Computers, Materials & Continua
DOI:10.32604/cmc.2022.019502
Article

Tech Science Press

Cross-Layer Hidden Markov Analysis for Intrusion Detection

K. Venkatachalam[1], P. Prabu[2], B. Saravana Balaji[3], Byeong-Gwon Kang[4], Yunyoung Nam[4,*] and Mohamed Abouhawwash[5,6]

[1]Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bangalore, 560074, India
[2]Department of Computer Science, CHRIST (Deemed to be University), Bangalore, 560029, India
[3]Department of Information Technology, Lebanese French University, Erbil, 44001, KR, Iraq
[4]Department of ICT Convergence, Soonchunhyang University, Asan, 31538, Korea
[5]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[6]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, 48824, MI, USA
[*]Corresponding Author: Yunyoung Nam. Email: ynam@sch.ac.kr

Received: 14 April 2021; Accepted: 15 May 2021

Abstract: *Ad hoc* mobile cloud computing networks are affected by various issues, like delay, energy consumption, flexibility, infrastructure, network lifetime, security, stability, data transition, and link accomplishment. Given the issues above, route failure is prevalent in *ad hoc* mobile cloud computing networks, which increases energy consumption and delay and reduces stability. These issues may affect several interconnected nodes in an *ad hoc* mobile cloud computing network. To address these weaknesses, which raise many concerns about privacy and security, this study formulated clustering-based storage and search optimization approaches using cross-layer analysis. The proposed approaches were formed by cross-layer analysis based on intrusion detection methods. First, the clustering process based on storage and search optimization was formulated for clustering and route maintenance in *ad hoc* mobile cloud computing networks. Moreover, delay, energy consumption, network lifetime, and link accomplishment are highly addressed by the proposed algorithm. The hidden Markov model is used to maintain the data transition and distributions in the network. Every data communication network, like *ad hoc* mobile cloud computing, faces security and confidentiality issues. However, the main security issues in this article are addressed using the storage and search optimization approach. Hence, the new algorithm developed helps detect intruders through intelligent cross layer analysis with the Markov model. The proposed model was simulated in Network Simulator 3, and the outcomes were compared with those of prevailing methods for evaluating parameters, like accuracy, end-to-end delay, energy consumption, network lifetime, packet delivery ratio, and throughput.

Keywords: Data transition; end-to-end delay; energy consumption; flexibility; hidden Markov model; intrusion detection; link optimization; packet delivery ratio; privacy; security; searching; throughput

1 Introduction

Ad hoc mobile cloud computing networks are arranged with several wireless communicating nodes [1]. These networks define a concept from a source to targeting approach for on-demand contact to pooled services. The ongoing review of the system's operational state is necessary to identify performance degradations and malfunctioning resources as fast as possible to manage the resources effectively. Any change in the load, computer state, or software code may affect the device status from regular to irregular. These changes deteriorate the service efficiency and quality. The supervision of *Ad hoc* mobile cloud computing networks is decentralized, and the nodes can move randomly [2]. Here, data transition and distributions from one node to another are achieved using a wireless link. This process facilitates the route identification for intruders in the network. Generally, the nodes in adhoc mobile cloud computing networks communicate without nearby base stations. For instance, the routing protocols in adhoc networks regulate the possible path for good communication through the participating mobile nodes [3]. Adhoc mobile cloud computing networks are utilized for many applications because of their decentralized peer-to-peer system. These networks are arranged in clusters from which one node is selected as the mobile cloud head, and the rest of the participating nodes are the cloud member nodes. Furthermore, mobile cloud clustering is applied to distinguish the decentralized peer-to-peer system from interconnected infrastructure, namely, adhoc mobile cloud computing networks. Each network in a particular environment has a mobile node, which is denoted as the mobile cloud head and performs the network route organizer's function [4].

Additionally, intrusion detection methods are required to address security issues and confidentiality concerns. The hidden Markov model works with high stability in terms of exact data transition and distributions. This model helps identify and prevent intrusions to address the security issues and confidentiality concerns of adhoc mobile cloud computing networks [5]. Several protocols, like the *ad hoc* on-demand distance vector, the border gateway protocol, location aided routing, optimized link state routing, open shortest path first, the routing information protocol, and the zone routing protocol, are used to enhance data communication. However, they fail to decrease the routing overhead. Thus, the developed clustering-based storage and search optimization approach model has enhanced adhoc features, such as addressing delay, energy consumption, and flexibility, and our main research analysis is based on the following questions:

(1) How can node stability be maintained while transferring data in an adhoc network during failure?
(2) How are intruders in the network who are waiting to attack at failure nodes analyzed?

Contribution

In this paper, a new clustering-based storage and search optimization approach using cross-layer analysis based on intrusion detection methods is proposed. To avoid the delay in data packet of the cloud environment and a significant increase in the route efficiency of adhoc mobile cloud computing networks, the following contributions are made in our research work:

- First, this research quantification converts individual mobile nodes into mobile cluster nodes using the proposed clustering approach based on the storage and search optimization technique.
- Second, this study helps address security issues and improve confidentiality without losing the delay, energy consumption, network lifetime, and link accomplishment characteristics.

- Finally, the hidden Markov model is used for stable data transition and distributions by preventing intrusions. This model helps address the security issues and confidentiality concerns of the adhoc mobile cloud computing network.

The remainder of the paper is organized as follows. In Section 2, the previous clustering approach, the storage and search optimization approach, and the hidden Markov model are discussed. In Section 3, we describe the proposed cross-layer analysis of intrusion detection methods using the clustering approach based on the storage and search optimization approach employed to enhance the adhoc mobile cloud computing network's performance. The experimental results are presented in Section 4, and the conclusions are shown in Section 5.

2 Related Works

Storage using an autonomous mobile infrastructure-based phoenix technique allows a system to make opportunistic use of mobile computing devices and adhoc networking to provide quick storage services to clients in a localized geographical region. A large amount of potential data is lost due to node mobility. An internode communication system can overcome the potential data loss through distributed communication and a storage protocol.

Pudlewski et al. [6] proposed a cross-layer perspective scheme for video transmission over lossy wireless networks. Li et al. [7] presented the construction of a dynamic cloudlet-assisted energy-saving routing mechanism for mobile adhoc networks. This approach detects the target nodes, where the intrusion is happening in network. Zhang et al. [8] proposed a communication workflow technology known as lightweight service-oriented architecture (SOA)-based multi-engine architecture for mobile smart devices.

3 Problem Definition and System Model

3.1 Problem Definition

Panta et al. [9] proposed an opportunistic system combined with mobile computing and *ad hoc* networking for quick storage services. However, the hidden Markov model suppresses the slope current and interferes with adhoc mobile cloud computing networks [10]. A standard clustering-based optimization model is required to allow the nodes to recover the original route and energy during transmission. This requirement affects issues, such as delay, energy consumption, network lifetime, and link accomplishment. This paper presents a simple and effective way of solving this problem and improving the cross-layer analysis based on the intrusion detection performance.

The main objectives of the proposed technique are as follows:

- To propose a new clustering-based storage and search optimization technique to enhance the delay, the energy consumption, the network lifetime, and the link accomplishment for routing.
- To introduce a cross-layer analysis method based on the intrusion detection technique to improve the data transition and distributions and help identify and prevent intrusions.

This article discusses the cross-layer analysis of intrusion detection methods using the clustering approach based on the storage and search optimization approach.

- Clustering-based storage and searching optimization model: we utilize the hybrid storage, search optimization, and clustering technique to maintain the delay, energy consumption, network lifetime, and link accomplishment characteristics.

- Here, the participating mobile nodes are first clustered using clustering-based storage. Then, the destination nodes are searched using the search optimization approach.
- The hidden Markov model is used to obtain the required data transition ratio for the entire routing process. The main motivation behind utilizing the hidden Markov model is to improve the identification and prevention of intrusions.
- The proposed approach can analyze intruders with a different route. The performance of the proposed approach is compared with that of existing state-of-art techniques in terms of accuracy, end-to-end delay, energy consumption, network lifetime, packet delivery ratio, and throughput.

3.2 System Model

In recent years, adhoc mobile cloud computing networks have become an efficient and exciting technology due to the rapid proliferation of communication devices in the wireless medium. Many mobile nodes wish to use adhoc mobile cloud computing network, but only restriction is high CPU power consumption and less battery life [11]. Here, routing protocols can be used to enhance the adhoc network communication, but several security issues remain as the main flaws. Route maintenance is another critical issue faced by adhoc networks and involves route search and storage [12].

Finding and recovering the exact route is challenging, because cross-layer analysis of intrusion detection methods uses Hidden Markov model for identifying and preventing intrusion in network [13]. Also, this method uses the clustering approach to rectify the security and confidentiality issues without losing data packets.

This research developed an innovative cross-layer analysis of intrusion detection methods for transmitting data in adhoc mobile networks. When the communication between nodes starts, cross layer focuses on clustering and route maintenance [14]. The proposed cross-layer analysis using clustering based on the storage and searching optimization approach is shown in Fig. 1 and explained in the following section [15,16].

Clustering can be facilitated by the cluster head nodes, which is energy-consuming, while data are transmitting in a wide range. Hence, a novel clustering algorithm is developed to reduce the energy utilization and improve the network lifetime.

4 Proposed System Architecture

The proposed adhoc mobile cloud computing network is established using cross-layer analysis-based intrusion detection methods with hidden Markova model [17,18]. This cross-layer analysis runs on cloud computing mechanisms and mobile adhoc networks, which extend the functionality of the analysis. Here, a practical mobile adhoc network denotes data sharing between different mobile nodes on a cloud environment [19]. The node's size is static for fast access between the cluster head and the nodes [20]. Hence, deciding which data should be present in the cloud or the mobile *ad hoc* network during interaction is crucial. Any mobile node can transfer stored data to the cloud. This facility allows unauthorized data (attacker data) to be stored in the cloud [21]. Each unauthorized data stored in the cloud will have a different token, which must be stored in the cloud [22]. The proposed clustering-based storage and search optimization approach (cross-layer analysis based on intrusion detection methods) was implemented on Network Simulator 3 (NS-3) [23]. This research employed the cross-layer analysis of intrusion detection (CLAID) methods as our key system for transferring and distributing data to the other nodes. Each node is identified by a token of its public/private key [24]. The complete application stack of any nearby node is illustrated in Fig. 2.

Fig. 2 describes the complete application stack of the node with smart routing using cloud software codes. These codes helps in verifying detail about any transmission and raise the token [25]. The CLAID cluster tool is used to coordinate nodes between the authorized mobile device and different nodes.

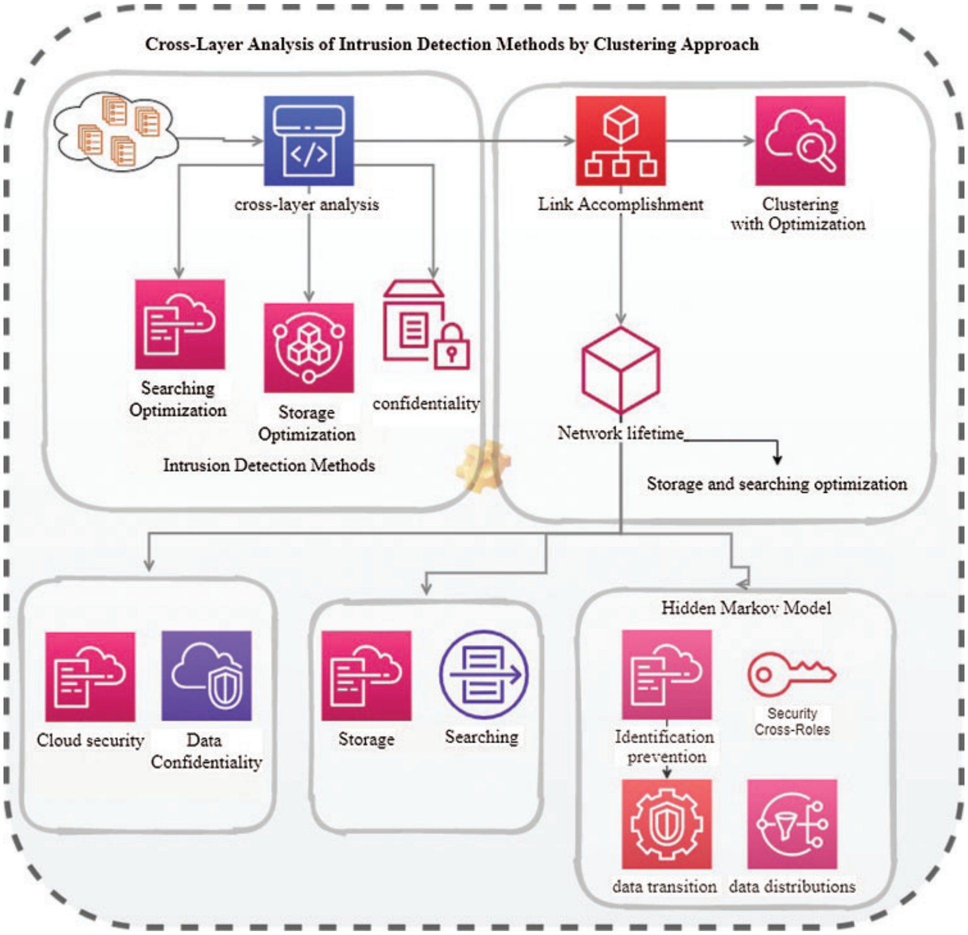

Figure 1: Proposed cross-layer analysis intrusion detection model

CLAID is the content-addressable cloud environment's transmission model. This model is used to maintain the data transaction within the linked node on the cloud environment and unify all data transactions that link to the decentralized peer-to-peer cloud system [26]. Whenever the decentralized peer-to-peer cloud system receives a request from the clustering-based search optimization, the hidden Markov model first handles this request [27]. Further, CLAID forwards the request to the clustering-based storage and search optimization for the allocation of the route in the adhoc mobile cloud computing network. Later CLAID replies to its route history in network [28]. The data communication between the two authorized mobile devices is processed using the route request/route response (RREQ/RRES) signal. This system is distinguished for the hidden Markov Model based on the intrusion detection system's cross-layer analysis [29,30].

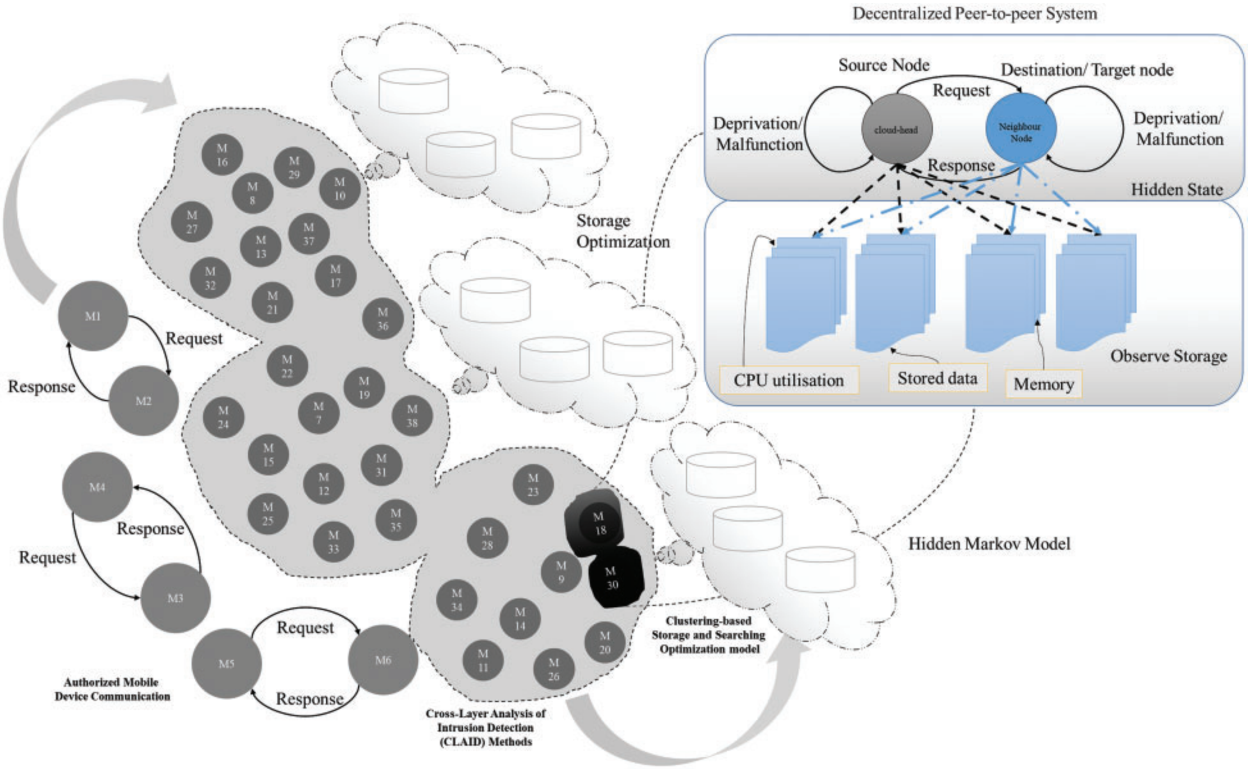

Figure 2: Complete application stack of the node illustration

The route between the source node and the destination/target node is connected by the cloud head for the clustering-based storage and search optimization [31–33]. This storage model allows decentralized routing peer-to-peer applications based on the following key terms:

- Clustering-based Storage: Data is stored in the interaction history.
- Clustering-based Searching: The content is store and organized during routing. The result based on the clustering-based storage is returned.
- Optimization model: Optimization is a data rendering tool through which users perform query operations.

4.1 Clustering-Based Storage and Search Optimization Model

The model is an automatic process in router configuration that allows the tokens from one source node to another neighbor node to be used securely within an adhoc mobile cloud computing network [34]. When a token is generated, the individual routing identification related to any route interaction in the CLAID must be stored inside the adhoc mobile cloud computing network history. This approach helps improve the node routing integrity and security [35]. Conventionally, the actual route is generally referred to as the "authorized mobile device communication."

Given that the proposed model calculates each node's distance in the network for transmitting data, the proposed cluster and route maintenance sets the distance between nodes to 0.2 which is next nearest value for alternate route calculation [36]. If the distance is greater than the condition, then the nodes are ignored [37,38]. Current routing activities are stored in the decentralized peer-to-peer system to be publicly accessible to the routing process for efficiency. Neighbor node token verification and route detection can decrease the waiting time for precise route confirmation [39]. In last few decades the decentralized peer-to-peer system helps to scale intruders by allowing suspectable attackers to form an unauthorized data transmission through the clustering-based storage and search optimization protocol.

The storage and search optimization algorithm can find nearby nodes by intending (route) to move toward a specific new_next_route node [40]. Search optimization equates the route nodes to the new_next_route nodes of the cloud server's cluster. If the storage and search optimization ends with the specific target discovery, then the remaining data are transferred to the nearby nodes. This process helps increases the data transmission speed and the routing efficiency [41–43].

The processing time of storage and search optimization is taken and compared with the transmission and RREQ/RRES times. Moreover, the adhoc mobile cloud computing network is a separate routing network connected to its source cluster using two-way communication. This communication is considered as the future communication, which allows node tokens and some other node properties to be used securely from source to destination. Fig. 3 represents how data is stored in CLAID using two-way communication [44].

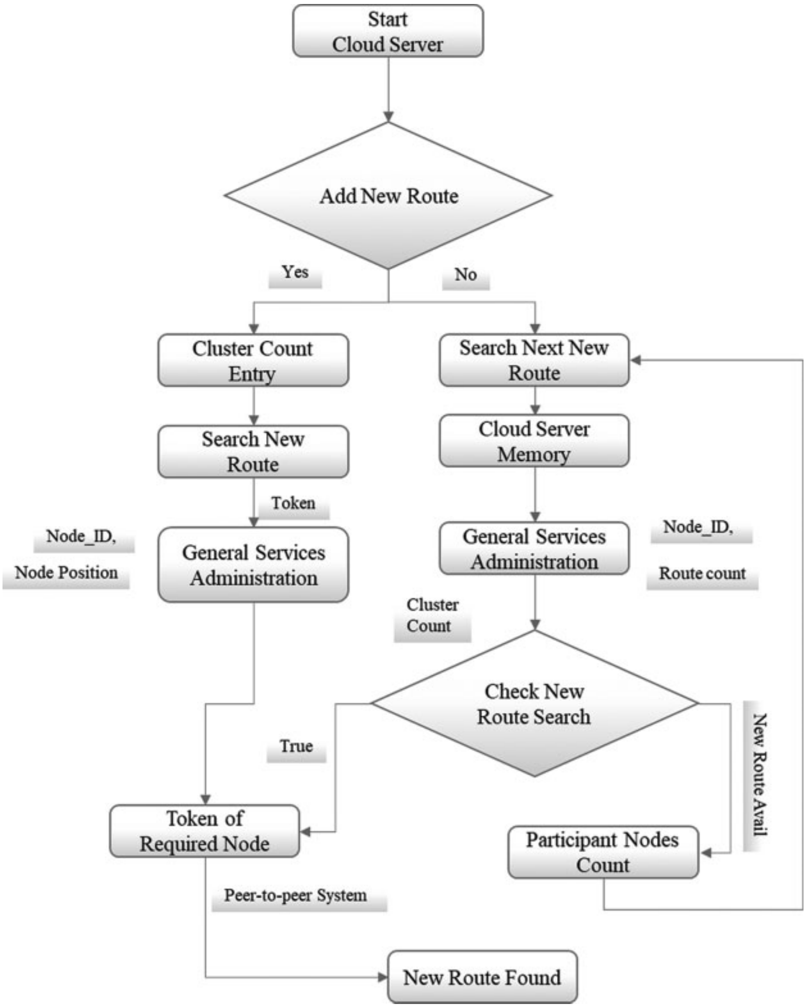

Figure 3: Flow chart for storage and searching optimization algorithm

CLAID provides efficient route communication using a novel clustering-based storage and search optimization approach [45,46]. This method checks whether the communicating node is active or not. If the node is inactive, then transmission overload occurs in the routing path; otherwise, temporal death occurs. This process results in imperfect packet broadcasting. The intrusion node suddenly changes in performance and reduces the packet delivery ratio.

4.2 Anomaly Detection with the Hidden Markov Model

Identification of abnormal behaviors: Identifying abnormalities is disturbed by detecting an anomaly as per the standard routing behaviors. A broad range of techniques, like clustering-based storage and search optimization, adhoc mobile cloud computing network, and hidden Markov models, have been prospected as distinct ways of accepting an anomaly identification challenge. Established attacks provide outlier-based elucidation to avoid interruption in the real-time networks. It also helps to examine the procedure-based attacks and multidimensional routing traffic in networks.

The hidden-Markov-models-based identification of abnormalities in connection with CLAID-HMM creates two premises.

- First, all the mobile nodes count actual conditions in the cloud environment depending merely on the initial condition, forming a complex structure in the cloud environment.
- Second, the efficiency of metrics depends on the authenticated source node hidden in the cloud server. This efficiency of metrics must account for this route history statement's incredibly low validity.
- CPU utilization: According to the percentage of availability in utility of CPU, the collection of CPU utilization, interpretation of quantitative sending data and probability of expected outcome route to estimate population parameters are calculated for usage.
- Available Memory (stored data and memory): This measure covers all the available memory on the virtual machine and is automatically accessible to applications. The free memory reflects the potential capability for additional instances of applications.
- Disk RREQ/RRES: The total numbers of observed RREQ/RRES operations on a disk per second is determined by Eqs. (1) and (2).

$$\mathrm{CUnode} = \left[\mathrm{MS}_{\mathrm{node}} * \mathrm{CCE}_{\mathrm{RREQ:RRES}}\right]_{\text{Var-low(Deprivation)}} \tag{1}$$

$$\mathrm{CUnode} = \left[\mathrm{MS}_{\mathrm{node}} * \mathrm{CCE}_{\mathrm{RREQ:RRES}}\right]_{\text{Var-high(Malfunction)}} \tag{2}$$

CUnode refers to the CPU utilization nodes, MSnode refers to the memory (stored data) node, and CCERREQ: RRES is the Cluster_count_Entry (RREQ/RRES). $\mathbf{MS_{node}}$ is a three-dimensional vector that represents the observed current state of Observe Storage, where 0 denotes a normal route and 1 denotes an abnormal route.

The crucial findings such as height of performance indicators causing anomalous conditions does not appear rapidly. Before performances achieved, the proportions of resource usage increase slowly toward the next_route point and it has potential for anomaly increases. A simple simulation scheme for changing the sampling distances dynamically depending on the degree of risk is introduced. The next _route _point is defined as follows: (Eq. (3)):

$$\mathbf{next_{route}point} = \frac{\mathbf{MS_{node}}}{\mathbf{CCE_{RREQ:RRES}}} * 100. \tag{3}$$

Algorithm 1: Hidden Markov models working principles.

```
Inputs: HMM Parameters $\lambda = (A, B, \pi)$, Experiential Sequence (from t-T to t)
Outputs: system anomaly alert,
1) initializing the count = 0 from CL = 0
2) looping statement starts for t = 1 to T
3) Time t starts with an algorithm
4) Second looping if $\mathbf{next_{route}point} =$ Anomaly indicates
5) increasing the value of count++
6) Finally, end if
7) if threshold ($\mathbf{CCE_{RREQ:RRES}}$) < P ($\mathbf{next_{route}point} =$ Anomaly reports) <50%
8) source_node_authentication (i) = 1
9) end if
10) end for
```

5 Result and Discussion

The developed clustering-based storage and search optimization approach (cross-layer analysis based on intrusion detection methods) is simulated using NS-3 to calculate the performance parameters, like the end-to-end delay, the energy consumption, the network lifetime, the packet delivery ratio, and the throughput. The simulation details using the proposed CLAID methods by the clustering approach based on the storage and search optimization approach are provided in Tab. 1.

Performance Metrics

The existing approaches such as MZBIDS [47] and EA-ICA [48] are compared with proposed CLAID technique which is based on storage and search optimization. CLAID calculates the QoS performance, such as the end-to-end delay, the energy consumption, the network lifetime, the packet delivery ratio, and the throughput. In addition, the area under the curve (AUC) is plotted for binary classification problems. AUC is the measure of a router's ability to distinguish between routes and summarize the score chart.

AUC Chart: An accurate system will detect the chart's intrusion, showing different values and stating the entire false positive and true positive rate (Fig. 4). In addition, the system also provides the accuracy of the proposed algorithm stated on the chart. With this data, the number of packets containing intrusion attacks is identified. To describe the efficiency established by CLAID methods', fine-tuned accuracy is evaluated based on the following action to achieve an accurate result [49].

$$\text{Accuracy} = \frac{\text{True Negative} + \text{True Positive}}{\text{True Negative} + \text{True Positive} + \text{False Negative} + \text{False Positive}} \tag{4}$$

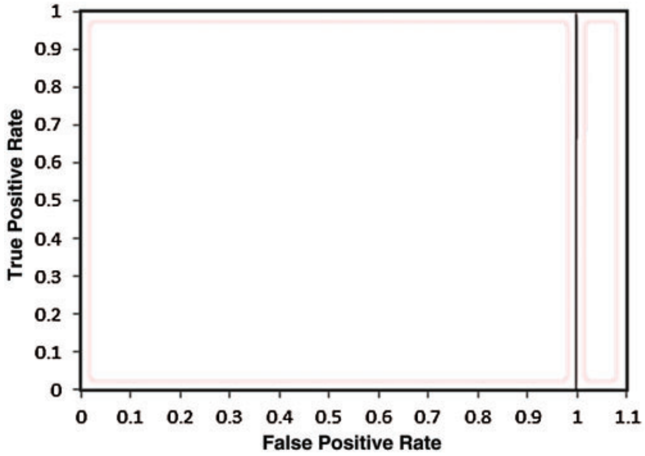

Figure 4: AUC chart

Fig. 5 indicates that accuracy is assessed using Eq. (4) for storage and route sustentation, employing the proposed CLAID. Using the existing methods MZBIDS and EA-ICA in Tab. 1, the proposed CLAID's efficacy is approximately 97.76%. Furthermore, an accuracy of nearly 97% was achieved by our proposed CLAID [49].

Packet is measured using Eq. (5):

$$P = \frac{Total\ no\ of\ participated\ data\ packets}{Total\ no\ of\ transmitted\ data\ \ packets} \times 100. \tag{5}$$

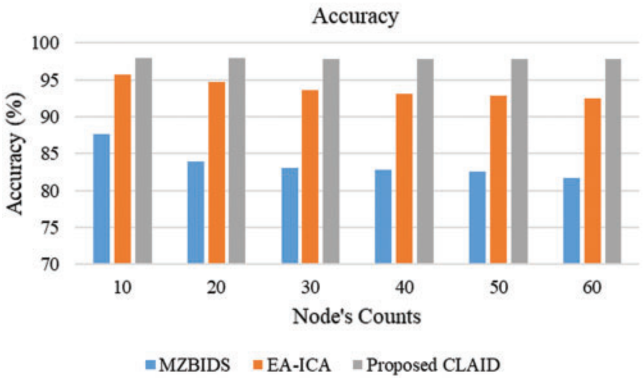

Figure 5: Accuracy comparison chart

Table 1: Accuracy comparison

Node's counts	MZBIDS [47]	EA-ICA [48]	Proposed CLAID
10	87.67	95.65	97.933
20	83.98	94.76	97.900
30	83.1	93.59	97.857
40	82.78	93.06	97.833
50	82.56	92.84	97.790
60	81.75	92.45	97.765

Tab. 2 proves that the proposed CLAID method can achieve a high packet delivery ratio. The evaluated measures indicate that the existing MZBIDS obtains 92% in packet delivery ratio, whereas CLAID obtains 97% in packet delivery ratio. Furthermore, a high PDR value of 97.856% was obtained by the proposed method, which is more powerful than the other methods (Fig. 6) [50].

Table 2: Packet delivery ratio (%) comparison

Node's counts	MZBIDS [47]	EA-ICA [48]	Proposed CLAID
10	87.56	94.87	97.856
20	88.98	93.93	97.856
30	87.75	93.54	97.570
40	85.83	94	96.361
50	84.67	95.5	94.680
60	83.87	92.56	93.489

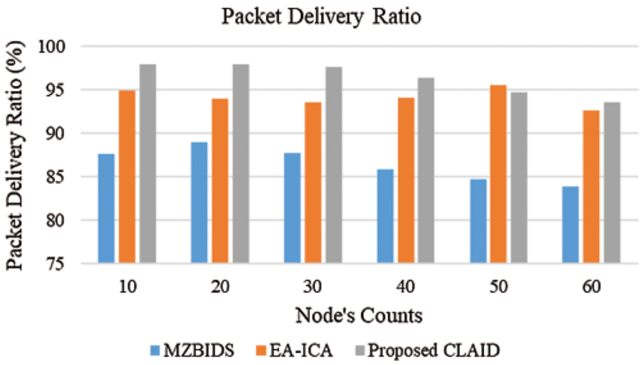

Figure 6: Packet delivery ratio (%) comparison chart

Tab. 3 shows the throughput value of the proposed CLAID (Fig. 7). Throughputs of approximately 30 and 43 kbps are achieved through existing approaches, such as MZBIDS and EA-ICA. The efficiency of the proposed CLAID is also higher than the throughput performance of nearly 121 kbps. Fig. 8 and Tab. 4 describe the adequate energy used for any node in the transmission path and show the measured values. Furthermore, the comparisons between energy usage and current approaches are based on the comparison in Fig. 8.

Table 3: Throughput (kbps) comparison table

Node's counts	MZBIDS [47]	EA-ICA [48]	Proposed CLAID
10	10	10	16.416
20	15	17	19.426
30	18	21	112.416
40	23	27	116.433
50	26	34	119.426
60	30	43	121.333

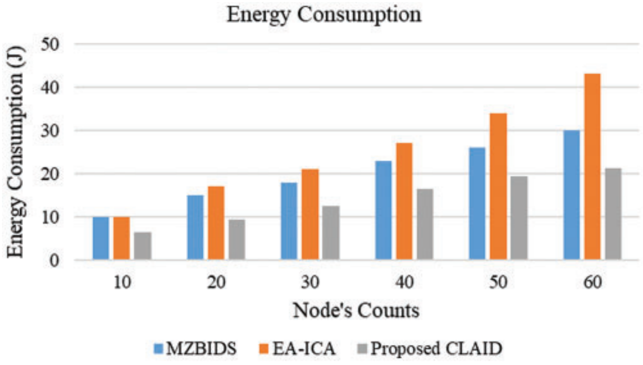

Figure 7: Energy consumption comparison chart

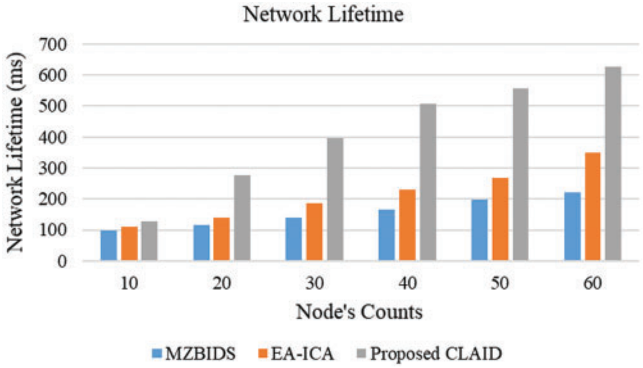

Figure 8: Network lifetime comparison chart

Table 4: Energy consumption comparison table

Node's counts	MZBIDS [47]	EA-ICA [48]	Proposed CLAID
10	98	110	127.133
20	115	140	277.324
30	140	186	397.199
40	167	230	507.199
50	198	267	557.613
60	220	350	627.133

The energy consumption of the nodes is estimated depending on the simulation time. The proposed CLAID model consumes minimal energy due to the minimal, efficient route. In an adhoc mobile cloud computing network, one of the required metrics to achieve successful connectivity is network lifetime. When the nodes' energy consumption is high, connecting with nodes to impact the network's lifespan is impossible. The energy consumption is minimal in this suggested method, indicating that the network's lifespan increased.

Fig. 8 and Tab. 5 describe the network lifetime for many nodes and the testing with predominant approaches. When sending messages across 60 nodes, the existing MZBIDS and EA-ICA have network lifetimes of 220 and 350 s, but the proposed CLAID method's maximum network lifetime 627.133 s. The delay is measured to identify the time required to reach the destination of the transmitted data. The ratio of time consumed for receiving packets to the time consumed by the transmitted packets is measured using Eq. (6).

$$\text{End-to-end delay} = \frac{\text{Time Duration (Received data packet)}}{\text{Time Duration (Transmitted data packets)}} \tag{6}$$

End-to-end delay value of the proposed CLAID method and compares the value with those of existing techniques. Here, MZBIDS and EA-ICA obtain delay values of approximately 59 and 43 s, respectively. The proposed CLAID method also obtains a delay value of 14 ms. In comparison, the proposed CLAID obtains a lower delay value of 0.6 s when transmitting 10 nodes.

Table 5: Network lifetime comparison table

Node's counts	MZBIDS [47]	EA-ICA [48]	Proposed CLAID
10	98	110	127.133
20	115	140	277.324
30	140	186	397.199
40	167	230	507.199
50	198	267	557.613
60	220	350	627.133

6 Conclusion

Adhoc mobile cloud computing networks face various issues, like delay, energy consumption, flexibility, infrastructure, network lifetime, security, stability, data transition, and link accomplishment issues. This research proposes the CLAID methods using the clustering approach based on the storage and search optimization approach to overcome the above issues against the routing in the cloud environment. These approaches are formed by cross-layer analysis is based on intrusion detection methods for clustering and route maintenance in an adhoc mobile cloud computing network. Hence, the developed clustering-based storage and search optimization approach model was evaluated using NS-3, and the outcomes were compared with those of existing methods, such as MZBIDS and EA-ICA, to evaluate parameters, like accuracy, end-to-end delay, energy consumption, network lifetime, packet delivery ratio, and throughput.

Ethical Approval: This article does not contain any studies with human participants or animals performed by any authors.

Funding Statement: This research was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0012724, The Competency Development Program for Industry Specialist) and the Soonchunhyang University Research Fund.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Brik, N. Lagraa, N. Tamani, A. Lakas and Y. Ghamri-Doudane, “Renting out cloud services in mobile vehicular cloud,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9882–9895, 2018.

[2] B. Zhou, A. V. Dastjerdi, R. N. Calheiros, S. N. Srirama and R. Buyya, “Mcloud: Acontext-aware offloading framework for heterogeneous mobile cloud,” *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 797–810, 2017.

[3] B. Liu, D. Jia, J. Wang, K. Lu and L. Wu, “Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network,” *IEEE Systems Journal*, vol. 11, no. 1, pp. 128–139, 2017.

[4] C. A. Ardagna, M. Conti, M. Leone and J. Stefa, “An anonymous end-to-end communication protocol for mobile cloud environments,” *IEEE Transactions on Services Computing*, vol. 7, no. 3, pp. 373–386, 2014.

[5] C. Lin, D. Deng and C. Yao, “Resource allocation in vehicular cloud computing systems with heterogeneous vehicles and roadside units,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3692–3700, 2018.

[6] S. Pudlewski, N. Cen, Z. Guan and T. Melodia, “Video transmission over lossy wireless networks: A cross-layer perspective,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 1, pp. 6–21, 2015.

[7] M. Li, S. Liu and Z. Zhang, “Deep tensor fusion network for multimodal ground-based cloud classification in weather station networks,” *Ad Hoc Networks*, vol. 96, no. 1, pp. 456, 2020.

[8] F. Zhang, R. Deng and H. Liang, “An optimal real-time distributed algorithm for utility maximization of mobile ad hoc cloud,” *IEEE Communications Letters*, vol. 22, no. 4, pp. 824–827, 2018.

[9] R. K. Panta, R. Jana, F. Cheng, Y. R. Chen and V. A. Vaishampayan, “Phoenix: Storage using an autonomous mobile infrastructure,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1863–1873, 2013.

[10] C. Tham and B. Cao, “Stochastic programming methods for workload assignment in an Ad hoc mobile cloud,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1709–1722, 2018.

[11] B. D. Deebak, F. Al-Turjman and L. Mostarda, “Seamless secure anonymous authentication for cloud-based mobile edge computing,” *Computers & Electrical Engineering*, vol. 87, no. 1, pp. 2346, 2020.

[12] F. Chi, X. Wang, W. Cai and V. C. M. Leung, “Ad-Hoc cloudlet based cooperative cloud gaming,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 3, pp. 625–639, 2018.

[13] M. Afaq, J. Iqbal, T. Ahmed, I. U. Islam, M. Khan *et al.* “Towards 5G network slicing for vehicular ad-hoc networks an end-to-end approach,” *Computer Communications*, vol. 149, no. 1, pp. 252–258, 2020.

[14] F. Sun, F. Hou, N. Cheng, M. Wang, H. Zhou *et al.* “Cooperative task scheduling for computation offloading in vehicular cloud,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11049–11061, 2018.

[15] A. Alarifi and A. Tolba, “Optimizing the network energy of cloud assisted internet of things by using the adaptive neural learning approach in wireless sensor networks,” *Computers in Industry*, vol. 106, no. 1, pp. 133–141, 2019.

[16] P. Bazydło, E. Niewiadomska-Szynkiewicz, K. Czerwiński and P. Rękawek, “Simulation-based design of mobile ad Hoc network for tracking and monitoring,” *Int. Conf. on Automation ICA 2016*, Warsaw, Poland, vol. 440, pp. 573–586, 2016.

[17] F. Hagenauer, T. Higuchi, O. Altintas and F. Dressler, “Efficient data handling in vehicular micro clouds,” *Ad Hoc Networks*, vol. 91, no. 1, pp. 2134, 2019.

[18] J. Guo, B. Song, S. Chen, F. R. Yu, X. Du *et al.* “Context-aware object detection for vehicular networks based on edge-cloud cooperation,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5783–5791, 2020.

[19] J. Li, X. Li, Y. Gao, Y. Gao and R. Zhang, “Dynamic cloudlet-assisted energy-saving routing mechanism for mobile ad hoc networks,” *IEEE Access*, vol. 5, pp. 20908–20920, 2017.

[20] R. Klauck and M. Kirsche, “Combining mobile XMPP entities and cloud services for collaborative post-disaster management in hybrid network environments,” *Mobile Networks and Applications*, vol. 18, no. 2, pp. 253–270, 2013.

[21] J. Zhang, T. Chen, S. Zhong, J. Wang, W. Zhang *et al.* “Aeronautical $Ad∼Hoc$ networking for the internet-above-the-clouds,” *Proc. of the IEEE*, vol. 107, no. 5, pp. 868–911, 2019.

[22] H. Gu and H. Wang, “A Distributed caching scheme using non-cooperative game for mobile edge networks,” *IEEE Access*, vol. 8, pp. 142747–142757, 2020.

[23] S. Kaja, M. S. Elhadi and A. Yasar, “Enhanced cloud acknowledgement scheme for a node network,” *Procedia Computer Science*, vol. 175, no. 155, pp. 369–377, 2019.

[24] I. J. Jebadurai, E. B. Rajsingh and G. J. L. Paulraj, “A novel node collusion method for isolating sinkhole nodes in mobile ad Hoc cloud,” in *Advances in Big Data and Cloud Computing, Advances in Intelligent Systems and Computing*, Coimbatore, India, Springer, vol. 645, pp. 319–329, 2018.

[25] L. Wang, M. Liu and M. Q. Meng, “A hierarchical auction-based mechanism for real-time resource allocation in cloud robotic systems,” *IEEE Transactions on Cybernetics*, vol. 47, no. 2, pp. 473–484, 2017.

[26] L. Vigneri, T. Spyropoulos and C. Barakat, “Quality of experience-aware mobile edge caching through a vehicular cloud,” *IEEE Transactions on Mobile Computing*, vol. 19, no. 9, pp. 2174–2188, 2020.

[27] Y. Lai, L. Zhang, F. Yang, L. Zheng, T. Wang *et al.* “CASQ: Adaptive and cloud-assisted query processing in vehicular sensor networks,” *Future Generation Computer Systems*, vol. 94, no. 1, pp. 237–249, 2019.

[28] C. Li, Z. Liye, T. Hengliang and L. Youlong, “Mobile user behavior-based topology formation and optimization in ad hoc mobile cloud,” *Journal of Systems and Software*, vol. 148, no. 1, pp. 132–147, 2019.

[29] P. Bharathisindhu and S. Selva Brunda, “An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network,” *Cluster Computing*, vol. 22, no. 1, pp. 265–275, 2019.

[30] C. Xu, W. Quan, H. Zhang and L. A. Grieco, “Grimes: Green information-centric multimedia streaming framework in vehicular ad Hoc networks,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 2, pp. 483–498, 2018.

[31] C. Tang, X. Wei, C. Zhu, Y. Wang and W. Jia, “Mobile vehicles as fog nodes for latency optimization in smart cities,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9364–9375, 2020.

[32] T. Chen, H. Zhang and Z. Zhao, “Control channel management in dynamic spectrum access-based ad hoc networks,” in *Cognitive Radio Mobile Ad Hoc Networks*. New York: Springer, pp. 181–205, 2011.

[33] J. F. Bravo-Torres, M. López-Nores, Y. Blanco-Fernández, J. J. Pazos-Arias and F. E. Ordióñez-Morales, “Leveraging ad-hoc networking and mobile cloud computing to exploit short-lived relationships among users on the move,” in *Intelligent Cloud Computing ICC 2014*, Lecture Notes in Computer Science, Muscat, Oman, Springer, vol. 8993, 2015.

[34] Y. Luo, O. Wolfson and B. Xu, “The mobi-dik approach to searching in mobile ad hoc network databases,” in *Handbook of Peer-to-Peer Networking*. USA: Springer, pp. 1105–1123, 2010.

[35] M. Ma, D. He, H. Wang, N. Kumar and K. R. Choo, “An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.

[36] M. Cui, D. Han, J. Wang, K. C. Li and C. C. Chang, "ARFV: An efficient shared data auditing scheme supporting revocation for fog-assisted vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15815–15827, 2020.

[37] H. Tseng, S. Sheu and Y. Shih, "Rotational listening strategy for IEEE 802.15.4 wireless body networks," *IEEE Sensors Journal*, vol. 11, no. 9, pp. 1841–1855, 2011.

[38] M. Radenkovic, J. Crowcroft and M. H. Rehmani, "Towards low-costprototyping of mobile opportunistic disconnection tolerant networks and systems," *IEEE Access*, vol. 4, no. 1, pp. 5309–5321, 2016.

[39] K. Pinte, A. L. Carreton, E. G. Boix and W. De Meuter, "Ambient clouds: Reactive asynchronous collections for mobile ad hoc network applications," in *IFIP Int. Conf. on Distributed Applications and Interoperable Systems*, Kongens Lyngby, Denmark, Springer, pp. 85–98, 2013.

[40] M. Qiu, W. Dai and A. V. Vasilakos, "Loop parallelism maximization for multimedia data processing in mobile vehicular clouds," *IEEE Transactions on Cloud Computing*, vol. 7, no. 1, pp. 250–258, 2019.

[41] F. Maly and P. Kriz, "An Ad Hoc mobile cloud and its dynamic loading of modules into a mobile device running google android," in *New Trends in Intelligent Information and Database Systems*. Gdynia, Poland: Springer, pp. 191–198, 2015.

[42] E. Yaqoob, E. Ahmed, A. Gani, S. Mokhtar and M. Imran, "Heterogeneity-aware task allocation in mobile ad hoc cloud," *IEEE Access*, vol. 5, no. 4, pp. 1779–1795, 2017.

[43] M. Usman, A. A. Gebremariam, U. Raza and F. Granelli, "A software-defined device-to-device communication architecture for public safety applications in 5G networks," *IEEE Access*, vol. 3, no. 3, pp. 1649–1654, 2015.

[44] S. Kim, "New bargaining game based computation offloading scheme for flying ad-hoc networks," *IEEE Access*, vol. 7, no. 2, pp. 147038–147047, 2019.

[45] G. Orsini, W. Posdorfer and W. Lamersdorf, "Efficient mobile clouds: forecasting the future connectivity of mobile and IoT devices to save energy and bandwidth," *Procedia Computer Science*, vol. 155, no. 2, pp. 121–128, 2019.

[46] D. Sorkhoh, R. Ebrahimi, R. Atallah and C. Assi, "Workload scheduling in vehicular networks with edge cloud capabilities," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8472–8486, 2019.

[47] R. S. Krishnan, E. G. Julie and Y. H. Robinson, "Modified zone-based intrusion detection system for security enhancement in mobile ad hoc networks," *Wireless Network*, vol. 26, no. 3, pp. 1275–1289, 2020.

[48] H. Faragardi, A. Rajabi, K. Sandström and T. Nolte, "EAICA: An energy-aware resource provisioning algorithm for real-time cloud services," in *IEEE 21st Int. Conf. on Emerging Technologies and Factory Automation*, Berlin, Germany, pp. 1–10, 2016.

[49] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan *et al.* "Software defined networking with pseudonym systems for secure vehicular clouds," *IEEE Access*, vol. 4, no. 3, pp. 3522–3534, 2016.

[50] X. Wang, "IPv6-based vehicular cloud networking," *IEEE Communications Letters*, vol. 19, no. 6, pp. 933–936, 2015.