A Secure Unmanned Aerial Vehicle Service for Medical System to Improve Smart City Facilities

Birasalapati Doraswamy[1]*
Research Scholar, Department of Electronics and Communications Engineering
JNTUA College of Engineering Anantapur, Jawaharlal Nehru Technological University Anantapur (JNTUA)
Ananthapuramu, Andhra Pradesh-515002, India

K. Lokesh Krishna[2]
Professor, Department of Electronics and Communications Engineering
SV College of Engineering
Tirupati, Andhra Pradesh-517502, India

M.N. Giriprasad[3]
Professor, Department of Electronics and Communications Engineering
JNTUA College of Engineering Anantapur, Jawaharlal Nehru Technological University Anantapur (JNTUA)
Ananthapuramu, Andhra Pradesh-515002, India

***Abstract*—The use of drone technology and drones are currently widespread due to their increasing applications. However, there are some specific security-based challenges in the authentication process. In most drone-based applications, there are many authentication approaches, which are subject to handover delay issues with security complexities for an attack. To end these issues, the presented research has focused on developing a novel Optimized deep learning model known as Fruit Fly based UNet Drone Assisted Security (FFUDAS) to remove the malicious attacks. Moreover, the user requests are stored in the cloud, and the stored data are trained to the drones. Hereafter, the drones can deliver medicine to the requestor's location; in that, the malicious attacks were changes the location of drones. Once the attack is identified, then the attack removal process is done. Finally, the new path location to the requested user was identified with the help of fruit fly fitness; then the medicines are delivered to the requested user's location. Furthermore, the designed procedure is executed in an NS2 platform with required nodes. The robustness of the presented model was verified by evaluating the metrics like confidential data rate, execution time, handover delay, pack perception and data delivery rate, and energy consumption. Furthermore, to identify the effectiveness of the presented work, the presented model is compared with other existing schemes. The comparison results show that the presented model has higher throughput, less execution time and handover delay.**

***Keywords*—Drones; security; FFUDAS; malicious attack; fruit fly fitness; path identification; medicine delivery**

I. Introduction

In real-world applications, the technology used in a wide range was the Internet of Things (IoT) [1]. It consists of enormous objects that are interconnected through the environment [2]. The IoT objects are utilized to gather data from different sources and the collected data were exchanged over the internet [3]. This confirms that the objects within IoT make their own decisions without the need of humans [4]. Hence, the IoT's fundamental motivations are to integrate real-world physical and computerized systems for increasing the economic gains and to secure the information efficiently and accurately [5]. The drone was a type of flying IoT object or unmanned aerial vehicle (UAV); it was increasingly being deployed and developed across the globe [6]. Initially, these devices was used for military applications, but now these devices are adopted for different services in a wide range such as service delivery, traffic management, industrial monitoring, agriculture and healthcare [7].

The drone's IoT framework is shown in Fig. 1. These types of drones are currently used in IoT technology to play their part as Internet of drones (IoD), which comprises drones, remote users and ground station [8]. IoD has treated as a controlled architecture of layer network [9]. It was primarily developed to interconnect the UAVs access to support different navigation activities and control airspace [10]. In the growing number of IoT-enabled smart cities, there was widespread concern in using drones [11]. In smart cities, the most important issue was the authentication of drones during flight [12]. Thus, the drone with a secure network is important in each zones of the smart city [13].

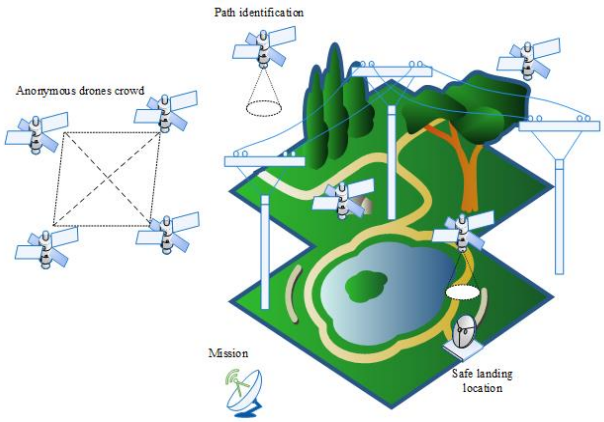

Fig. 1. Drones IoT Framework.

*Corresponding Author

Most importantly, security with low latency-based authentication mechanism is required for drone-assisted applications [14]. Moreover, preserving the service quality and eliminating the parameter effects may affect drones own mechanism [15].

In the IoD environment, the emerging application was drones in healthcare services. Using the healthcare drone services, the tasks like medicine delivery, medical equipment supply and collection of samples can be delivered to a particular area of patients [16]. Moreover, these services are also useful in tribe areas, the restriction imposed areas and rural areas [17]. However, the IoT healthcare service faces many privacy and security issues such as environmental-based attacks [18]. To secure the IoD environment, access control, key management and authentication are the primary services in security. Moreover, the utilization of blockchain technology makes the systems more robust against different attacks such as transparency, decentralization and immutability [19]. The information communicated through the IoT drone, the data were strictly confidential and private [20]. Several research works were done in the past such as authentication-based blockchain technology [21], 5G-based IoD environments blockchain challenges [22], drones system management and privacy [23], etc. are implemented in the past for secure sharing of things via UAV, but it gave poor outcomes due to inefficient algorithms and attack harmfulness. Hence the present work has aimed to develop a novel optimized deep learning methods in the UAV to enhance the monitoring function of malicious activities. By improving the monitoring function, the malicious attacks are identified and removed from the network environment. The main objective of this research is secure sharing of data.

The rest of the paper is described as follows: the recent literatures related to the drone for sharing things is described in Section 2, the system model and its problem statement is explained in Section 3, Section 4 explains the proposed methodology and its process, the result and discussion of the presented framework is described in Section 5 and Section 6 concludes the paper.

II. Related Work

Some recent literatures related to the drone for medicine sharing are described as follows:

The utilization of drone technology and the drone was widespread because of its rising applications such as safety surveillance, intelligent transportation, delivery, shipping, and military packages in IoT global landscape. However, the drone applications led to latency-based issues in real-time. To address this, Yazdinejad *et al.* [21] have presented a secure authentication-based model with less latency for drones which looks like leverage-based blockchain technology. Also, they implement an architecture zone in a drone network i.e., delegated drone stake proof. The results clearly demonstrated that the presented model has high throughput, less delay in end-to-end and less packet rate. Moreover, the energy consumption of drones is high and control of drone speed is difficult.

The 5G-based IoT-enabled Internet of Drones (IoD) environments blockchain applicability issues and in-depth challenges were presented by Bera et al. [22]. Moreover, IoD communication entities' data management's new blockchain secure framework was presented and analyzed. The result indicated that the presented method offers better functionality requirements and security. However, there were latency issues and threats are at high-level.

Due to the higher traffic demands of UAVs, it faces many challenges such as security, system management and privacy. To end this issue, Labib et al. [23] have presented a study about the UAV's current state-of-art and low-altitude traffic management in the airspace. It additionally explored the landscape technical standardization and highlighted the synergies among UAV operations standardization efforts and scientific research. The study result demonstrated that the IoT with drones has good privacy and security. Moreover, without guidelines, it does not identify the risk strategies.

Yahuza et al. [24] has assessed the recent trends in privacy and security issues, which affect the IoD-based network. Also, they investigated the privacy and security threat levels under various categories of the drone. The needed architecture for secured IoD networks and the comprehensive attacks taxonomy were highlighted. Moreover, the performance metrics and evaluation methods employed using techniques are also provided. However, many techniques face privacy-related issues and it was not rectified.

To tackle the Authenticated key management (AKM) issues in IoD environment, Tanveer et al. [25] have presented a robust AKM for IoD (RAMP-IoD), which utilizes lightweight cryptography. It also verifies the authenticity of users and it set a session-key among specific drones and users. The results indicated that the presented RAMP-IoD method had enhanced communication, computational overheads and high security. Furthermore, this protocol was not resource-efficient in IoD environmental security. The overall state-of-art comparison of existing literature is described in Table I.

The recent existing techniques did not resolve the security-based issues. Therefore, a novel nature inspired algorithm with network is designed in this research to resolve the security issues. Moreover, the key contribution of this research work is summarized as follows:

- Initially, the required number of nodes is designed in the NS2 environment.
- Consequently, a novel FFUDAS was designed to monitor the malicious activities in the present nodes.
- Hereafter, the malicious nodes are predicted and removed from the network environment.
- Thus, the drone-based IoT system was protected against the harmful activities; also the malicious nodes are in the way of data transfer, then data is handed over to other nodes by the fitness of fruit fly.
- Finally, the key metrics are calculated in terms of data delivery rate, confidentiality, handover delay, execution time, packet drop, energy consumption.

TABLE I. STATE-OF-ART COMPARISON

Sl.no	Authors	Techniques	Merits	Demerits
1	Yazdinejad *et al.* [21]	DDPOS	It can detect the attacks in an efficient manner with good accuracy	The energy consumption of drones is high and control of drone speed is difficult
2	Bera *et al.* [22]	BSD2C-IoD	It offers better functionality requirements and security	Latency issues and threats are in high-level
3	Labib *et al.* [23]	Study of UAV	The study reports that IoT enabled drone has precise results in security	This study does not provide future scopes and risk strategies
4	Yahuza *et al.* [24]	IoD security assessment	The performance of the drones security under variety of categories are determined	The privacy-based challenges are not resolved yet
5	Tanveer *et al.* [25]	RAMP-IoD	It improves the security, communication and performance	The process consumes more energy

III. SYSTEM MODEL AND PROBLEM DESCRIPTION

To improve the lifestyle of people and to reduce the human efforts and risks, drone application has become the most required sector in recent era. In drone communication securing the information is a much need task because the sensed data has remained in a wide range. So, it is vulnerable to get attacked by harmful malicious events.

Once the data is corrupted during the transmission, then the receiver or user can attain the wrong data, which is not useful for the specific users. Also, it might cause any wrong incident to that specific user. Moreover, in the medical field, security is the primary task; if the medical information from doctor to patient or from patient to doctor has got collapse, and then it tends to happen huge loss in the sense of money and health. The system model with problem in sharing is shown in Fig. 2.

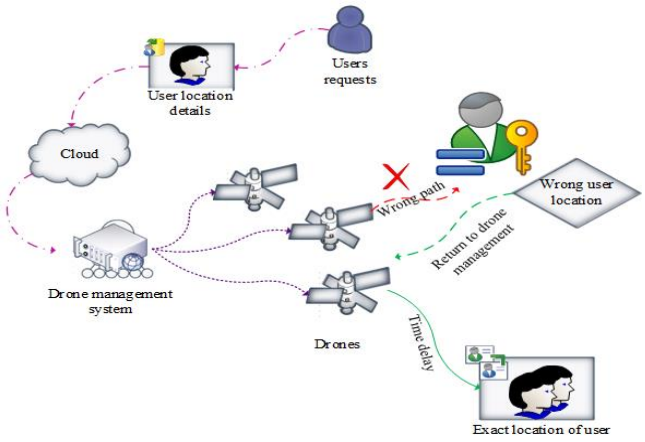

Fig. 2. System Model with Issues.

IV. PROPOSED METHODOLOGY

The drone-based medical delivery system is introduced in many rare situations to support the people from the tragedy. Hence, the medical assist drone contains user profile and location details. So to secure those data, the present research has aimed to design the security framework based on the monitoring and prediction model.

Moreover, the novel technique is named Fruit Fly based UNet Drone Assisted Security (FFUDAS) architecture was designed in the NS2 network. Subsequently, the malicious activities in between the drone were predicted and neglected from the drone environment. The proposed architecture is detailed in Fig. 3.

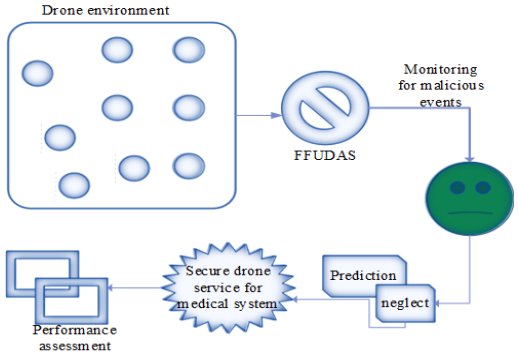

Fig. 3. Proposed Architecture.

A. Proposed FFUDAS Framework

The proposed FFUDAS model is a combination of Fruit fly optimization [26] and UNet based deep learning [27] approach. Initially, the cloud receives the user requirements and location, and is stored in the memory of UNet. Various blocks are designed to store the user details, but the current research work has focused on the supply of medicine in the emergency period. Moreover, from the requested data, the requested user is identified in the starting stage. Initially, the node selection is described in (1):

$$R(ny) = N^{*}\{1,2,3,.....,n\} \quad (1)$$

Where, $R(ny)$ represents the objective function, and N^{*} denotes the designed number of nodes in the network environment. After designing of nodes, the user needs and locations are collected, and then stored in the memory layer of the UNet. Hereafter, the information's are sent to the drone management or drone controller to supply the medicine to the requestor. The requested users' information gathering process is expressed in (2):

$$C_r^{*} = G.(U_r^{*}) \quad (2)$$

Where, C_r^{*} denotes the cloud receiver, G represents the gathering of user information, and U_r^{*} is the user needs. Moreover, the drone controller randomly initialized the location of the drone using a fruit fly-based location to send the

medicines. The fruit fly-based location identification is shown in (3):

$$D_{axis,i} = rand \times (D_{\max} - D_{\min}) + D_{\min} \quad (3)$$

Where, $D_{axis,i} = D_{axis,1}, D_{axis,2}, ..., D_{axis,n}$, $rand$ is the randomly generated drone in uniform and its range is [0,1], $D_{\max}$ and $D_{\min}$ are the distances of drone from the location of the requestor to drone management $i = 1,2,...,n$. Moreover, due to some attacks, the drone was moved to the wrong location. Hence, attacks in network is identified based on UNet and it is expressed in (4),

$$m(a) = m_x(a) + m_l . \exp\left(- \frac{(D_1(a) + D_2(a))^2}{2\beta^2} \right) \quad (4)$$

Where, $m(a)$ represents the presence of malicious attack, $m_x(a)$ denotes the moving location of drones through the attack, m_l denotes the drone pathway, $D_1(a)$ and $D_2(a)$ represents the distances between drones and attacks, and β is the range of drones. Based on the above expression, the attacks in the frames are identified. Moreover, after identification of attacks, it was removed by following (5),

$$A(r) = -\kappa\delta(m(a) - D_{axis,i}) \quad (5)$$

Where, κ represents the fitness of fruit fly, δ denotes the identified attack. Moreover, the proposed FFUDAS layer is shown in Fig. 4.

After the elimination of the attack, the new locations for the requestor are randomly generated through the search process, which is shown in (6),

$$D_{i,j} = D_{axis,i} + random \quad (6)$$

Where, $j = 1,2,.....N_{loc}$, N_{loc} represents the new location, and $random$ were range in the range of [-1,1]. Then the location of the user is calculated using (7),

$$U_{loc}^{*} = R(ny)_D \quad (7)$$

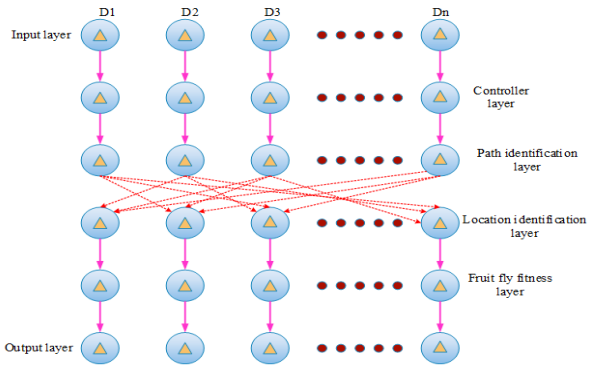

Fig. 4. Proposed FFUDAS Layer.

Here, U_{loc}^{*} is the location of user, and $R(ny)_D$ represents the searching process of locations. Moreover, by removing the attacks, the drones were successfully delivered the medicines to the requested user. Then the medicine-delivered drones are return to drone management. The pseudocode of the proposed FFUDAS framework is shown in Algorithm 1.

Algorithm 1: Proposed FFUDAS framework

```
Start
{
    Initialize: D1,D2,D3
    // here D1,D2,D3 are the used drones
      Information gathering process ()
       {
          user ⟶ requirements + location ⇒ S*m
        // here S*m denotes the storing and memory layer
    Analyze ⇒ requestor needs (subject)
     // analyzing the needs of requestor: requested things
       if (subject ⇒ medicine}
        {
          Medicine requested user
        }else (other things)
     Location identification process ()
     {
          int D → Daxis,i                    // using (3)
              // here D is the drone controller
     }
    Identification of attack ()
    {
        UAV → l*t + m(a)
        // here l*t represents the location of attack and m(a) represents the presence of attack
    }
       UAV working frame
       {
          int R, S;
            // here R is drones travel initiating point and S is the location of target
          Start (R) → End (S)
        start (R) =drone l*c; end (S) = requestor l*c
        // here l*c represents the location
     Drone ↔ requestor = initial ↔ ending
       // by defining the location of requestor, the initial and ending time of drone is fixed
       Return ⇒ starting point
       }
         Performance evaluation
}
    Stop
```

The travelling time of the drone from starting point to the target attaining point is determined using (8),

$$\eta^t = S_{ty} - E_{ty} \Rightarrow \min\_distance \quad (8)$$

Where, η^t represents the time taken to deliver the medicine to the requestor, S_{ty} denotes the drone starting time for medicine delivery, and E_{ty} represents the time at which the medicine was delivered in the correct location of the requestor. Furthermore, the drone speed depended on the weather condition, if the atmosphere has a high range of humidity, then the drone speed is low. Also, it takes more time to reach the target location. In addition, the flow chart of the proposed FFDUAS framework is shown in Fig. 5.

The presented FFUDAS model removes the malicious attacks from the nodes and creates a new path to deliver the medicine to the requested user. By removing the attacks, the paths were cleared and it delivered the medicine safely to the requestor location.

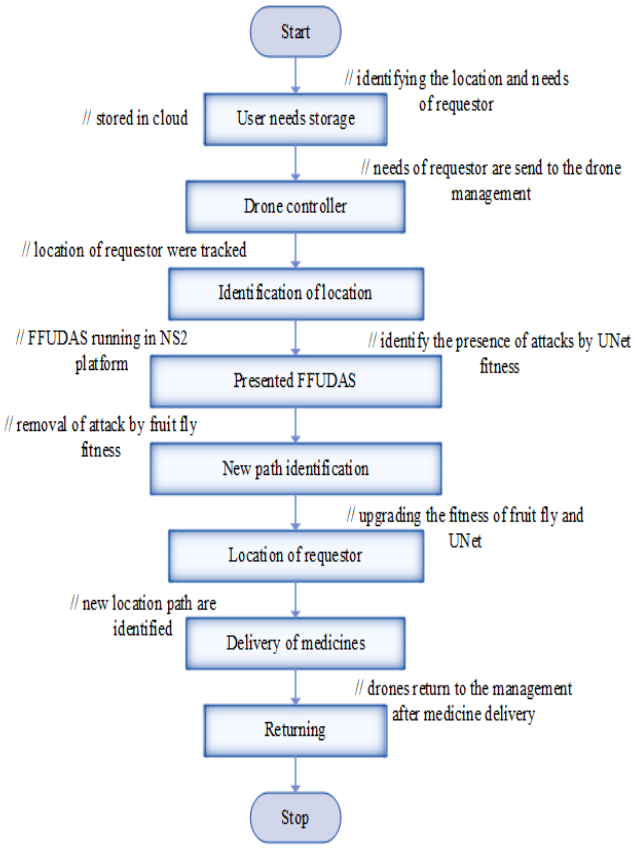

Fig. 5. Flow Chart of Proposed FFUDAS.

V. Result and Discussion

The presented research work is executed in the NS2 platform and running in the UBUNTU OS platform. Initially, the required number of nodes is designed with required labels; in these, some nodes are requested nodes (medicine), drone nodes, drone controller nodes and other normal nodes. In this process, initially, the requestor's needs and locations are stored in the memory of the cloud. Moreover, in the NS2 platform, the cloud memory is named as drone controller or drone management. The stored details are trained to the drones for medicine delivery to the target location of the requestor.

For numerical solutions, there are several optimizations, but the reason for selecting this particular fruit fly algorithm is to find the new path for the target location and to identify the location of attacks. The correlation of fruit fly and UNet removes the attack from paths and develops a new pathway. Generally, the fitness of the fruit fly algorithm is based on the location search. This reason has turned the interest to make use of fruit fly in this research.

A. Case Study

To validate the robustness of the presented model, 130 nodes are designed initially in the NS2 environment. According to this current research, the 130 nodes are considered as users and 6 nodes are requestors which are mentioned in sky blue color. The requestor needs are stored in the memory of the cloud that hub is colored as blue. The presented FFUDAS model node is represented in light brown color.

Moreover, to train the drones, drone management is required and it is represented in green color. Here, 3 nodes were totally used as a drone, which is mentioned in rose color. The node designed frame in NS2 is shown in Fig. 6.

Furthermore, after training the user location and requests to the drone, it has initiation the finding process of location, which is shown in Fig. 7. After the identification of paths, GPS helps to identify the location. The identified request or location frame is shown in Fig. 8.

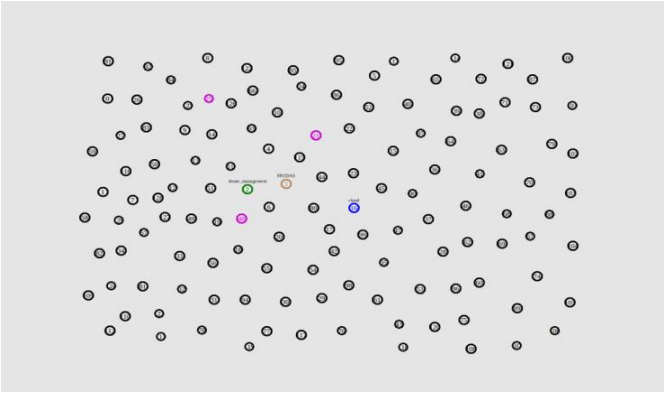

Fig. 6. Node Designed Frame.

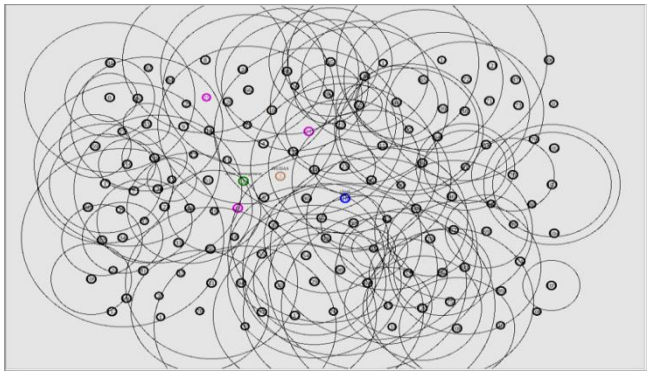

Fig. 7. Location Searching Frame.

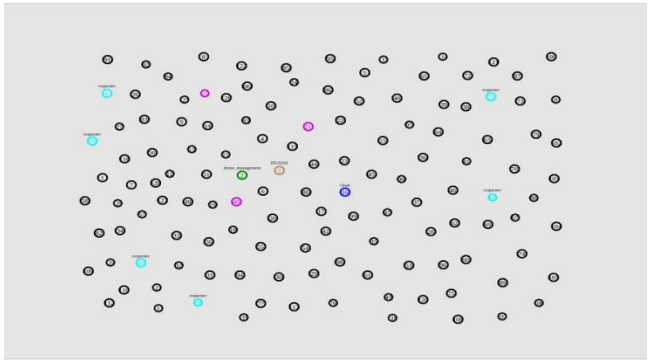

Fig. 8. Identified Requestor Location Frame.

After the identification of the requestor location, the drones were moved through the location. While the drone attempts to reach a zone, the malicious attack i.e., DoS (Denial of Service) like AUTH attack was happened. Moreover, the presented DoS attack was mentioned in red color and it is removed by the presented FFUDAS model. Moreover, the designed attacks and removed attacks in the designed frame are shown in Fig. 9 and 10, respectively.

Finally, the initiated drones have reached the destination and delivered the medicines after the removal of attacks which is represented in Fig. 11. When the things delivered, then the drone returns to the location of drone management, where it has been started.

The green color indicates the medicine delivered to the particular requestor. After delivery of medicines, the drones return to the drone management is represented as pink color.

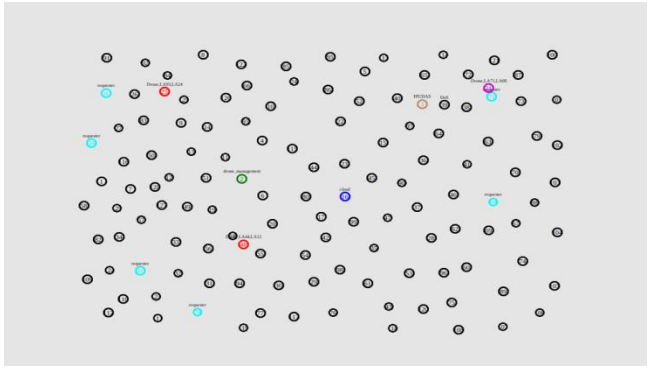

Fig. 9. Attacks in Designed Frame.

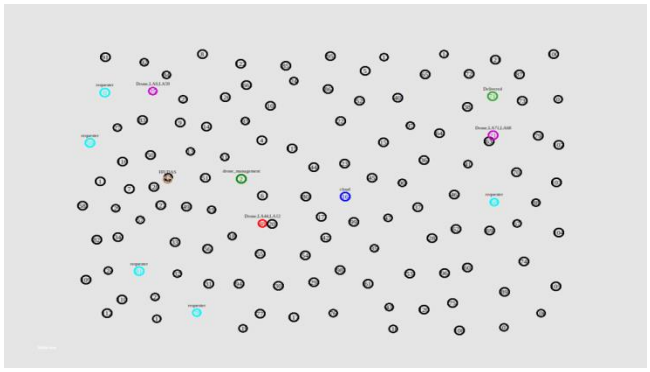

Fig. 10. Removed Attacks in Frame.

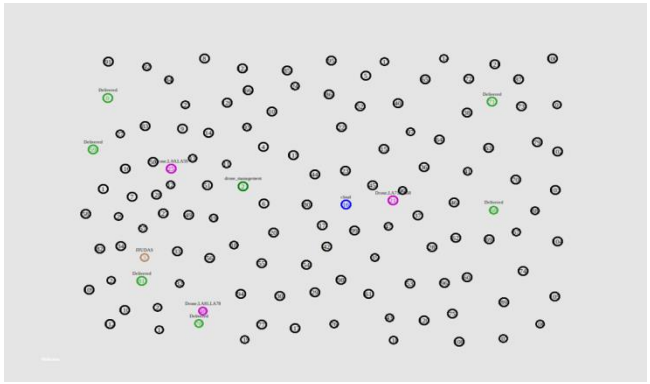

Fig. 11. Request Delivered.

B. Performance Evaluation

To validate the presented FFUDAS models proficient score, the function validation is a crucial task. Moreover, the robustness and working of the designed model were analyzed by evaluating the key metrics with different data counts. Hence, the metrics like data delivery rate (DDR), confidential rate, handover delay, execution time, packet reception rate (PRR), and energy consumption were validated for the different data counts.

1) Data delivery rate (DDR) and packet perception rate (PPR): Data delivery rate is defined as the ratio of a difference between the number of data sent and the number of data bounces to the number of data sent. It is calculated using (9),

$$DDR = \frac{N_{ds} - N_{db}}{N_{ds}} \quad (9)$$

Where, N_{ds} represents the total number of sent data and N_{db} denotes the total number of data bounces. The obtained DDR are shown in Fig. 12 and the results obtained are shown in Table II.

The packet perception rate is defined as the ratio of the number of packets delivered in the target location to the number of packets sent to the target location. It is expressed in (10):

$$PPR = \frac{\sum D_{p.t}}{\sum S_{p.t}} \quad (10)$$

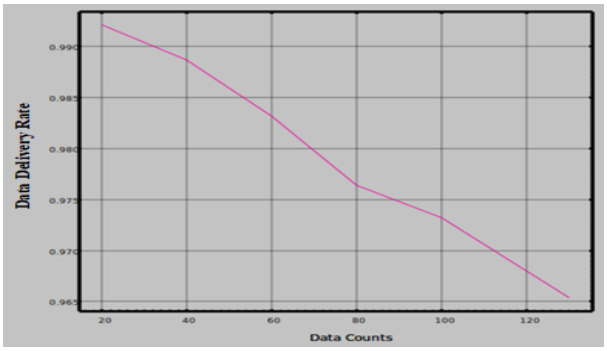

Fig. 12. Data Delivery Rate.

TABLE II. OBTAINED DATA DELIVERY AND PACKET PERCEPTION RATE

Sl.no	Data count	DDR	PPR
1	20	0.9921	0.98
2	40	0.9887	0.975
3	60	0.9832	0.951
4	80	0.9764	0.932
5	100	0.9732	0.925
6	130	0.9654	0.918

Where, $\sum D_{p.t}$ represents the total number of packets delivered to the requestor and $\sum S_{p.t}$ represents the total number of packets sent to the requestor. Moreover, the obtained PPR at different data counts is shown in Fig. 13.

The results indicated that the presented model has higher DDR and PPR at 130 nodes. The proposed framework has the finest result in both data delivery and packet perception rate. The DDR and PPR has attained mean as 0.98, and 0.95, respectively, which are effective for successive data sharing.

2) Execution time and Handover delay: The length of the time needed to perform a complete process is known to be execution time. It is also known as computation time or running time. Moreover, it is proportional to the rule applications. Its unit is meter second and the time obtained to complete the process in different data counts is shown in Fig. 14.

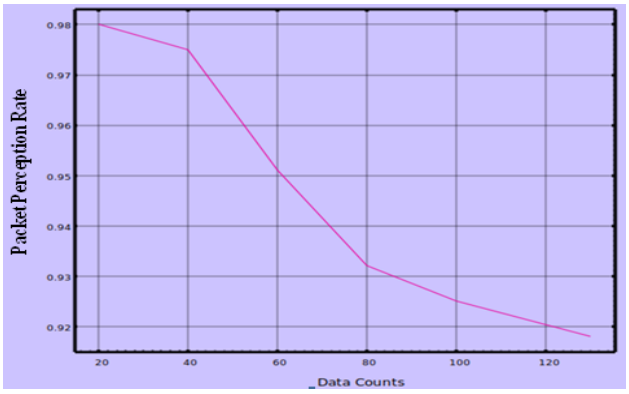

Fig. 13. Obtained PPR at different Data Counts.

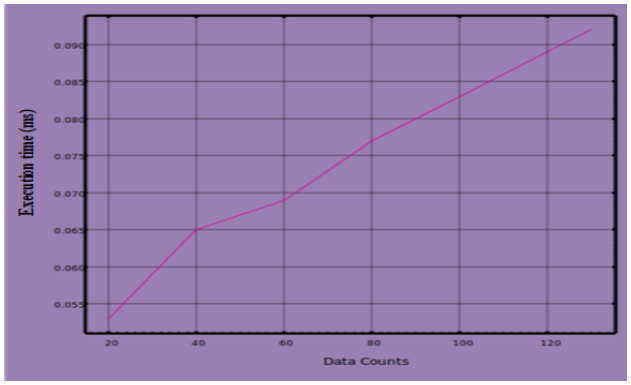

Fig. 14. Execution Time in different Data Counts.

Due to attacks, the delivery of the material was delayed to the requestor from the setting time. However, the presented FFUDAS framework has less handover delay due to removal of attacks in the network. Furthermore, the obtained result of execution time and handover delay is shown in Table III.

TABLE III. RESULT OF EXECUTION TIME AND HANDOVER DELAY

Sl.no	Data count	Execution time (ms)	Handover delay (ms)
1	20	0.053	0.2
2	40	0.065	0.25
3	60	0.069	0.39
4	80	0.077	0.4
5	100	0.083	0.5
6	130	0.092	0.8

Moreover, handover delay is the time, which taken for redirecting the ongoing location, when the node changes its point from one location to another. The obtained handover delay is shown in Fig. 15 and its unit is meter second (ms).

3) Confidential rate and energy consumption: In contrast, when the drone is close to the requested user, the drone usually slows down and it increases the transmission power for the confidential data rate. The confidential data rate is high at 20 data counts and less at 130 data counts. Moreover, the test results of confidential rate and energy consumption at different data counts is shown in Table IV.

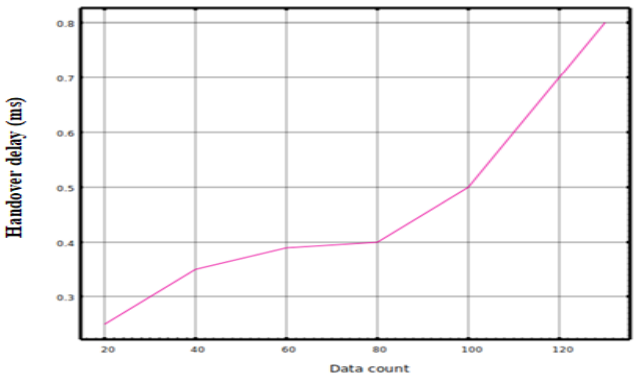

Fig. 15. Handover Delay at different Data Counts.

TABLE IV. RESULT OF ENERGY CONSUMPTION AND CONFIDENTIAL RATE

Sl.no	Data count	Confidential data rate (Mbps)	Energy consumption (Joule) $\times 10^4$
1	20	130	2.10
2	40	125	2.12
3	60	120	2.16
4	80	110	2.18
5	100	100	2.22
6	130	95	2.25

Furthermore, the accumulated test result of confidential data rate and the energy consumption is shown in Fig. 16 and 17 respectively. The result indicated that the presented model has less energy consumption in all the nodes and the confidential rate were decreased gradually due to the elimination of attack nodes.

In UAVs, the important part is energy consumption; the drone with less energy consumption only reaches the target location without any delay. The energy of drones receives through wireless charging, which is utilized to process the user's tasks in the drone coverage area. The unit of energy consumption is joule.

Energy consumption is evaluated for determining how much energy is being consumed by the FFUDAS framework. The result demonstrated that the presented framework consumes less energy over a large distance. Normally, due to changes in weather conditions, the drone consumes higher energy.

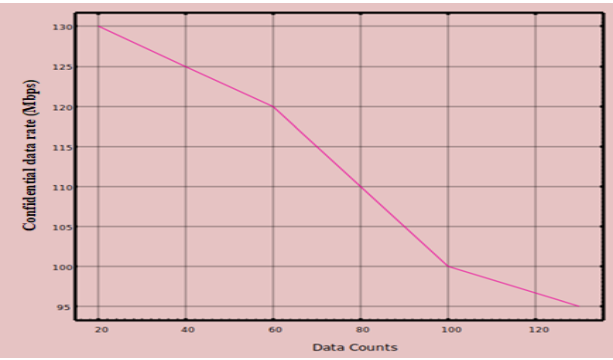

Fig. 16. Confidential Data Rate.

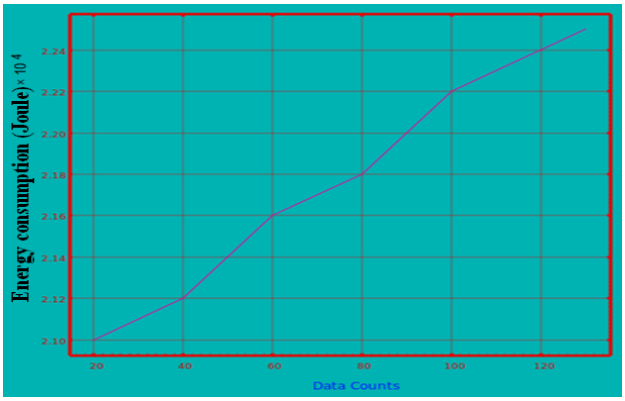

Fig. 17. Energy Consumption.

C. Comparative Analysis

The performance of any application can be valued by validating the chief metrics like throughput, execution time, and handover delay. To identify the effectiveness of the presented research work, the presented model was compared with other existing models like DDPOS [21], BSD2C-IoD [22], BACS-IoD [28], and SDN-MIH [29]. The comparison result is shown in Table V.

The comparison result indicated that the presented model has higher throughput than other models. The presented FFUDAS model has attained the throughput of 0.96 Mbps, DDPOS has attained the throughput as 0.000275 Mbps, and SDN-MIH-UAV has attained 0.167 Mbps as throughput. The comparison of throughput and handover delay is shown in Fig. 18.

From the comparison result, the attained handover delay of the proposed FFUDAS model was 0.423ms, DDPOS was 0.425ms, and SDN-MIH-UAV was 3.02ms. The result indicated that the presented model has less handover delay than other existing works. Moreover, the comparison of execution time with other existing models is shown in Fig. 19.

Moreover, the yielded execution time of the presented FFUDAS model was 0.073ms, DDPOS was 5.57ms, BSD2C-IoD was 0.97 and BACS-IoD was 1.33ms. The comparison result demonstrated that the presented model has less execution time than other models.

TABLE V. COMPARISON OF METRICS WITH EXISTING WORKS

Sl.no	Techniques	Throughput (Mbps)	Execution time (ms)	Handover delay (ms)
1	DDPOS [21]	0.000275	5.57	0.425
2	BSD2C-IoD [22]	-	0.97	-
3	BACS-IoD [28]	-	1.33	-
4	SDN-MIH-UAV [29]	0.167	-	3.02
5	Proposed (FFUDAS)	0.96	0.073	0.423

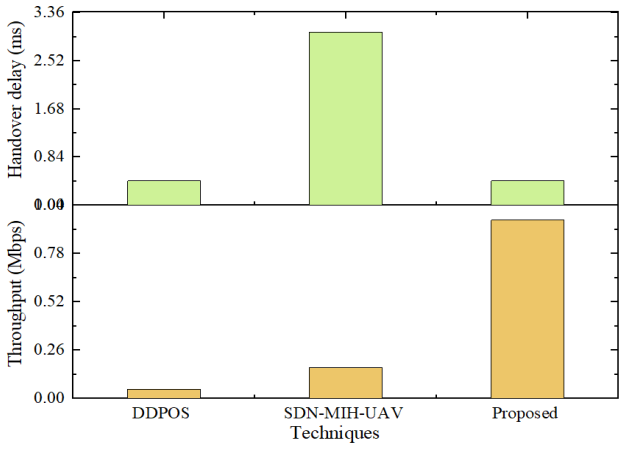

Fig. 18. Comparison of Throughput and Handover Delay.

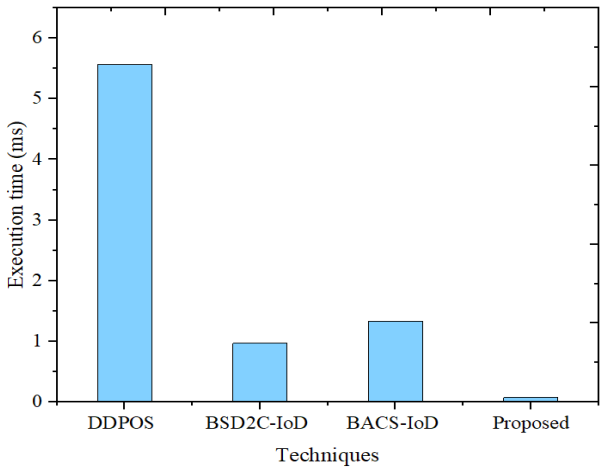

Fig. 19. Comparison of Execution Time.

D. Discussion

The outcome of the designed model has gained the finest results in all key metrics, which shows the effectiveness of the model. Also, the present research method's plan will help to enlarge the smart city applications. Moreover, the presented model has less execution time of 0.073ms. So, considering that the proposed FFUDAS technique has gained the best outstanding results within a short duration. The proposed FFUDAS overall performances mean is shown in Table VI.

TABLE VI. OVERALL PERFORMANCE OF FFUDAS

Performance of FFUDAS	
Parameters	**Obtained score**
DDR	0.98
PPR	0.95
Execution time (ms)	0.073
Handover delay (ms)	0.423
Confidential data rate (MbPS)	113
Energy consumption x 10^4 (Joule)	2.17

Hence, the presented model is applicable to supply medicines through drones and adoptable for monitoring and removing attacks. The novel FFUDAS takes average 0.98 as DDR that is high; the techniques with high data delivery rate are applicable for smart city applications.

VI. CONCLUSION

To ensure secure communication and less delay between UAVs in a smart city, the process of authentication must be established properly between the requestors in each zone. In some cases, the security of drones is a complex problem due to attacks. Moreover, the presented research has developed an FFUDAS model to remove and identify the attacks. The fitness of fruit fly is upgraded in the location identification layer to gain the finest results. Finally, the robustness of the presented model was evaluated by measuring the metrics like data delivery and packet perception rate, confidential data rate, execution time, energy consumption and handover delay. In all metrics, the presented FFUDAS model has yielded better results by attaining 0.96 Mbps throughput, 0.073 ms execution time and 0.423 ms hand over delay. By comparing with other models, the presented model has attained the finest outcome.

REFERENCES

[1] A. Khanna, and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," Wirel. Pers. Commun. vol. 114, pp. 1687-1762, 2020.

[2] A. Aslam, U. Mehmood, M. H. Arshad, A. Ishfaq, J. Zaheer, A. Ul Haq Khan, and M. Sufyan, "Dye-sensitized solar cells (DSSCs) as a potential photovoltaic technology for the self-powered internet of things (IoTs) applications," Sol. Energy, vol. 207, pp. 874-892, 2020.

[3] R. Yugha, and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," J. Netw. Comput. Appl. pp. 102763, 2020.

[4] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, and A. Vaish, "Industry 4.0 technologies and their applications in fighting COVID-19 pandemic," Diabetes Metab. Syndr.: Clin. Res. Rev. vol. 14, no. 4, pp. 419-422, 2020.

[5] M. M. Nair, S. Kumari, and A. K. Tyagi, "Internet of Things, Cyber Physical System, and Data Analytics: Open Questions, Future Perspectives, and Research Areas," Proceedings of the Second International Conference on Information Management and Machine Intelligence, Singapore: Springer, 2021.

[6] F. Al-Turjman, M. Abujubbeh, A. Malekloo, and L. Mostarda, "UAVs assessment in software-defined IoT networks: An overview," Comput. Commun. vol. 150, pp. 519-536, 2020.

[7] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Veh. Commun. vol. 23, pp. 100249, 2020.

[8] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," IEEE Access, vol. 8, pp. 43711-43724, 2020.

[9] P. Boccadoro, D. Striccoli, and L. A. Grieco, "An extensive survey on the Internet of Drones," Ad Hoc Netw. vol. 122, pp. 102600, 2021.

[10] C. Xu, X. Liao, J. Tan, H. Ye, and H. Lu, "Recent research progress of unmanned aerial vehicle regulation policies and technologies in urban low altitude," IEEE Access, vol. 8, pp. 74175-74194, 2020.

[11] Z. Qadir, F. Ullah, H. S. Munawar, and F. Al-Turjman, "Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review," Comput. Commun. 2021.

[12] S. Garg, G. S. Aujla, A. Erbad, J. J. P. C. Rodrigues, M. Chen, and X. Wang, "Guest Editorial: Blockchain Envisioned Drones: Realizing 5G-Enabled Flying Automation," IEEE Netw. vol. 35, no. 1, pp. 16-19, 2021.

[13] H. Teng, M. Dong, Y. Liu, W. Tian, and X. Liu, "A low-cost physical location discovery scheme for large-scale Internet of things in smart city through joint use of vehicles and UAVs," Future Gener. Comput. Syst. vol. 118, pp. 310-326, 2021.'

[14] M. Aloqaily, O. Bouachir, A. Boukerche, and I. Al Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," IEEE Netw. vol. 35, no. 1, pp. 64-71, 2021.

[15] A. S. Khan, G. Chen, Y. Rahulamathavan, G. Zheng, B. Assadhan, and S. Lambotharan, "Trusted UAV network coverage using blockchain, machine learning, and auction mechanisms," IEEE Access, vol. 8, pp. 118219-118234, 2020.

[16] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, Deployments, and Integration of Internet of Drones (IoD): A Review," IEEE Sens. J. 2021.

[17] D. S. Prashanth, J. Swamy, and S. S. Rao, "Internet of Things and Web Services for Handling Pandemic Challenges," Sustainability Measures for COVID-19 Pandemic, Singapore: Springer, 2021, pp. 1-19.

[18] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, and G. H. Cho, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," Sustain. Cities Soc., vol. 63, pp. 102364, 2020.

[19] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," Comput. Commun. vol. 166, pp. 91-109, 2021.

[20] J. Chen, W. Wang, Y. Zhou, S. H. Ahmed, and W. Wei, "Exploiting 5G and blockchain for medical applications of drones," IEEE Netw. vol. 35, no. 1, pp. 30-36, 2021.

[21] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," IEEE Internet Things J. vol. 8, no. 8, pp. 6406-6415, 2020.

[22] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," IEEE Trans. Veh. Technol. vol. 69, no. 8, pp. 9097-9111, 2020.

[23] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles," IEEE Access, vol. 9, pp. 115466-115487, 2021.

[24] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges," IEEE Access, vol. 9, pp. 57243-57270, 2021.

[25] M. Tanveer, N. Kumar, and M. M. Hassan, "RAMP-IoD: A Robust Authenticated Key Management Protocol for the Internet of Drones," IEEE Internet Things J. 2021.

[26] Y. Fan, P. Wang, A. A. Heidari, M. Wang, X. Zhao, H. Chen, and C. Li, "Rationalized fruit fly optimization with sine cosine algorithm: a comprehensive analysis," Expert Syst. Appl. vol. 157, pp. 113486, 2020.

[27] H. Huang, L. Lin, R. Tong, H. Hu, Q. Zhang, Y. Iwamoto, X. Han, Y. W. Chen, and J. Wu, "Unet 3+: A full-scale connected unet for medical image segmentation," ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2020.

[28] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," Comput. Commun. vol. 153, pp. 229-249, 2020.

[29] S. Goudarzi, M. H. Anisi, D. Ciuonzo, S. A. Soleymani, and A. Pescapé, "Employing Unmanned Aerial Vehicles for Improving Handoff using Cooperative Game Theory," IEEE Trans. Aerosp. Electron. Syst. vol. 57, no. 2, pp. 776-794, 2020.