

# Black Box Logging System for Drones

Smrithi.S<sup>#1</sup>, Ms.Vijayalakshmi .R<sup>#2</sup>, Dr.Veeralakshmi.P<sup>#3</sup>

<sup>#1</sup>Student, Department of Information Technology, Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar, Chennai, India.

<sup>#2</sup>Assistant Professor, Department of Information Technology, Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar, Chennai, India.

<sup>#3</sup>Associate Professor, Department of Information Technology, Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar, Chennai, India.

## Abstract

Unmanned aerial vehicles (UAVs) like drones are in dire need of efficient data retrieval and regular updates. This project aims to create a software use a fully autonomous system for the effective functioning of drones either implicitly or partially independent of human control. The implementation is done by providing access only to any one of two designated aviation controller who is given with an irreplaceable token by the Administrator at a time using an asymmetric cryptographic algorithm-RSA Algorithm. This algorithm ensures the avoidance of vulnerability to the drone system. The goal of the proposed research architecture is to provide the recovery mechanism for the obstacles encountered by the drones in the real-time scenarios and momentary payload information. This approach will be further evolved based on adaptive learning software (SCENGEN) to facilitate the drones with appropriate solutions for wisely dealing with the security attacks such as repudiation, masquerade during its fly time. The drone's momentary payload information is gathered with respect to three scenarios namely: Target Reached, Midway Hurdle encountered and Hacking of drone control is finally embedded in the Black Box cloud.

**Keywords:** Unmanned Aerial Vehicles (UAVs), Adaptive Learning, Artificial Intelligence Cryptography and network security, Deep Learning, Database and Cloud computing.

## I. INTRODUCTION

The multifarious drones are differentiated in terms of their level of autonomy, the maximum flight duration and security. These specifications play a vital role in determining the efficiency and efficacy of the drones. Drones also include a vivid type of payloads (Camera, Sensor, GPS location, flight controls, freight, etc.) which reckon the whereabouts and its factors lead to an expected and good performance measure. There is a need for communication between the drone(s) and its aviation controller through fixed signal strength to avoid interference prompted by any unwanted glitches. Existing studies which attribute to determine flight distance of drones by using trajectory motions, sensor locations, among others.

## 1. Levels of Autonomy

The momentous distinction in the levels of autonomy is with respect to unmanned systems are automatic and autonomous systems. Automatic systems are fully pre-programmed systems that can perform a pre-programmed assignment on its own. Automation also includes flight stabilization. Autonomous systems can deal with unexpected situations by using a pre-programmed rule-set to help them make appropriate decisions. A higher level of autonomy is a human delegated system that can perform many functions independent of human control, i.e., it can perform tasks when delegated to do so. The next level of autonomy is a human-supervised system that can perform various tasks when it is given certain permissions and directions by a human. The final level of autonomy is a fully autonomous system that receives commands input by a human and translates it into specific tasks without further human interruption [1].

## 2. Types of Payloads and its Utility

The most important category of payloads in UAVs is sensors. This sort of sensors is being used to the drones of present security techniques equipped with cameras and microphones. Such cameras may enable night vision and heat sensing. Other sensors include location sensors – it is to locate the current location of the drones, biological sensors – trace microorganisms, chemical sensors – also called as sniffers which measure chemical compositions and trace of particular chemical substance such as radioactive substance and meteorological sensors that can measure wind, temperature, humidity, etc [1].

These types of cameras are used for criminal investigation, military, freight, live surveillance, inspection and maintenance of infrastructure, cinematography, science and infotainment and archaeology .Law enforcement applications are not restricted to the use of cameras. For instance, heat sensors may be useful for detecting influx to other countries. In the security domain drones are useful as observation as well as surveillance instruments which are distinguished with three mechanisms: non active systems, in which cameras work as a visual deterrent by using fake cameras to create the illusion of surveillance without monitoring or storage; reactive

systems, which have recording, storage and playback facilities for an event related to fatal incidents; proactive systems with live surveillance from a dedicated control room with recording, storage and playback facilities allowing, for an immediate response to incidence as they occur[1].

The paper is stratified as follows: Section II describes the Literature Review of the Existing System. Section III presents the Proposed System. Section IV presents the experimental results of the drones.

## **II. LITERATURE REVIEW**

In the Existing System, the drones are operated automatically and it has been controlled by either a non-active system or a reactive system. The frequency spectrum is provided on a national basis and facilitated by Licence Free Spectrums.

The flight characteristics and the payloads depending on the Level of Autonomy of the drones. The drones can only be controlled in a minimum calculated distance. As the momentary data from the payload of the drones are unable to access by the aviation controller, the cause of drone's damage is unknown. The level of autonomy has not increased to the higher level. i.e., no drones in the last 2 decades have used a human delegated system or beyond.

Drones are often seen as remote control aircraft, but there are technologies that enable autonomous operations, in which the remote control by a human operator is partially or completely excluded. Most drones that are commercially available are remotely controlled, but at the same time they already contain elements of autonomy, mostly software for flight stabilization. More professional drones offer the possibility to pre-program flights. In the near future, more autonomy is expected with regard to determining flight routes, sense and avoid systems for performing evasive maneuvers (e.g., birds, airplanes), adapting to changing weather conditions and defensive reactions when drones are under attack [1].

ScenGen extends a human's ability to think of all possibilities for any given situation by over tenfold. ScenGen has broad applicability which is most commonly used to exhaustively "think of" and then "execute" all user actions or systems message. This technology has been proven to work successfully in most complexes of environments to eliminate issues with new releases that would otherwise cause damage, downtime or misinformation such as memory exceptions, memory leaks, crashes, failed installations . The use of Adaptive Learning - ScenGen Software for achieving a fully autonomous drone with less complex sensors and low computational and processing power for adaptive obstacle detection in real world environments and collecting data from the damaged drones. [2],[4].

A drone directly communicates with one or a few rendezvous nodes because it is impossible to communicate with all sensor nodes directly. Earlier schemes only focus on the drone's energy and flight distance with pre-acquisition information. A new rendezvous point estimation scheme is proposed which takes into account the drone's speed and direction as well as the data collection delay of the entire network without any pre-acquisition information. We designed the rendezvous node selection steps with the new approach and verified the performance of the proposed scheme through a simulation. The simulation results show that our scheme is more reliable than other schemes in terms of the drone speed and data collection delay [3].

There are diverse sorts of drone services that can be executed in various situations. For instance, a drone can act as a security monitor to ensure the safety of somebody strolling home alone around evening time or a drone can act as a flying camera that can be leased basically by calling the drone to go to a particular area to take photographs or to record videos. Another scenario is a drone that can be used to deliver computing services [5].

Deep learning is a fast-growing domain of machine learning, mainly for solving problems in computer vision. It is a class of machine learning algorithms that use a cascade of many layers of nonlinear processing. It also part of the broader machine learning field of learning representations of data facilitating end-to-end optimization. Deep learning has ability to learn multiple levels of representations that correspond to hierarchies of concept abstraction [6].

Numerous commercial interests are developing UTM instrumentation for compliant and non-compliant drone detection and counter measures, but performance in terms of ability to detect, track, classify(bird, bug, drone, general aviation), identify, and localize aerial objects has not been standardized or well developed to compare multi sensor solutions [7].

Passive methods have its attraction in simplicity, reliability, low cost and require no additional power. Drones can fly automatically and can be controlled at certain elevations and are usually equipped with sensors or cameras to detect and playback record objects underneath. It is easy-to-learn way of operation makes many people use drones in different fields. The use of drones can now be used to support daily living needs such as the use of drones for military security, interpersonal services, research or field exploration, watering or spraying plant pesticides, using drones to take pictures of an area and much more [8],[9].

The high-level modules in this architecture are: (i) the user interface; (ii) the ground station comprising mission control, mission planning, and sensor data analysis; i.e., coordination; (iii) a communication

infrastructure; and (iv) the UAVs with their on-board processing and sensing capabilities. (Fig.2) [10].

### III. PROPOSED SYSTEM

The main intention is to emasculate overtly the vulnerability in order not to hack the drones. With the active help of a higher Level of Autonomy (Fully Autonomous Systems) for the effective functioning of drones either implicitly or partially independent of human control. The accessibility to Fully Autonomous Systems is, in a sense, given only to one aviation controller authenticated by the Administrator through an irreplaceable RSA Token at a time (Fig.1). In addition, a unique Software Program is used to generate all possible scenarios for any given situation at a very high speed (ScenGen). The said Software is predominantly used for recovering the payload information of the drones gathered instantly during any snags or aberration which had been embedded in the Black Box Cloud. This uses Regression testing to avoid deadlocks and external mishaps. The system architecture is appended in Fig.2.

#### A. User Authentication

User Authentication (see Fig.1) is a plug-in that collects user information such as a user ID and password and compares the information against entries in a database. Only if the aviation controller is bona fide with valid data then he is granted permission to go ahead with the controlling of the drones.

The User Authentication is classified into 3 (three) sessions viz.

1. Authenticated user verification.
2. RSA Token generation.
3. User Accessibility through the generated RSA token.

The general details of the above-mentioned sessions are illustrated as the Administrator authorizes only two aviation controllers with the RSA token to control the drones which are implemented by using an Asymmetric key cryptographic algorithm- **RSA Algorithm**. If the member who tries to get control over the drone is not the assigned member then he/she may be routed to the log in page and start again. If the member is authorized by the Administrator, then he/she is given with the RSA token with last for only 12-15 seconds. If the member is unable to log in within the session time then he is provided with another the RSA token with is also updated in the Local Database of the Administrator.

In particular, for network security purpose the **RSA Algorithm** can be mentioned vividly as follows:

1. A random 8-digit token is generated as a password for the designated aviation controller one at a time which lasts for only 12 seconds ensuring the avoidance of timing attacks of **RSA Algorithm**.

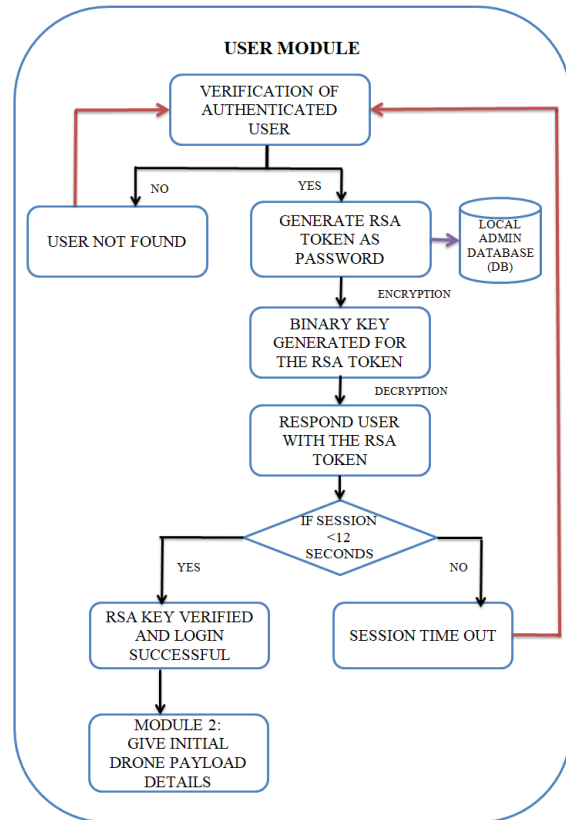


Fig.1: Workflow of User Authentication

2. In the first instance, this 8-digit token is encrypted using the public key of the aviation controller sent to the Administrator in order to get hold of a random 8-bit binary key.
3. Secondly, the aviation controller receives the encrypted key and decrypts it by using his private key and logs in to activate the drones.
4. This RSA Token is unique and irreplaceable to both aviation controllers.

#### B. Initial Drone Activation Details

Initial Drone Activation Details includes the following specifications:

##### I. SOURCE

1. Name of the drone.
2. Purpose of launch.
3. Location of launch in latitude and longitude.

##### II. DESTINATION

1. Location of a target in latitude and longitude.

##### III. VERTICAL SPEED (VS).

##### IV. HORIZONTAL SPEED (HS).

The Initial Drone Activation Details are manually given by the aviation controller to launch the drones. Horizontal and vertical Speed is given to

avoid initial turbulence due to imbalance or human error.

**C. Private Database Initial Payload Information**

The drone's payload information is stored in the private database of the aviation controller and the Black Box cloud. This is done to identify the source, destination and purpose of drones (criminal investigation, military, freight, live surveillance, inspection and maintenance of infrastructure, cinematography, science and infotainment and archaeology.)

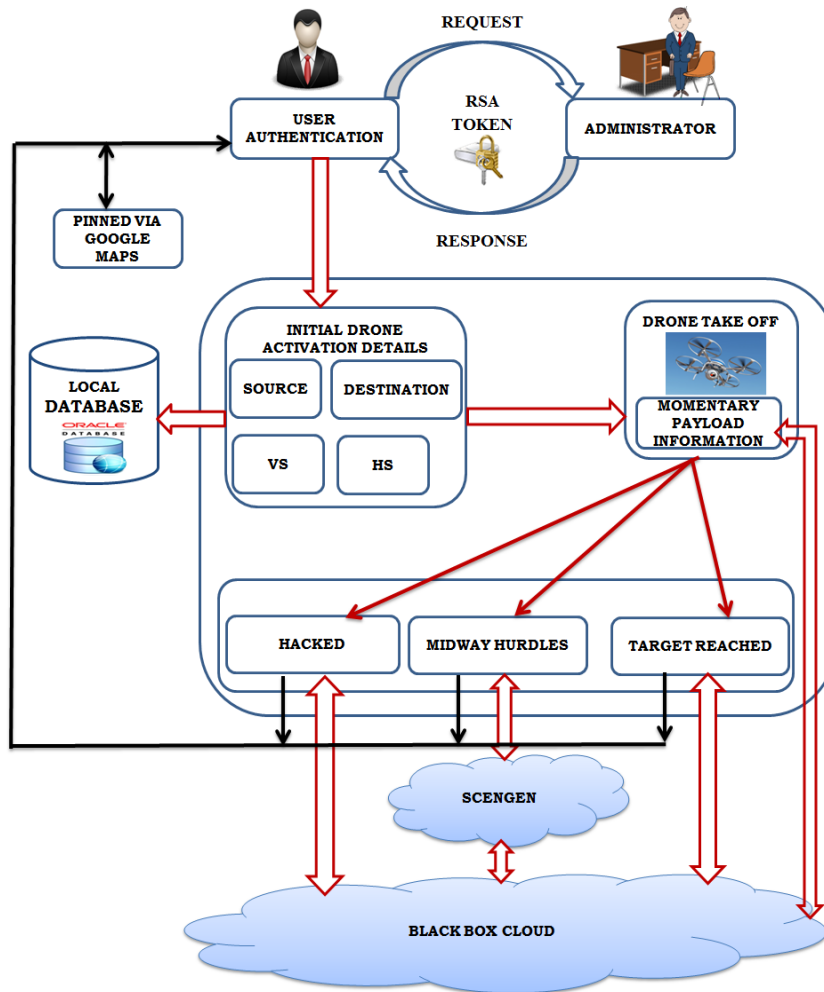
**D. Black Box Cloud**

The Black Box Cloud consists of the momentary payload information of the drones which is obtained from communicating with the drones payload and the type of destruction encountered en route to its target if any. The solution to the unexpected situation which may be expected by the drones is given by the Adaptive Learning-ScenGen software. ScenGen extends a human's ability to think of all possibilities for any given situation by over tenfold. ScenGen has

broad applicability which is most commonly used to exhaustively "think of" and then "execute" all user actions or systems message. This technology has been proven to work successfully in most complexes of environments to eliminate issues with new releases that would otherwise cause damage, downtime or misinformation such as memory exceptions, memory leaks, crashes, failed installations [2]. ScenGen contains the possible ways in which a drone can get damaged such as Weather condition, Bird strike, Crash landing, Sniper shot, Stone throw, Hacking and Improper signal using advanced AI in Adaptive Learning and provide the best solution for these damages caused to the drones. The Black Box cloud also consists of the path in which the drones travel to reach the stipulated target.

**E. Last Sync Location Retrieval**

The last sync location is retrieved from the Black Box Cloud and pinned via a Google Map with the cause of drone destruction, if any, en route to the target.



**Fig.2: Workflow of the Proposed System**



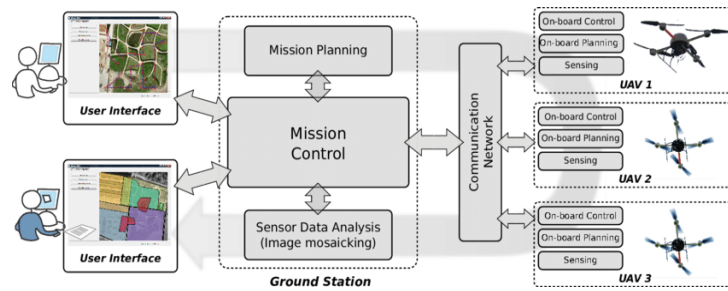


Fig.3: Drone Network Architecture [10]

IV. EXPERIMENTAL RESULTS

The software is programmed as a fully autonomous system based on Java and a basic processor i5 hardware requirement, in order to fly the drone with high degree of throughput. It uses a MySQL server to store the necessary information of the drones for the administrator and the aviation controller and CloudMe is used to store the momentary data of the drones with reasons of the damages caused en route to the target. The last sync location is depicted via a Google Map indicating the source and destination, also having the location where the drone has encountered an obstacle.

The performance analyses comparing the Proposed and Existing Drone System are represented as follows:

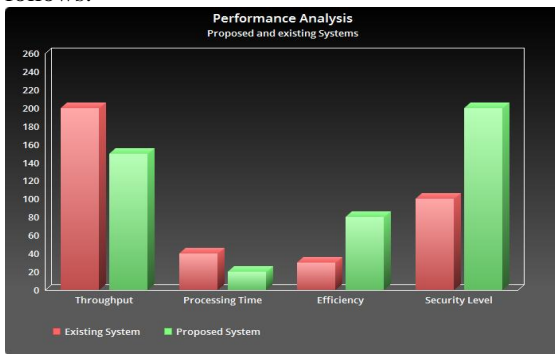


Fig.4 Performance Analyses of the Proposed and Existing Drone System.

Fig.5.1, 5.2, 5.3 results show the last sync location of the drones safely reaching the target.

Fig.6.1, 6.2, 6.3 results show the last sync location of the drones getting damaged before reaching the target.

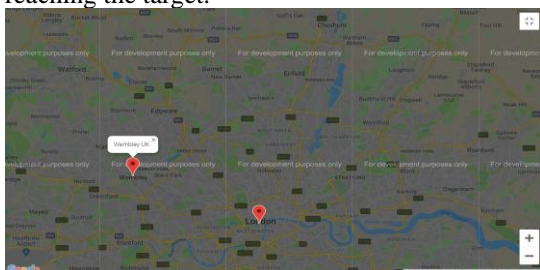


Fig.5.1: Last Sync Location of the drone safely reaching the target.

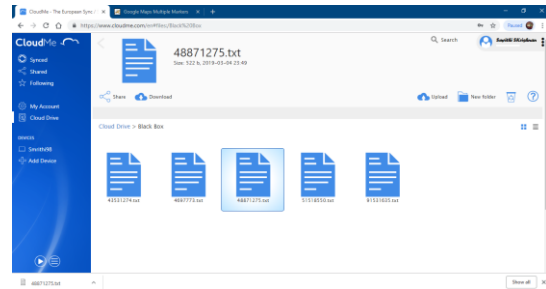


Fig.5.2: Black Box cloud having the file containing the momentary details.

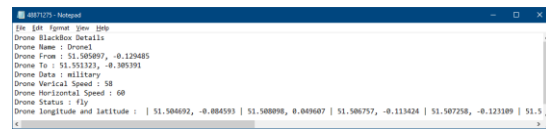


Fig.5.3: Contents of file containing the drone's momentary details and its status.

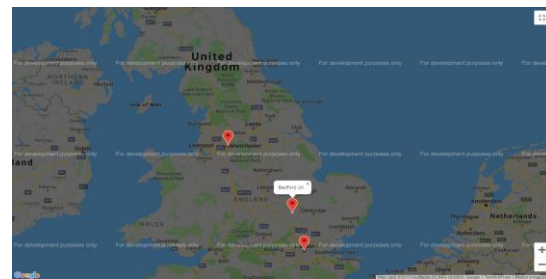


Fig.6.1: Last Sync Location of the drone damaged by Birds Strike before reaching the target.

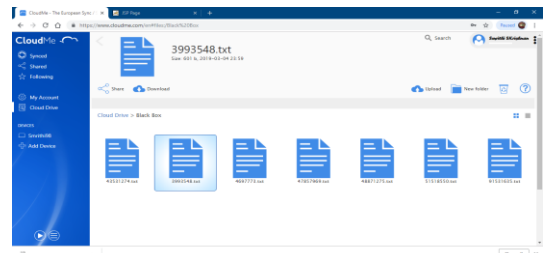


Fig.6.2: Black Box cloud having the file containing the momentary details.

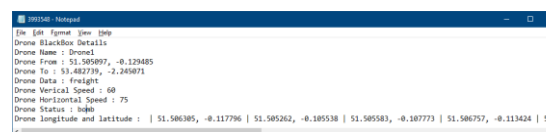


Fig.6.3: Contents of file containing the drone's momentary details and its status.

## V. CONCLUSION

This paper presents the creation of software for the Black Box Logging System in Drones for efficient retrieval of drone's momentary details without any loss of payload information.

The Adaptive Learning Software enables a user to operate drones by a fully autonomous system more efficiently for the common good in various areas of applications such as:

1. Military
2. Criminal Investigation
3. Live Surveillance
4. Aerial Photography
5. Inspection and Maintenance of Construction Infrastructure
6. Cinematography, Television and Infotainment
7. Science and Education
8. Archeology
9. Goods Freight
10. Agriculture

The further development in drone technology can be with respect to swarms embedded with Black Box System for momentary data retrieval and drone recovery is only possible when those drones are capable of rebounding back to its trajectory path.

## REFERENCES

- [1] Bas vergouw, Huub Nagel, Geert Bondt and Bart custers, "Drone Technology: Types, Payloads , Applications, Frequency Spectrum Issues and Future Developments" ,2016, B. Custers (ed.), The Future Of Drone Use, Information Technology and Law Series 27.
- [2] Scengen Product, 2011, <https://scorpioncomputerservices.com/scengen>.
- [3] Kwangsoo joa , Junyoung Heo , Jinman Jung , Bongjae Kim, Hong Min , "A Rendezvous Point Estimation considering Drone Speed And Data Collection Delay" ,2017, 4th International conference on Computer Applications and Information Processing Technology (CAIPT).
- [4] Arne Devos, Emad Ebeid, Poramate Manoonpong, "Development of Autonomous Drones for Adaptive Obstacle Avoidance in Real World Environments", 2018, 21st euro micro conference on Digital System Design (DSD).
- [5] Majed Alwateer , Seng W. Loke , Wenny Rahayu, "Drone Services: An Investigation via Prototyping and Simulation", 2018, IEEE 4th World Forum On Internet Of Things(WF-IOT).
- [6] Widodo Budiharto, Alexander A S Gunawan, Jarot S. Suroso, Andry Chowanda, Aurello Patrik and Gaudi Utama , "Fast Object Detection for Quadcopter Drone using Deep Learning" ,2018 , 3rd International Conference on Computer and Communication Systems (ICCCS).
- [7] Sam Siewert, Andalibi Mehran, Stephen Bruder, Iacopo Gentilini, Jonathan Zuchholz, "Drone Net Architecture for UAS Traffic Management Multi-modal Sensor Networking Experiments",2018 ,IEEE Aerospace Conference.
- [8] Dubravko Miljković , "Methods for Attenuation of Unmanned Aerial Vehicle Noise",2018, 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
- [9] Lukas Sada Arihta Sinulingga, Fatwa Ramdani, Mochamad Chandra Saputra, "Spatial Multi-criteria Evaluation to Determine Safety Area Flying Drone", 2017, International Symposium On Geoinformatics (ISyG).
- [10] Evsen Yanmaz, Markus Quaritsch, Saeed Yahyanejad, Bernhard Rinner, Hermann Hellwagner, and Christian

Bettstetter, "Communication and Coordination for Drone Networks", 2016.