. An iteration-based measurement method was created in [7] to reach Nash equilibrium after uniqueness analysis. By establishing secured virtual zones, a reliable identification and authentication method was created in [8]. The system did not, however, guarantee security. [9] described yet another data-driven approach using rules-supported reasoning and queries. The outcomes guaranteed both security and scalability. Although protection for a sizable number of users was given, it came at the expense of more time. A CAPPCHA method that effectively distinguished between humans and computers was investigated in [10] in order to reduce the time needed. The two most crucial challenges to be addressed are data security and data integrity due to the impressive growth of IoT in healthcare sector. Under [11], a hybrid encryption scheme was created to provide security by first encrypting secret data as well as concealing it in a cover image. According to [12], a model-based security toolkit made it easier to protect user data by utilising various features of trust relationships. The Cauchy Integral Theorem and Laplace Transform were designed in [13] in such a way that the chance of a secrecy outage was calculated using the signal-to-interference ratio modelling of each group of cooperating eavesdroppers. The most often used strategies in cloud data centres to lower energy consumption and SLA violations are optimization procedures [14]. For resource allocation, energy consumption, VM migration, SLA, and QoS, the cloud uses the firefly method, WAO, heuristic approach, and cat swarm optimization [15–17]. As a result, multi-objective optimization techniques [18] are used to concurrently enhance QoS, lower energy usage, and lower SLA violation. One of the significant optimization techniques employed in cloud data centres that offers efficient performance is the NSGA-II. To manage the cloud resource, the NSGA-II with ANN [19] was used, and it performed well. In terms of energy consumption, resource load balance, average resource use, and availability, IBBO technique performed well. The multi-objective optimization techniques address trade-off between several specifications, hence optimization techniques are crucial in cloud data centre to deliver effective solutions [20].

3. System model:

This section discuss novel technique in multipath routing based energy optimization of autonomous networks. The main goal of this research is to enhance the secure data transmission in cloud computing with network energy optimization. The secure data transmission is carried out using multi-authentication attribute based encryption with multipath routing protocol. Then the network energy has been optimized using multi-objective fuzzy based reinforcement learning. The proposed cloud based secure and energy optimization architecture is represented in figure-1.

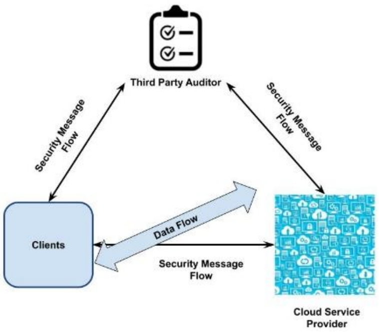

Figure-1 proposed cloud based secure and energy optimization architecture

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2093
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Data owner: Data is directly transferred from the data owner to the cloud server. Data owners encrypt information records for security reasons before storing them in the cloud. The encrypted content file can be managed by the data owner. Additionally, owner of data may delegate arrangement for access rights to the record of encoded information.

Cloud server: CSP manages a cloud to enable remote access and stockpiling management. Data owners encrypt the information documents and store them in the cloud for user participation. End users download encrypted data from the cloud based on their needs and then decrypt it in order to recover the supplied information records.

Multi-authentication attribute based encryption with multipath routing protocol based secure data transmission:

The independent management of each attribute collection is entrusted to the attribute authorities. The secret key is then created by the authorities for each authorised user. The authorities will produce new key for nonrevoked users when one user has their access revoked. The cloud storage system has four different entities, as shown in Fig. 2: the data owner, the CSS, the N attribute authorities (AAs), and the data user.

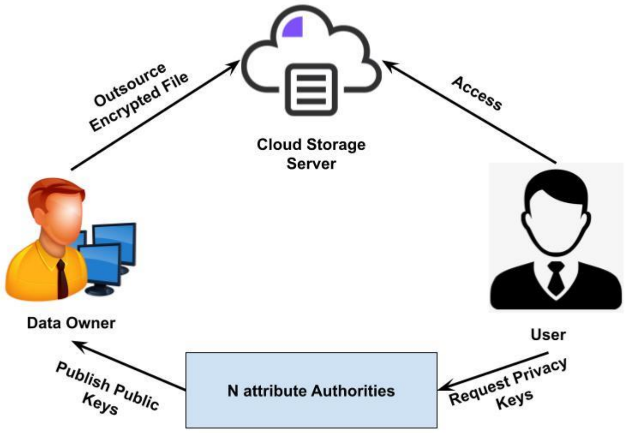

Figure-2 multi-authentication attribute based encryption

Let g be a generator of group G1, and let G1 and G2 be two cyclic groups with prime order p. The following five steps make up our decentralised MA-ABE access control method with policy hidden: System initialization: AA Setup method is executed by each authority Aj (j ∈ N) that possesses a set of attributes L j. The set of characteristics $\left(L_i \cap L_j = \emptyset, i \neq j\right)$ is disjoint.

1. For each attribute βj ∈ Z∗ p where vx is an attribute version key, authority Aj selects a number Aj (j ∈ N) and three random numbers $\alpha_x, y_x, v_x \in Z_p^*$and $x\left(x \in L_j\right)$. eq. (1) is the secret code for authority Aj (j N):

$$SK[j] = \left(\{\alpha_x, y_x, v_x\}_{x \in L_j}, \beta_j\right) \qquad (1)$$

2) Key generation: When user GID wants to access data, it asks all pertinent authorities for the secret keys. Each authority executes the K enGen algorithm after validating the user's identification. The user is given the characteristics set Ij,GID and matching private key K j,GID in equation (2) by the authority Aj(j ∈ N):

$$K_{j,GID} = \left(\{D_{1,x} = g^{\alpha_x v_x} H(GID)^{y_x}\right.$$

$$\left. D_{2,x} = H(x)^{\beta_j}\}_{x \in I_{j,GID}}\right) \qquad (2)$$

where $\alpha_x, y_x, v_x, \beta_j \in SK[j]$ Note that user’s private keys are disseminated under secure channel.

1) Encryption: After employing a content key MSG ∈ G2 and symmetric encryption, data owner outsources data to CSS. Data owner then creates an access policy T that covers connected AAs' related characteristics. Owner then uses the encryption technique to encrypt MSG. The owner chooses a number at random, $a \in Z_p^*$, and calculates $s_y = e\left(\left(g^{\beta_j}\right)^a, H\left(\lambda_y\right)\right)$ and $\lambda_y (y \in Y)$ signifies one attribute of access policy T. We can be pre-computed sy once and for all, it is important to remark.

2. The owner uses sy to replace the attribute λy in access policy in order to implement privacy preservation policy. The access policy T is then transformed into the LSSS access matrix, where Mi is I th row of $(M_{m \times h}, \rho)$.

3. Owner encrypts MSG by using eq. (3) to execute the Encrypt algorithm:

(a) Randomly chooses a number $s \in Z_p^*$ and a vector

$$v = (s, r_2, r_3, \ldots, r_h)^{\mathrm{T}} \in Z_p^h \qquad (3)$$

(b) Evaluate μi = Mi · ν.

(c) Choose a random vector $\omega = (0, t_2, t_3, \cdots, t_h)^{\mathrm{T}} \in Z_p^h$

(d) Evaluate $\varphi_i = M_i \cdot \omega$

(e) Randomly chooses a number $\sigma_i \in Z_p^*$ for every row Mi of M.

(f) Evaluates ciphertext components as eq. (4)

$$C_0 = \text{MSGe } (\text{g}, g)^s, h_0 = g^a$$

$$C_{1,i} = e(g,g)^{\mu_i} e(g,g)^{v_{\rho(i)}\alpha_{\rho(i)}\sigma_i}, \forall i \in [m]$$

(4)

$$C_{2,i} = g^{\sigma_i}, \forall i \in [m]$$

(g) Cipher text CT are outsourced to cloud storage method by eq. (5).

$$CT = \left(C_0, \{C_{1,i}, C_{2,i}, C_{3,i}\}_{\forall i \in [m]}, h_0, (M,\rho)\right)$$

(5)

4) Decryption The user can obtain its MSG and further obtain the owner's data if their attributes comply with the access rules.

1. Firstly, user evaluates $s' = e\left(h_0, H(x)^{\beta_j}\right) = e\left(g^a, H(x)^{\beta_j}\right)$ for $\forall x \in I_{j,u}$ by utilizing component $h_0 = g^a$ from CT .

2. Utilizing s to replace attribute x, it can construct an attributes set $I'_{GID} = \{I'_{j,GID}, j \in [N]\}$. User gains access policy (M, ρ) from CT , and evaluates set $R' = \{i: (\rho(i) \cap I'_{GID})_{i \in [m]}\}$

3. User selects constants $c_i \in Z_p^*$ such as $\sum_{i \in R'} c_i M_i = (1,0, \ldots ,0)$ Decryption method is as follows:

(a) For evert i ∈ R , it evaluates by eq. (6)

$$\text{Dec } (i) = \frac{C_{1,i} e\left(H(GID), C_{3,i}\right)}{e\left(K_{\rho(i),GID}, C_{2,i}\right)} \qquad (6)$$

(b) It obtains plaintext by eq. (7)

$$MSG = C_0 / \prod_{i \in [m]} \text{dec } (i)^{c_i}$$

(7)

5) User revocation The authority Aj is designed to revoke the user GID's attributes set $\phi_{j,GID'}$. The three stages of the user revocation are as follows:

1. Update key by AAs: Aj executes U K eyGen algorithm when the user is revoked. For each property $x \in \phi_{j,GID'}$, it first selects a random version key $v'_x \in Z_p^*$. The authority Aj then determines the public key $P'_{1,x} = P_{1_1 x} \cdot e(g,g)^{\alpha_x (v'_x - v_x)} = e(g,g)^{\alpha_x v'_x}$ and the update key $UK_j = \{g^{\alpha_x (v'_x - v_x)}, x \in \phi_{j,GID'}\}$. The authority Aj then uses the encrypted channel to deliver U K j to users and data owners who have not had their access revoked.

2. Non-revoked users updating secret keys The user will use SKUdate method to update its secret key as by eq. (8) after receiving update key U K j from authority Aj.

$$\begin{aligned} K'_{j,u} = \big(\forall x \in \phi_{j,GID'}: D'_{1,x} = D_{1,x} \cdot UK_j \\ = g^{\alpha_x v'_x} H(GID)^{y_x}, D'_{2,x} = D_{2,x} \\ \forall x \notin \phi_{j,GID'}: D'_{1,x} = D_{1,x}, D'_{2,x} = D_{2,x} \end{aligned} \qquad (8)$$

The nonrevoked users can be recognised by the authority since theU K j is connected to the revoked user GID'. Therefore, the user GID with revocation cannot receive update key U K j.

3. Ciphertext update by data owner: CTU update procedure will be used by the data owner to update its ciphertext after it gets updated key U K j from authority Aj. First, data owner gathers ciphertext components (C1,i,C2,i) in CSS that contain attributes s (j,GID'). Equation (9) is used to determine each of the following stages for each ciphertext component:

$\forall i = 1$ to m: if $\rho(i) \in \phi_{j,GID}$

$$\begin{aligned} C'_{1,i} = C_{1,i} \cdot e\left(C_{2,i}, g^{\alpha_{\rho(i)}\left(v'_{\rho(i)} - v_{\rho(i)}\right)}\right) \\ = e(g,g)^{\mu_i} e(g,g)^{v' \rho(i) \alpha_{\rho(i)} \sigma_i} \\ \text{else } C'_{1,i} = C_{1,i} \end{aligned} \qquad (9)$$

Finally, the cloud storage system receives the updated values of $C'_{1,i}(i \in [1,m])$. Only the component C1,i in our scheme needs to be modified for each revoked attribute. The user revocation is therefore more effective. The following equations hold, proving that our plan is sound. Eq. (10), which gives us:

$$\text{dec } (i) = \frac{C_{1,i} e\left(H(GID), C_{3,i}\right)}{e\left(K_{\rho(i)} \cdot GID, C_{2,i}\right)}$$

$$= \frac{e(g,g)^{\mu_i} e(g,g)^{v_{\rho(i)}\alpha_{\rho(i)}\sigma_i} e(H(GID), g^{y_{\rho(i)}\sigma_i} g^{\varphi i})}{e(g^{\alpha_s v_x} H(GID)^{yx}, g^{\sigma_i})}$$

$$= \frac{e(g,g)^{\mu_i} e(g,g)^{v\rho(i)^{\alpha} p(i)^{\sigma_i}} e\left(H(GID), g^{y p(i)^{\sigma_i}}\right) e\left(H(GID), g^{\varphi_i}\right)}{e(g^{\alpha_x v_x}, g^{\sigma_i}) e(H(GID)^{y_x}, g^{\sigma_i})} \quad (10)$$

$$= e(g,g)^{\mu_i} e(H(GID), g^{\varphi^i})$$

Then, calculating Eq. (11), we can get:

$$C_0 / \prod_{i\in m} \text{dec } (i)^{c_i}$$
$$= MSGe(g,g)^s / \prod_{i\in m} \left(e(g,g)^{\mu_i} e(H(GID), g^{\varphi_i})\right)^{c_i}$$
$$= MSGe(g,g)^s / e(g,g)^{\sum_{i\in m} \mu_i c_i} e(H(GID), g)^{i\in m} \omega_i c_i \quad (11)$$
$$= MSGe(g,g)^s / e(g,g)^{\Sigma\in m} \mu_i c_i = MSG$$

Take the positive variable $f_{e_i}^{l_0+\cdots h_4}$ as an example. Since each variable in Program RMP has a length of $\lambda \in [0, L]$ and is zeroed by equation (6), this holds for the positive variable $\sum_{\varepsilon=1(0)}$. Or, each path has a corresponding series of positive variables, denoted by $f_{e_i}^{l_0+\cdots h_4}$. Therefore, finding a series of positive variables $f_{e_i}^{l_0+\cdots h_4}$ is sufficient to create a path p∈P (s,t) with a length of at most L. in which the link 0 e originates from the source s and the link h 1 e enters the destination t, i.e., $e_0 \in O(s)$ In order to achieve this, we make use of the following characteristic of Program RMP solutions. There must be a connection e'=(v,w)such that $f_{e_i}^{l_0+\cdots h_4}$ if a positive flow f (e i)(l 0+h 4) arrives through the link e=(u,v)∈E into the node. The total flow along e=(u,v)E is directed from s to u along pathways with a combined total length of λ is denoted by e f. $O(v) = \{(v, I)(v, l) \in E\}$ and $l(v) = \{(w, v)(w, v) \in E\}$ by eq (12)

$$\text{Minimize}\alpha \sum_{e=(0)}^{\text{Subject to:}} f_e^2 - \sum_{\varepsilon=1(0)} f_e^{\alpha-1} = 0 \ \forall v \in V \setminus \{s,t\}, \forall \sum_{\omega=0(x)} f_e^0 = \gamma$$
$$\begin{cases} \sum_{i=1}^{c} u_{ij} = 1, & j = 1,2,\dots n \\ 0 \le u_{jj} \le 1, & i = 1,2,\dots,C; \\ 0 < \sum_{j=1}^{n} u_{ij} < n_, & i = 1,2,\dots,C \end{cases} \quad (12)$$

The network congestion factor is minimised via objective function (1). There are three nodal flow conservation constraints: (2), (3), and (4). Lastly, equation (2) must be met for every node aside from source s and target t. Validity of eqn (2) is extended by eqn (3) to include traffic that encounters sources after having travelled through paths of non-zero length. The constraint on connection capacity consumption is given by equation (5). Maximum link utilisation is not greater than variable's value α, according to this statement, which means that the network congestion factor is at most α. Expression (6) excludes impractical flows and Expressions (7) and (8) demand that none of the variables be negative. The notations that are utilised are shown in Table 2 along with descriptions of each.

Table 1 Notations and their descriptions

Notation	Description	Notation	Description
EK_{SKD}	Encryption by using SKD	C0,c1,r,I,j	Variables
DK_{SKD}	Decryption by using SKD	GID_{XDT}	Data type of xth GP_ID
EK_{PRKDO}	Encryption by using *PRKDO*	D_{DT}	Data type of authorized DO
DK_{PCKDO}	Decryption by using PCKDO	D_{PV}	PV of authorized DO
EK_{PCKCSP}	Encryption by using PCKCSP	GID_{XDO_ID}	DO_ID of xth GP_ID
EK_{PRKCSP}	Encryption by using PRKCSP	GID_{RDO_ID}	DO_ID of rth GP_ID
DK_{PRKCSP}	Decryption by using PRKCSP	GID_{RDT}	PV of rth GP_ID
DK_{PCKCSP}	Decryption by using PCKCSP	GID_{RPV}	Users requested data type
EK_{PRKUSR}	Encryption by using PCKUSR	U_{DT}	Time and data of authorized DO
EK_{PCKUSR}	Encryption by using PCKUSR	$D_{T\&D}$	DO_T&D of rth GP_ID
DK_{PRKUSR}	Decryption using PRKUSR	$GID_{RDO\_T\&D}$	GP_T&D of rth GP_ID
DK_{PCKUSR}	Decryption using PCKUSR	$GID_{RGP\_T\&D}$	PV of xth DO_ID
$DO_{ID\,NEW}$	DO_ID after processing	DID_{XPV}	Search DIDx having minimum PV
$DO_{ID\,PREV}$	DO_ID before processing	$SEARCH_{MIN}$	Search DIDx based on LRU

Count(m)	A function to calculate the number of DO's IDs in m[]	$SEARCH_{LRU}$	Search GIDx based on LRU

Multi-objective fuzzy based reinforcement learning in network energy efficiency:

The total number of nodes should equal X = {X1, X2, . . . , Xn}. With every node having a total of motions, there are Xi nodes in total. V = {V1, V2, . . . , VC} is utilised as cluster head matrix to create C fuzzy groups. According to equation (13):

$$R = \sum_{k=0}^{\infty} \gamma^k r_{k+1} \qquad (13)$$

where $U = (u_{ij})$ is a membership matrix with n and c dimensions, and uij denotes relationship between Vi and Xj. The Euclidean distance between node j and CH I is dij = xj – Vi. Fuzzy exponent in method is m (m > 1). The following equation must also be satisfied by equation (14)

$$\begin{cases} \sum_{i=1}^{c} u_{ij} = 1, & j = 1,2, \dots n \\ 0 \le u_{jj} \le 1, & i = 1,2, \dots, C;\ j = 1,2, \dots, \\ 0 < \sum_{j=1}^{n} u_{ij} < n_{,} & i = 1,2, \dots, C \end{cases} \qquad (14)$$

State space X, action space U, transition function f: X U X, and reward function : ρ : X × U → R comprise a deterministic Markov decision process (MDP). In this study, we just take deterministic scenario into account for simplicity. It is also feasible to formulate the problem stochastically; in this instance, predicted returns under probabilistic transitions must be taken into account. If the expectations can be precisely assessed, our method and findings are simply applied to stochastic MDPs. Controller decides what to do based on its policy h : X → U, where uk = h (xk). Controller's objective is to discover a strategy that maximises discounted return by equation (15) starting from the present time (k = 0) and any initial state (x0):

$$R = \sum_{k=0}^{\infty} \gamma^k r_{k+1} = \sum_{k=0}^{\infty} \gamma^k \rho(x_k, u_k) \qquad (15)$$

where γ ∈ [0, 1) and xk+1 = f(xk,uk) for k ≥ 0. Reward accrued by controller over time is effectively represented by the discounted return. The goal of learning is to improve performance over the long term while simply using input on short-term, one-step performance. Performing the optimal action value function computation is one method of achieving this by eqn (15)

$$Q^h(x,u) = \rho(x,u) + \sum_{k=1}^{\infty} \gamma^k \rho\big(x_k, h(x_k)\big) \qquad (15)$$

where x1 = f(x,u) and xk+1 = f(xk,h(xk)) for k ≥ 1. Q∗ (x,u) = maxh Qh (x,u)is definition of ideal action-value function (x,u). Best policy is one that chooses the action with highest optimal Q-value for each state: h ∗ (x) = arg maxu Q∗ (x,u). The Bellman optimality equation (16) is a key result in RL, and many methods rely on it.

$$Q^*(x,u) = \rho(x,u) + \gamma \max_{w' \in \mathbb{X}} Q^*(f(x,u),u') \qquad (16)$$

Q-value iteration approach is utilized to resolve this equation. Let Q stand for the set of all Q-functions. Describe Q-iteration mapping T : Q → Q, which, using eqn (17), calculates right-hand side of any Q-Bellman function's eqn:

$$[T(Q)](x,u) = \rho(x,u) + \gamma \max_{u' \in \mathcal{U}} Q(f(x,u),u') \qquad (17)$$

Bellman eqn (16) indicates that Q∗ is a fixed point of T using this notation, i.e., Q∗ = T(Q∗). Since T is a contraction with factor 1 in infinity norm, it is true that for each pair of functions Q and Q0, kT(Q) − T(Q0)k∞ ≤ γ kQ − Q0k∞. The transition and reward functions f, ρ, which are used by Q-value iteration method (also known as Q-iteration) serve as an a priori description of the job. The Q-function is updated in each iteration utilizing formula Q'+1 = T(Q') starting from an arbitrary Q-function Q∗. The fact that T is a contraction gives it a distinct fixed point. This point is Q from (3), therefore Q-iteration leads to Q∗ as ` → ∞.

A fuzzy division of state space as well as discretization of action space are foundations of suggested approximation approach. MF ϕi : X → [0, 1], i = 1,... ,N describes each of the N fuzzy sets that make up the fuzzy partition. According to a degree of membership I a state x belongs to every set ϕi(x). The following presumptions are made in the sequel. The action space contains a discrete collection of actions U0 = {uj |uj ∈ U,j = 1,... ,M}. One component I j of the N ×M matrix of parameters stored by the fuzzy approximator corresponds to every pair of the fuzzy core and discrete action (xi ,uj). An approximate Qfunction is produced by the approximation mapping F, which accepts a parameter as input. This approximate Q-function is calculated as eq. (18) for each pair of state-action variables (x, u):

$$R = \sum_{k=0}^{\infty} \gamma^k r_{k+1} = \sum_{k=0}^{\infty} \gamma^k \rho(x_k, u_k) \qquad (18)$$

where Euclidean norm of the argument, k · k, is used both here and in the sequel. It is a form for linear basis functions. According to the relationship by eq. (19), the projection mapping infers the values of the approximator parameters from a Q-function:

$$\theta_{i,j} = [P(Q)]_{i,j} = Q\left(x_i, u_j\right) \qquad (19)$$

This is solution θ to issue by eq. (20):

$$\Sigma_{i=1,\ldots,N,j=1,\ldots,M}\left|[F(\theta)]\left(x_i,u_j\right) - Q\left(x_i,u_j\right)\right|^2 = 0 \qquad (20)$$

The fuzzy Q-iteration technique approximates Q-iteration mapping by beginning with an arbitrary 0 value. Composition of mappings P, T, and F by equation (21) is used for this.

$$\theta_{\ell+1} = PTF(\theta_\ell) \qquad (21)$$

Up until convergence, this composite mapping is applied iteratively. The approximate convergence criterion is maxi,j |θ`+1,i,j − θ`,i,j | ≤ ε. Then, using equation (22) you can determine a roughly ideal policy:

$$h(x) = u_{j^*},\ j^* = \arg\ \max_j\left[F(\theta^*)\right]\left(x,u_j\right) \qquad (22)$$

Specify ε = minQ Q∗ − Q ∞ Any fixed point of composite mapping FP : Q → Q is denoted by symbol Q. The convergence point satisfies equation (23) as follows:

$$\|Q^* - F(\theta^*)\|_\infty \leq \frac{2\varepsilon}{1-\gamma} \qquad (23)$$

Establish the fuzzy approximator's resolutions over state space and, accordingly, over action space using equation (24):

$$\delta_x = \max_{x\epsilon X}\ \min_{i=1,\ldots.N} |||x - x_i||$$

$$\delta_u = \max_{u\epsilon U}\ \min_{i=1,\ldots.M} |||u - u_j|| \qquad (24)$$

where uj is j-th discrete action and xi is core of i-th membership function. The objective is to demonstrate that limδx→0, δu→0 F(θ ∗) = Q∗. There is a finite v > 0 such that fuzzy membership functions satisfy eq. (25) regardless of N.

$$sup\,\Sigma_{i=1}^{N}\varphi_i(x)||x - x_i|| \leq v\,\delta_x \qquad (25)$$

With Lipschitz constants Lf and Lρ, they are Lipschitz continuous according to equation (26):

$$||f(x,u) - f(x,u)|| \leq L_f\{\left||x - x|\right| + \left||u - u|\right|) \qquad (26)$$

When Lf < 1/γ, Lipschitz constant of f is satisfied. To demonstrate the consistency of approximate RL algorithms, Lipschitz criteria akin to Assumption 3.1 are often required. It is established that Q∗ has Lipschitz continuity as a first step in demonstrating consistency. This will be useful in demonstrating later that a fixed-point of FP is arbitrarily near to Q∗ by raising approximator's resolution. A finite LQ exists such that by eq (27)

$$Q^*(x,u) - Q^*(x,u) \leq L_Q((||x - x\grave{}) + ||u - u\grave{}|| \qquad (27)$$

$$|\rho(x,u) - \rho(x,u)| \leq L_\rho((\left||x - x|\right| + \left||u - u|\right|) \qquad (28)$$

for second term by eq. (29),

$$\gamma|\max_{u\grave{}}[Q_l(f(x,u),u\grave{} - Q_l(f(x,u),u\grave{})] \leq \gamma\max_{u\grave{}} L_{Qt}\left||f(x,u) - f(x,u)|\right| \qquad (29)$$

where we utilized Lipschitz continuity of Q` and f. Therefore, $L_{Qt+1} = L_\rho + \gamma L_{Qt}, L_f = L_\rho + \gamma L_{Qt}\sum_{k=0}^{l}\gamma^k L_f^k$ and induction is complete. Define Q = FPQ∗ , i.e., by eq. (30)

$$Q(x,u) = \Sigma_{i=1}^{N}\varphi_i(x)Q^*\left(x_i,u_j\right)\ with\ j = \arg\min||u - uj|| \qquad (30)$$

This Q-function is a fixed point of FP. Start an upper bound on $||Q - Q^*||\infty$. Q∗ (xi ,uj) − Q(xi ,uj)= 0 because Q(xi ,uj) = Q∗ (xi ,uj). Take now x,u such that $x \neq xi, \forall i, or\ u \in U_0$ and let $j = \arg\min j\ \left||u - u_j|\right|$. Then by eq. (31):

$$\begin{aligned}|Q^*(x,u) - Q(x,u)| &= \left|Q^*(x,u) - \sum_{i=1}^{N}\varphi_i(x)Q^*\left(x_i,u_j\right)\right| \\ &\leq \left|Q^*(x,u) - Q^*\left(x,u_j\right)\right| + |Q^*\left(x,u_j\right) \\ &- \sum_{i=1}^{N}\varphi_i(x)Q^*\left(x_i,u_j\right)|\end{aligned}$$

$$|\,\Sigma_{i=1}^{N}\varphi_i(x)|Q^*\left(x_i,u_j\right) - \varphi_i(x)Q^*\left(x_i,u_j\right)| \leq \Sigma_{i=1}^{N}\varphi_i(x)L_Q|x - x_i|| \leq L_Q v\delta_x \qquad (31)$$

where Lipschitz continuity of Q was applied, and final step follows from Assumption 2. By using the Lipschitz continuity of Q and definition of u once more, we may

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2093
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

write: δu, |Q∗ (x,u) − Q∗ (x,uj)| ≤ LQku − ujk ≤ LQδu. Using this (31) and eq. (32) we discover:

$$|Q^{*}(x,u) - Q(x,u) \leq L_Q(\delta_u + v\delta_x) \qquad (32)$$

The definition of eq(33) states that there exist Nd triangular fuzzy membership functions for every state variable xd with d = 1,..., n.

$$\varphi_{d,1}(x_d) = \max\left(0, \frac{c_{d,2} - x_d}{c_{d,2} - c_{d,1}}\right)$$

$$\varphi_{d,1}(x_d) = \max\left(0, \min\left(\frac{x_d - c_{d,i-1}}{c_{d,i} - c_{d,i-1}}, \frac{c_{d,i+1} - x_d}{c_{d,i+1} - c_{d,i}}\right)\right) \qquad (33)$$

$$\varphi_{d,N_d}(x_d) = \max\left(0, \frac{x_d - c_{d,2}, N_{d-1}}{c_{d,N_d} - c_d N_{d-1}}\right)$$

where $x_d \in [c_{d,1}, c_d N_d]$ is array of cores, which entirely dictates structure of MFs. At a membership level of 0.5, adjacent functions always intersect. After that, a pyramid-shaped n-dimensional MF in fuzzy partition of X is produced by multiplying each combination of (single-dimensional) membership functions.

4. Experimental analysis:

An overview of the performance of the suggested system is included in this section. Java is used to implement the suggested system. The physical configuration of the Java platform includes an Intel i5/i7 processor, 4 GB of RAM, and a 3.20 GHz CPU speed. The design proposal proposes a mathematical paradigm to improve cloud storage security. In this plan, the security method collaborates with both the data owner as well as end user simultaneously. The owner's data will be safe throughout data uploading as well as data transfer to appropriate user, even when cloud storage is unreliable. Scalability, Quality of Service, Encryption Time, Latency, Energy Efficiency, Communication Cost, and End-to-End Delay are evaluated for the proposed mechanism.

Table-1 Comparative analysis of Scalability

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	55	59	63
75	59	63	66
100	61	65	69
125	63	68	71
150	65	71	73
175	68	73	75
200	71	75	79

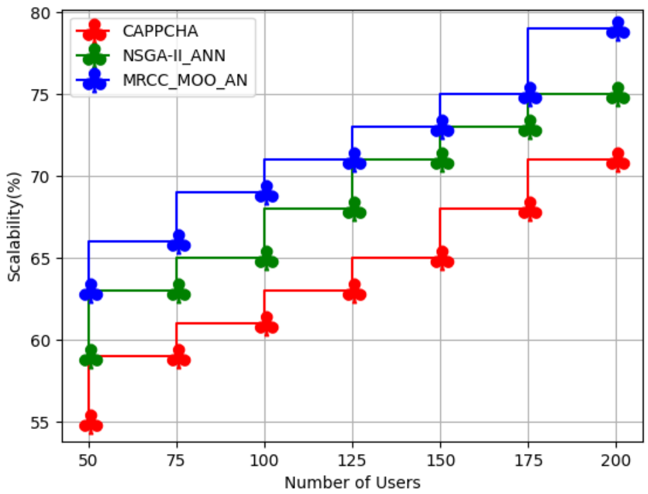

Figure-3 comparative analysis of Scalability

Comparative analyses of the scalability of the proposed technique and the existing technique are shown in the aforementioned table 1 and figure 3. Cloud scalability in CC refers to capacity to increase or decrease IT resources to meet changing demand. Scalability is one of the cloud's unique qualities as well as primary cause of its explosive growth in favour among businesses. By calculating how a system's performance changes in relation to the expansion of input size and the number of processors, its scalability can be examined. One of three goals—preserving a set execution time, utilising all available memory, or maintaining fixed efficiency—can drive the rise of the input size. Relation between multi-tier cloud software service's capacity as well as its usage of cloud resources is described by resource scalability metric function, whereas cloud resources are substituted with costs in the cost scalability metric function.

Table-2 Comparative analysis of QoS

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	45	51	61
75	49	53	63
100	51	55	66
125	53	61	68
150	55	65	69
175	59	68	72
200	61	72	75

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2093
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

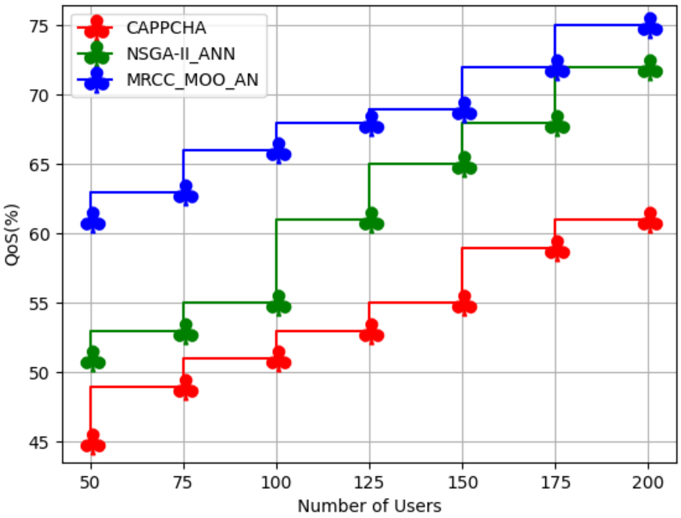

Figure-4 Comparative analysis of QoS

Comparative analysis of proposed and existing techniques in terms of QoS is shown in the aforementioned table-2 and figure-4. QoS is description or measurement of a service's total performance, particularly the performance experienced by network users, whether it be a cloud computing service, a telephony service, or a computer network.

Table- 3 Comparative analysis of Encryption time

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	71	66	61
75	68	63	59
100	65	61	55
125	61	59	52
150	58	55	51
175	55	51	48
200	52	45	42

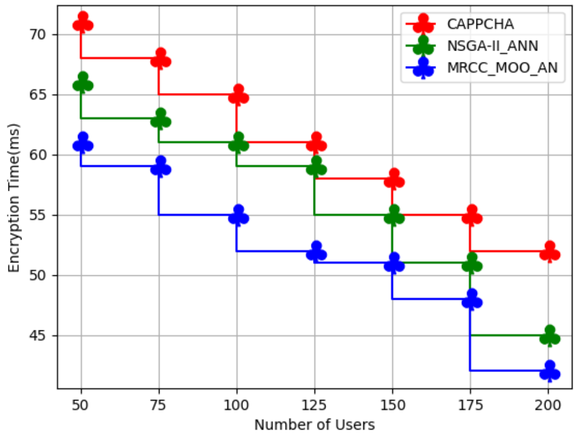

Figure-5 Comparative analysis of encryption time

Table 3 and Figure 5 above provide a comparison of encryption times. Data transformation and encoding before uploading to the cloud is referred to as cloud encryption. Using mathematical methods, this procedure turns plaintext data into unintelligible ciphertext, shielding it from unwanted and potentially dangerous users. In the event that data is lost, stolen, or unintentionally shared, data encryption assures that the contents are essentially useless without the encryption key. Keys are only accessible to authorised users once more.

Table- 4 comparative analysis of Latency

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	77	79	82
75	78	81	85
100	81	83	88
125	83	85	91
150	85	88	93
175	89	89	95
200	91	92	96

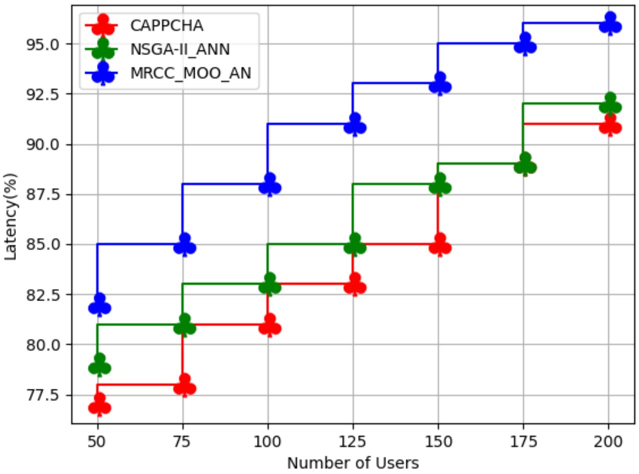

Figure-6 Comparative analysis of Latency

A client request and a cloud service provider's answer are separated in time by the cloud service provider's latency, which is determined from table 4 and figure 6. Device and communication use and enjoyment are significantly impacted by latency. Cloud service communications, which might be particularly susceptible to delay for a number of reasons, can amplify such issues. In other words, the user will have a better experience if the latency and millisecond count are lower and the network is acting more effectively. The bandwidth of a network and connection speed are closely related to latency.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2093
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Table- 5 Comparative analysis of Energy Efficiency

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	65	68	75
75	68	72	79
100	71	75	82
125	73	79	85
150	75	81	89
175	78	83	92
200	81	88	98

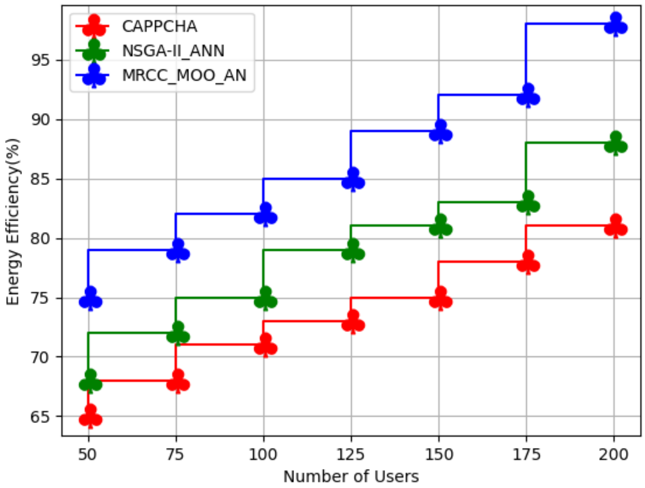

Figure7 Comparative analysis of energy efficiency

Comparative analysis of energy efficiency is shown in Table 5 and Figure 7. It offers a thorough overview of global trends in energy efficiency through study of energy data, legislation, and technological trends. Achieving global climate and sustainability goals and accelerating the transition to sustainable energy depend heavily on energy efficiency.

Table- 6 Comparative analysis of End-End Delay

Number of users	CAPPCHA	NSGA-II_ANN	MRCC_MOO_AN
50	79	71	65
75	75	65	62
100	71	62	59
125	68	61	55
150	65	59	54
175	61	55	51
200	60	52	45

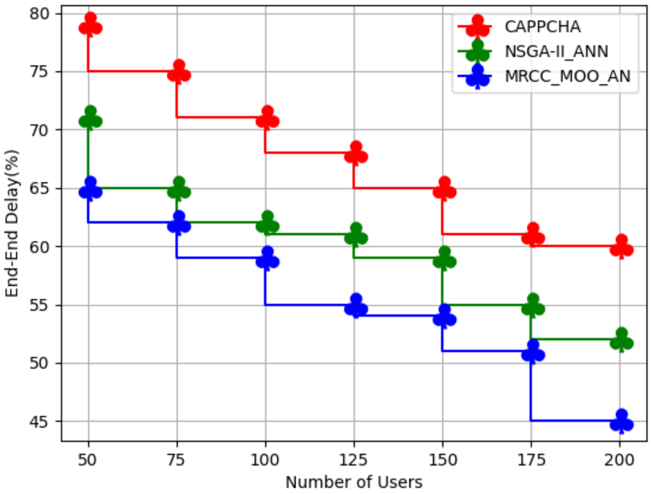

Figure-8 comparative analysis of end-end delay

Comparative examination of proposed analysis's end-to-end delay is provided in aforementioned table 6 and figure 8. When store-and-forward packet switches are employed, the formula for end-to-end delay for sending a single packet of length L over N connections, each with a transmission rate R, is d = N*L/R. the length of time it takes for a packet to get from source to destination across a network. This term, which is frequently used in IP network monitoring, varies from RTT in that it only measures journey from source to destination in a single direction.

5. Conclusion:

This research propose novel technique in multipath routing based energy optimization of autonomous networks. The main goal of this research is to enhance the secure data transmission in cloud computing with network energy optimization. The secure data transmission is carried out using multi-authentication attribute based encryption with multipath routing protocol. Then the network energy has been optimized using multi-objective fuzzy based reinforcement learning. The parameters analysed in terms of scalability of 79%, QoS of 75%, encryption time of 42%, latency of 96%, energy efficiency of 98%, end-end delay of 45%. In order to solve the issue of estimating the junction area, the multipath routing algorithm is utilised to find the greatest number of disconnected pathways in the graph. As a result, an algorithm is described that creates a variety of nonoverlapping and slightly intersecting pathways between any two nodes. Last but not least, the prerequisites for the creation of multipath virtual channels that provide the shortest build-time posts for its parts' parallel transmission. The future scope of this work can be carried out based on

CC BY NC SA

multifactor biometric analysis by cloud computing integrated with machine learning techniques.

Reference:

[1]. Hossen, M. S., Rahman, M. H., Al-Mustanjid, M., Nobin, M. A. S., & Habib, M. A. (2019, December). Enhancing Quality of Service in SDN based on Multi-path Routing Optimization with DFS. In *2019 International Conference on Sustainable Technologies for Industry 4.0 (STI)* (pp. 1-5). IEEE.

[2]. Song, L., Jin, Y., Wang, P., Ma, D., Chen, W., & Cui, L. (2021, September). Multi-path Routing Deployment Method Based on SRv6. In *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* (pp. 723-730). IEEE.

[3]. Govindaraj, M., & Arumugam, S. (2021). A trust-based mechanism in multipath routing using Biogeography-Shun Optimization. *International Journal of Communication Systems*, *34*(6), e4560.

[4]. Ghawy, M. Z., Amran, G. A., AlSalman, H., Ghaleb, E., Khan, J., AL-Bakhrani, A. A., ... & Ullah, S. S. (2022). An Effective Wireless Sensor Network Routing Protocol Based on Particle Swarm Optimization Algorithm. *Wireless Communications and Mobile Computing*, *2022*.

[5]. Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C. (2021). TBSMR: a trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network. *Security and Communication Networks*, *2021*.

[6]. Wang, C., Ren, Z., Cheng, W., & Zhang, H. (2022). CDMR: Effective Computing-Dependent Multi-path Routing Strategies in Satellite and Terrestrial Integrated Networks. *IEEE Transactions on Network Science and Engineering*.

[7]. Hemalatha, R., Umamaheswari, R., & Jothi, S. (2021). LF distribution and equilibrium optimizer based fuzzy logic for multipath routing in MANET. *Wireless Personal Communications*, *120*(2), 1837-1861.

[8]. Alappatt, V., & PM, J. P. (2021). Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E. *Int. J. Comput. Netw. Appl.*, *8*(4), 400.

[9]. Alghamdi, S. A. (2022). Cuckoo energy-efficient load-balancing on-demand multipath routing protocol. *Arabian Journal for Science and Engineering*, *47*(2), 1321-1335.

[10]. Yajun, W., & Liang, Z. (2022). Optimization Algorithm for Multipath Transmission of Distance Education Resources Using Reinforcement Learning. *Mobile Information Systems*, *2022*.

[11]. Chen, L., Hu, B., Guan, Z. H., Zhao, L., & Shen, X. (2021). Multiagent meta-reinforcement learning for adaptive multipath routing optimization. *IEEE Transactions on Neural Networks and Learning Systems*.

[12]. Sumathi, A. C., Javadpour, A., Pinto, P., Sangaiah, A. K., Zhang, W., & Mahmoodi Khaniabadi, S. (2022). NEWTR: a multipath routing for next hop destination in internet of things with artificial recurrent neural network (RNN). *International Journal of Machine Learning and Cybernetics*, 1-21.

[13]. GowriPrakash, R., Shankar, R., & Duraisamy, S. (2021). Resource utilization prediction with multipath traffic routing for congestion-aware VM migration in cloud computing. *Indian Journal of Science and Technology*, *14*(7), 636-651.

[14]. Jha, A., Singh, K. K., Devi, K. V., & Manjula, V. (2021). Reinforcement learning based weighted multipath routing for datacenter networks. *Materials Today: Proceedings*.

[15]. Cai, S., Zhou, F., Zhang, Z., & Meddahi, A. (2021, May). Disaster-resilient service function chain embedding based on multi-path routing. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-7). IEEE.

[16]. Chahlaoui, F., Dahmouni, H., & El Alami, H. (2022, March). Multipath-routing based load-balancing in SDN networks. In *2022 5th Conference on Cloud and Internet of Things (CIoT)* (pp. 180-185). IEEE.

[17]. GOWRIPRAKASH, R., SHANKAR, R., & DURAISAMY, S. (2021). Optimized Load-balancing in Cloud Computing based on Traffic and Workload-aware VM Migration.

[18]. Gowriprakash, R. (2021). A Combined Traffic and Workload-aware Optimized Virtual Machine Migration in Cloud Computing. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 3354-3365.

[19]. Wang, Z. (2021, February). Probabilistic Connectionless Multipath Routing Algorithm for Reliability and Stability Evaluation. In *Journal of Physics: Conference Series* (Vol. 1744, No. 4, p. 042183). IOP Publishing.

[20]. Neenavath, V., & Krishna, B. T. (2022). An energy efficient multipath routing protocol for manet. *Journal of Engineering Research*.

CC BY NC SA