Journal of Computer Science

Original Research Paper

Semantic Forensic Investigation Framework for Drone Field

Omair Ameerbakhsh

Department of Information Systems, College of Computer Science and Engineering, Taibah University Medina, Saudi Arabia

Article history
Received: 15-09-2022
Revised: 10-11-2022
Accepted: 24-11-2022

Email:
oameerbakhsh@taibahu.edu.sa

Abstract: The application of Unmanned Aerial Vehicles (UAVs) is extensive, with uses ranging from smart agriculture to photography, maintaining infrastructure, and disaster recovery. However, incidents involving unmanned aerial vehicles are increasing daily due to their widespread use in smart technologies. Therefore, this study focuses on the ground of drone forensic investigation to capture and investigate incidents involving unmanned aerial vehicles. To find drone incidents and identify the perpetrators, forensic drone investigation is used, such as determining when the drone incident occurred, what type of drone incident it was, and the exact moment the drone incident occurred. Several forensic models and frameworks for drones have been proposed to identify, capture and analyze various cybercrimes committed by drones. However, these works deal with drones from a technical standpoint; thus, a semantic forensic framework for unmanned aerial vehicles is required to facilitate the investigation process among domain investigators. Therefore, the objective of this study is to use the design science method to develop a semantic forensic investigation framework for drones. The designed framework includes three main abstract processes: (1) Preparation, (2) Gathering and preservation, and (3) Analysis and documentation. The qualitative technique was used to validate the designed framework (Comparison against other models). The designed framework is compared with other models to ensure that it is logical, complete, and useful in comparison to another drone forensic investigation domain models. The designed framework enables domain practitioners to easily create solution models based on their requirements. It proposed a modeling process that uses modeling rules to generate solution models.

Keywords: Drone Forensics, UAV, Metamodeling, Design Science Research, Smart City

Introduction

Unmanned Aerial Vehicles (UAVs) are now used in a wide variety of applications ranging from smart agriculture to photography, infrastructure maintenance, and disaster recovery. Many researchers are interested in UAVs due to their ability to be controlled and monitored via pre-programmed flight paths, without requiring the presence of a pilot. This technology was initially used in military and agricultural applications, but it is now serving the needs of ordinary people in their daily lives (Barton and Azhar, 2017). Smart agriculture, for example, is a product organization concept that enables agriculturalists to achieve spatial and sequential inconsistency, such as dropping natural properties in agriculture, irrigation organization, construction organization, fertilizer organization, and intrusion attacks. Over the last decade, applications based on statistical and Machine Learning (ML) algorithms have been used in classification/regression tasks. The advancement of remote sensing systems has aided in the collection of various types of data from all types of targets on the Earth's surface. Since the introduction of UAVs, aerial imaging has become a popular method of data collection (Yu *et al*., 2021a-d). This technology has primarily been used for area monitoring, surveillance, inspection, and cargo (Yu *et al*., 2021e; 2015). It has improved people's lives, particularly by monitoring public events and utilizing shared space (Tan *et al*., 2021a). In the agriculture domain, for example, the named entities include food, farm, climate, disease, and temperature. On the other hand, many challenges have arisen, such as increased airspace traffic, which has increased collision accidents in the air (Tan *et al*., 2021b). In comparison to conventional networks, the unique traffic patterns and technology of UAVs have

made dealing with congestion and incidents more difficult (Tan *et al*., 2021c; Awan *et al*., 2021). As a result of such conditions, control systems have experienced high interference, overhead, data dropping, and a variety of other anomalies. The sky is gradually filling with various types of UAVs, such as small drones and weaponized drones (Li *et al*., 2021). Small drones fly around an area of interest, monitoring vital signs and movements and transmitting the data to a base station for further decision making. Another issue is that data in such networks is widely dispersed across devices such as sensor nodes, routers, switches, and SD cards (Feng *et al*., 2021a-b; Ullah and Pun, 2021). To extract the forensic features effectively, the situation demands appropriate investigation and planning. Different components, such as the on-board Power Management System (PMS), Electronic Speed Controller (ESC), Flight Control Board (FCB), onboard ground-station controller, Transceiver Control Unit (TCU), and (multi) rotor system, are involved in the drone functionalities (Feng *et al*., 2020; Ding *et al*., 2020). The aforementioned items are thus potentially reliable sources for gathering data (Ding *et al*., 2021a). The ground station controller unit's log and memory data can be retrieved by the forensic investigator. This device might be a software platform or a specially-made base station with the ability to communicate with FCB. TCU plays a crucial role in drones (especially given that these devices are unmanned); this unit acts as an intermediary for communication and control between FCB and the base station as well as among the drone's sensors. The FCB serves as the drone's "brain" (Al-Dhaqm *et al*., 2021a; Ding *et al*., 2021b). It integrates and organizes data sent by the functional drone units (e.g., the mounted sensors, inertial measurement and controls, power management, flight trajectory, and navigation controls), as well as by corresponding with the ground-based station. The ESC is an electronic circuit house that controls the speed and monitors the overall effectiveness of the drone's movements, in addition to having several other fundamental functions (Zhou *et al*., 2022). Therefore, data stored in the memory, the contents of different log files, and Electromagnetic (EM) wave data can all be obtained as DRFI artifacts from drone devices. It is well known that the FCB and ESC are two significant potential sources of memory artifacts, which are directly extracted from the FCB and ESC's constituent parts, respectively. These parts are made up of various types of data, including flight record data, flight control data, data from mounted transceivers and sensors, and data from internal monitoring units. In general, data extraction and forensic identification processes are accomplished with the aid of signal processing techniques. However, the digital artifacts (which manifest as EM signals from the corresponding mounted sensors and transceivers) can offer additional corroborating data that could be useful in the investigation process. TCU can be used in this situation to extract primary EM signals that are then proceeded to extract secondary corroborative digital artifacts. The architecture of a UAV and the protocols supporting the communication is illustrated in Fig. 1, which forensic investigators could use to their advantage when investigating drone crimes.

The domain of DRFI is therefore complex and unstructured due to its dispersed nature and the redundant artifacts, processes, tasks, and associated activities. Consequently, there is a lack of a semantic framework or model to reduce misunderstandings and aid in the formation and organization of DRFI knowledge.

Therefore, the goal of this study is to integrate and organize the DRFI domain knowledge among domain users in an abstract framework known as the Semantic Forensic Investigation Framework (SFIF). The proposed SFIF will combine and unify all redundant tasks, artifacts, processes, and activities into reusable blocks, which are a type of abstract building block. These blocks are conceptual blocks that enable domain users to reuse them in various situations. The term "drone volatile data," for instance, may be used interchangeably with terms like "cache memory," "sensors data," "live flight data," "live camera data," etc. Additionally, the proposed semantic framework offers domain users a derivation process so they can build models according to their specifications. Besides that, it provides a centralized layer for all investigation artifacts, which facilitates domain users to understand the investigative steps when drone crime occurs.

This study contributes to the management, sharing, and reuse of DRFI domain knowledge through the proposal of a new structured and unified model (SFIF), that addresses the complexity, heterogeneity, and interoperability challenges in the DRFI field. This explicit artifact describes the entirety of the DRFI knowledge. After the research process is finished and the benefits of DRFI are explained from the viewpoint of experts, the research's findings can help domain practitioners (incident responders, investigators, examiners, and analysts) develop solution models for their problems and also offer guidance to encourage newcomers to adopt this abstract model as a framework for examining drone incidents. The strengths of the proposed SFIF towards the domain practitioners include:

1) Facilitate communication between experts in various DRFI domains by creating a common representation layer that contains all the procedures, ideas, and tasks that must be accomplished in the DRFI domain
2) Establish guidelines and a new model development process to assist domain practitioners to manage, share and reuse DRFI domain knowledge
3) Authorize domain experts to effectively develop new solution models by the selection and integration of groups of concept elements (attributes and operations) in accordance with their own model requirements
4) Enable quick access to prior relevant DRFI domain knowledge and permit reuse by domain practitioners

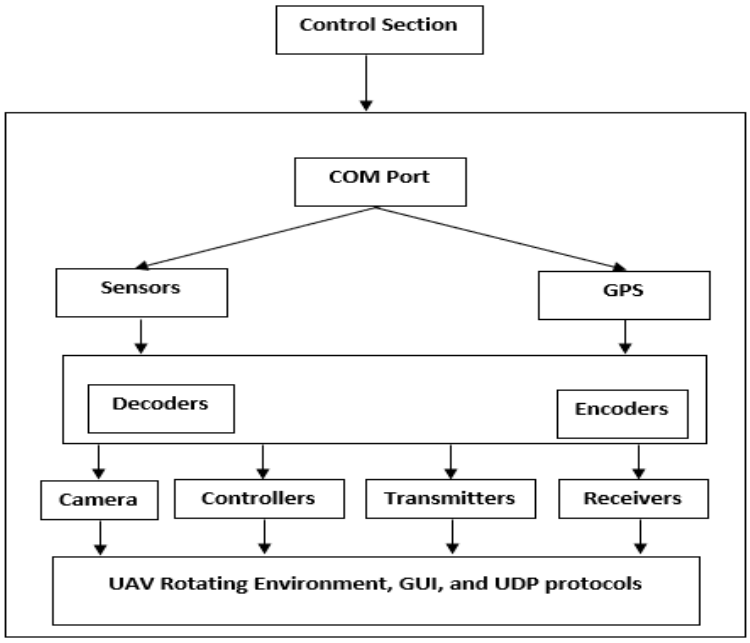

Fig. 1: UAV architecture components (Alotaibi *et al*., 2022a)

Materials

The digital forensics domain is significant for identifying and analyzing cybercrimes, database forensics, drone forensics, networks forensics, mobile forensics, IoT forensics, cloud forensics, and computer forensics are just a few of its many subfields. For context, database forensics is used to identify database incidents and crimes. The application of database forensics is widely explored by many authors (Alotaibi *et al*., 2022a-b; Al-Dhaqm *et al*., 2020a-e; Onwuegbuzie *et al*., 2020; Al-Dhaqm *et al*., 2017a-b; 2021b; Alhussan *et al*., 2022; Al-Dhaqm *et al*., 2016a-b; Aldhaqm *et al*., 2015; Ngadi *et al*., 2012; Al-Dhaqm *et al*., 2014). Specifically, this study highlights the DRFI field.

The literature on DRFI offers a variety of frameworks/models established in various studies for various objectives. Despite their differences, they share consideration for the following four perspectives: Forensic analysis, non-forensic analysis, forensic framework, and its applications (Al-Dhaqm *et al*., 2021a). Tan *et al*. (2021a-b) concentrated on the most effective ways to strengthen the evidence when a drone is investigated using digital forensics techniques. They focused on the wireless forensic aspects to achieve this. Kovar *et al*. (2016), the researchers focused on every component of a drone and highlighted the Linux operating system's implementation and its significance to acquire data on the Linux file system. It should be noted that a drone needs to use an OS to operate properly. Mhatre *et al*. (2015) are to develop a tool using Java-FX for the purpose of visualizing real-time flight control. Although the tool suggested in that study cannot be used directly in the field of drone forensics, it can establish strong connections for data transfer processes between a drone and the controller. Correspondingly, their proposed tool can provide pilots with a visual representation of sensor parameters like IMU, GPS, and altitude. For any flight, this provides a high level of safety (Yu *et al*., 2021a-b).

Similar to how the authors (Roder *et al*., 2018) investigated whether a UAV's flight path could be recreated with the use of positional data gathered from the UAV, they conducted a forensic test on the DJI Phantom 2 vision plus. The study also briefly looked at the existing counter-forensic techniques to determine if a flight path record could be found.

Horsman (2016) performed a preliminary forensic analysis on the Parrot Bebop, which is known as UAV that resembles the Parrot AR Drone 2.0. The main difficulties that frequently occur when performing a UAV forensic analysis were covered by Feng *et al*. (2021b). They prioritized the flight controller and UAV. They built a new ".pud" file at each session between the UAV and the controller after retrieving the flight data in the form of ".pud" files from the device. The UAV serial number, flight date/time, flight controller model, and application utilized for flight controlling were all examined as part of the metadata set that was examined at the file opening point for each of the ".pud" files. Then they attempt to locate the videos and pictures the UAV's onboard camera had taken. The images had EXIF data, which revealed some details about the locations' longitude and latitude coordinates. The device owner can only be identified if the device's serial number could be discovered.

Kovar *et al*. (2016) reviewed generally DRFI using the DJI Phantom 2. In this case, a partial breakdown analysis was conducted on both the software and hardware of the drone system. They then investigated how to use the components when using DRFI. Their outcomes resulted in a presumption in the DRFI's persistence and scope. The outcomes also provided a thorough understanding of this concept and improved its quality. Procházka (2016) investigated the Parrot AR Drone 2.0 with the aim of integrating the visualizing data retrieved from drones with a non-forensic approach. The visualization of the log parameters from the flight data was proposed as an application. However, they were only able to investigate a small number of drones. Mohan (2016), the application and vulnerability of drones were examined and their associations with the dilemmas typically encountered in the cybersecurity field were covered. It was contended that serious risks or outcomes might occur if a drone were subject to hacking and abuse by adversaries. The main focus of that study was identifying the advantages of using drones in a variety of contexts, from using them as toys for kids to using them to execute acts of mass destruction.

Jain *et al*. (2017), a new forensic framework was developed comprising 12 phases in order to systematically investigate UAVs. In that study, the researchers thoroughly dissected five commercial UAVs, including the Parrot AR Drone 2.0, to identify the relationships between different parts. For assessing the effectiveness of the framework, another experiment was conducted. All the investigated UAVs underwent some modifications, including the addition and removal of some parts. Their goal was to determine whether the framework they had developed included all the various components of any fundamental commercial UAV and to test its applicability to produce a comprehensive UAV analysis. Their findings demonstrated that the lack of law enforcement training procedures for UAVs prevents the attacks from being mitigated effectively. None of the UAVs were subjected to forensic analysis, but they did come up with a useful framework that could be used for testing and examining the various stages of the framework.

The first comprehensive analysis of the DJI Phantom 3 Standard was performed by Clark *et al*. (2017). The data was categorized into three categories: Controller, drone, and phone/tablet. The researchers then allowed the UAV to fly toward two different locations. Finally, they were able to locate two important files: A ".dat" file generated by the UAV and a ".txt" file generated by the DJI GO app. Prior to extracting the data about the flight status, GPS locations, Wi-Fi connections, motors, remote control, etc., they first decrypted and decoded the files. The DROP tool was designed to examine the evidentiary files after the data was obtained and the proprietary file structures were analyzed. In this study, a forensic tool named Drone Open-source Parser (DROP) was used and recommended.

Prastya *et al*. (2017), an inclusive discussion was presented with the application of GPS coordinates as location evidence when inspecting drone-based criminalities. Particularly, the authors retrieved the system logs, displayed the GPS coordinates on maps, and used third-party websites to plot the flight paths.

Llewellyn (2017) compared the flight data correlations of three different items: Drones, SD cards, and mobile phones. Investigating a link between a suspect and the drone that was used could greatly aid any forensic criminal investigation. Investigators would be able to provide numerous digital artifacts from GPS timestamps and waypoints, various connected satellites, battery status, pitch, barometer, roll, distance, azimuth, videos, and photos by applying specific software to private UAVs.

Renduchintala *et al*. (2017) conducted some analyses on the important log parameters for autonomous drones and suggested using inclusive software architecture for DRFIs with early results. They anticipated that the developed software would be able to provide an easy-to-use Graphical User Interface (GUI) for the extraction and examination of the onboard flight data. Furthermore, they stated that by offering a novel tool useful for the investigation of drone-performed criminal acts, their study may have contributed to the DRFI field.

Barton and Azhar (2017), the authors stated that mobile forensics techniques have been applied extensively in the literature to extract artifacts from drone mobile applications using open-source tools like Csv View and ExifTool. The operating system used was Windows and Kali, a Linux distribution, as forensic workstations to examine the A.R Drone and DJI Phantom 3. The primary use of several open-source tools (like Geo player) is to visualize the relevant flight path data. This option necessitates substantial changes to the data already present in the UAV due to the lack of an appropriate build environment (including configuration tools, a package manager, and a compiler in the UAV system). Thus, it came to an end in favor of acquiring the logical level. This was accomplished by staging a forensic mass storage device into a UAV and then using the "cp" command to copy all of the files from the mounted "/data" partition.

Maune (2018) attempted to identify and discuss the difficulties that can arise when a UAV or drone is analyzed under forensic circumstances. They evaluated the effectiveness of the current forensic regulations when used in conjunction with the DRFI study. The authors then offered their own recommendations for doing this. Additionally, they described how to effectively apply their recommendations when conducting a forensic analysis of a drone. They also included a case study on the DJI Phantom 3 drone in their research. The lack of a confirmed forensically useful tool in the literature is a significant

limitation of UAV forensics (which could direct to a topic for future research). For instance, different parsing tools must be developed to overcome this limitation and provide accurate and comprehensible information. Additionally, UAVs should be created in the future so that they can be properly integrated with radio communication services.

A novel architecture was developed (Benzarti *et al*., 2018) using the ID-based signcryption with the aim of assuring the authentication process and privacy protection. The authors started by outlining the fundamental components of the architecture. Then, to understand how the process proceeds, the interactions between these components were looked at. The proposed authentication scheme was then thoroughly explained. They used the temporary identity for privacy protection and the RFID tags to track the drones. Additionally, by comparing the various times and speeds of drones, it was possible to simulate the computation of the average renewal of temporary identity.

Renduchintala *et al*. (2019) forensic analysis was performed on a captured UAV. When security forces use various tactics or tools (such as a shotgun) to pursue suspected UAVs, the UAVs may break into private properties. Finding the hardware and software components to use when looking into a UAV is necessary. The investigator (s) must then perform the following three tasks: Gather readily available evidence; establish the chain of custody; and analyze the media or artifact loaded onto the UAV. The increasing number of incidents involving the unauthorized use of UAVs demonstrates how unclear the current aviation regulations are which proved the lack of supporting data and basic standards.

Dawam *et al*. (2018) concentrated on identifying potential cyber-physical security threats. They also discussed existing problems associated with UAV security. Furthermore, they proposed the use of a specific method to investigate large scale cyber security attack vectors while considering four classes of systems that are critical to UAV operations. Besides, they suggested some effective methods for preventing such attacks.

Esteves *et al*. (2018), arbitrary software was integrated into a secured target in order to gain access to the device's interior sensors and logs. To that end, they used neutralization and hardening strategies to measure the effectiveness of the developed software.

Fitwi *et al*. (2019), proposed a novel Distributed, Agent-based Secure Mechanism for IoD and Smart grid sensor monitoring (DASMIS) scheme that integrates Peer to Peer (P2P) and Client Server (C/S) network architectures via low protocol overheads to provide a sound foundation for bandwidth efficient communications. Each node in this system received a starting status and was given a python-based agent that could scan and detect modifications, installed programs, all currently running system programs and applications, system calls made, burned in read only node IDs, node MAC addresses, and node IP addresses. Three tasks are carried out by the agent: Secure node authentication, encoding of communications, and approval of access between nodes. This method can prevent and identify a variety of attacks, including DoS, modification, and masquerading attacks. This can also hash and encrypt data, reporting the changes to the server at the C&C center as well as to other peer nodes.

The main aim of the author (Jones *et al*., 2019) was to expedite the analysis, generation, optimization, and validation of data in order to trace the recovery of evidence. Since the target fiber retrieval context was taken into account, the method chosen to solve this problem was introduced and elaborated using self-adhesive tapes.

Salamh *et al*. (2019), the researchers modified digital forensic techniques and integrated them with the DRFI analysis process to improvise drone incident response plans. More precise information was given regarding the developed Drone Forensics and Incident Response Plan. The Federal Aviation Administration (FAA) can update the standards for Unmanned Aerial Systems (UAS) based on two categories of UAS, it has been discovered. A thorough analysis of the existing literature also demonstrates a lack of analyses on incident responses and forensic analysis frameworks built specifically for remote UAS.

Esteves (2019) invented the "electromagnetic watermarking" technique to exploit the IEMI and implant a watermark into UAVs used for civilian purposes in order to improve forensic tracking.

In order to better understand how forensics frameworks are applied when conducting forensic inspections on drones, (Mei, 2019) surveyed a large number of DRF investigators and aircraft accident investigators. The gathered data were examined using the Chi-square independence test. The results proved no evidence of a correlation between their drone investigations and the techniques employed for UAS forensics.

A novel method to determine whether a drone is lying on the ground or flying through the air was introduced by Sciancalepore *et al*. (2019). Instead of using any active methods, the radio traffic should be eavesdropped on and thoroughly processed using standardized machine-learning techniques. They argued that by using the ArduCopter operating system as a whole and properly classifying network traffic, users would be able to precisely determine a drone's status (for example, a few DJI and Hobbyking vehicles). Correspondingly, a lower bound on the detection delay needs to be developed when the previously mentioned method is used. Their experimental results demonstrated that the suggested solution could ascertain the state of a drone (moving or fixed) with roughly 0.93 SR in 3.71 sec.

Lakew Yihunie *et al*. (2020) the author investigated the security vulnerabilities of two drones: The Parrot Mambo FPV and Eachine E010. After that, the proper

defenses were implemented to improve their adaptability and efficiency in the face of potential assaults. The findings demonstrated the vulnerability of the Parrot Mambo FPV to de-authentication and FTP service attacks, while the vulnerability of the Eachine E010 to custom controller attacks and RF replay was identified.

Mistry and Sanghvi (2021), the researchers concentrated on the general legal procedures necessary for the collection of drones from crime scenes and their examination in a lab. Moreover, Yang *et al*. (2021) developed a new model that could be used to gather and record digital information from flight artifacts and associated mobile devices in order to aid forensic examinations of the DJI Spark and Mavic Air, two widely-used drone systems.

Recently, many researchers have introduced their work in the DRFI field. These include, (Alotaibi *et al*., 2022b), the authors introduced a new framework for drone forensic readiness. They address several issues in the DRFI field, despite the fact that their framework hasn't been put into practice (Al-Dhaqm *et al*., 2021a; Alotaibi *et al*., 2022b; Atkinson *et al*., 2021; Lan and Lee, 2022; Husnjak *et al*., 2022; Parghi *et al*., 2022).

Due to the wide range of drone infrastructures, the DRFI domain is complex, diverse, and ubiquitous. Based on the study findings, researchers and developers working in this field approach DRFI by considering three perceptions: (1) The perception of drone infrastructures; (2) The perception of technology; and (3) The perception of drone incidents. However, they have varied in how they address the perceptions. As an illustration, some of the models put forth in the literature address all three perceptions, while others only address two or one DRFI perception. Figure 2 shows the DRFI problems and suggested fixes. The summaries of the existing DRFI models are shown in Table 1.

Table 1: Summary of existing DRFI models

ID	Year	Existing DRFI models	Purpose of the model
1	2015	Mhatre *et al*. (2015)	The main objective is to build a Java FX tool for visualizing real time flight control. Although the the tool suggested in that study cannot be used directly in the field of drone forensics, it can create strong connections for data transfer processes between a drone and the controller. They also included a tool that allows pilots to see sensor parameters like IMU, GPS, and altitude. Thus, this ensures a high level of safety for any flight
3	2016	Mohan (2016)	The use and vulnerability of drones were investigated and their connections to the problems that typically arise in the cybersecurity field were also covered. It was argued that serious risks or outcomes might occur if a drone were subject to hacking and abuse by adversaries. The aim was to identify the advantages of using drones in a variety of contexts, from using them as toys for kids to using them to execute acts of mass destruction
4	2016	Kovar *et al*. (2016)	DRFI was generally examined during the utilization of the DJI Phantom 2. Some breakdown analyses were performed on the drone's software and hardware components. They then investigated how to use the components with DRFI. Their results resulted in a belief in the DRFI's persistence and scope. The results presented a deeper understanding of this concept and better quality
6	2016	Procházka (2016)	The Parrot AR Drone 2.0 was investigated by researchers with the goal of integrating visualization data retrieved from drones using a non-forensic approach. The visualization of the log parameters derived from flight data were suggested as a use case. However, they were only able to focus a small number of drones
7	2017	Prastya *et al*. (2017)	A comprehensive analysis of the use of GPS coordinates as location evidence during the ongoing drone-based crimes investigation. The authors extracted the system logs, displayed the GPS maps coordinates and also used web based third party platforms to plot the flight paths
8	2017	Jain *et al*. (2017)	A new forensic framework with 12 phases was introduced to investigate UAVs systematically. In order to determine the relationships between different components, the study's researchers thoroughly examined five commercial UAVs, including the Parrot AR Drone 2.0. Another test was conducted to evaluate the framework's efficacy. All of the UAVs under investigation had some changes made to them, including the addition and removal of some parts. The purpose of this study is to determine whether the framework they had created adequately addressed all the different parts of any basic commercial UAV and to assess its applicability to a thorough UAV analysis. Their findings showed that the attacks cannot be effectively mitigated because there is a lack of UAV training procedures for law enforcement. However, they eventually developed a comprehensive the basis that could be used for testing and analyzing the different stages of the framework despite the fact that none of the UAVs were subjected to forensic analysis
9	2017	Clark *et al*. (2017)	An extensive analysis of the DJI Phantom 3 Standard was conducted. The data was divided into three categories by the researchers: Controller, drone, and phone/tablet. The UAV was given permission to fly toward two different locations. In the end, they were able to locate two important files: A ".dat" file generated by the UAV and a ".txt" file generated by the DJI GO app. Prior to extracting the data about the flight status, GPS locations, Wi-Fi connections, motors, remote

Table 1: Continue

			control, etc., they first decrypted and decoded the files. Following the analysis of the proprietary file structures and the data that was collected, the DROP tool was created to examine the evidentiary files. Additionally, their study recommended the reliable open-source Drone Open-source Parser (DROP) tool
11	2017	Llewellyn (2017)	The author focused on investigating the flight data correlations between three different objects, namely, mobile phones, drones, and SD cards. Exploring a correlation between the drone used and a suspect could greatly aid any forensic criminal investigation. Investigators would be able to provide a wide variety of digital artifacts, including GPS timestamps and waypoints, various integrated satellites, battery status, roll, distance, azimuth, pitch, barometer, videos, and photos by implementing specific software to private UAVs
12	2017	Barton and Azhar (2017)	To extract artifacts from drone mobile applications using open-source tools like Csv View and ExifTool, the authors claim that mobile forensics techniques have been thoroughly explored in literature. Forensic workstations running Windows and the Linux distribution Kali were used to examine the A.R Drone and DJI Phantom 3. Several open-source tools have primarily been used to visualize the data relating to flight paths (like Geo player, for example). This option would require significant changes to the data already present in the UAV system due to the lack of an adequate build environment (which would include configuration tools, a package manager, and a compiler). This was achieved by mounting a forensic mass storage device onto a UAV, which was then used to copy all of the files from the mounted "/data" partition using the "cp" command
16	2018	Maune (2018)	The authors aim to identify and discuss the difficulties that arise when analyzing a UAV/drone under forensic conditions. They evaluated the effectiveness of the current forensic guidelines as they applied to the DRFI study. This was further justified by discussing how to implement effective forensic analysis of a drone. A case study on the DJI Phantom 3 drone is also included in their study. The absence of a confirmed forensically useful tool in the literature is a significant limitation of UAV forensics (which could direct to a topic for future research). For example, different parsing tools must be developed that can analyze the original data and provide accurately and comprehensible information to address this limitation. Additionally, UAVs should be created in the future so that they can be integrated effectively with radio communication services
17	2018	Benzarti *et al*. (2018)	A novel architecture with the use of ID Based Signcryption was introduced to ensure the authentication process and privacy protection. The fundamental components of architecture were first described by the authors. Then, to ascertain how the process proceeds, the interactions between these components were looked at. Following that, the recommended authentication scheme was heavily discussed. They used the temporary identity for privacy protection and the RFID tags to track the drones. Furthermore, the computation of the average renewal of temporary identity was simulated by examining the variations in times and speeds of drones
19	2018	Dawam *et al*. (2018)	The researchers concentrated on identifying potential dangers to physical and cyber security. Their the study discusses the current challenges associated with UAV security. They also recommended using a specific approach to investigate the broad cyber security attack vectors of such systems while considering four system classes that are extremely significant for UAV operations. In a nutshell, they offered suggestions for effective strategies for preventing such attacks
20	2018	Esteves *et al*. (2018)	Arbitrary software was developed and used to unlock a locked target and gain access to the device sensors and logs. They projected the effectiveness of the developed software using neutralization and hardening techniques to achieve this
24	2019	Renduchintala *et al*. (2019)	An intercepted UAV was subjected to a forensic examination. When security forces use various tactics or tools (such as a shotgun) to pursue suspected UAVs, the UAVs may break into private properties. The hardware and software components that should be used to investigate a UAV must be identified. The investigator(s) must then perform the following three tasks: Gather readily available evidence; establish the chain of custody; and analyze the media or artifact loaded onto the UAV. The rise in incidents involving the unauthorized use of Unmanned Aerial Vehicles (UAVs) demonstrates how unclear the current aviation regulations are. It showed a lack of supporting data and basic standards
25	2019	Fitwi *et al*. (2019)	The monitoring of IoD and Smart grid sensors under the DASMIS scheme is a novel distributed, agent-based secure mechanism. In order to create a suitable platform for quick and bandwidth efficient communications, the study's main objective was to combine Client Server (C/S) and Peer to Peer (P2P) network architectures with minimal protocol overheads. Each node in this system was given access and it was given a starting status, for a python based agent with the ability to scan and detect modifications, system calls made, installed applications, all currently running system programs, burned in read only node IDs, node MAC addresses, and node IP addresses. Three tasks are carried out by the agent: (1) Secure node authentication; (2) Encoding of communications; and (3) Authorization of inter-node access. This approach can detect and prevent a variety of attacks,

Table 1: Continue

			including DoS, modification, and masquerading attacks. This can also hash and encrypt data, reporting the changes to the server at the C&C center as well as to other peer nodes
26	2019	Jones *et al*. (2019)	The authors expected to accelerate procedures like data generation, analysis, validation and optimization to trace evidence recovery. Since the target fiber retrieval context was taken into account, the method chosen to solve this problem was introduced and elaborated using self adhesive tapes
27	2019	Salamh *et al*. (2019)	The application of the DRFI analysis process was used by the researchers to modify digital forensic procedures in order to enhance drone incident response plans. As a result, they provided comprehensive information for the incident response plan and drone forensics that were developed. The Federal Aviation Administration (FAA) has two categories of Unmanned Aerial Systems (UAS) that it can use to update the requirements for UAS. Based on previously published research, it was confirmed that more study is needed on incident responses and forensic analysis frameworks specifically designed for use with remotely piloted aerial systems
28	2019	Esteves (2019)	invented the "electromagnetic watermarking" technique to take advantage of the effects of IEMI on UAVs used for civilian purposes to better facilitate forensic tracking
29	2019	Mei (2019)	For a better understanding of how forensics frameworks are applied when conducting forensic inspections on drones, the researchers polled a large number of DRF investigators and aircraft accident investigators. The gathered information was examined using the Chi square independence test. The results proved no evidence of a connection between their drone investigations and the techniques they employ when conducting UAS forensics
31	2019	Sciancalepore *et al*. (2019)	The studies proposed a cutting edge technique for accurate and effective in determining whether a drone is in the air or lying on the ground. Instead of using any active methods, the radio traffic should be eavesdropped on and thoroughly processed using standardized machine learning techniques. They asserted that by using the ArduCopter operating system as a whole and properly classifying network traffic, users would be able to precisely determine a drone's status (for example, several DJI and Hobbyking vehicles). The detection delay must also have a lower bound established before the method can be put into practice. According to their experimental results, the suggested the solution could ascertain a drone's state (moving or fixed) with approximately 0.93 SR in 3.71 sec
32	2020	Lakew Yihunie *et al*. (2020)	Two drones, the Parrot Mambo FPV and Eachine E010 were compared for their security susceptibilities. Then, some rational and reasonable defenses were set up forth to increase them adaptability and effectiveness in the face of potential assaults. The results demonstrated the Parrot Mambo FPV's susceptibility to FTP service attacks and de-authentication, while the Eachine E010 was discovered to be susceptible to custom controller attacks and RF replay
33	2021	Mistry and Sanghvi (2021)	Emphasized the overall significant legal processes necessary to collect or transfer drones from crime scenes and bring them for inspection in a laboratory
34	2021	Yang *et al*. (2021)	Developed a new model applicable to gathering and documenting digital data from flight artifacts as well as the relevant mobile devices to assist investigators in conducting forensic analyses on the Mavic Air and DJI Spark, are two widely used drone systems

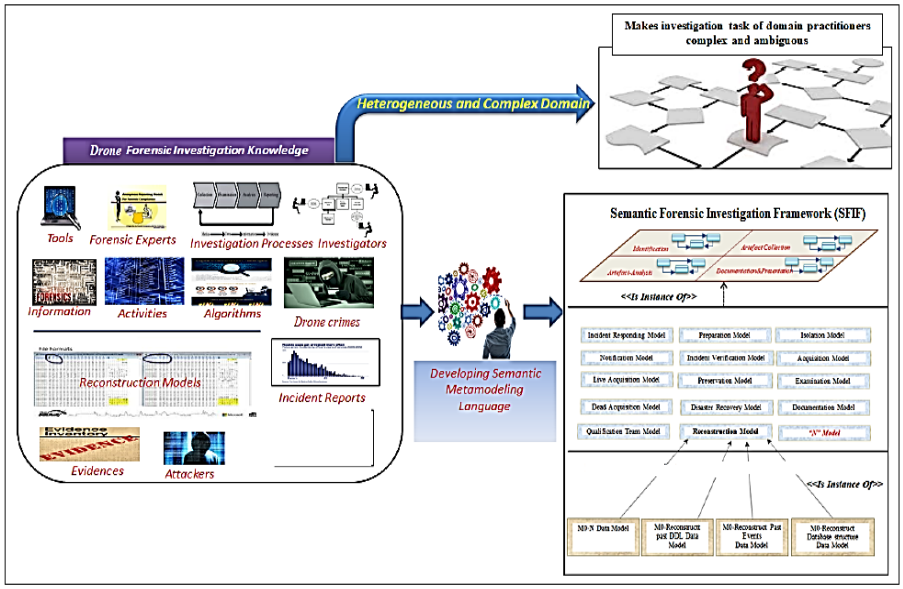

Fig. 2: DRFI issues and proposes solutions

Methods

The current study adopts the Design Science Research (DSR) method to create the SFIF. DSR refers to a method that could be used to create distinctive and prolonged objects for a particular issue, enabling the study of analytics (March and Smith, 1995). Therefore, this study adopts the metamodeling strategy suggested by Al-Dhaqm *et al*. (2017b).

Identifying DRFI Domain Models

This step will involve identifying DRFI models and extracting and unifying the common investigation artifacts. The literature has therefore covered a number of DRFI models. Models for this study were selected based on coverage factors discovered in previous research (Caro *et al*., 2014; Kelly and Pohjonen, 2009). To accomplish the goal of proposing common investigation artifacts for the DRFI domain, extensive coverage of broadly applicable DRFI perspectives is necessary. If a model can account for all DRFI perceptions, it is said to have a high coverage value (i.e., full coverage). If the model only describes a substantial part of a specific DRFI perception, it has a lower coverage value.

In this step, several DRFI artifacts have been extracted, merged, and proposed. The definitions of the proposed DRFI artifacts have also been reconciled to avoid any confusion. This step aims to resolve discrepancies between artifact definitions. The proposed DRFI artifacts and definitions are shown in Table 2.

Identifying Relationships Among Proposed DRFI Artefacts

This is the second step of the development and validation process of the SFIF. It is used to determine connections between suggested DRFI artifacts. A review of DRFI models revealed a large number of UML connections between the DRFI artifacts. association, specialization/generalization, and aggregation relationships were found to be the three main types of common UML relationships. A task-related connection between two classes is typically maintained in an association relationship. A drone incident needs to be verified and discovered, as shown by the association relationship between the investigation team and the artifact labeled "Verifies" between the two. The relationship between specialization and generalization links a subclass to its superclass. It indicates the transmission of properties and functions from a superclass to a subclass, as in the case of the volatile-artifact concept "kind of" Resources concept. Consequently, the subclass Volatile-Artifact may be inherited by the Resources class, which could affect its features and abilities. Usually, implied ownership exists in an aggregation relationship. Drone Incident is connected to the Drone concept and the relation "belongs to" is an example of an aggregation relationship. Because of this, this study uses the semantic UML relationships that were found and identified during the survey of the DRFIs domain to illustrate the relationships between artifacts. Accordingly, the version of the proposed SFIF is the outcome of this step. Therefore, the results from this step are the version of the proposed SFIF. It consists of three SFIF process classes, as illustrated in Fig. 3-5. The UML notations have been used to draw the SFIF.

The preparation SFIF process class 1 depicted in Fig. 3 consists of eighteen (18) investigation artifacts, including the drone, GPS module, camera, battery, resources, volatile artifact, nonvolatile artifact, flight controller, electronic speed controller, drone location, sensors, and altimeter, as well as the drone incidents, theft, crash, and suicide, as well as the investigation team and forensic tool.

The gathering and preservation SFIF class 2 shown in Fig. 4 is composed of fourteen (14) investigation artifacts: Investigation team, forensic tool, live acquiring data, acquired data, preservation, acquiring data, dead acquiring data, backup, hashing, resources, volatile artifact, nonvolatile artifact, logfile and memory records.

The ten (10) investigation artifacts that constructed the analysis and documentation SFIF class 3 depicted in Fig. 5 are the investigation team, acquired data, examination, rehashing, reconstruction, timeline events, patterns, evidence, forensic tool, and final report.

Validating Semantic Forensic Investigation Framework

In this step, the proposed SFIF is validated in terms of its logic, comprehensiveness, and usefulness using a validation technique that contrasts the framework's performance of other models in the existing literature (Sargent, 2015). The objectives include finding any concepts that are missing from the suggested SFIF and making sure it has a sufficiently wide scope. Table 3 displays the findings from contrasting the performance of the proposed framework (SFIF) with current models. The outcomes supported the comprehensiveness of SFIF and showed how well it could operate from both proactive and reactive forensic perspectives.

Table 2: The proposed DRFI artifacts

ID	Proposed common DRFI artifacts	Reconciled definitions
1.	Drone	The drone is a radio controlled flying quadcopter helicopter built by Parrot
2.	GPS module	GPS module is used to navigate location. It is an electronic device that is developed using nanotechnology. It aids in locating the victim and the related incident that occurred based on google maps
3.	Camera	A camera is used for live streaming and capturing images during a drone flight. Often, a professional set the camera is used for investigation purposes such as racing HD cameras
4.	Battery	A battery is crucial to ensure the longevity and durability of the devices life span used during the event of investigation
5.	Flight controller	When signals are sent from other electronic components, it is used to process and coordinate commands. It includes a variety of sensors, including an accelerometer, magnetometer, and gyroscope
6.	Altimeter	The altimeter is used to determine the location and altitude of the quadcopter
7.	Sensors	The sensor is utilized to estimate the altitude of the drone
8.	Electronic speed controller	This device controls the speed of motors by generating high frequency signals at different phase
9.	Resources	The resource is the main forensics data in drones that consist of volatile and non-volatile files storing histories relating to the drones
10.	Non-volatile artifact	Non-volatile artifact is a collection of related non-volatile drone operating system artifacts such as log files, records and OS log artifacts that hold non-volatile data
11.	Volatile artifact	Volatile artifact is a collection of related volatile drone resources and operating system artifacts such as memories artifacts that hold volatile data
12.	Investigation team	An experienced and qualified team has been assigned by the business or the court to investigate the drone incident. The investigation team must identify the data that are relevant to the investigation to reduce the number of metadata, Investigators could contrast actual drone statements executed with attempted attacks found in logs and memory dumps
13.	Forensic tool	It is used to acquire, preserve and analyze drone incidents
14.	Drone incident	A drone incident is an action or event that corrupts data unintentionally or on purpose and jeopardizes its integrity, confidentiality, and availability. Events related to Drone Incidents are copied to the forensic workstation for examination. Drone Crashes, Drone Steal, and Drone Suicides are among its features
15.	Drone steal	This happens when a drone is stolen by the perpetrator
16.	Drone crash	This happens when a drone lost control and crashes abruptly
17.	Drone suicide	occurs when there is no physical evidence of the drone attack's perpetrator. It is more difficult to determine who was operating the drone because it is probably destroying,
18.	Acquiring data	This process is performed to acquire and capture all volatile and non-volatile data from the drone
19.	Live acquiring data	A live data acquisition occurs when the drone system analyzed is still running during the analysis
20.	Dead acquiring data	The dead acquisition method involves copying data from the investigated drone system without using the system itself
21.	Acquired data	The data gathered from drone resources
22.	Preservation	It is used to protect the acquired data of the drone incident from tampering
23.	Hashing	It is used to protect the integrity and consistency of the transmitted data from the acquired stage to analyzing stage
24.	Backup	A backup is a kind of preservation that provides an exact copy of a former overall snapshot that can be played back efficiently as a whole
25.	Log files	The log file, a specific type of drone log file, is one of the tools used to track drone attacks and consists of the most crucial data fact for an investigation. They contain the text of statements that include private data like flight paths and passwords. Log files could show where the drone device's original file systems were compromised
26.	Memory records	It is used to keep the live events of the drone device such as the GPS, locations, altitude, etc
27.	Examination	Drone forensic analysis is used during the examination to ensure the data gathered is accurate and intact (no alteration done)
28.	Rehashing	Rehashing is a component used to match old hash values with a rehash tuple
29.	Reconstruction	Reconstruction is a process used to retrace past systems, past execution history, and user databases in order to reconstruct events that may responsible for drone incidents from collected volatile and non-volatile artifacts/data.
30.	Timeline events	Timeline events are a collection of occasions that help illustrate the significant digital occurrences so far identified and establish an investigation scope for use in the analysis stage. An investigation timeline can be updated with significant events like failed login attempts, successful user logins, and unusual activity. This the timeline will help a detective spot drone activity patterns that might not have been sequentially recorded in log files that have been gathered
31.	Patterns	The keywords that help investigators to find out the relevant malicious attacks/activities
32.	Evidence	Evidence is specific data that can be found mostly in GPS, control units, or drone log files (Mobile or Laptop). In court, one may rely on data that has been stored or transmitted in binary form. It includes the who, why, what, when, how, and where of the malicious transaction
33.	Final report	The report is a document that consists of detailed activities and occurrences related to investigation procedures

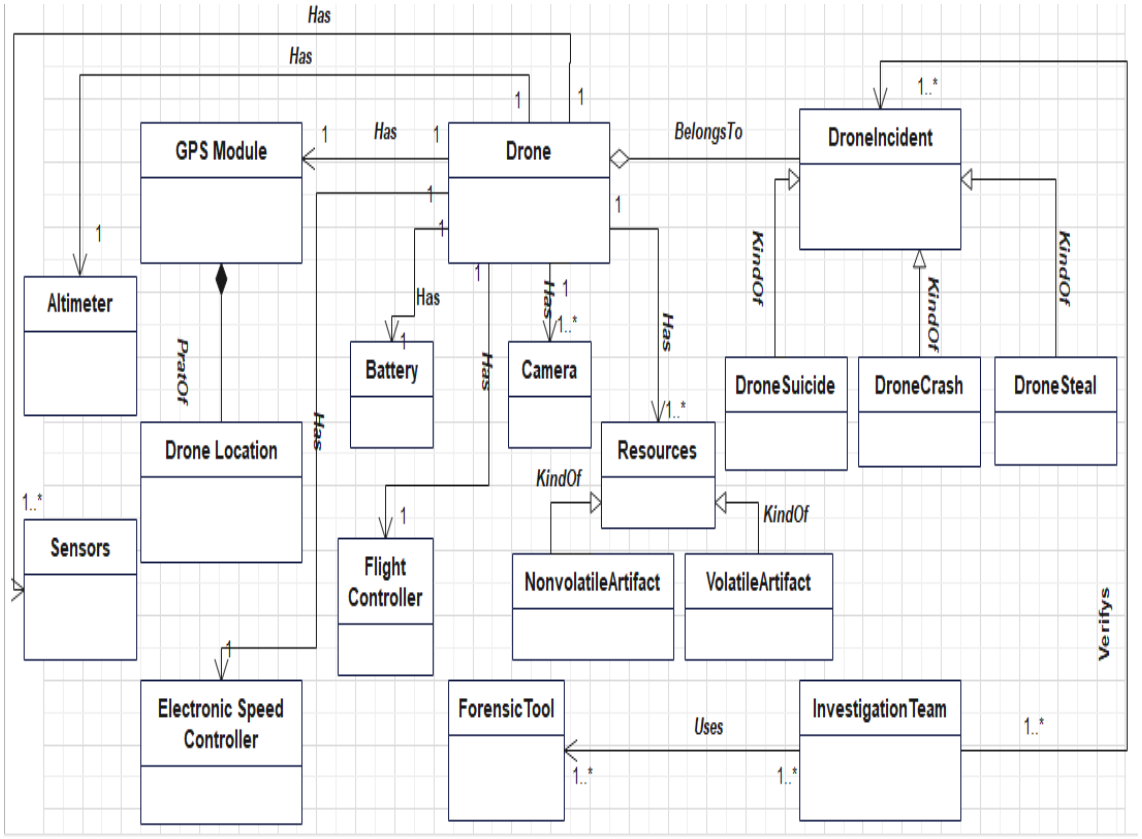

Fig. 3: Preparation SFIF class 1

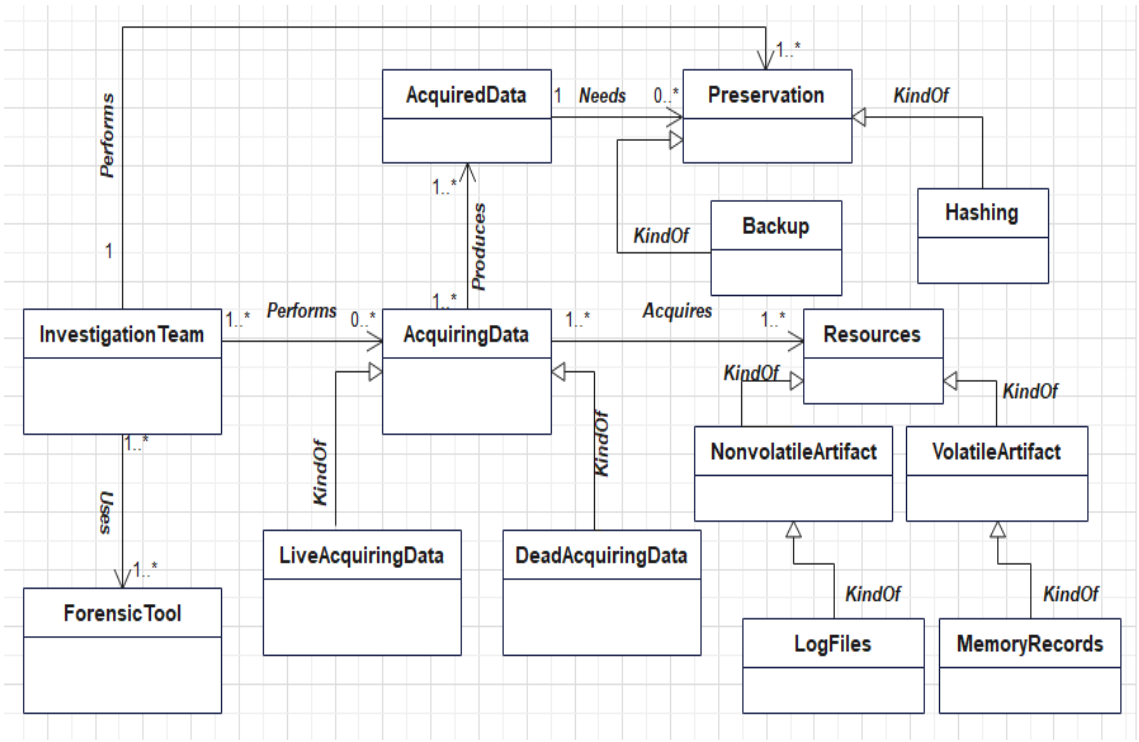

Fig. 4: SFIF: Gathering and preservation of evidence class 2

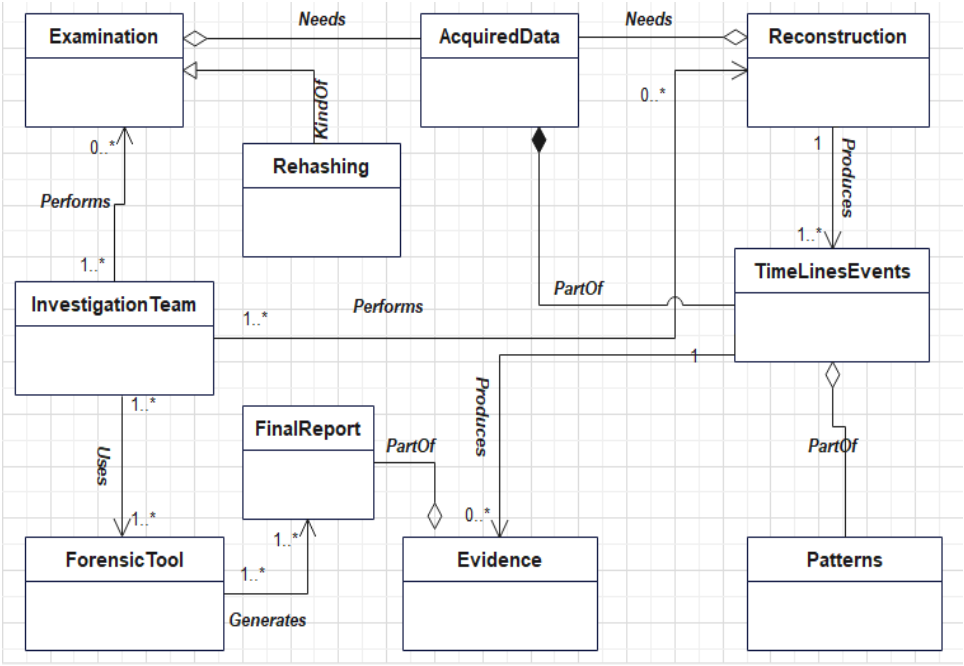

Fig. 5: SFIF: Analysis and Documentation class 3

Table 3: Comparison between the exiting DRFI models and proposed SFIF

ID	Year	Existing DRFI Models	Proposed SFIF	Status
1	2015	Mhatre *et al*. (2015)	þ	Covered
2	2016	Horsman (2016)	þ	Covered
3	2016	Mohan (2016)	þ	Covered
4	2016	Kovar *et al*. (2016)	þ	Covered
5	2016	Maarse *et al*. (2016)	þ	Covered
6	2016	Procházka (2016)	þ	Covered
7	2017	Prastya *et al*. (2017)	þ	Covered
8	2017	Jain *et al*. (2017)	þ	Covered
9	2017	Clark *et al*. (2017)	þ	Covered
10	2017	Bucknell and Bassindale (2017)	þ	Covered
11	2017	Llewellyn (2017)	þ	Covered
12	2017	Barton and Azhar (2017)	þ	Covered
13	2017	Renduchintala *et al*. (2017)	þ	Covered
14	2018	Bouafif *et al*. (2018)	þ	Covered
15	2018	Roder *et al*. (2018)	þ	Covered
16	2018	Maune (2018)	þ	Covered
17	2018	Benzarti *et al*. (2018)	þ	Covered
18	2018	Gülataş and Baktır (2018)	þ	Covered
19	2018	Dawam *et al*. (2018)	þ	Covered
20	2018	Esteves *et al*. (2018)	þ	Covered
21	2018	Shi *et al*. (2018)	þ	Covered
22	2018	Guvenc *et al*. (2018)	þ	Covered
23	2018	Ding *et al*. (2018)	þ	Covered
24	2019	Renduchintala *et al*. (2019)	þ	Covered
25	2019	Fitwi *et al*. (2019)	þ	Covered
26	2019	Jones *et al*. (2019)	þ	Covered
27	2019	Salamh *et al*. (2019)	þ	Covered
28	2019	Esteves (2019)	þ	Covered
29	2019	Mei (2019)	þ	Covered
30	2019	Le Roy *et al*. (2019)	þ	Covered
31	2019	Sciancalepore *et al*. (2019)	þ	Covered
32	2020	Lakew Yihunie *et al*. (2020)	þ	Covered

Results and Discussion

In this study, the interoperability, heterogeneity, and complexity of the DRFI domain were addressed by developing a novel semantic framework known as SFIF. The SFIF was created to address the DRFI domain's interoperability. The DRFI domain's general investigation artifacts are identified and combined as necessary. Analyzing the DRFI domain's frameworks, models, techniques, concepts, activities, tasks, and other components is a part of this process.

The study generalizes the SFIF creation process using metamodeling. A comparison against other models has been used as a validation technique to guarantee that the SFIF can be interoperable in many drone systems and can cover all DRFI domain models. In a nutshell, the SFIF can be interoperable with any drone system. The three (3) proposed common investigation processes and 33 proposed common investigation artifacts have addressed the heterogeneity of the DRFI domain. The three (3) suggested common investigation processes included many of the DRFI domain's investigation processes. Numerous investigation artifacts of the DRFI domain were covered by the 33 proposed common investigation artifacts. Therefore, under common processes and investigation artifacts, all DRFI activities and attributes have been organized and unified. By creating SFIF, the DRFI domain's complexity has been resolved. It enables domain experts to quickly create their solution models based on their needs. To make all investigation tasks easier, the SFIF is represented as UML notations. The advantages of the suggested SFIF include:

1. Address the heterogeneity and ambiguity of the DRFI domain
2. The generality and reuse of common investigation artifacts: Common investigation artifacts may include a number of distinct domain artifacts and be applied in various scenarios. For example, the proposed Drone Incident may include the entire UAV Drone Incident
3. Each investigation artifact that is being proposed includes all of the features of the existing artifacts. The proposed investigation artifacts combine the requirements (attributes) and operations (operations) of the existing artifacts. This enables experts in a given domain to instantiate particular objects from high-level artifacts

Conclusion

In recent years, the academic community has given drone forensics a lot of attention. This area of study includes all inquiries made to locate and identify drone-related offenses. The literature includes a variety of models and methods created by various academics for the DRFI field. These simulations can replicate the flight paths that professionals could use for any forensic investigation. They typically use the controller's and the device's internal logs to spot malicious activity. Drones have been improved to prevent any intrusion, particularly in terms of security and verification.

However, there is no standardized forensics model or framework that can address a range of drone-related crimes in the literature at this time. As a result, the current paper put forth the SFIF, a brand-new forensic framework that applies to crimes involving drones and the DRFI field from both pre-and post-incident perspectives. Preparation, gathering, and preservation of evidence and analysis and documentation are the three abstract phases of SFIF. The second process, where the chain of custody and chain of evidence are both well assured, is fed the output of the first one. The analysis and documentation procedures are typically considered an afterthought, which theoretically leads to frequent drone crimes. Considering this, SFIF could be described as an all-encompassing framework that can be effectively used to anticipate, be ready for and prevent the occurrence of drone-related events. The SFIF was also assessed by contrasting it with other models that are currently used in the literature. A real scenario is necessary to evaluate the effectiveness of SFIF; consequently, in the future, the authors of the current article will concentrate on using SFIF in a real case.

Acknowledgment

I highly appreciate researchers who supported this study with all the required references.

Funding Information

This research is self-funded and there was no funding from any organization.

Ethics

It is undersigned by me that this article has not been published elsewhere, and there are no ethical issues involved after the publication of this article.

References

Al-Dhaqm, A. M. R., Othman, S. H., Abd Razak, S., & Ngadi, A. (2014, August). Towards adapting metamodelling technique for database forensics investigation domain. In *2014 International Symposium on Biometrics and Security Technologies (ISBAST)* (pp. 322-327). IEEE. https://doi.org/10.1109/ISBAST.2014.7013142

Aldhaqm, A., Abd Razak, S., & Othman, S. H. (2015). Common Investigation Process Model for Database Forensic Investigation Discipline. In *the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia* (pp. 297-300). https://core.ac.uk/reader/83531920

Al-Dhaqm, A., Abd Razak, S., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020a). A review of mobile forensic investigation process models. *IEEE Access*, *8*, 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

Al-Dhaqm, A., Abd Razak, S., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020b). Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access*, *8*, 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

Al-Dhaqm, A., Abd Razak, S., Dampier, D. A., Choo, K. K. R., Siddique, K., Ikuesan, R. A., ... & Kebande, V. R. (2020c). Categorization and organization of database forensic investigation processes. *IEEE Access*, *8*, 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Ali, A., Ghaleb, F. A., Rosman, A. S., & Marni, N. (2020d). Database forensic investigation process models: A review. *IEEE Access*, *8*, 48477-48490 https://doi.org/10.1109/ACCESS.2020.2976885

Al-Dhaqm, A., Abd Razak, S., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020e). Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access*, *8*, 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Ali, A., & Ngadi, A. (2016a). Conceptual investigation process model for managing database forensic investigation knowledge. *Research Journal of Applied Sciences, Engineering and Technology*, *12*(4), 386-394. https://doi.org/10.19026/rjaset.12.2377

Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Nagdi, A., & Ali, A. (2016b). A generic database forensic investigation process model. *Jurnal Teknologi*, *78*, 6-11. https://doi.org/10.11113/jt.v78.9190

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S., & Ghabban, F. M. (2021a). Research challenges and opportunities in drone forensics models. *Electronics*, *10*(13), 1519. https://doi.org/10.3390/electronics10131519

Al-Dhaqm, A., Razak, S., Ikuesan, R. A., R. Kebande, V., & Hajar Othman, S. (2021b). Face validation of database forensic investigation metamodel. *Infrastructures*, *6*(2), 13. https://doi.org/10.3390/infrastructures6020013

Al-Dhaqm, A., Razak, S., Othman, S. H., Choo, K. K. R., Glisson, W. B., Ali, A., & Abrar, M. (2017a). CDBFIP: Common database forensic investigation processes for Internet of Things. *IEEE Access*, *5*, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Ali Mohammed, A. (2017b). Development and validation of a database forensic metamodel (DBFM). *PloS One*, *12*(2), e0170793. https://doi.org/10.1371/journal.pone.0170793

Alhussan, A. A., Al-Dhaqm, A., Yafooz, W. M. S., Emara, A. H. M., Bin Abd Razak, S., & Khafaga, D. S. (2022). A Unified Forensic Model Applicable to the Database Forensics Field. Electronics 2022, 11, 1347. https://doi.org/10.3390/electronics11091347

Alotaibi, F. M., Al-Dhaqm, A., Al-Otaibi, Y. D., & Alsewari, A. A. (2022a). A comprehensive collection and analysis model for the drone forensics field. *Sensors*, *22*(17), 6486. https://doi.org/10.3390/s22176486

Alotaibi, F. M., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022b). A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/8002963

Atkinson, S., Carr, G., Shaw, C., & Zargari, S. (2021). Drone forensics: The impact and challenges. In *Digital Forensic Investigation of Internet of Things (IoT) Devices* (pp. 65-124). Springer, Cham. https://doi.org/10.1007/978-3-030-60425-7_4

Awan, S., Ahmed, S., Ullah, F., Nawaz, A., Khan, A., Uddin, M. I., ... & Alyami, H. (2021). IoT with blockchain: A futuristic approach in agriculture and food supply chain. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/5580179

Barton, T. E. A., & Azhar, M. H. B. (2017, September). Forensic analysis of popular UAV systems. In *2017 Seventh International Conference on Emerging Security Technologies (EST)* (pp. 91-96). IEEE. https://doi.org/10.1109/EST.2017.8090405

Benzarti, S., Triki, B., & Korbaa, O. (2018, April). Privacy Preservation and Drone Authentication Using ID-Based Signcryption. In *SoMeT* (pp. 226-239). https://doi.org/978-1-61499-900-3-226.

Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2018, February). Drone forensics: Challenges and new insights. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-6). IEEE. https://doi.org/10.1109/NTMS.2018.8328747

Bucknell, A., & Bassindale, T. (2017). An investigation into the effect of surveillance drones on textile evidence at crime scenes. *Science & Justice*, *57*(5), 373-375. https://doi.org/10.1016/j.scijus.2017.05.004

Caro, M. F., Josyula, D. P., Cox, M. T., & Jiménez, J. A. (2014). Design and validation of a metamodel for metacognition support in artificial intelligent systems. *Biologically Inspired Cognitive Architectures*, *9*, 82-104. https://doi.org/10.1016/j.bica.2014.07.002

Clark, D. R., Meffert, C., Baggili, I., & Breitinger, F. (2017). DROP (DRone Open-source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digital Investigation*, *22*, S3-S14. https://doi.org/10.1016/j.diin.2017.06.013

Kovar, D.; Dominguez, G., Murphy, C. (2016). UAV (aka drone) Forensics. Presented at the SANS DFIR Summit, Austin, TX, USA, pp: 23-24.

Dawam, E. S., Feng, X., & Li, D. (2018, June). Autonomous arial vehicles in smart cities: Potential cyber-physical threats. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1497-1505). IEEE. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00247

Ding, F., Zhu, G., Alazab, M., Li, X., & Yu, K. (2020). Deep-learning-empowered digital forensics for edge consumer electronics in 5G HetNets. *IEEE consumer electronics magazine*.

Ding, F., Yu, K., Gu, Z., Li, X., & Shi, Y. (2021a). Perceptual enhancement for autonomous vehicles: Restoring visually degraded images for context prediction via adversarial training. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2021.3120075

Ding, F., Zhu, G., Li, Y., Zhang, X., Atrey, P. K., & Lyu, S. (2021b). Anti-forensics for face swapping videos via adversarial training. *IEEE Transactions on Multimedia*. https://doi.org/10.1109/TMM.2021.3098422

Ding, G., Wu, Q., Zhang, L., Lin, Y., Tsiftsis, T. A., & Yao, Y. D. (2018). An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Communications Magazine*, *56*(1), 29-35. https://doi.org/10.1109/MCOM.2017.1700452

Esteves, J. L. (2019, September). Electromagnetic watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In *2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE* (pp. 1144-1149). IEEE. https://doi.org/10.1109/EMCEurope.2019.8872027

Esteves, J. L., Cottais, E., & Kasmi, C. (2018, August). Unlocking the access to the effects induced by IEMI on a civilian UAV. In *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)* (pp. 48-52). IEEE. https://doi.org/10.1109/EMCEurope.2018.8484990

Feng, C., Liu, B., Guo, Z., Yu, K., Qin, Z., & Choo, K. K. R. (2021a). Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones. *IEEE Internet of Things Journal*, *9*(8), 6224-6238. https://doi.org/10.1109/JIOT.2021.3113321

Feng, C., Liu, B., Yu, K., Goudos, S. K., & Wan, S. (2021b). Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Transactions on Industrial Informatics*, *18*(5), 3582-3592. https://doi.org/10.1109/TII.2021.3116132

Feng, C., Yu, K., Aloqaily, M., Alazab, M., Lv, Z., & Mumtaz, S. (2020). Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV. *IEEE Transactions on Vehicular Technology*, *69*(11), 13784-13795. https://doi.org/10.1109/TVT.2020.3027568

Fitwi, A., Chen, Y., & Zhou, N. (2019, May). An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring. In *Signal Processing, Sensor/Information Fusion and Target Recognition XXVIII* (Vol. 11018, pp. 173-188). SPIE. https://doi.org/10.1117/12.2519006

Gülataş, İ., & Baktir, S. (2018). Unmanned aerial vehicle digital forensic investigation framework. *Journal of Naval Sciences and Engineering*, *14*(1), 32-53.

Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking and interdiction for amateur drones. *IEEE Communications Magazine*, *56*(4), 75-81. https://doi.org/10.1109/MCOM.2018.1700455

Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, *16*, 1-11. https://doi.org/10.1016/j.diin.2015.11.002

Husnjak, S., Forenbacher, I., Peraković, D., & Cvitić, I. (2022). UAV Forensics: DJI Mavic Air Noninvasive Data Extraction and Analysis. In *5th EAI International Conference on Management of Manufacturing Systems* (pp. 115-127). Springer, Cham. https://doi.org/10.1007/978-3-030-67241-6_10

Jain, U., Rogers, M., & Matson, E. T. (2017, March). Drone forensic framework: Sensor and data identification and verification. In *2017 IEEE Sensors Applications Symposium (SAS)* (pp. 1-6). IEEE. https://doi.org/10.1109/SAS.2017.7894059

Jones, Z. V., Gwinnett, C., & Jackson, A. R. (2019). The effect of tape type, taping method and tape storage temperature on the retrieval rate of fibres from various surfaces: An example of data generation and analysis to facilitate trace evidence recovery validation and optimisation. *Science & Justice*, *59*(3), 268-291. https://doi.org/10.1016/j.scijus.2018.12.003

Kelly, S., & Pohjonen, R. (2009). Worst practices for domain-specific modeling. *IEEE Software*, *26*(4), 22-29. https://doi.org/10.1109/MS.2009.109

Lakew Yihunie, F., Singh, A. K., & Bhatia, S. (2020). Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. In *Smart systems and IoT: Innovations in computing* (pp. 701-710). Springer, Singapore. https://doi.org/10.1007/978-981-13-8406-6_66

Lan, J. K. W., & Lee, F. K. W. (2022, February). Drone Forensics: A Case Study on DJI Mavic Air 2. In *2022 24th International Conference on Advanced Communication Technology (ICACT)* (pp. 291-296).

Le Roy, F., Roland, C., Le Jeune, D., & Diguet, J. P. (2019, August). Risk assessment of SDR-based attacks with UAVs. In *2019 16th International Symposium on Wireless Communication Systems (ISWCS)* (pp. 222-226). IEEE. https://doi.org/10.1109/ISWCS.2019.8877144

Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., & Srivastava, G. (2021). An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1949-1960. https://doi.org/10.1109/JBHI.2021.3075995

Llewellyn, M. (2017). Dji phantom 3-drone forensic data exploration. *Edith Cowan University: Perth, Australia*, *2*, 017.

Maarse, M., Sangers, L., van Ginkel, J., & Pouw, M. (2016). Digital forensics on a DJI Phantom 2 Vision+ UAV. *University of Amsterdam*, *1*, 22.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

Maune, K. G. (2018). A project completed as part of the requirements for BSc (Hons) Computer Forensic Investigation.

Mei, N. (2019). *Unmanned Aircraft Systems Forensics Framework an Approach to Unmanned Aircraft Systems Forensics Framework* (Doctoral dissertation, Capitol Technology University).

Mhatre, V., Chavan, S., Samuel, A., Patil, A., Chittimilla, A., & Kumar, N. (2015, November). Embedded video processing and data acquisition for unmanned aerial vehicle. In *2015 International Conference on Computers, Communications and Systems (ICCCS)* (pp. 141-145). IEEE. https://doi.org/10.1109/CCOMS.2015.7562889

Mistry, N. R., & Sanghvi, H. P. (2021). Drone forensics: investigative guide for law enforcement agencies. *International Journal of Electronic Security and Digital Forensics*, *13*(3), 334-345. https://doi.org/10.1504/IJESDF.2021.114950

Mohan, M. (2016). *Cybersecurity in drones* (Doctoral dissertation, Utica College).

Ngadi, M., Al-Dhaqm, R., & Mohammed, A. (2012). Detection and prevention of malicious activities on RDBMS relational database management systems. *Int. J. Sci. Eng. Res*, *3*(9), 1-10.

Onwuegbuzie, I. U., Abd Razak, S., Fauzi Isnin, I., Darwish, T. S., & Al-Dhaqm, A. (2020). Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach. *PloS One*, *15*(8), e0237154. https://doi.org/10.1371/journal.pone.0237154

Parghi, P., Dhamija, R., & Agrawal, A. K. (2022). Innovative Approach to Onboard Media Forensic of a Drone. In *IOT with Smart Systems* (pp. 307-314). Springer, Singapore. https://doi.org/10.1007/978-981-16-3945-6_30

Prastya, S. E., Riadi, I., & Luthfi, A. (2017). Forensic analysis of unmanned aerial vehicle to obtain GPS log data as digital evidence. *IJCSIS*, *15*(3).

Procházka, T. (2016). Capturing, visualizing and analyzing data from drones. https://dspace.cuni.cz/handle/20.500.11956/84552

Renduchintala, A. L. S., Albehadili, A., & Javaid, A. Y. (2017, December). Drone forensics: Digital flight log examination framework for micro drones. In *2017 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 91-96). IEEE. https://doi.org/10.1109/CSCI.2017.15

Renduchintala, A., Jahan, F., Khanna, R., & Javaid, A. Y. (2019). A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digital Investigation*, *30*, 52-72. https://doi.org/10.1016/j.diin.2019.07.002

Roder, A., Choo, K. K. R., & Le-Khac, N. A. (2018). Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv preprint arXiv:1804.08649*.

Salamh, F. E., Karabiyik, U., Rogers, M., & Al-Hazemi, F. (2019, June). Drone disrupted denial of service attack (3DOS): Towards an incident response and forensic analysis of remotely piloted aerial systems (RPASs). In *2019 15th international wireless communications & mobile computing conference (iwcmc)* (pp. 704-710). IEEE. https://doi.org/10.1109/IWCMC.2019.8766538

Sargent, R. G. (2015). Model verification and validation. In *Modeling and simulation in the systems engineering life cycle* (pp. 57-65). Springer, London. https://doi.org/10.1007/978-1-4471-5634-5_6

Sciancalepore, S., Ibrahim, O. A., Oligeri, G., & Di Pietro, R. (2019, May). Detecting drone's status via encrypted traffic analysis. In *Proceedings of the ACM Workshop on Wireless Security and Machine Learning* (pp. 67-72). https://doi.org/10.1145/3324921.3328791

Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., & Chen, J. (2018). Anti-drone system with multiple surveillance technologies: Architecture, implementation and challenges. *IEEE Communications Magazine*, *56*(4), 68-74. https://doi.org/10.1109/MCOM.2018.1700430

Tan, L., Yu, K., Shi, N., Yang, C., Wei, W., & Lu, H. (2021a). Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach. *IEEE Transactions on Network Science and Engineering*, *9*(1), 271-281. https://doi.org/10.1109/TNSE.2021.3101842

Tan, L., Yu, K., Ming, F., Cheng, X., & Srivastava, G. (2021b). Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness. *IEEE Consumer Electronics Magazine*, *11*(3), 69-78. https://doi.org/10.1109/MCE.2021.3081874

Tan, L., Yu, K., Lin, L., Cheng, X., Srivastava, G., Lin, J. C. W., & Wei, W. (2021c). Speech Emotion Recognition Enhanced Traffic Efficiency Solution for Autonomous Vehicles in a 5G-Enabled Space–Air–Ground Integrated Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2830-2842. https://doi.org/10.1109/TITS.2021.3119921

Ullah, F., & Pun, C. M. (2021). The role of Internet of Things for adaptive traffic prioritization in wireless body area networks. In *Healthcare Paradigms in the Internet of Things Ecosystem* (pp. 63-82). Academic Press. https://doi.org/10.1016/B978-0-12-819664-9.00004-1

Yang, C. C., Chuang, H., & Kao, D. Y. (2021). Drone forensic analysis using relational flight data: A case study of DJI Spark and mavic Air. *Procedia Computer Science*, *192*, 1359-1368. https://doi.org/10.1016/j.procs.2021.08.139

Yu, K., Arifuzzaman, M., Wen, Z., Zhang, D., & Sato, T. (2015). A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. *IEEE Transactions on Instrumentation and Measurement*, *64*(8), 2072-2085. https://doi.org/10.1109/TIM.2015.2444238

Yu, K., Tan, L., Lin, L., Cheng, X., Yi, Z., & Sato, T. (2021a). Deep-learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health. *IEEE Wireless Communications*, *28*(3), 54-61. https://doi.org/10.1109/MWC.001.2000374

Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A. K., & Khan, F. A. (2021b). Securing critical infrastructures: Deep-learning-based threat detection in IIoT. *IEEE Communications Magazine*, *59*(10), 76-82. https://doi.org/10.1109/MCOM.101.2001126

Yu, K., Guo, Z., Shen, Y., Wang, W., Lin, J. C. W., & Sato, T. (2021c). Secure artificial intelligence of things for implicit group recommendations. *IEEE Internet of Things Journal*, *9*(4), 2698-2707. https://doi.org/10.1109/JIOT.2021.3079574

Yu, K., Tan, L., Yang, C., Choo, K. K. R., Bashir, A. K., Rodrigues, J. J., & Sato, T. (2021d). A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3125190

Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021e). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Transactions on Industrial Informatics*, *17*(11), 7669-7678. https://doi.org/10.1109/TII.2021.3049141

Zhou, Z., Dong, X., Li, Z., Yu, K., Ding, C., & Yang, Y. (2022). Spatio-temporal feature encoding for traffic accident detection in vanet environment. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3147826