International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Smart Device-Machine-To-Machine Approach for Enhancing Communication in MANET Using IoT and Cloud

Erode Dhanapal Kanmani Ruby[1*], M.Pushpavalli[2], Aruliah Selvarani[3], S. D. Thilagavathy[4], Shruti Bhargava choubey[5],Dondapati Harika[6]

Submitted: 18/01/2024 **Revised**: 27/02/2024 **Accepted**: 04/03/2024

Abstract: Mobile Ad Hoc Networks (MANET) are crucial for the next generation of computing in the Internet of Things (IoT). All devices in a MANET can transfer from one location to another in any direction. Data processing and resource management can be implemented in all components by providing cloud services to users in MANET to access smart devices within the IoT framework. However, security is a major challenge for the growth of Cloud Computing (CC). Establishing a secure network connection takes time and effort. Nevertheless, embracing CC includes frequent outages, improper management, lack of resources, interoperability issues, privacy concerns, and reliability problems. Therefore, to solve this problem, they initially selected the Cluster Head (CH) to calculate the parameters of a mobility and energy node using a weighted metric. Furthermore, the Load Balancing Cluster Head (LBCH) algorithm can reduce the delay in sending and receiving packets through CH. In addition, the variation between the communication workload of each mobile node can be assessed. Then, the Velocity of the IoT node can be calculated using the Cloud Data Transfer Rate (CDTR) approach at the base of the cloud-maintained IoT integration. Finally, the proposed technique can detect the new positions using a Smart Device-Machine-To-Machine (SD-M2M) approach and enhance communication network security. Implementing the proposed method can enhance secure communication in MANET's IoT structure systematically and efficiently. Simulation results evaluate the algorithm's performance regarding channel number, throughput, data transmission rate, energy consumption, energy efficiency, network security and packet delivery rate. The proposed method attains a throughput performance of 79% and security performance of 83% in MANET..

Keywords: *IoT, MANET, Cloud Computing, Security, CH, LBCH, SD-M2M, CDTR, network security, and data transmission rate*

1. Introduction

The IoT is an emerging technology growing rapidly, and the number of devices linked to the IoT has reached around 22 billion. The MANET platform can connect to the CC, data processing, and resource allocation, providing customers with cloud-based services through smart IoT devices. IoT devices can be centralized without depending on nearby systems to form networks with other devices. MANET operates without a central management team or fixed infrastructure of wireless nodes. Furthermore, MANET can communicate IoT devices with each other in an infrastructure-free environment within an IoT system. These IoT nodes can interactively connect, transmit and share knowledge between multiple nodes. IoT can gather vast amounts of diverse data from various networks to provide essential services to healthcare, manufacturing, and utility networks. Smart environs should be compatible with Wireless Sensor Networks (WSNs) and MANETs to ensure successful IoT implementation and attract end users economically [1-2].

IoT systems are inviting targets for attackers as manufacturers focus on price, size, and ease of use when developing IoT devices. At the same time, the security and forensics elements are often ignored. The IoT has the potential to provide a wealth of valuable data evidence. However, forensics experts need to be familiar with everything, from non-standard formats and disparate IoT devices to multi-tenant cloud infrastructure and the cases that come from it. We deal with various issues [3]. Due to the lack of bandwidth and resources, the increasing number of IoT devices and their data traffic at the network edge will pressure the complex centralized Cloud Computing (CC) paradigm. In addition, IoT devices are now more advanced and can function in complex environments due to their complex computing, processing, and sensing capabilities [4].

Despite its significance, data security is still an overlooked and critical concern. In addition, the large number of mobile devices and overloaded edge servers can lead to increased latency and disrupted performance. The computing power of these devices creates new challenges in building applications that meet the required Quality of Service (QoS). However, high loads and limited latency on edge servers and mobile devices have delayed implementation [5].

[1]*Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai-600062, Tamil Nadu, India,Email: bewinbewin54@gmail.com*

[2]*Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam. Email: pushpavallim@bitsathy.ac.in.*

[3]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Chennai-600123, Tamil Nadu, India. Email: selvaraninaac2022@gmail.com*

[4]*Department of Information Technology, Adhiyamaan College of Engineering Hosur, Tamil Nadu 635109, India. Email: thilagakarthick@gmail.com*

[5]*Dean-Innovation, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science & Technology, Hyderabad-501301, Telangana, India. Email: Shrutibhargava@sreenidhi.edu.in*

[6]*Department of Electronics and Communication Engineering, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupati-517102.India. Email: harikadondapati408@gmail.com*

This section introduces an innovative approach that utilizes selected weights to calculate the parameters of motion and energy nodes, referred to as CH. Additionally, The LBCH algorithm can minimize packet delay in sending and receiving through mobile nodes in CH. By integrating cloud and IoT, the CDTR method can calculate the Velocity of IoT nodes. This proposed technology implements the MANET communication model through the SD-M2M approach to detect new positions. Furthermore, security communication is very useful for improving energy efficiency and communication. The proposed technique also improve network security communication by implementing relevant and effective analysis in the IoT architecture of MANETs. The algorithm's performance was assessed through simulation results, including the number of channels, data transfer rate, energy consumption, energy efficiency, load balancing, and packet delivery ratio.

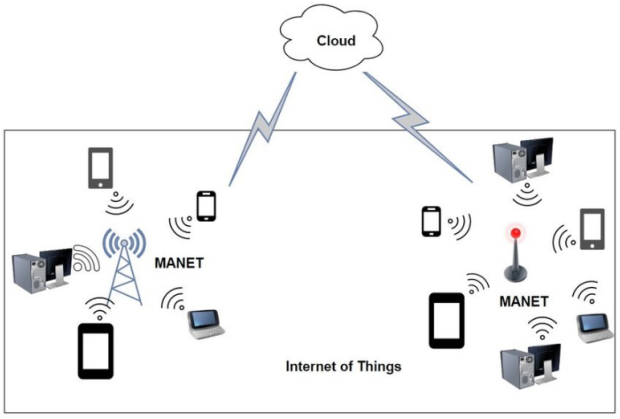

Fig. 1. Architecture Diagram for Cloud-MANET IoT Framework

Figure 1 introduced the Cloud-MANET-IoT framework, allowing information transmission to all connected devices. Additionally, smart devices can exchange data with each other.

1.1 Contribution of this research

This section illustrates the contribution of the paper as follows.

- In this novel main contribution is to enhancing communication in MANET using IoT and cloud.
- This paper carries out the Smart Device-Machine-To-Machine (SD-M2M) approach and enhance communication network security.
- The proposed system efficiently elect the CH based on node weight factors.
- Then use of Load Balancing Cluster Head (LBCH) algorithm can reduce the delay in sending and receiving packets through CH.
- Next, Cloud Data Transfer Rate (CDTR) method for efficient transmission in IoT and cloud.
- Finally, the proposed improve network security in MANET using IoT and cloud.

2. Literature Survey

The author proposed a mobile framework for MANETs leveraging CC to deliver a secure communique between IoT devices. However, there are many challenges to achieving secure transmission across established networks [6]. The author presented that IoT architectures allow users to access and provide cloud services through smart devices. Additionally, they exhibit computing, data processing, and resource management [7]. The novel proposed that IoT and CC can be implemented to test cloud compatibility issues and computing [8]. The author proposed establishing reliable communication between physical objects at the Transmission Control Protocol (TCP) layer. Reliable communication between smart devices requires the TCP layer to detect errors, correct errors, and provide confirmation for information transfer [9]. The author proposed a routing solution for IoT systems that combines MANET protocol and WSN routing code. But at the same time, new problems have also emerged on the network side [10].To improve the network lifetime in Software Defined MANET, Cluster Head Gateway Switch routing protocol along with Particle Swarm Optimization technique is proposed[11].

The author proposed to implement design and test data for mobile CC for classes of IoT-connected devices and employ them regarding measurable security, energy consumption, delay metrics, and packet loss rates [12]. The author proposed to create a maximum number of routes between pairs of nodes to ensure correct and accurate packet delivery. The future key is conditioned on the routing capability with minimum bandwidth consumption [13]. The author proposed and developed a defective node identification system based on the Adaptive Neural Fuzzy Inference System (AFIS) classifier. However, intensity reduction becomes a complex problem as reliable nodes have similar characteristics in the sensing region [14]. The author proposed that an intelligent and creative security architecture can secure IoT networks by implementing the Vectorization Boosted Quantization Network (VBQ-Net) technique. However, IoT systems require continuous development and technological progress [15]. The author proposed an accurate inverse carry selective add (IRCSLA) method with inverse carry propagation. Backward carry propagation technique for 16-bit carry-select adder with Ripple Carry Adder (RCA) Design [16].

The author proposed a load-balancing algorithm to efficiently redistribute Mobile Device Users (MDUs) among Small Base Stations (SBS) [17]. The author proposed that an evaluation framework for cloud service security and reliability can be enforced to combine reputation-based trust assessment approaches to secure cloud-based IoT environments [18]. The author proposed that a hierarchical architecture of IoT networks can be realized to test the manners of IoT requests in a fog computing paradigm. However, unique characteristics pose challenges to standard real-time security [19]. The author mentioned that homomorphic multiplications can be computed without obtaining useful information about the encrypted data using a new method for optimizing semi-trusted servers [20]. The author proposed that the security service architecture can be implemented with the power to adapt to IoT cloud environments. In addition, security mechanisms have been implemented to be effective in such environments [21].

The author proposed a mobile cloud-based infrastructure that opportunistically uses communication opportunities to facilitate efficient data exchange and secure process management [22]. The novel proposed to IoT improve the capabilities of cloud services. Deploy service parameter templates in the cloud and find service analysis templates on edge platforms [23]. The author proposed a novel approach that establishes a secure way for private IoT data to move between sensor nodes with different amounts of available power using the multipath link routing protocol and improved blow fish model (MLRP-IBFM)[24]. The novel

suggested that healthcare data privacy in IoT can be protected using S-Alexnet Convolutional Neural Network and Dynamic Game Theory (SCNN-DGT) [25]. The author proposed combining the advantages of common characteristics of CC and IoT [26]. The author suggested combining cloud/fog computing and IoT to enable universal sensing services and robust processing capabilities [27]. Table 1 explains various methods and their advantages and disadvantages.

Table 1. IoT Network Security for MANET

Author Name	Previous Update	Methods	Advantages	Disadvantages
I. A. Elgendy [28]	2020	Mobile edge computing (MEC)	Multi-user and multi-task computing offloading model in an efficient and secure operation.	Evaluating offload strategies brings up resource allocation and security challenges.
Hemanand, D [29]	2022	Cuckoo Search Greedy Optimization (CSGO)	The NSL-KDD and UNSW-NB15 datasets are widely used to validate network models.	Nevertheless, it has some drawbacks, including high processing time, delayed response, decreased efficiency, and incorrect output classification.
G. V. Reddy [30]	2022	Difference of Gaussian (DoG)	Enables the DoG filter to extract scale-invariant features.	Analyzing human activities now requires the crucial and essential step of recognizing behaviour.
Satyanarayana [31]	2023	Modified Updating Harris Hawks Optimization Algorithm (MU-HHO)	An Enhanced Key Management Scheme Using Confusion Diagram.	To incorporate smart environments in MANETs, developing new protocols for connecting devices to the internet is necessary.
X. Wang [32]	2020	Fuzzy Petri Net (FPN)	Assess the reliability of the node.	However, the network topology is distributed, it frequently varies dynamically and lacks an entire control center.
S. C. Y. Ng [33]	2016	Network Traffic Noise Pattern	To find the advanced persistent attack in	However, the offered method doesn't improve communication in the network
W. M. H. Ahmad Azamuddin [34]	2016	Traffic Policing	To enhance QoS service performance	The suggested method doesn't analysis the energy efficient transmission in the network.
Khalil F Ramadan [35]	2017	energy-efficient MAC protocol	To reduce energy consumption	Efficient communication is challenging task.
Tavanam Venkata Rao, V [36]	2023	Trust Aware Energy Efficient Routing Protocol (TAE2RP), and Secure Surf-Channel Multicast Routing Protocol (SSCMRP)	To enhance the high security in MANET	It reduces packet delivery ratio performance.
Ahmed Mohamed Anwar [37]	2023	ECC33	Improves the QoS performance in mobile networks	The offered method produced high energy consumption

Table 2. MANET based on Cloud Computing Framework

Author	Year	Techniques	Benefit	Drawback
Alam, Tanweer [38]	2017	MANET	Easily determine proximate devices and establish connections without activating central infrastructure.	Another smart device connectivity issue in wireless networks is a distributed system.
Alam T [39]	2018	Cloud-Internet framework	To ensure secure communication between networks of smart devices.	There are several issues regarding the security of communication within networks of smart devices.
RM SP [40]	2020	Energy Efficient Cloud-Based Internet of Everything (EECloudIoE)	Used to deliver valuable services to end operators.	There is a strong demand for data storage.
Kaur I [41]	2017	key management scheme (KMS)	Reduce mobility overhead and improve network security	Performance and safety are the main issues.
Bharany S[42]	2022	Fault Tolerance Techniques (FTT)	Exploring the connection between disability and energy cost	Dealing with failures is the biggest challenge when working in the cloud.
Gopalakrishnan Subburayalu [43]	2021	Adaptive Neuro Fuzzy Inference System (ANFIS)	This study efficiently identify the malicious node in the network.	However, this method didn't elect CH.
S.Gopalakrishnan [44]	2021	Multi-Agent-Based Zone Routing (MAZR)	Nodes that communicate and leaders of zones are responsible for creating the backbone of the network, which facilitates the routing of multicast messages.	However, this method didn't focus security for transmission.

Table 2 carried out cloud computing secure communication techniques of benefits and drawbacks.

3. Proposed Methodology

In this section, Internet security communication can be improved through appropriate and effective analysis of the IoT architecture of MANETs. Initially, the selected CH weights can be implemented to estimate the parameters of mobility and energy nodes. Moreover, The LBCH algorithm can minimize packet delay in sending and receiving through mobile nodes in CH. Then, based on cloud and IoT integration, the CDTR method can calculate the Velocity of IoT nodes. Finally, implementing the MANET communication model between smart devices using the proposed SD-M2M network technology can save energy and efficiency and discover a new position. The accuracy can be obtained by evaluating the algorithm performance through the simulation results and improving the network security communication.

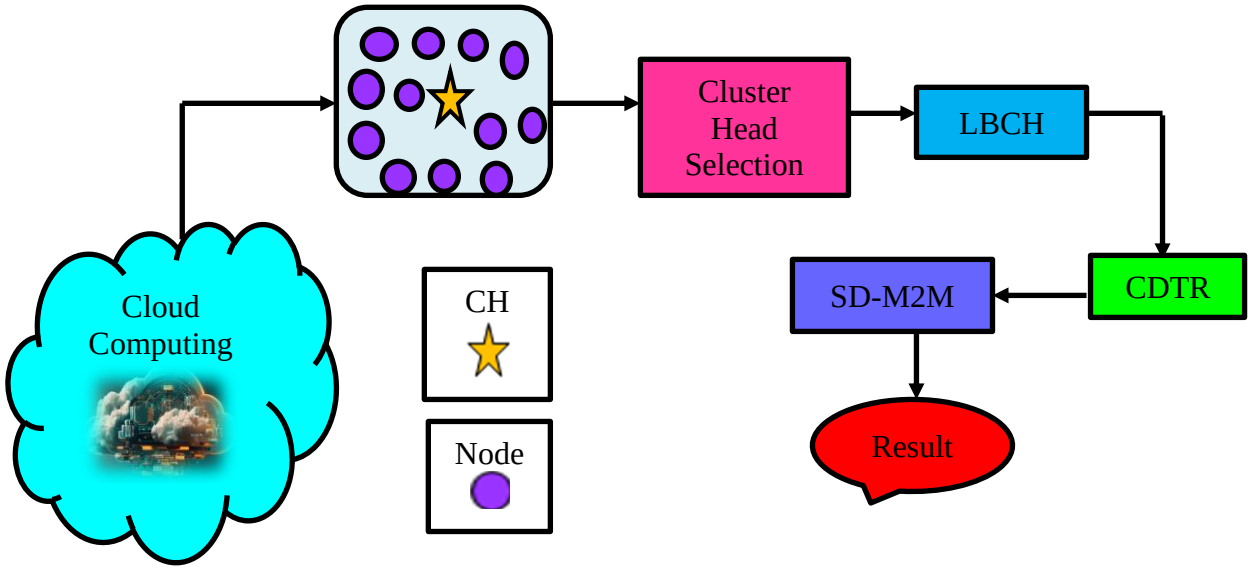

Fig. 2. The Proposed Architecture Diagram for SD-M2M

Figure 2 illustrates the Proposed Architecture Diagram for SD-M2M. Based on these, network security communication can be enhanced through appropriate and effective analysis of the IoT architecture of MANETs using CH, LBCH, CDTR, and SD-M2M network technology.

3.1 Cluster Head (CH) Selection

In this category, CH weight metrics are selected to estimate the parameters of the mobility and energy nodes. The clustering technique reduces energy consumption, communication transportation, and overhead while enhancing network stability. Additionally, thresholds can be established for different parameters in designed dynamic staging environments. Thus, in such a condition, the node movement functions unconstrained. A weight-based CH method can utilize the best energy and mobility parameters to select. Furthermore, it can be enforced based on the application that uses the network to allocate appropriate weights to these parameters. Energy requirements for the transmission and reception of data vary for each node. A stable cluster can be formed by creating a continuous link between less mobile nodes and CHs. The node with the highest weight among neighbouring nodes can be selected as the main CH to form a cluster, and all node's weight values can be estimated.

Estimate the weight of each node as described in Equation 1. Let's assume, z-weight, x-parameter, c-node, a-value.

$$z_{(c_a)} = \sum z_c * x_c(c_a) \quad (1)$$

The node is evaluated by considering the energy and mobility parameters, as shown in Equation 2. Where, $\mathbb{E}$-energy, $\mathbb{M}$-mobility.

$$z_{(c_a)} = z_1 * \mathbb{E}_{(c_a)} + z_2 * \mathbb{M}_{(c_a)} \quad (2)$$

Calculate the time essential for the data transmission at the node as shown in Equation 3. Let's assume $\mathcal{B}_Z$ −band width, y-bits.

$$\mathbb{E}_{send(c_a)} = \mathbb{e}_{send(c_a)} * {}^{y}/_{\mathcal{B}_Z}(c_a) * tatal_{(\mathcal{B}_Z)} \quad (3)$$

As shown in Equations 4 and 5, estimate the energy required to transmit one bit and the available bandwidth. Where s-time, $\mathcal{D}_\mathcal{T}$ −data transfer, m_k −data rate, x_c −packet size, a_u -initial energy.

$$\mathcal{B}_z(c_a) = a_{(u_{c_a})} * \left({}^{m_k}/_{x_c}\right) * s \quad (4)$$

$$\mathbb{e}_{send}(c_a) = sum_{\mathcal{DT}}(s)/total_s \quad (5)$$

Calculate the energy time the single node motion expended as shown in Equation 6.

$$\mathbb{E}_{knF}(c_a) = \mathbb{e}_{knF}(c_a) * {}^{R}/_{\mathcal{B}_Z}(c_a) * total_{(\mathcal{B}_Z)} \quad (6)$$

Calculate the total power time of the node as shown in equation 7.

$$\mathbb{E}_{(total)}(c_a) = \mathbb{E}_{send}(c_a) + \mathbb{E}_{knF}(c_a) \quad (7)$$

Estimate the time to calculate the residual energy, as shown in Equation 8. Where $\varepsilon -$ remaining energy.

$$k\varepsilon F_{(c_a)} = \mathbb{E}_{(c_a)} - \mathbb{E}_{(total)}(c_a) \quad (8)$$

Equation 9 shows the estimation of the velocity time of the mobile node. Let's assume F_s and F_{s-1}- Velocity of node, s, s-1-two-time instances, α −level of dependency degree, σ −standard deviation, μ −Asymptotic mean.

$$F_s = \alpha * F_{s-1} + (1-\alpha) * \mu + \sigma * \sqrt{(1-\alpha * i)} * z_{s-1} \quad (9)$$

In this category, the CHs of each node group are selected using a weighted method such that the speed of the moving nodes should be time-dependent and expressed as a CH model.

3.2 Load Balancing Cluster Heads (LBCH)

The LBCH algorithm can be implemented in this category to reduce the delay in sending and receiving data packets over CH. To ensure effective communication between LBCH nodes, the CHs are occasionally overloaded for extended periods. However, using LBCA can help alleviate the resulting performance delays. LBCA can reduce delays in sending and receiving packets through the CH and improve the burden on any CH. Throughput slots on a CH can be increased to prevent serving all active nodes in the cluster. Furthermore, LBCH can create an unloaded CH when operating the LBCH algorithm, diverting down the network throughput. The presented LBCH algorithm can improve the performance by distributing the load between CHs. Based on them, LBCH can ensure high energy and low mobility within all clusters. Thus, CHs become an important energy source in MANETs and can implement more energy than conventional nodes. An end-LBCH algorithm can be sent to neighboring CHs based on the successful loading of the LBCH, allowing the transmission to continue under normal conditions.

Calculate the neighbors of each node within the transmission range, as shown in Equation 10. Let's assume z-node and s_p −transmission range.

$$n_{(z,z_1)} = F_s\{z \neq z_1, \mathfrak{D}_{(z,z_1)} = s_p\} \quad (10)$$

Equation 11 estimates the total distance between all neighbours.

$$c_z = \sum_{z\in c} m_{(z,z_1)} \quad (11)$$

The average Velocity of each node is calculated as a function of the motion magnitude, as shown in Equation 12. Where $\left(p_{(s)} - p_{(s-1)}\right)^2 + \left(q_{(s)} - q_{(s-1)}\right)^2$ −bandwidth node.

$$d_z = \frac{1}{s}\sum_{s=1}^{s}\sqrt{\left(p_{(s)} - p_{(s-1)}\right)^2 + \left(q_{(s)} - q_{(s-1)}\right)^2} \quad (12)$$

Calculate the Energy Consumed (EC) by the nodes in the network as described in Equation 13. Let's assume a, b- node, $d_{(ab)}$-energy packet send, u_n −energy consumed, u_x-position by the node.

$$u_n = \sum_{a=1,b=2}^{c} d_{(ab)} + u_x \quad (13)$$

Calculate the position of the node in the network as shown in Equation 14. Let's assume u_k −residual energy, u_s −total power of node.

$$u_k = u_s - u_n \quad (14)$$

Calculate the current load of the election function node, as shown in Equation 15. Where $n_{\mathbb{O}}$ −cluster node, uv_z −election function.

$$uv_z = \frac{(R_1 \times u_k)}{(R_2 \times M_2) + (R_3 \times d_z) + (R_4 \times n_{\mathbb{O}})} \quad (15)$$

Calculate each load CH at present, as shown in Equation 16. Where o_{ch} −load cluster head, $n_{\mathbb{O}(z)}$-current load of the node, d-CH members.

$$o_{ch} = \sum_{z\in d} n_{\mathbb{O}(z)} \quad (16)$$

In this section, loaded and unloaded CHs can identify new transmission thresholds by downloading the LBCH algorithm to transmit sufficient energy. Furthermore, the latency of data collection can be reduced.

3.3 Cloud Data Transfer Rate (CDTR)

In this category, the Velocity of an IoT node can be estimated using the CDTR approach based on cloud-managed IoT integration. MANET functionality depends on cluster mobility, resource connectivity, storage, and energy efficiency. In addition, cloud service operators can provide versatile, high-performance warehouses and mobile applications to maintain communication infrastructure. CDTR metric is used to calculate IoT node speed in Cloud-MANET-IoT architecture. The CDTR algorithm allows smart devices to send session reports to the cloud and improve communication with other cloud devices. The offered CDTR approach can efficiently transmit and receive information whenever a smart device evaluates the communication lifetime between MANET and the cloud. Smart devices can connect directly to heterogeneous cloud storage services through MANETs. The entropy of each symbol is used to distinguish probability density functions for smart device locations.

Algorithm

Input: The total number of IoT nodes $o_{ch}(z)$

Output: The speed of the IoT node.

Start

Counter (c) =0

Speed (v) =0.

Step 1: Choose all the IoT nodes in every direction.

Step 2: Use directions to calculate communication sessions. Where, $\mathbb{C}_s$ −communicate session, ℓ −life, ∞ −infinity, α −Alpha, uk_v −expression function, E-Computational value.

$$\mathbb{C}_s[\ell] = \frac{\left(\int_{\alpha}^{\infty}\left(\frac{1}{2}\right) - \left(\frac{1}{2}\right)uk_v\left(\log\frac{E}{\mu}\right) \div \sqrt{2\delta}\right)m_E}{\left(\left(\frac{1}{2}\right) - \left(\frac{1}{2}\right)uk_v\left(\log\frac{E}{\mu}\right) \div \sqrt{2\delta}\right)} + E^{\mu(1/2)\sigma^2} \quad (17)$$

Step 3: Calculate the Velocity and direction. Let's assume δ −random degree velocity, s-period smart device, H-Gauss Markov utility system, S-multifaceted function, nt-cloud storage service, s_R −transmission, a_R −data, x-inverse data, $\propto$ −proportional data,

$$\mathcal{T}_{(s)} = \delta\mathcal{T}_{(s-1)} + (1-\delta)\bar{T} + \sqrt{(1-\delta^2)}T_{s-1}^{H} \quad (18)$$

$$\mathbb{D}_{(s)} = \delta\mathbb{D}_{(s-1)} + (1-\delta)\bar{\mathbb{D}} + \sqrt{(1-\delta^2)}\mathbb{D}_{s-1}^{H} \quad (19)$$

$$S = nt_c \times s_R \times a_R$$

$$X_R \propto \frac{1}{a_R} \quad (20)$$

Step 4: Estimate the value of the transfer function. Where δ −delta,

$$x_R(T_c|\varepsilon_n, a_R, s_R) = 1 - \int_{-\infty}^{\infty} d_y\left(\sqrt{\left(\frac{2\delta^2}{1-\delta^2}\right)}.\frac{T_c}{s_R}\sqrt{\frac{T_c}{1-\delta^2}}.2\delta\right) \quad Where\ \delta = 1 \quad (21)$$

Step 5: Compute the entropy of each symbol for all smart devices in 3D locations. Let's assume ϵ −Epsilon variant, $\varepsilon_2\left(\frac{\delta}{\alpha}, T_c.\gamma\right)$ −chi square distribution method.

$$G_{\alpha\delta\epsilon} = \sum_{p=0,q=0,z=0}^{\infty}\left[x_{p_R}.x_{q_R}.x_{z_R}\log_3\frac{1}{x_{p_R}}.\frac{1}{x_{q_R}}.\frac{1}{x_{z_R}}\right]\alpha_{\beta^{-1}}\varepsilon_2\left(\frac{\delta}{\alpha}, T_c.\gamma\right) \quad (22)$$

Step 6: Discover the baud rate in $\mathscr{b}/_{\mathcal{S}}$. Where $\mathscr{b}/_{\mathcal{S}}$ − bits by seconds.

Step 7: Discovery the Speed (V) in $\mathscr{b}/_{\mathcal{S}}$

Step 8: c=c+1;

If counter! = Approximately the number of systems, otherwise, go to step 2.

Stop

3.4 Smart Device-Machine-To-Machine (SD-M2M)

In this section, the SD-M2M algorithm is proposed to improve network communication security by detecting new states in the MANET communication model—security communication performance. The proposed method significantly benefits SD-M2M communication, as multiple devices are close to SD-M2M networks. This approach enhances the overall performance of

mobile communication between devices and expands the communication range while minimizing energy consumption through direct communication. SD-M2M communication in the Cloud MANET framework for IoT is a new method for locating and securing nearby smart devices without depending on a centralized approach. Using the MANET model to enable communication between SD-M2M devices is highly efficient, leading to energy savings and improved performance. SD-M2M devices are interconnected through a cloud-maintenance measure, which forms a self-organizing network and vigorously connects to access the cloud. To ensure the optimal performance of smart devices within a MANET, they must be registered in the cloud. Once the MANET is set up, real-time cloud services are activated for SD-M2M communication and services within the network. The smart device then retrieves a reference session from the cloud. The proposed SD-M2M approach can detect new positions and smart devices within MANETs.

Algorithm

Input: Velocity and direction (V)

Output: Find the new position

Start

Step 1: Locate the smart device in MANET p_1, q_1

Step 2: Find the current speed $(\mathbb{C}_s)$ of mobile devices in MANET.

Step 3: Distance and time can be used based on the speed process.

$$velocity_{(s)} = (dist_{\mathbb{D}} | time_{\mathbb{S}}) \quad (23)$$

Step 4: When θ is negative, the smart device's new location estimate can be used to predict time and angle.

$$\mathcal{p}_2 = \mathcal{p}_1 + T * S * cos_{(\vartheta)} \quad (24)$$

$$\mathbb{q}_2 = \mathbb{q}_1 + T * S * sin_{(\vartheta)} \quad (25)$$

$$\mathcal{p}_2 = \mathcal{p}_1 - T * S * cos_{(\vartheta)} \quad (26)$$

$$\mathbb{q}_2 = \mathbb{q}_1 - T * S * sin_{(\vartheta)} \quad (27)$$

Step 5: Estimate the smart device's real location. Let's assume o-location, $\mathbb{N}_{\mathbb{O}}$ −new location, $\mathbb{s}_{\mathbb{o}}$ − smart device location, and $\mathbb{N}_{\mathbb{P}}$-new point.

$$\mathcal{O}\ loc = get\_\mathbb{N}_{\mathbb{O}}\left(\mathbb{N}_{\mathbb{P}(\mathbb{s}_{\mathbb{o}})}\right) \quad (28)$$

$$\mathcal{O} = (p_1, q_1) \quad (29)$$

Step 6: Get a theoretical position at the smart device.

$$M = \sqrt{(\mathcal{p}_2 - \mathcal{p}_1)^2 - (\mathbb{q}_2 - \mathbb{q}_1)^2} \quad (30)$$

Step 7: Find the smart device's random position on the triangle's diagonal. Where m_r −math random location.

$$\mathcal{p} = m_r(\mathbb{M}.get^{\mathcal{p}}()) \quad (31)$$

$$\mathbb{q} = m_r(\mathbb{M}.get^{\mathbb{q}}()) \quad (32)$$

Step 8: A smart device can get its true location when it is above the triangle diagonal.

$$\mathcal{p} = \mathcal{p} + \delta\mathcal{p} \quad (33)$$

$$\mathbb{q} = \mathbb{q} + \delta\mathbb{q} \quad (34)$$

Else

$$\mathcal{p} = \mathcal{p} - \delta\mathcal{p} \quad (35)$$

$$\mathbb{q} = \mathbb{q} - \delta\mathbb{q} \quad (36)$$

Return $\mathbb{N}_{\mathbb{O}}$- p and q.

Stop

4. Result and Discussion

In this fragment, we evaluate the implementation of the existing and proposed algorithms using diverse parameters, including packet delivery rate, throughput, energy consumption, energy efficiency, data transfer rate, and network security. The approach presented here allows for a relevant and effective analysis of IoT architectures in MANETs and the development of new levels of secure communication within the network. To evaluate performance analysis, the simulation work implies using specific methods. This involves running multiple simulations on a 1000m x 1000m grid with varying network sizes of 100 to 400 mobile nodes, transmission ranges from 1 to 255m, and node speeds from 700 to 3000m/s. The performance of the presented method was assessed by employing the simulation constraints in Table 3.

Table 3. Simulation Parameters

Parameter	**Variable**
Tool	Network Simulator version 2
Number of nodes	100-400
Size of Network	1000m*1000m
Transmission assortment	1m-255m
Node velocity	700-3000 m/s
Data traffic	CBR (Constant Bit Rate)
Payload Data	215 bytes
Data Rate	4 Packets
No bandwidth node	2Mbps
Run Time	100s

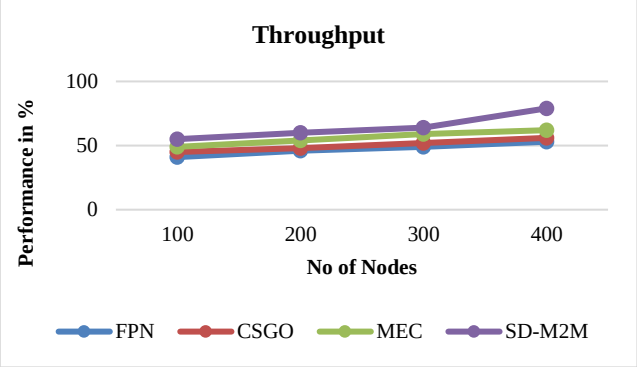

Fig. 3. Analysis for Throughput

In this section, based on the generative approach, the proposed method can be evaluated compared to other methods, as shown in Figure 3. The proposed SD-M2M algorithm improves performance efficiency by 79% compared to other methods in the literature. However, another method scored 41% lower. Therefore, the algorithm will discover new stations and improve network communication security.

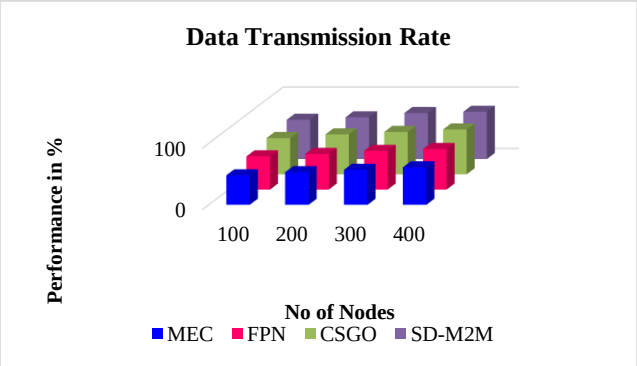

Fig. 4. Analysis of Data Transmission Rate

In this section, we can compare the proposed method with other generation methods. This is illustrated in Figure 4. The algorithm is designed to discover new locations and enhance network communication security, increasing data transmission rates. The

proposed SD-M2M algorithm is found to be 77% more accurate than other methods mentioned in the literature. However, in another study, MEC, CSGO, and FPN scored 49% lower.

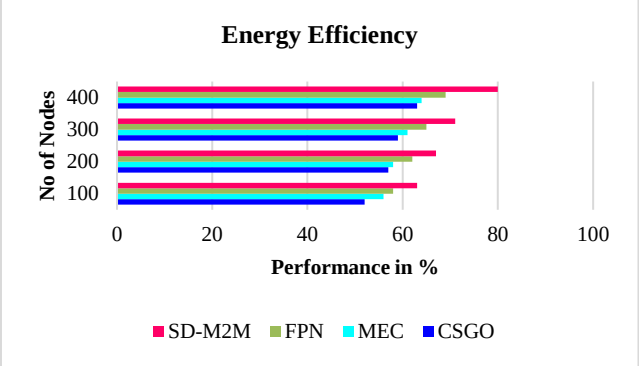

Fig. 5. Analysis for Energy Efficiency

The proposed algorithm, depicted in Figure 5, can be compared to various methods for accurately estimating energy efficiency. Accordingly, the algorithm will locate new positions and improve network communication security for energy efficiency. However, another FPN, CSGO, and MEC method scored 53% less. Furthermore, the accuracy of the proposed SD-M2M algorithm is improved by 80% compared to other methods obtained in the literature.

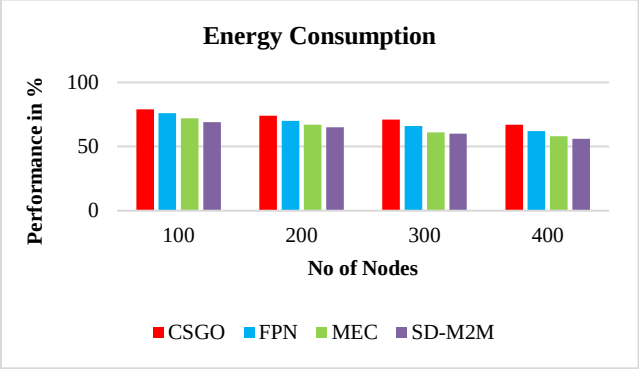

Fig. 6. Analysis of Energy Consumption

Figure 6 describes their low accuracy in comparing the proposed algorithm with different methods to estimate energy consumption. The proposed method makes low latency-based transmission. Therefore, energy consumption is decreased. Consequently, the algorithm will locate new positions and enhance network communication security for energy consumption. Furthermore, the accuracy of the proposed SD-M2M algorithm is lesser by 79% compared to other methods obtained in the literature. However, other CSGO, FPN and MEC methods achieved a 79% improvement.

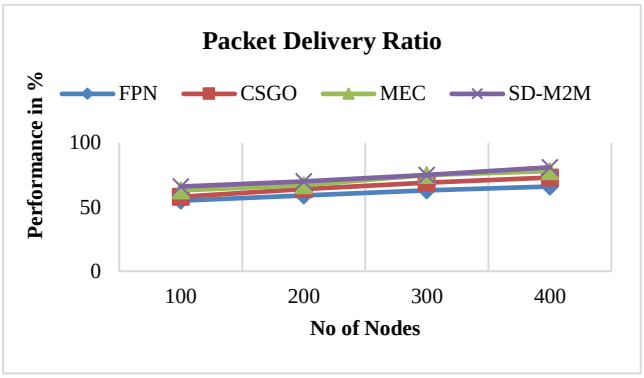

Fig. 7. Analysis of Packet Delivery Ratio

Comparing the proposed algorithm with the methods obtained from the literature to estimate the packet delivery rate, their accuracy is described in Figure 7. The algorithm works to identify new locations to enhance network communication security and decrease the packet delivery ratio. Moreover, compared to other methods found in the literature, the proposed SD-M2M algorithm has an 81% improvement in accuracy. However, the MEC, FPN, and CSGO methods have a low success rate of only 55%.

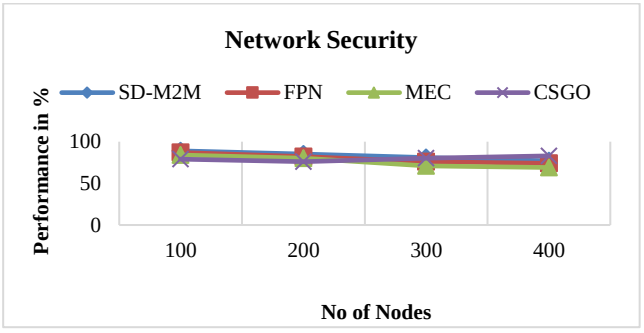

Fig. 8. Analysis for Network Security

As shown in Figure 8, the proposed SD-M2M algorithm improves network security assessment compared to methods obtained from the literature. Furthermore, the value of the proposed SD-M2M algorithm increases to 89%.

Table 3: Overall performance

Parameters	Performance
Throughput	79%
Transmission	77%
Energy efficiency	80%
Packet Delivery Ratio	81%
Security performance	83%

Table 3 explains the overall performance for secure communication numerical results presented.

5. Conclusion

In this segment, we will deliberate the secure exchange of data between IoT nodes using the Cloud MANET-IoT framework. Furthermore, a terminal connected to the cloud can initiate the sharing of connections and information exchange, creating a cloud-MANET mobility model. The primary benefit of this model is that it enhances network communication speed and efficiency in both the cloud and MANET. The first selected CH

uses weighted metrics to calculate mobility and power node parameters. The LBCH algorithm can also reduce the delay in sending and receiving data packets in the CH. Furthermore, it can evaluate the differences in communication workload among the mobile nodes. Regarding cloud management IoT integration basics, the CDTR method estimates the speed of IoT nodes. Finally, the SD-M2M approach can be employed to detect new locations and improve the security of communication networks. By implementing this proposed technique, the secure communication of IoT architectures in MANETs can be improved systematically and effectively. The simulation results evaluate the algorithm's performance based on various factors such as channel number, throughput, data transfer rate, power consumption, energy efficiency, network security, and packet delivery rate. Performance analysis was conducted using various indicators to evaluate current techniques and compare them to the proposed method for effectiveness. The proposed SD-M2M algorithm has achieved an 89% increase in accuracy compared to literature methods. This allows for improved network security communication and the detection of new positions. We found that the proposed framework outperforms other techniques. In future work, the use of the shortest path technique for quick transmission to the destination. Also, it will improve the security performance by employing the authentication key in the MANET network.

Reference

[1] Tanweer Alam, "Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework", May 2020 SSRN Electronic Journal 12(1):2289-8131, DOI:10.2139/ssrn.3639058.a

[2] Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. Sensors 2019, 19, 1467. https://doi.org/10.3390/s19061467.

[3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Second quarter 2020, doi: 10.1109/COMST.2019.2962586.

[4] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4004-4022, 15 March 15, 2021, doi: 10.1109/JIOT.2020.3015432.

[5] W. Almuseelem, "Energy-Efficient and Security-Aware Task Offloading for Multitier Edge-Cloud Computing Systems," in IEEE Access, vol. 11, pp. 66428-66439, 2023, doi: 10.1109/ACCESS.2023.3290139.

[6] Tanweer Alam. “Internet of Things: A Secure Cloud-Based MANET Mobility Model." International Journal of Network Security. Vol 22(3), 2020. DOI: 10.6633/IJNS.202005_22 (3).17.

[7] Mr. Guguloth Ravi Kumar, Dr. R.M.S Parvath "The Significance of an Embedded Design of CloudMANET Framework in the Internet of Things (IoT) & 5G Networks", June 2022 | IJIRT | Volume 9 Issue 1 | ISSN: 2349-6002.

[8] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami and R. R. Zebari, "IoT and cloud computing issues challenges and opportunities: A review", Qubahan Academic J., vol. 1, no. 2, pp. 1-7, Mar. 2021.

[9] Tanweer Alam. "A Reliable Communication Framework and Its Use in Internet of Things (IoT)." International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Vol 3(5), 2018.

[10] I. A. Alameri, "MANETS and Internet of Things: The Development of a Data Routing Algorithm," Engineering, Technology & Applied Science Research Vol. 8, No. 1, 2018, 2604-2608 2604.

[11] Sahaya Sheela MA, Prabakaran R. Improvement of battery lifetime in software-defined network using particle swarm optimization based cluster-head gateway switch routing protocol with fuzzy rules. Computational Intelligence. 2020;36:813–823. https://doi.org/10.1111/coin.12271

[12] AlShahwan, F. Adaptive Security Framework in Internet of Things (IoT) for Providing Mobile Cloud Computing. 2018, https://doi.org/10.5772/intechopen.75190.

[13] Hai, T., Zhou, J., Lu, Y. et al. Enhanced security using multiple paths routine scheme in cloud-MANETs. J Cloud Comp 12, 68 (2023). https://doi.org/10.1186/s13677-023-00443-5.

[14] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118.

[15] Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. Systems, 11(8), 436. MDPI AG. Retrieved from http://dx.doi.org/10.3390/systems11080436.

[16] Turaka, R., Chand, S. R., Anitha, R., Prasath, R. A., Ramani, S., Kumar, H., Gopalakrishnan, S., & Farhaoui, Y. (2023). A novel approach for designing energy-efficient inexact reverse carry select adders for IoT applications. Results in Engineering, 18, 101127. https://doi.org/10.1016/j.rineng.2023.101127.

[17] W. -Z. Zhang et al., "Secure and Optimized Load Balancing for Multitier IoT and Edge-Cloud Computing Systems," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8119-8132, 15 May 15, 2021, doi: 10.1109/JIOT.2020.3042433.

[18] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in IEEE Access, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[19] M. Burhan et al., "A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions," in IEEE Access, vol. 11, pp. 73303-73329, 2023, doi: 10.1109/ACCESS.2023.3294479.

[20] F. Rezaeibagha, Y. Mu, K. Huang, L. Chen and L. Zhang, "Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 217-228, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3087614.

[21] C. Choi and J. Choi, "Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service," in IEEE Access, vol. 7, pp. 110510-110517, 2019, doi: 10.1109/ACCESS.2019.2933859.

[22] D. K. Sharma, K. K. Bhardwaj, S. Banyal, R. Gupta, N. Gupta and L. Nkenyereye, "An Opportunistic Approach for Cloud Service-Based IoT Routing Framework Administering Data, Transaction, and Identity Security," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2505-2512, 15 February 15, 2022, doi: 10.1109/JIOT.2021.3078810.

[23] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan and Q. Jin, "A Secure IoT Service Architecture With an Efficient Balance Dynamics Based on Cloud and Edge Computing," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4831-4843, June 2019, doi: 10.1109/JIOT.2018.2870288.

[24] T Shanthi, M Sahaya Sheela, JJ Jayakanth, M Karpagam, G Srividhya, TVS Gowtham Prasad,” A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission,” in International Journal of Intelligent Systems and Applications in Engineering, vol. 11, pp.455-460, July. 2023.

[25] F. Kong, Y. Zhou, B. Xia, L. Pan and L. Zhu, "A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment," in IEEE Access, vol. 7, pp. 161822-161830, 2019, doi: 10.1109/ACCESS.2019.2950731.

[26] C. Stergiou, K. E. Psannis, B.-G. Kim and B. Gupta, "Secure integration of IoT and cloud computing", Future Gener. Comput. Syst., vol. 78, pp. 964-975, Jan. 2018

[27] C.-M. Chen, S. A. Chaudhry, K.-H. Yeh and M. N. Aman, "Security trust and privacy for cloud fog and Internet of Things", Secur. Commun. Netw., vol. 2022, pp. 1-2, Jan. 2022.

[28] I. A. Elgendy, W. -Z. Zhang, Y. Zeng, H. He, Y. -C. Tian and Y. Yang, "Efficient and Secure Multi-User Multi-Task Computation Offloading for Mobile-Edge Computing in Mobile IoT Networks," in IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2410-2422, Dec. 2020, doi: 10.1109/TNSM.2020.3020249.

[29] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopala Krishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using the CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2167.

[30] G. V. Reddy et al., "Human Action Recognition Using Difference of Gaussian and Difference of Wavelet," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 336-346, September 2023, doi: 10.26599/BDMA.2022.90

[31] Satyanarayana, P., Diwakar, G., Subbayamma, B. V., Phani Sai Kumar, N. V., Arun, M., & Gopalakrishnan, S. (2023). Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile ad-hoc networks for IoT applications. Computer Communications, 198, 262–281. https://doi.org/10.1016/j.comcom. 2022.12.006.

[32] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network," in IEEE Access, vol. 8, pp. 47675-47693, 2020, doi: 10.1109/ACCESS.2020. 2978143.

[33] S. C. Y. Ng, and M. Bakhtiari, "Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis", Journal of Advanced Research in Computing and Applications, Vol. 2, No. 1. Pages 1-18, 2016.

[34] W. M. H. Ahmad Azamuddin, Z. A. M. Noh, A. S. H. Basari and A. S. H. Shibghatullah, "Enhancement Quality of Service at ADTECBP LAN Using Traffic Policing", Journal of Advanced Research in Computing and Applications, Vol. 4, No. 1. Pages 9-19, 2016.

[35] Khalil F Ramadan, M I Dessouky, Mohammed Abd-Elnaby, Fathi E Abd EL-Samie, "An energy-efficient MAC protocol based on node power for wireless sensor networks", Journal of Advanced Research in Computing and Applications 9, Issue 1 (2017) 1-13.

[36] Tavanam Venkata Rao, V. Kumara Swamy, K. A. Karthigeyan, S. Gopalakrishnan, T. Kalaichelvi, & S. Koteswari. (2023). Energy Efficient Trust Based Data Communication using AODV Protocol in MANET. Journal of Advanced Research in Applied Sciences and Engineering Technology, 32(1), 390–405.

[37] Ahmed Mohamed Anwar, Mohamed Shehata, Safa M. Gasser, & Hesham El Badawy. (2023). Handoff Scheme for 5G Mobile Networks Based on Markovian Queuing Model. Journal of Advanced Research in Applied Sciences and Engineering Technology, 30(3), 348–361.

[38] Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94.

[39] Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI:https://doi.org/10.3991/ijim.v12i6.6776.

[40] RM SP, Bhattacharya S, Maddikunta PKR, Somayaji SRK, Lakshmanna K, Kaluri R, Hussien A, Gadekallu TR (2020) Load balancing of energy cloud using wind-driven and firefly algorithms in the internet of everything. J Parallel Distrib Comput 142:16–26.

[41] Kaur I, Rao A (2017) A framework to improve the network security with less mobility in MANET. Int J Comput Appl 167:21–4.

[42] Bharany S, Badotra S, Sharma S, Rani S, Alazab M, Jhaveri RH, Gadekallu TR (2022) Energy efficient fault tolerance techniques in green cloud computing: a systematic survey and taxonomy. Sustain Energy Technol Assess 53, Part b: 102613.

[43] Gopalakrishnan Subburayalu, Hemanand Duraivelu et al., "Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier", Journal of Applied Security Research, pp.1-20, 2021.

[44] S.Manthandi Periannasamy, S.Gopalakrishnan et al., "Performance analysis of multicast routing using multi agent zone based mechanism in MANET", Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 1047–1055.