International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212338 Volume 9, Issue 2, March – April (2022)

RESEARCH ARTICLE

Hybrid Optimization-Based Secure Routing Protocol for Cloud Computing

Vatchala B
Department of Computer Science, PRIST Deemed University, Thanjaur, Tamil Nadu, India
vatchala2020@gmail.com

G. Preethi
Department of Computer Science, PRIST Deemed University, Thanjaur, Tamil Nadu, India
mgpreethi@gmail.com

Received: 24 February 2022 / Revised: 22 March 2022 / Accepted: 27 March 2022 / Published: 30 April 2022

Abstract – Cloud Computing (CC) combines the computer paradigm and a shared environment allowing multiple users to access services and resources. In addition to being accessible internationally via the Internet, this ecosystem may be shared at all levels. Resources, infrastructure, and platforms at all levels may be traded with a wide range of customers. Through the Internet, CC enables remote server access. To create cloud environments, CCuses a wide range of already existing technologies, including internet servers, web browsers, and virtualization. These system vulnerabilities can have a significant impact on the cloud as well. The majority of data breaches occur on the way to their final destination. Because of this, the route that data takes must be protected. In this paper, Hybrid Optimization-based Secure Routing Protocol (HOSRP) is proposed to find the best route to destination and provide security to data that passes on it. HOSRP initially clusters the network into different numbers via modified particle swarm optimization strategy and selects the cluster head. HOSRP detects the shorted routes among clusters via firefly optimization strategy to minimize the delay and maximize the delivery ratio of packets. HOSRP applies security to data transmission using the message digest and cryptographic strategy. The performance of HOSRP is analyzed using greencloud simulator with standard performance metrics. Results indicate that HOSRP has better performance in minimizing the delay to save energy consumption and protecting security to the data.

Index Terms – Hybrid, Optimization, Routing, Cloud, Security, Swarm.

1. INTRODUCTION

Cloud Computing (CC) has great potential to benefit and alter the whole IT sector because of its various features. Considerations including service availability, security, and system performance are important considerations for potential cloud customers. Still, according to an IDC Enterprise Panel poll performed in 2008, security is by far the most pressing issue. While CC's security challenges are complicated, they may be explained because CC is implemented on top of established techniques and architectures like SaaS, SOA, and distributed computing[1]. CC would inevitably inherit many of the security flaws introduced by these diverse methodologies and architectural approaches when they are all combined. As a result, as cloud users migrate their apps out of the enterprise/organizational barrier into the open cloud, their trust model will also change. If this is the case, cloud customers may be relinquishing physical access to their data and apps. With no physical boundaries between the cloud and its users' devices, traditional security measures such as firewalls become obsolete in this new context[2], [3].

Users of cloud services must rely significantly on cloud service providers to safeguard them against security breaches. However, CC consumers and cloud service providers are not always from the same trust domain for CC. When cloud service providers and accompanying system, administrators adhere to proper regulations/compliances, they may be denied access to private user data in domains such as healthcare[4].

To fulfil the security needs of individual cloud customers, cloud service providers must deliver security services that match those needs while also complying with legislation. For non-sensitive apps, cloud users' vital data must be protected, and they must verify the cloud's security[5]. For this aim, secure auditing procedures are often required. Because of the multitenancy trait, multiple organizations and trust domains share the same computer resources in CC. A consequence of this is that any purposeful or unintentional misbehavior on the part of a single cloud user puts other co-residents in danger and opens the door to additional Internet-based hostile attacks[6], [7].

Essentially, the cloud is a location where information may be exchanged through satellite networks. The hosting company's responsibility is to manage the enormous data centres that offer security, storage capacity, and processing power required to keep all of the information customers submit to the cloud. Google Drive, Apple iCloud, Amazon Web

RESEARCH ARTICLE

Services, and Microsoft Azure are some of the most well-known cloud hosting providers, but many more are both big and small. As a result, these hosting businesses may hold the rights to utilize their cloud and transfer files on their servers while also providing customers with an infrastructure to connect between devices and applications.

Security in the cloud refers to measures taken to ensure that the data, apps, and infrastructure housed within are safe from intrusion. Software, hardware and storage may all be delivered via the Internet in the form of a cloud-based service. When it comes to CC, it's almost universally used by enterprises of all sizes because of the advantages of flexibility, quick deployment, scalability and minimal up-front expenses. Routing is transferring a data packet from one location to another in a network.

Routing concepts may be used for a wide range of networks, including circuit-switched and network connectivity. A router is a specialized device that is often used to carry out routing tasks. To go from one point to another, packets of Internet Protocol (IP) pass across the network through the router. Routing tables, which keep track of the routes to multiple network destinations, are often used to guide forwarding by routers. Train passengers check the schedule to choose which train to board while looking at a routing table. Routing tables are similar to railway schedules. However, they are used for network routes instead of trains. They may be defined by an administrator or learnt from network traffic by using routing protocols to build these tables.

1.1. Problem Statement

The ease of data exchange between intelligent devices may wander the Internet. CC networks do not need any external infrastructure. Protocols for discovering routes between nodes that may move and are randomly located are crucial in CCs. Routing protocols are the backbone of CCs, making design research difficult. CCs have far more capacity, mobility, and node power than conventional networks, breaking connections and increasing packet loss ratio. Routine route-finding and maintenance waste electricity and time. CCs have massive control message exchanges between mobile nodes. Several academics have studied alternative topologies to minimize latency, energy consumption, routing overhead, and service quality.

1.2. Objective

The significant objective of HOSRP is to find the best path by performing clustering in the cloud network and finding the shortest route to minimize the delay and energy consumption. For performing clustering and finding the best route, HOSRP utilizes bio-inspired strategies. The data that travels in the best route is protected using message digest cum cryptographic techniques.

1.3. Organization of the Paper

The current section of the article has provided information about CC and issues in CC. Also, it has discussed the statement of problem regarding the research and objective of the research. Section 2 reviews the literatures related to the current research work. Section 3 proposes the protocol for routing the data in CC. Section 4 illustrates the simulator. Section 5 discusses the simulation setting and metrics used to measure the performance. Section 6 provides the discussion about the results obtained from the simulation. Section 7 concludes the research with future work.

2. LITERATURE REVIEW

"Efficient and Secure Trusted Routing Mechanism" [8]is proposed for secure and efficient routing from one node to another if the path adopted fails in delivering the message to the node at the destination. The malware activities, namely, botnet size, bot distribution, and membership recruitment for patterns, were handled for defined networks to route its data.

"Securing Data based Multipath Routing" [9] is proposed to enable multipath routing for efficient data transmission in an ad-hoc network. Security for the message is provided by splitting the data, which are encrypted and fused to transmit data in disjoint paths that already exist. The probability is measured for reconstituting the original data. "Spatial and Energy-Aware Trusted Dynamic Distance Source Routing" [10]is proposed for enhancing network lifetime in Wireless Sensor Network. The efficiency, energy level, and spatial data were measured using Quality of Service. Also, performance metrics are innovated to evaluate the data size, energy usage and speed of data communication. Time for the sliding window is also enhanced to detect the attackers, and Network Simulator-2 is used for evaluation. "Ad-hoc Monitoring Routing Protocol" [11]is proposed for constructing MANET using network-based functionalities: security, network monitoring, resource management, routing, and security. The quality of link and connectivity are designed with a routing process for defining the topologies with IPv6 and IPv4 addressing. Integration of the techniques was unified for supporting the mobile nodes. "Enhanced Energy Efficient-Secure Routing protocol" [12]is proposed for accessing the data protected in the network for transmission. Nodes are selected, and the routing path is fetched based on the energy threshold to forward the packets in the ad-hoc network. The neighbor nodes are chosen to enforce the security policy to avoid end-to-end delay and packet loss in the network.

"Intellectual and Secure Edge-Enabled Computing" [13] is proposed for building the strategy for communication by the transmission of data for energy and data management in the network. A chaining strategy with distributed hashing is presented for an efficient computing system. The optimal features are fetched using data routing in deep learning for

RESEARCH ARTICLE

training and routes are predicted over servers at the edges. "Secure Load Balanced Routing" [14]is proposed for clustering in WSN. Metric called trust-based security handles the wavering state from good to bad for load balancing. Better packet transmission, energy efficiency and security were achieved and evaluated using Exponential Cat Swarm Optimization. "Moth-Flame Optimization for Secured Communication" [15] is proposed for optimizing the process of routing in Low-power and lossy Networks. The Moth-Flame technique is used for detecting rank attacks for avoiding the malicious nodes in the network. The rank attack detection is enabled, and the petal technique is employed to select the nodes at the next hop and from the source node. "Delay Tolerant Networks" [16]is analyzed for security concerns in the proposed study. Message forwarding is enabled in DTN in which connectivity loss is detected. The integrity of the transmitted message is validated, and appropriate nodes are forwarded. Overhead ratio, delivery ratio and delay of delivering the data were enhanced based on its routing strategies. "Taylor grounded Cat Salp Swarm Algorithm" [17] is proposed for enabling the multi-hop routing in WSN. Low Energy Adaptive Clustering Hierarchy algorithm is used for selecting the cluster heads. The nodes at the sensor are selected for transmitting data through the base station and optimal hop. The trust model is built with integrity, direct, indirect, and data forwarding rate.

"Cost Optimization-based Mathematical Framework" [18]is proposed to minimize the cost and maximize the reliability in Software-Defined Networks. The optimal number of devices are determined using the NSGA–II technique. The cost for technique is minimized, and security issues, namely packet removal and change, analysis of traffic, erroneous routing, and network downtime, were handled. "Secure-Intrusion Detection System" [19]is proposed for MANET in the wireless network. Data is received for consistency, and the framework is built to detect the security issue using the Secure Energy Routing protocol. The attacks are detected, and distorted node in the network is sensed using a simulator. "Sequence Number based Secure Routing" [20]is proposed to detect the structure of the packet. The node availability, resource availability and communication among nodes were identified based on proactive and reactive routing. The packet's delivery ratio is enhanced, and the network's lifetime is improved. "Ontological Security Frameworks" [21]is proposed for drawing the method and structure of the placement based on landscape, displacement and migration. The sense of time-space and routine loss was drawn, and the framework built a security and attachment theory model. Spatial routinization was detected with the method of routinization.

"Finite-State Chaotic Compressed Sensing (FSCCS)"[22]proposed for secure data transmission in the cloud. It aims to reduce the amount of data transmitted and improve the security of that data (i.e., routing). By combining global and local information, the detected data similarity got reduced in sensed data. Even though the similarity level reduced but it creates the networking congestion while the data passes in cloud. For DevSecOps inter-cloud adoption, "Conceptual Security Model (CSM)"[23]is proposed. As a result, CSM focuses on integrating security service apps so that open-source software consumers don't experience long delays when using it. Security, routing, and user operations are integrated into a single system. Major focus of CSM is on security where it minorly focuses on routing to send data. To improve the security of the cloud network, "Lightweight Cryptography (LC)"[24] was developed. The design of LC is based on the amount of time it takes to compute the key used for providing security (i.e., encryption and decryption), (ii) statistics and (iii) entropy.LC too focuses on providing security and not yet focused on routing.

From the above discussed literatures, it was identified the need for common algorithm which focuses on finding the best route and also to provide security while data gets transmitted in the cloud.

3. HYBRID OPTIMIZATION-BASED SECURE ROUTING PROTOCOL

3.1. Node Clustering

Clustering in CC consists of nodes in the range of clusters and selection of the Cluster Head (CH) using a modified PSO technique. The CH will move the data fused by communicating with the cloud server. The selection of CH plays a significant role in the CC network. The model for node energy usage in CC network is illustrated as follows:

Energy usage during transmission of data is mathematically expressed in Eqn.(1).

$$\varepsilon_S = (\alpha_1 + \alpha_2 E^{\gamma})N \quad (1)$$

Energy usage while receiving the data is mathematically expressed in Eqn.(2).

$$\varepsilon_R = \alpha_3 N \quad (2)$$

Energy usage while reaching an idle state is mathematically expressed in Eqn.(3).

$$\varepsilon_I = (\alpha_4 I_s) Q(N) \quad (3)$$

From Eqns.(1)-(3), E represents the distance for transmission, γ refers to exponent for path loss, N denotes the size of the message, I_s refers to idle time, α_1 and α_2 are the parameters that are system dependent,and$Q(N)$ refers to the cloud processing rate for the message.

RESEARCH ARTICLE

Secured clusters are created using different variables for a cloud node using the PSO algorithm. The algorithm is a computational optimization method that is bio-inspired naturally for finding the best optimal solution. At first, the system initializes the random solutions via searching, and the solutions are generated at every iteration, and these solutions are known as a particle. Each particle in the PSO preserves the record for all its subordinates to retrieve the best optimum solution. Also, the value of fitness is measured, which is stored as its best optimum solution and is denoted as $Qbest$. The best value called $Fbest$is chosen as the solution from the generated population and calculated as a neighbor. The particle's velocity is measured using random parameters, and it is fetched utilizing the amount of velocity based on $Qbest$. The fitness value of the individual is replaced and updated with its candidate by comparing with the fitness of other cloud nodes using Eqn.(4) and Eqn.(5).

$$v(s+1) = v(s) + C_1 \times r() \times \left(y_{qbest} - y(s)\right) + C_2 \times r() \times \left(y_{fbest} - y(s)\right) \quad (4)$$

$$y(s+1) = y(s) + v(s+1) \quad (5)$$

Here, every particle's velocity and vector position are denoted as $y(s)$and $v(s)$ for time s. The rate of social and self-learning is represented using B_1 and B_2. The replacement of global fitness is performed using a new fitness value called,y_{Fbest}, i.e., when the new fitness value is better than the global fitness value. The formulation of the fitness function is performed using Eqn.(6).

$$G = U_1 \times M_e + U_2 \times M_{RD} + U_3 \times E_{ij} + U_4 \times M_{SV} \quad (6)$$

Here, the node degree is M_e, residual-node energy is M_{RD}, the distance among node i to j is E_{ij}, and the node's trust value is M_{SV}. U_1 denotes the weight values, U_2, U_3 andU_4, where $U_1 + U_2 + U_3 + U_4 = 1$. When a cluster is ready to transmit the data to the next cluster after the CH is fixed using PSO, the sink node carries the same procedure. Algorithm 1 provides the pseudocode of performing clustering with modified PSO.

1. Begin
2. Sink node sends "Hello" message.
3. Identify $Qbest$ and $Fbest$ for all particles
4. For all particle
5. Add location and velocity using Eq.(4) and Eq.(5)
6. Calculate the position of nodes with neighbor nodes
7. Compute individual particle fitness
8. Update $Qbest$ and $Fbest$
9. If count of iteration attains maximum value, then
10. Select that specific particle value as best particle
11. $Else$
12. Increment particle count by 1
13. $End\ If$
14. $End\ for$
15. End

Algorithm 1 Clustering with Modified PSO

3.2. Safe Routing

Here, the safe routing for selection is performed using three different operations: encryption of data, detection of the shortest path, and data integrity.

3.3. Encryption of Data

Here, the message block is segregated into two different sub-blocks where encryption is performed at the first block using the AES algorithm, and RC-6 is used in the second block for encryption.

The plain text is segregated into two blocks in the encryption procedure, and every block holds 128 bits. Suppose M is non-integer number and a fraction, then it is categorized into two parts $q_i[0: M/2-1]$ and $q_i[M/2 : M-1]$blocks. The first $M/2$blocks are encrypted with key Lgenerated by AES with 128 bits and length K.

Using the encryption procedure, the standard text is segregated into two main blocks in which each block holds 128 bits, namely, $q_i[0: M/2-1]$ and$q_i[M/2 : M-1]$. Here, the value of M is a non-integer value and holds a fraction. Encryption of the first $M/2$ blocks is performed using L keys generated with 128-bit size and length K using the AES algorithm.

$$q_i = \sum_{j=0}^{j=\frac{m}{2}-1} C_j \; 0 \le i \le m/2-1 \quad (7)$$

$$B_i = d_{AES}(L, C_j) \quad (8)$$

Here, the input ciphers are denoted using C_j based on the secret keys of AES, and the function of encryption is represented using d_{AES}. Also, the encryption of message blocks of $q_i[M/2 : M-1]$ is carried out using the RC6 algorithm. The security level is increased using the RC6 algorithm, and the execution time is stable. It works four times faster for the encryption and decryption process, and it is expressed as Eqn.(9) and Eqn.(10).

RESEARCH ARTICLE

$$q_i = \sum_{i=m/2}^{i=m-1} C_i \; m/2 \le j \le m-1 \quad (9)$$

$$C_i = d_{RC6}(L, C_i) \quad (10)$$

Based on the process, two ciphertexts were produced.

3.4. Detection of the Shortest Path

Multi-hop-based improved firefly algorithm detects the shortest path for data transmission. Using multi-hop and intra-cluster communication, data were transmitted using CH. Firefly algorithm is generally a bio-inspired technique required to search the problem. The enhanced firefly algorithm coded routing using a novel fitness function using node degree, distance, and residual energy to the sink node from the sensor node. The behavior of firefly is detected using the brightness and intensity value: every firefly, $GG_i \forall_i, 1 \le j \le M_{gg}$ has the position of $y_{i,e}$.Here, i denote the intensity of the firefly and its dimension. In detecting the shortest path, every firefly represents the forwarding of data to the sink node from every cluster using relay CH. Every brighter firefly catches the brighter one, which is measured using Eqn.(11).

$$Y_i = Y_i + \beta_0 d^{-\gamma r_{i,j}^2}(y_j - y_i) + \alpha\left(R - \frac{1}{2}\right) \quad (11)$$

Here, $\alpha \epsilon (0,1)$and β were the randomized parameters, and the variable $R$is random. The ith position of the firefly is represented using y_i, and jth position of the firefly is y_j. The main aim of the enhanced firefly algorithm is to fetch the finest route from the CH. Instead of measuring the distance among i and another key, the radius is computed using Eqn.(12)

$$r_{ibest} = \sqrt{(y_i - y_{fbest})^2} \quad (12)$$

Here, y_{fbest} refers to the restoration for y_j that provides a better factor for scaling.

For achieving the lesser fitness solution than the traditional firefly algorithm, the appended size is generated in which the step size of first-order $\Delta_{1i,j}$ is smaller than the step size of the second one,$\Delta r_{2i,j}$.Normal distribution (R_m) is used instead of random distribution (R) to diversify the search area,and it is expressed as Eqn.(13).

$$Y_i = Y_i + \beta_0 d^{-\gamma r_{i,j}^2}(y_j - y_i) + \alpha\left(R_m - \frac{1}{2}\right) \quad (13)$$

In every optimization algorithm based on population, the convergence for pre-mature local minima is a problem. There is no proper exploitation and exploration in a traditional firefly algorithm, and to eradicate the issue, a value called A is used at the time s.

$$A = 3 * a * R - a \quad (14)$$

$$a = 2 - iteration * \left((2)/\ Max\_Generation\right) \quad (15)$$

$$\alpha = abs(best - y_i^s) \quad (16)$$

$$y_i^s = best - A * \alpha \quad (17)$$

3.5. Integrity of Data

At every BH, data integrity is validated using Message Digest – 5 algorithms where the hash value for every node is provided. These hash values are then passed to the node at the sink, and raw data is received at the sink node. It applies two different ciphertexts, namely, $b_i$and b. The best performance for the hash function with security keys was obtained using Eqn.(18) and Eqn.(19).

$$E_i = MD5(b_i) \quad (18)$$

$$e_i = MD5(B_i) \quad (19)$$

Two different ciphertext blocks are generated with m blocks and are forwarded to the node at the sink. The hash value for E_i and e_i are then sent with 128 bits to the sink node using Eqn.(20) and Eqn.(21).

$$D = B_i + b_i \quad (20)$$

$$H = e_i + E_i \quad (21)$$

3.6. Validation of Security at the Sink Node

For static deployment of environment for sensor node, the security is not static and is dynamic. Security validation is used with fuzzy logic to present the information with varied membership degrees. The value of membership in FIS for every element lies between 0 and 1, termed membership degree. Here, 1 represents the high-security value, and 0 represents the low security, whereas the values range 0 and 1 represent the intermediate level of security. Therefore, the dimension of membership for 0 and 1 represent the node's presence and absence in the network. Figure 1 provides the Framework of HOSRP.

RESEARCH ARTICLE

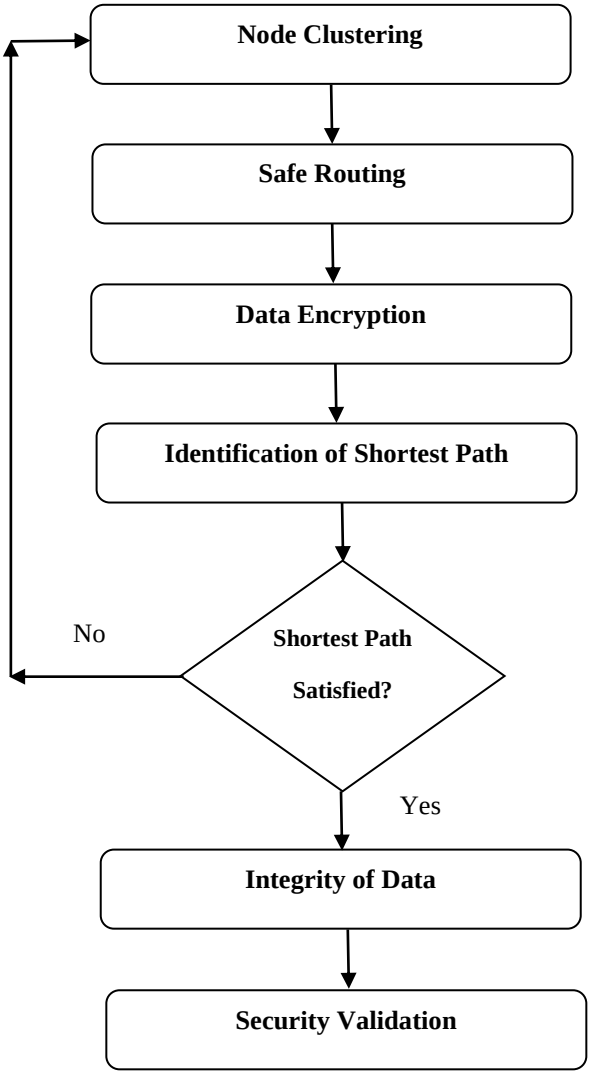

Figure 1 HOSRP Framework

4. ABOUT SIMULATOR

CloudSim is a free simulation tool that enables cloud application developers to test their outcomes iteratively. It helps reduce congestion before real-time deployment (i.e., bottlenecks). Cloudsim is a technology-oriented cloud scenario modelling programme. That is, it runs an environment model in hardware, not actual software.

The management rules for different system components, including planning and provisioning, are all covered in the core classes of this document. Using these factors, evaluating new cloud-based techniques is simple. Cost and deployment time may also be considered when evaluating a method's competency. Cloudsim completely supports green IT policy review. It may provide additional features and load balancing to a cloud system.

5. SIMULATION SETTING AND PERFORMANCE METRICS

Standard computer network performance metrics [25]–[32] is utilized to measure the performance of HOSRP. Cloudsim Simulator[33], [34] is used in this research to evaluate the performance of EACOSR against the current routing protocols. Additionally, this research work uses the Avalanche Effect performance metric to measure security performance. Table 1 lists the simulation parameters utilized in the assessment.

Table 1 Simulation Setting

Parameters	Values
Bandwidth Capacity of Cloudlet	12500
Cloudlet Count	200-1000
Cloudlet Length	1000
CPU Count	3
Data Center Count	3
Host Count	3
Initial Energy of Cloudlet	15 Joule
Packet Size	512 KB
RAM Capacity of Cloudlet	8192 MB
Storage Capacity of Cloudlet	40960 MB
Total Simulation Time	100 sec
User Count	15
VM Bandwidth	2048 MB
VM Count	20
VM Operating System	Linux
VM RAM	1024 MB
VM Size	10240 MB

6. RESULTS AND DISCUSSION

6.1. Throughput Analysis

Figure 2 discusses the throughput performance of routing protocols with a different number of cloudlets ranging from 200 to 1000. Figure 3 showcases the average throughput attained by the proposed routing protocol (HOSRP) and existing protocol (FSCCS, CSM and LC). From Figure 2 and Figure 3 it is evident that HOSRP has attained better throughput than existing routing protocols. It is because of finding the optimized cum stable route to the destination that does not face any routing issues. Existing routing protocols

RESEARCH ARTICLE

attempt to seek route without checking its stability and quality, resulting in poor route selection and route failure. PSO plays a significant role in HOSRP in finding the better path. The result values of Figure 3 is given in Table 2 for better understanding.

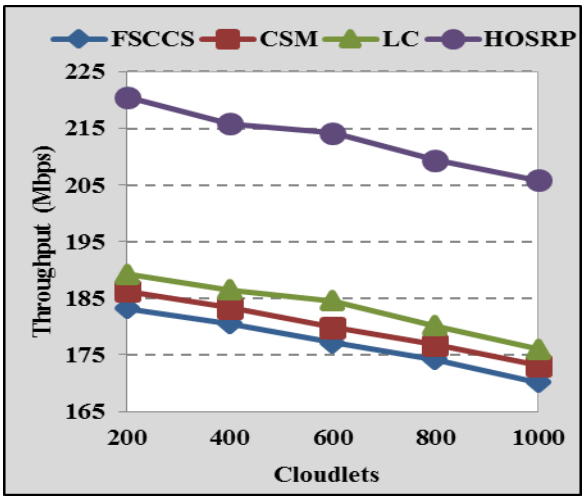

Figure 2 Throughput

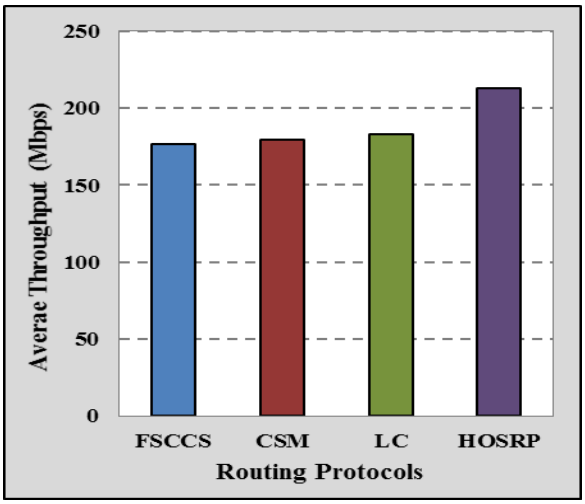

Figure 3 Average Throughput

Table 2 Average Throughput

Routing Protocols	Average Throughput (Mbps)
FSCCS	177.019
CSM	179.843
LC	183.279
HOSRP	213.155

6.2. Packet Delivery Ratio Analysis

Figure 4 highlights the average packet delivery ratio attained by the proposed routing protocol (HOSRP) and existing protocol (FSCCS, CSM and LC). Figure 5 discusses routing protocols' packet delivery ratio performance with a different number of cloudlets ranging from 200 to 1000. From Figure 4 and Figure 5, it is clear for an understanding that HOSRP outperforms FSCCS, CSM and LC in terms of delivering packets to the destination. The clustering strategy followed in HOSRP leads to identifying the trusted nodes and stable route to the destination, leading to increased packet delivery ratio than other FSCCS, CSM and LC that focuses on identifying the route in short duration rather than selecting the trusted cum stable route to the destination. It is also to be noted that the performance of HOSRP gets lowered when the count of cloudlets increases, but it comparatively gives better performance than other routing protocols. The result values of Figure 5 are given in Table 3 for better understanding.

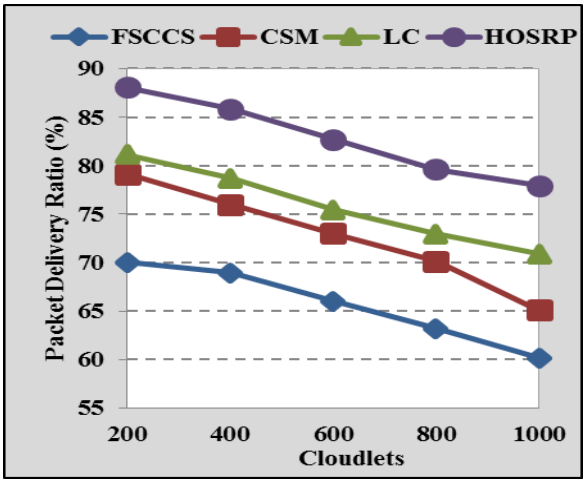

Figure 4 Packet Delivery Ratio

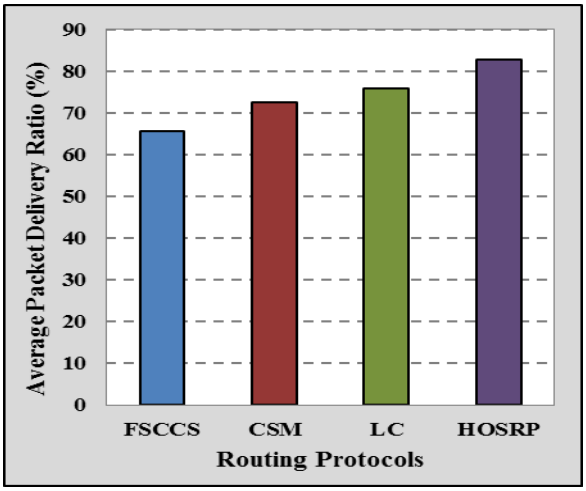

Figure 5 Average Packet Delivery Ratio

RESEARCH ARTICLE

Table 3 Average Packet Delivery Ratio

Routing Protocols	Average Packet Delivery Ratio (%)
FSCCS	65.659
CSM	72.682
LC	75.820
HOSRP	82.846

6.3. Packet Drop Ratio Analysis

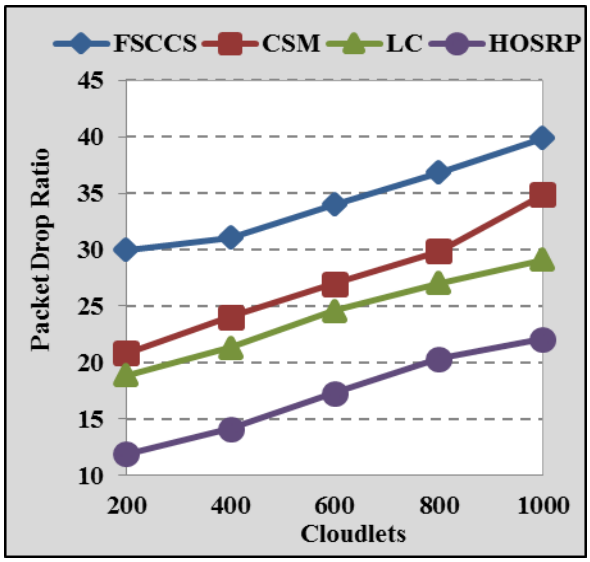

Figure 6 Packet Drop Ratio

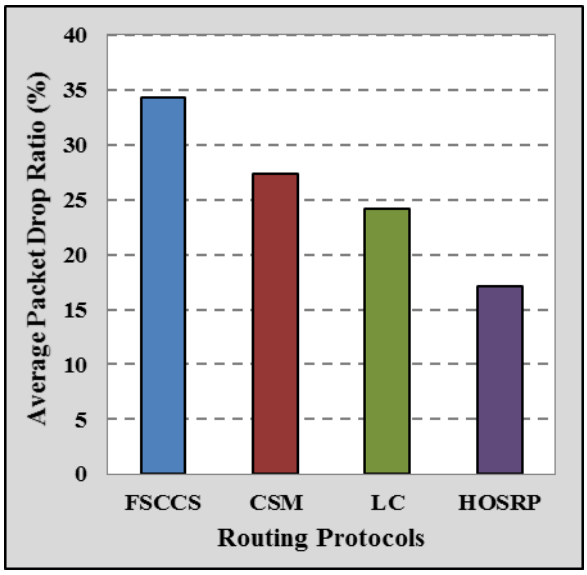

Figure 7 Average Packet Drop Ratio

Figure 6 discusses routing protocols' packet drop ratio performance with a different number of cloudlets ranging from 200 to 1000. Figure 7 demonstrates the average packet drop ratio of the proposed routing protocol (HOSRP) and existing protocol (FSCCS, CSM and LC). From Figure 5, it is possible to understand that the packet drop ratio of all protocols increases with the increase of cloudlets. It is to be noted from Figure 6 and Figure 7 that HOSRP outperforms FSCCS, CSM and LC in terms of meagre packet drop ratio. Detection of shortest route cum stable route is the specific reason HOSRP gets a meager packet drop ratio. The existing routing protocols select the route without checking the distance and quality of the route. The result values of Figure 7 are given in Table 4 for better understanding.

Table 4 Average Packet Drop Ratio

Routing Protocols	Average Packet Drop Ratio (%)
FSCCS	34.341
CSM	27.318
LC	24.180
HOSRP	17.154

6.4. Delay Analysis

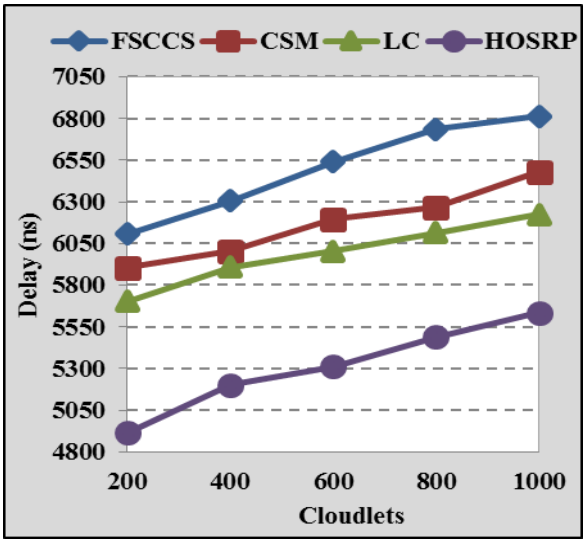

Figure 8 Delay

Figure 8 compares the delay faced by the proposed routing protocol HOSRP against the existing routing protocols (FSCCS, CSM and LC). Figure 9 compares the average delay faced by HOSRP and existing routing protocols. From Figure 9, it is evident that the delay of all routing protocols gets

RESEARCH ARTICLE

increased when the count of cloudlets increases, but when comparatively HOSRP faces a minimum delay than the considered existing routing protocols. The main intention of HOSRP is to securely deliver the data packet to the destination, where it focuses on avoiding congestion. The routes identified by existing routing protocols face more congestion due to poor quality routes that lead to more delay. HOSRP selects the best route in an optimized manner focusing on its quality and avoiding congestion and reduced delay. The result values of Figure 9 are given in Table 5 for better understanding.

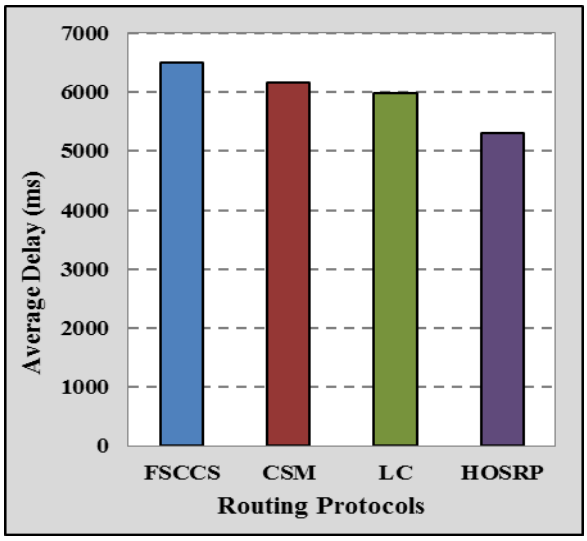

Figure 9 Average Delay

Table 5 Average Delay

Routing Protocols	Average Delay (ms)
FSCCS	6499.2
CSM	6169.6
LC	5989.8
HOSRP	5309.4

6.5. Energy Consumption Analysis

Energy Consumption Analysis is demonstrated in Figure 10 and Figure 11. In Figure 9, HOSRP proves that it consumed a low energy level to deliver the data packet to the destination over simulation duration. Consumption of energy to deliver the packet to the destination drastically increases when the count of cloudlets increases. Figure 11 compares the average energy consumption of HOSRP and existing routing protocols (FSCCS, CSM and LC). Finding the minimum distance cum optimized route is the root cause for consuming low energy by HOSRP. The significant reason for consuming more energy to deliver the packet to the destination by existing routing protocols is the selection for the poor-quality route, non-avoidance of congestion and multiple retransmissions of data packets. The result values of Figure 11 are given in Table 6 for better understanding.

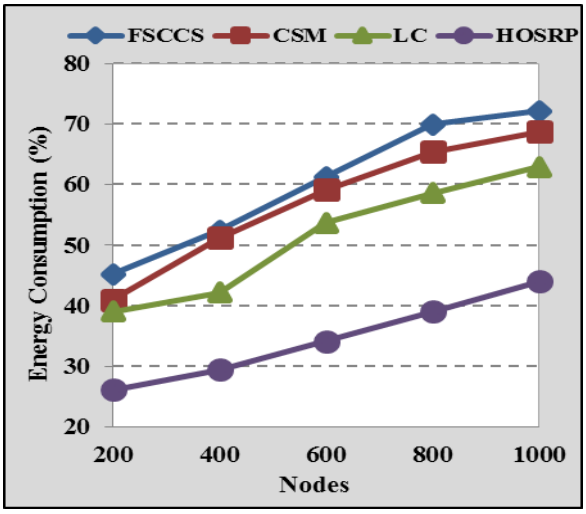

Figure 10 Energy Consumption

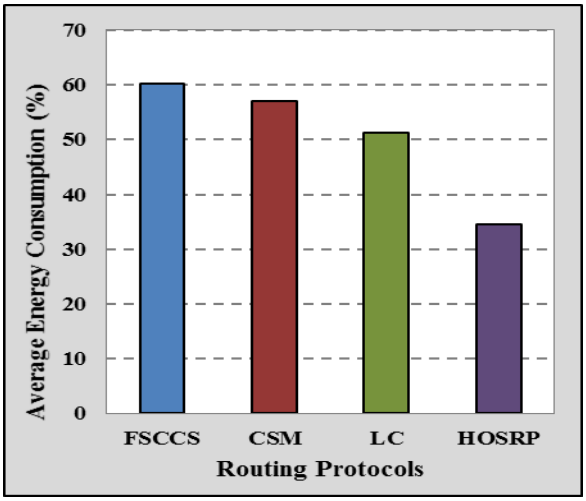

Figure 11 Average Energy Consumption

Table 6 Average Energy Consumption

Routing Protocols	Average Energy Consumption (%)
FSCCS	60.151
CSM	57.073
LC	51.256
HOSRP	34.527

RESEARCH ARTICLE

6.6. Avalanche Effect Analysis

Figure 12 illustrates the avalanche effect of the proposed routing protocol HOSRP against existing routing protocols (FSCCS, CSM and LC). From Figure 12, it is likely to understand that HOSRP has a better avalanche effect than the current protocols. HOSRP provides security via message-digest algorithm and cryptographic techniques. Also, it is to be noted that the performance of CSM is lower than LC in all other considered performance metrics, but in the avalanche effect metric, it has better performance than LC in terms of providing security. The result values of Figure 12 are given in Table 7 for better understanding.

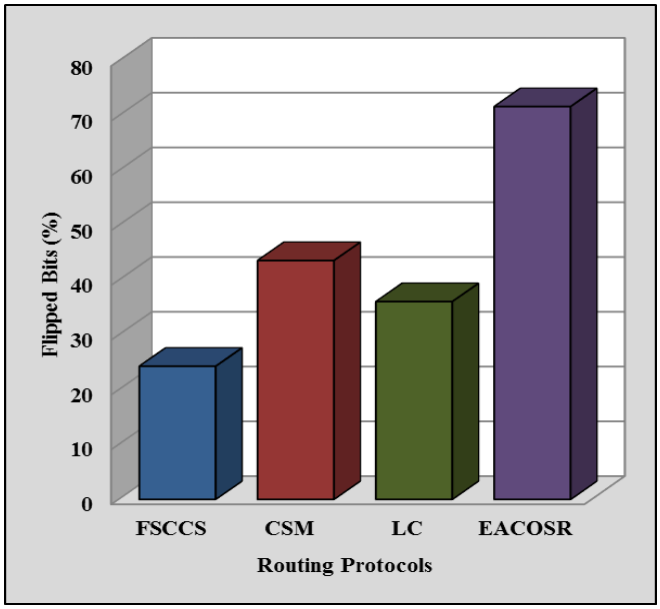

Figure 12 Avalanche Effect

Table 7 Average Avalanche Effect

Routing Protocols	Average Avalanche Effect (%)
FSCCS	24.3
CSM	43.6
LC	36.1
HOSRP	71.7

7. CONCLUSION

This paper has proposed a Hybrid Optimization-based Secure Routing Protocol (HOSRP) to find the best route in a cloud network to reach data to destination with reduced delay and increased security. HOSRP performs clustering before finding the best route. For clustering, a modified version of particle swarm optimization is used and to find the best cum shortest route, HOSRP utilizes modified reliable firefly optimization. Security for the data is provided using message digest cum cryptographic techniques. Performance of HOSRP is analyzed in Green Cloud simulator with standard performance metrics. HOSRP is faster and uses less energy than any previously used techniques. In HOSRP, the avalanche effect is 71.7%, demonstrating the efficiency of data transport security. In the future, improved bio-inspired based ideas may be applied to improve routing and security.

REFERENCES

[1] R. Yarinezhad et al., “An energy efficient cluster head selection approach for performance improvement in network-coding-based wireless sensor networks with multiple sinks,” Ad Hoc Networks, vol. 64, pp. 514–526, Apr. 2021, doi: https://doi.org/10.1016/j.future.2018.12.024.

[2] H. Han, S. Shakkottai, C. V Hollot, R. Srikant, and D. Towsley, “Multi-Path TCP: A Joint Congestion Control and Routing Scheme to Exploit Path Diversity in the Internet,” IEEE/ACM Trans. Netw., vol. 14, no. 6, pp. 1260–1271, 2006, doi: 10.1109/TNET.2006.886738.

[3] O. Samuel, N. Javaid, T. A. Alghamdi, and N. Kumar, “Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence,” Sustain. Cities Soc., vol. 76, p. 103371, 2022, doi: https://doi.org/10.1016/j.scs.2021.103371.

[4] M. Ganesan and N. Sivakumar, “IoT based heart disease prediction and diagnosis model for healthcare using machine learning models,” in 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 2019, pp. 1–5, doi: 10.1109/ICSCAN.2019.8878850.

[5] S. Luo, G. Zhang, C. Wu, S. U. Khan, and K. Li, “Boafft: Distributed Deduplication for Big Data Storage in the Cloud,” IEEE Trans. Cloud Comput., vol. 8, no. 4, pp. 1199–1211, 2020, doi: 10.1109/TCC.2015.2511752.

[6] I. Bolodurina and D. Parfenov, “Comprehensive approach for optimization traffic routing and using network resources in a virtual data center,” Procedia Comput. Sci., vol. 136, pp. 62–71, 2018, doi: https://doi.org/10.1016/j.procs.2018.08.238.

[7] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare,” Futur. Gener. Comput. Syst., vol. 78, pp. 659–676, 2018, doi: https://doi.org/10.1016/j.future.2017.04.036.

[8] A. S. Alqahtani, “Security threats and countermeasures in software defined network using efficient and secure trusted routing mechanism,” Comput. Commun., vol. 153, pp. 336–341, 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.020.

[9] J. Ben Othman and L. Mokdad, “Enhancing data security in ad hoc networks based on multipath routing,” J. Parallel Distrib. Comput., vol. 70, no. 3, pp. 309–316, 2010, doi: https://doi.org/10.1016/j.jpdc.2009.02.010.

[10] V. Mythili, A. Suresh, M. M. Devasagayam, and R. Dhanasekaran, “SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks,” Cogn. Syst. Res., vol. 58, pp. 143–155, 2019, doi: https://doi.org/10.1016/j.cogsys.2019.02.005.

[11] G. C. Hadjichristofi, L. A. DaSilva, S. F. Midkiff, U. Lee, and W. De Sousa, “Routing, security, resource management, and monitoring in ad hoc networks: Implementation and integration,” Comput. Networks, vol. 55, no. 1, pp. 282–299, 2011, doi: https://doi.org/10.1016/j.comnet.2010.09.001.

[12] R. Prasad P and Shivashankar, “ENHANCED ENERGY EFFICIENT SECURE ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORK,” Glob. Transitions Proc., 2021, doi:

RESEARCH ARTICLE

https://doi.org/10.1016/j.gltp.2021.10.001.
[13] K. Haseeb, I. Ud Din, A. Almogren, I. Ahmed, and M. Guizani, "Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things," Sustain. Cities Soc., vol. 68, p. 102779, 2021, doi: https://doi.org/10.1016/j.scs.2021.102779.
[14] G. Thahniyath and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor networks," J. King Saud Univ. - Comput. Inf. Sci., 2020, doi: https://doi.org/10.1016/j.jksuci.2020.10.012.
[15] A. Seyfollahi, M. Moodi, and A. Ghaffari, "MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications," Comput. Stand. Interfaces, vol. 82, p. 103622, 2022, doi: https://doi.org/10.1016/j.csi.2022.103622.
[16] C. C. Sobin, C. Labeeba, and K. Deepika Chandran, "An Efficient method for Secure Routing in Delay Tolerant Networks," Procedia Comput. Sci., vol. 143, pp. 820–826, 2018, doi: https://doi.org/10.1016/j.procs.2018.10.384.
[17] A. Vinitha, M. S. S. Rukmini, and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm," J. King Saud Univ. - Comput. Inf. Sci., 2019, doi: https://doi.org/10.1016/j.jksuci.2019.11.009.
[18] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, G. Srivastava, S. Mohan, and A. M. Rababah, "Cost optimization of secure routing with untrusted devices in software defined networking," J. Parallel Distrib. Comput., vol. 143, pp. 36–46, 2020, doi: https://doi.org/10.1016/j.jpdc.2020.03.021.
[19] R. Prasad and S. shankar, "Secure Intrusion Detection System Routing Protocol for Mobile Ad-Hoc Network," Glob. Transitions Proc., 2021, doi: https://doi.org/10.1016/j.gltp.2021.10.003.
[20] D. Kothandaraman, S. Naik Korra, A. Balasundaram, and S. Magesh Kumar, "Sequence number based secure routing algorithm for IoT networks," Mater. Today Proc., 2021, doi: https://doi.org/10.1016/j.matpr.2020.11.703.
[21] H. Helly, E. Efrat, and J. Yosef, "Spatial routinization and a 'secure base' in displacement processes: Understanding place attachment through the security-exploratory cycle and urban ontological security frameworks," J. Environ. Psychol., vol. 75, p. 101612, 2021, doi: https://doi.org/10.1016/j.jenvp.2021.101612.
[22] Z. Liu, L. Wang, X. Wang, X. Shen, and L. Li, "Secure Remote Sensing Image Registration Based on Compressed Sensing in Cloud Setting," IEEE Access, vol. 7, pp. 36516–36526, 2019, doi: 10.1109/ACCESS.2019.2903826.
[23] R. Kumar and R. Goyal, "Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC)," Comput. Secur., vol. 97, p. 101967, 2020, doi: https://doi.org/10.1016/j.cose.2020.101967.
[24] F. Thabit, P. S. Alhomdy, and P. S. Jagtap, "Security Analysis and Performance Evaluation of a New Lightweight Cryptographic Algorithm for Cloud Computing Environment," Glob. Transitions Proc., 2021, doi: https://doi.org/10.1016/j.gltp.2021.01.014.
[25] J. Ramkumar and R. Vadivel, "Meticulous elephant herding optimization based protocol for detecting intrusions in cognitive radio ad hoc networks," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 8, pp. 4549–4554, 2020, doi: 10.30534/ijeter/2020/82882020.
[26] J. Ramkumar and R. Vadivel, "Bee inspired secured protocol for routing in cognitive radio ad hoc networks," INDIAN J. Sci. Technol., vol. 13, no. 30, pp. 3059–3069, 2020, doi: 10.17485/IJST/v13i30.1152.
[27] R. Vadivel and J. Ramkumar, "QoS-Enabled Improved Cuckoo Search-Inspired Protocol (ICSIP) for IoT-Based Healthcare Applications," pp. 109–121, 2019, doi: 10.4018/978-1-7998-1090-2.ch006.
[28] J. Ramkumar and R. Vadivel, "Intelligent Fish Swarm Inspired Protocol (IFSIP) For Dynamic Ideal Routing in Cognitive Radio Ad-Hoc Networks," Int. J. Comput. Digit. Syst., vol. 10, no. 1, pp. 1063–1074, 2020, doi: http://dx.doi.org/10.12785/ijcds/100196.
[29] J. Ramkumar, R. Vadivel, and B. Narasimhan, "Constrained Cuckoo Search Optimization Based Protocol for Routing in Cloud Network," Int. J. Comput. Networks Appl., doi: 10.22247/ijcna/2021/210727.
[30] J. Ramkumar and R. Vadivel, "Performance Modeling of Bio-Inspired Routing Protocols in Cognitive Radio Ad Hoc Network to Reduce End-to-End Delay," Int. J. Intell. Eng. Syst., vol. 12, no. 1, pp. 221–231, 2019, doi: 10.22266/ijies2019.0228.22.
[31] J. Ramkumar and R. Vadivel, "Whale Optimization Routing Protocol for Minimizing Energy Consumption in Cognitive Radio Wireless Sensor Network," Int. J. Comput. Networks Appl., vol. 8, no. 4, doi: 10.22247/ijcna/2021/209711.
[32] J. Ramkumar and R. Vadivel, "Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks," Wirel. Pers. Commun., pp. 1–23, Apr. 2021, doi: 10.1007/s11277-021-08495-z.
[33] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, "Towards DNA based data security in the cloud computing environment," Comput. Commun., vol. 151, pp. 539–547, 2020, doi: https://doi.org/10.1016/j.comcom.2019.12.041.
[34] S. R. Jena, R. Shanmugam, K. Saini, and S. Kumar, "Cloud Computing Tools: Inside Views and Analysis," Procedia Comput. Sci., vol. 173, pp. 382–391, 2020, doi: https://doi.org/10.1016/j.procs.2020.06.045.

Authors

Mrs. Vatchala B obtained MCA degree in Anna University, M.Phil in PRIST University and now Pushing PhD in same University. I worked as Assistant Professor in Rajiv Gandhi Eng. College, Puducherry, and Assistant Professor in Theivanai Ammal College for Women, Villupuram, Assistant Professor in PRIST University, Puducherry. Now working as CLP staff in Dr. M.G.R. Govt. Arts and Science College for Women, Villupuram. I had published 6 journals. My research area is Cloud Computing.

Dr. G. Preethi obtained M.Phil, M.Tech., Ph.D degrees from various Universities. After that worked as Lecture in Sami Arul College, and T.U.K. Arts College, Thanjaur, She joined Assistant Professor (School of Computing) in SASTRA University, Thanjaur, She joined HOD in Annai Vailankanni Arts and Science College, Thanjaur. She is currently working as Associate Professor Dept. of Computer Science in PRIST University, Thanjaur. She was attended 5 Workshops and 2 International Conferences and she has published 19 Journals. Her research interest includes Data Mining, Cloud Computing, Big Data and IoT.

How to cite this article:

Vatchala B, G. Preethi, "Hybrid Optimization-Based Secure Routing Protocol for Cloud Computing", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 229-239, 2022, DOI: 10.22247/ijcna/2022/212338.