2-1-2022

ECU-IoFT: A dataset for analysing cyber-attacks on internet of flying things

Mohiuddin Ahmed
Edith Cowan University, mohiuddin.ahmed@ecu.edu.au

David Cox
Edith Cowan University, dcox5@our.ecu.edu.au

Benjamin Simpson
Edith Cowan University, bjsimpso@our.ecu.edu.au

Aseel Aloufi
Edith Cowan University, aaloufi@our.ecu.edu.a

10.3390/app12041990
Ahmed, M., Cox, D., Simpson, B., & Aloufi, A. (2022). ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internet of Flying Things. Applied Sciences, 12(4), 1990. https://doi.org/10.3390/app12041990

applied sciences

MDPI

Article

ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internet of Flying Things

Mohiuddin Ahmed *,†, David Cox †, Benjamin Simpson † and Aseel Aloufi †

School of Science, Edith Cowan University, Perth 6027, Australia; dcox5@our.ecu.edu.au (D.C.); bjsimpso@our.ecu.edu.au (B.S.); aaloufi@our.ecu.edu.au (A.A.)

* Correspondence: mohiuddin.ahmed@ecu.edu.au

† These authors contributed equally to this work.

Abstract: There has been a significant increase in the adoption of unmanned aerial vehicles (UAV) within science, technology, engineering, and mathematics project-based learning. However, the risks that education providers place their student and staff under is often unknown or undocumented. Low-end consumer drones used within the education sector are vulnerable to state-of-the-art cyberattacks. Therefore, datasets are required to conduct further research to establish cyber defenses for UAVs used within the education sector. This paper showcases the development of the ECU-IoFT dataset, documenting three known cyber-attacks targeting Wi-Fi communications and the lack of security in an affordable off-the-shelf drone. At present, there are no publicly available labeled datasets that reflect cyberattacks on the Internet of Flying Things (IoFT). The majority of the publicly available network traffic datasets are emulated and do not reflect the scenarios/attacks from a real test setup. This dataset will be beneficial for both cybersecurity researchers to develop defense strategies and UAV manufacturers to design more secure products. In the future, endeavors will be taken to incorporate newer attacks and create datasets appropriate for big data analysis.

Keywords: cyberattack; UAV; dataset; STEM; IDS; IoFT

Citation: Ahmed, M.; Cox, D.; Simpson, B.; Aloufi, A. ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internet of Flying Things. *Appl. Sci.* **2022**, *12*, 1990. https://doi.org/10.3390/app12041990

Academic Editors: Gianni Pantaleo and Pierfrancesco Bellini

Received: 19 January 2022
Accepted: 9 February 2022
Published: 14 February 2022

1. Introduction

The Internet of Things (IoT) has shifted from an up-and-coming technology concept to a heavily utilised technology. IoT embeds everyday devices with small, low-powered computers and wireless networks to add "Smart" functionality to a regular item, allowing for inter-connectivity between devices, the cloud, and enabling automation [1]. A domain where IoT has significantly grown is within the Internet of Flying Things (IoFT). The adoption of IoFT devices often referred to as drones or the more accurate terminology unmanned arial vehicles (UAV), has significantly increased within government, enterprise, and personal use over the past years [2]. In 2018, The Australian Government Civil Aviation Safety Authority (CASA) estimated that over 150,000 UAVs were in operation within Australia [3]. This increase in UAV use is due to UAV's increased capabilities and endurance, the ease of flight and the minimal training required for flying, and the reduced operational cost compared to traditional aviation mediums such as helicopters and small planes [4]. Government agencies and private sector businesses are utilising UAVs for cinematography, crisis management, environmental and maritime research, traffic monitoring and for courier deliveries [2,5].

With this increase in adaptation of UAV's, educators are embedding UAV's (drones) within their STEM (science, technology, engineering and mathematics) programs [6]. The lack of cybersecurity awareness surrounding IoFT within the educational context (staff, students and parents) can contribute to vulnerabilities to IoFT Devices. Notable attack vectors targeting UAV's (but not limited to) include denial-of-service (control signals and GPS), Man-in-the-middle attacks and exploited Application Programmable Interface

(API) [7]. The consequences of such attacks not only contribute to the loss of assets or cause reputational damage but, more importantly, could place children and teens in physical harm or breach their privacy [2].

Appropriate security cannot be implemented while attacks against IoFT platforms remain undocumented. UAVs will present as a target to cyber-attackers [2]; hence, it is essential that a deeper understanding of cyber-vulnerabilities relating to IoFT is pursued. Researchers require data into cyber-attacks launched against IoFT devices in order to develop behaviour signatures that can be used to identify, mitigate and develop counter-measures [8]. Table 1 shows that there is a significant lack of real world data in the context of IoFT and Drones. While there are emulated datasets available for intrusion detection systems (IDS), these are not going to be effective in real-world scenarios, and hence in this paper, we have tried to develop a dataset portraying realistic scenarios.

Table 1. IDS Dataset Comparison.

Dataset	Year	Publicly Available	Traffic Type	Labelled	IoFT
DARPA 1998 [9]	1998	Yes	Emulated	Yes	No
UNSW-NB15 [10]	2015	Yes	Emulated	Yes	No
TRAbID citeRING2019147	2017	Yes	Emulated	Yes	No
CSE-CIC-IDS2018 [11]	2018	Yes	Real	Yes	No
ECU-IoHT [8]	2020	Yes	Emulated	Yes	No
UAV Attack [12]	2021	Yes	Emulated	No	Yes
ECU-IoFT	2022	Yes	Real	Yes	Yes

Although many risks to commercial UAVs have been documented, many of these are attacks are documented in a theoretical context [7]. This paper aims to investigate the risks associated with the usage of drones in education domain. In addition, to understand the cyberattacks better in IoFT, a dataset has been developed, and allowing further research to establish cyber defences for UAVs. The dataset is named ECU-IoFT as the contributors are all from Edith Cowan University and it has been a general practice by the research community to name the datasets based on the institution, i.e., DARPA, UNSW, etc. The key objectives and contributions of the paper are as follows:

- Cyber vulnerability analysis of an off-the-shelf low-cost drone used in educational purpose.
- Risk associated of using vulnerable drones.
- Simulation of three cyber attacks on Internet of Flying Things scenario.
- Development of a benchmark dataset capturing the network traffic (Available in GitHub).
- Performance analysis of most popular anomaly detection algorithms using the developed dataset.
- Future research directions in IoFT cyber security.

Figure 1 shows the paper structure. The following sections of this paper will provide a brief discussion of UAVs within the education domain and highlight the risk that these could pose to students (Section 2). Section 3 discusses the development of the ECU-IoFT; Section 4 includes the performance analysis of the most widely used anomaly detection algorithms applied on the ECU-IoFT dataset. Section 5 will present the interesting findings about commercial off the shelf drones, and Section 6 concludes the paper and presents possible future research.

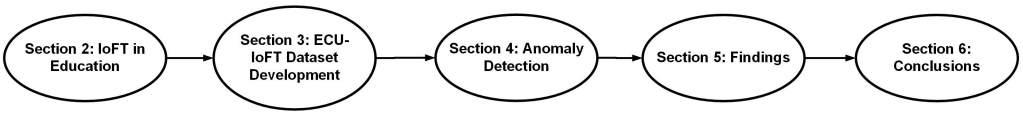

Figure 1. Paper roadmap.

2. IoFT within the Education Domain

As schools and educational institutions strive to educate students within Science, Technology, Engineering and Mathematics (STEM) and with the increase of affordability of UAV's, their implementation within the education sector has increased [13,14]. However, with this increase in adoption, the understanding of the cyber security implications of the use of low-end UAV's (IoFT) within the education sector is lacking.

2.1. IoFT in the Classroom

In December 2015, the Australian Education Ministers endorsed a 10-year (2016–2026) National STEM strategy focusing on delivering foundational skills in Science, Technology, Engineering and Mathematics. This plan promotes creative and critical thinking for K-12 students undertaking project-based learning [15]. This growth of Project-Based STEM projects has led to the increase in the use of UAVs within the education sector [14]. The UAV's that stand out within the education K-12 domain (Adapted from "7 Best Drones For Education To Build, Learn To Code and Configure" By F. Corrigan, 2020 (https://www.dronezon.com/learn-about-drones-quadcopters/best-educational-drones-kits-to-build-and-code-uavs/ (accessed on 18 January 2022)). Copyright 2020 by Drone-Zon.com (accessed on 18 January 2022) due to their price and features discussed below:

- Robolink CoDrone Lite: 8 min of flight time, Programable in Snap, Python and Blockly.
- Sky Viper e1700 Stunt: Two flight modes, Controller can be adjusted to match the best sensitivity, Auto Launch and Land.
- Ryze Tello EDU: Programable in Python, Swift and Scratch, 13 min of flight time, HD video streaming, Auto Launch and landing.
- Parrot Mambo Fly: Programmable in Blockly, Tynker, Python and JavaScript, 60 fps camera and Fly range 20 m with smart phone or 100 m with remote controller.

Of particular significance of UAVs referenced was the Ryze Tello. The Tello was DJI's first UAV directly targeted to the education sector and allows for students to learn to control the UAV using programming languages such as python or scratch. Although the Tello is not directly produced by DJI, it does utilise DJI's high-quality flight technology that is utilised in their high-end drones [16]. The Ryze Tello is currently heavily used in schools in Japan [17]. However, the use of the DJI Tello does pose cyber risks to the learning institute, staff and students that utilise this and similar IoFT devices.

2.2. Cyber Risk to Students

We identified three potential risks to students, staff, and the school community that exist if a cyber-attack was executed against a UAV used within an educational institution. Firstly, a total loss of an asset (UAV), secondly the safety to students, teachers, and community. Thirdly, the potential consequences for a breach in students' (Persons Under 18) privacy. The loss of an asset in the context discussed within this paper can refer to physical damage or total loss of the UAV. Given the low cost of most UAV's used within the education sector, such as the Ryze Tello costing less than two hundred Australian dollars (as of 21 September 2021) from DJI's Online Store (https://m.dji.com/au/product/tello (accessed on 18 January 2022)), the loss of a single UAV due to a cyber-attack poses minimal financial loss to an educational institution. This loss could be considered more as an inconvenience than a major financial risk to students or staff. However, due to the swarming capabilities of many of these education-based UAV's [18], the cost incurred by the loss of assets could exponentially grow.

Under the Duty of Care Policy dictated by the Western Australian Department of Education, staff members of a school (teachers and administration) are responsible for protecting students from unreasonable risk or harm. As such, identifying the physical risks UAVs pose to students is essential. For example, if a student or staff member was to lose control of a UAV due to a cyber-attack. The potential to cause significant injury to a student,

staff member, or the wider community exists. In addition to the physical harm to humans, there also exists the risk to the education institute's reputation. Reputational damage has the potential to jeopardize future enrolments, plans, and goals the education institute may have [19].

The final concern relates to a breach of a student's privacy. If an attacker was able to access the video feed of the UAV or stored images on internal storage or accessed via the memory of the device an attacker may compromise the privacy of the students using the UAV. Under the Privacy Act 1998 [20], the act places the responsibility for privacy on a guardian of that child. As such, the school would be responsible to protect the student's privacy while under the school's care. In addition, many schools have school photograph policies dictating what students' photographs can be published in the community, breaches to this policy could result in legal consequences or loss of reputation [21].

In this paper, two different hypothetical scenarios of potential cyber-attacks are considered that could be launched against UAV's used within the education sector. The first is that the student or teacher loses control of the UAV due to a cyberattack, resulting in the UAVs flying into the student, endangering their safety. The second attack would be that student's privacy may be breached by a cyber attacker accessing the camera of the UAV while under the control of students or the attacker takes control of the drone and flying it, out of the operators reach and into the cyber attacker's possession, where they can extract images of the students forensically [22,23]. Each of these attacks contains a different motive; The first motive would be to place the student in harm's way. The second hypothetical motive would be to breach the privacy of students using the UAVs.

3. ECU-IoFT Dataset Development

When comparing mainstream IDS Datasets (Table 1), the need to develop a purpose-made IoFT dataset needs to be created to adequately identify security threats targeted by Low-end consumer IoFT devices, often used within the education sector. The development of the ECU-IoFT dataset followed the philosophy of a remote grey box penetration test. A penetration test is considered a grey box when some but not all of the information and internal workings of the target is known [24]. For example, knowing the drone that is being targeted without knowledge of the inner workings. The recognizance, modeling, and exploitation follow the seven-phase framework of the Penetration Testing Execution Standard (PTES). The seven-stage framework can be seen in Figure 2.

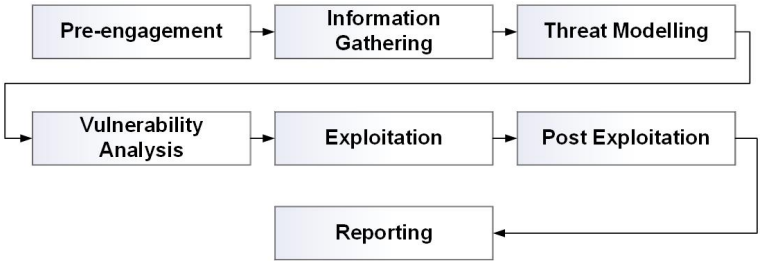

Figure 2. Flow Chart of the PTES framework Note: Adapted from "High Level Organization of the Standard" by Penetration Testing Execution Standard, n.d. (https://pentest-standard.readthedocs.io/en/latest/index.html) (accessed on 18 January 2022). Copyright 2016 by The PTES Team Revision 968a38d0.

3.1. Environment

The Ryze Tello TLW004 running firmware version 01.04.92.01 was used for developing the ECU-IoFT. A pre-shared key (PSK) had been set on the default wireless network to produce the dataset, assuming that a user may attempt to add some security to the UAV. The UAV was controlled via a Google Pixel 2 running Android 10 (QQ3A.200805.001) using the Tello app (1.6.0.0) available from the Google play store. To execute the attack and collect the data, an attack machine used to generate the dataset was running a Kali Virtual Machine build 2021.2 running within VMware Workstation Pro 16.1.2. To intercept and listen to

Wi-Fi signals generated between the phone and UAV, the Alpha Networks AWUS036NEH was passed through to the virtual machine, allowing kali to enter the adapter into monitor mode. The lab configuration can be seen in Figure 3.

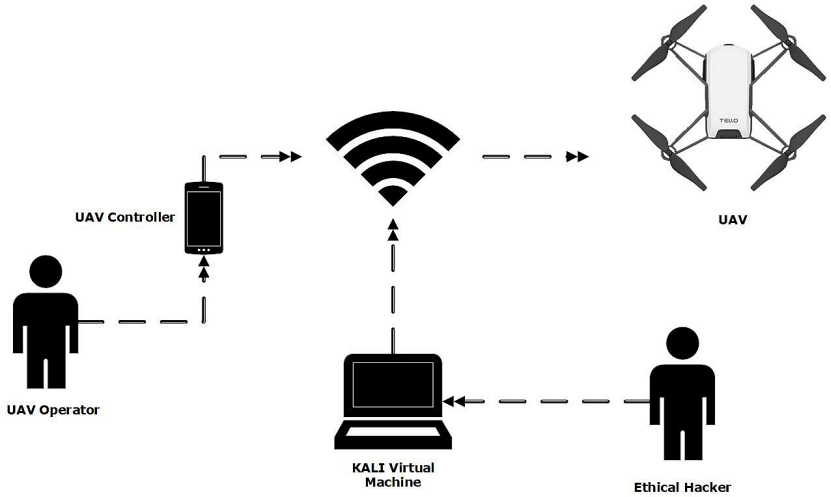

Figure 3. ECU-IoFT Dataset—Testbed Design.

3.2. Cyber Attacks Launched

Three cyber-attacks were used to exploit and gain control of the Ryze Tello Drone: Wi-Fi Deauthentication Attack, WPA2-PSK Wi-Fi Cracking Attack, and Tello API Exploit [25]. A High-Level Overview of the attack scenario used to generate the dataset can be seen in Figure 4.

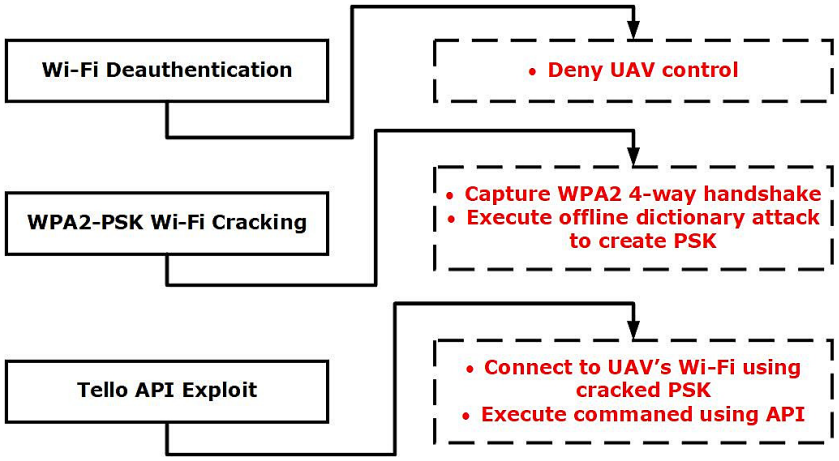

Figure 4. High-level Overview of Attack scenario.

3.2.1. Wi-Fi Deauthentication Attack

A Wi-Fi deauthentication (DEAUTH) attack is a form of Denial of Service (DoS) attack that denies communication between the access point (Ryze Tello) and the Client (UAV Control Phone). Within this attack, the attacker will send crafted packets, where the access point thinks that the client has sent a packet that wishes them to disconnect from the network. A Wi-Fi DEAUTH attack is achievable because the DEAUTH command is within the Wi-Fi control frames, hence unencrypted, regardless of whether a WPA2-PSK is configured. This attack does not require the attacker to be a member of the network, the attacker just needs to be within the range of the Wi-Fi Access Point [26].

3.2.2. WPA2-PSK Wi-Fi Cracking Attack

WI-FI Networks that utilise WPA2-PSK (Pre-shared Keys) are often used within homes and small businesses where a single passphrase is shared between many users and is

configured within the wireless access point. The passphrases set on these networks are often too simple and are susceptible to brute force or dictionary attacks [27]. WPA2-PSK utilised AES (Advanced Encryption Standard) in order to secure the communications between the access point and the client device (drone and phone); AES is a symmetric-key algorithm, meaning the same key is used for encryption and decryption [28]. When a client device (Phone) wishes to connect to the access point (Drone), a four-way handshake is initiated to authenticate the client, allowing for communication of the encryption ciphers. Exchanged within this handshake are three critical pieces of information, The Pairwise Cipher suite (encrypts Unicast Data), the group cipher suite (encrypts multicast data) and the Authentication information (PSK). If an attacker can capture this handshake, the PSK can be brute-forced using an offline dictionary attack [28].

3.2.3. Tello API Exploit

Once connected to the Wi-Fi network of the Tello, the API trust that you are an authorised and authenticated user and allows for commands to be sent via the API. Within the attack scenario used to create the data set, the Wi-Fi password has been discovered via the steps discussed in Section 3.2.2. The attacker has then issued the emergency stop command that stops all the props no matter what the current state of the drone is. Hence, the extinction of this attack would cause the drone to fall to the ground without any control by the operator [29].

3.3. Dataset Development

For the period in which the dataset was captured (Table 2), attacks were executed from the attack machine (Kali Linux), this behaviour was captured using Wireshark. As each attack was independent from each other they were not captured in a continuous sequence and the timestamps are showcased in Table 3. It additionally highlights each attack scenario's influence on the dataset by identifying the number of observations (N) and the represented percentage (%). As seen, 74.4% of the dataset was captured under the WAP2-PSK Wi-Fi Cracking Attack scenario.

Table 2. ECU-IoFT Attack Scenario Timings, Writings and Line IDs.

ID	N (%)	Time	Attack Scenario
1–534	535 (1%)	12 September 2021: 4:34:49–4:34:49	No Attack
535–13,757	13,222 (24.3%)	12 September 2021: 10:27:40–10:28:43	Wi-Fi De-authentication
13,758–54,283	40,526 (74.4%)	13 September 2021: 03:04:09–03:05:49	Wi-Fi Cracking
54,283–54,492	209 (0.4%)	13 September 2021: 03:29:20–3:29:40	API Exploit

The dataset contains 10 Features; Table 3 provides an overview and description of the features. The dataset contains 54,492 instances of network traffic. Three features are used to label the data, the field "Type" represents a Binary Classification, the field "Type.of.attack" identifies the exploit that is being used and "attack.scenario" identifies what attack scenario conditions that sample was collected under.

Table 3. ECU-IoFT dataset structure.

Feature	Data Type	Description
ID	Integer	ID Number identifying a collected sample.
Time	Factor	Timestamp of the collected sample.
Source	Factor	The source address of collected sample.
Destination	Factor	Destination address of collected sample.
Protocol	Factor	Protocol used.
Length	Integer	Length of the Frame in bytes.
Info	Factor	Captured details relating to the captured sample.
Type	Factor	Binary Classification.
Type.of.Attack	Factor	Identifying the type of attack.
Attack.Scenario	Factor	The attack Scenario in which the sample was collected.

Figure 5 displays different statistical features of the dataset including the protocols used and the types of attacks logged. Much of the data collected used the 802.11 protocol due to the attacks primarily targeting the Wi-Fi communications (Table 4). The data are additionally skewed to the No attack behaviour, representing 60.8% of the data. This data analysis was conducted by importing the dataset into R Studio, this code can be found in GitHub.

Table 4. ECU-IoFT Dataset–Protocol distribution.

Protocol	Observation
802.11	54,280 (99.6%)
EAPOL	3 (close to 0%)
ICMP	2 (close to 0%)
UDP	207 (0.40%)

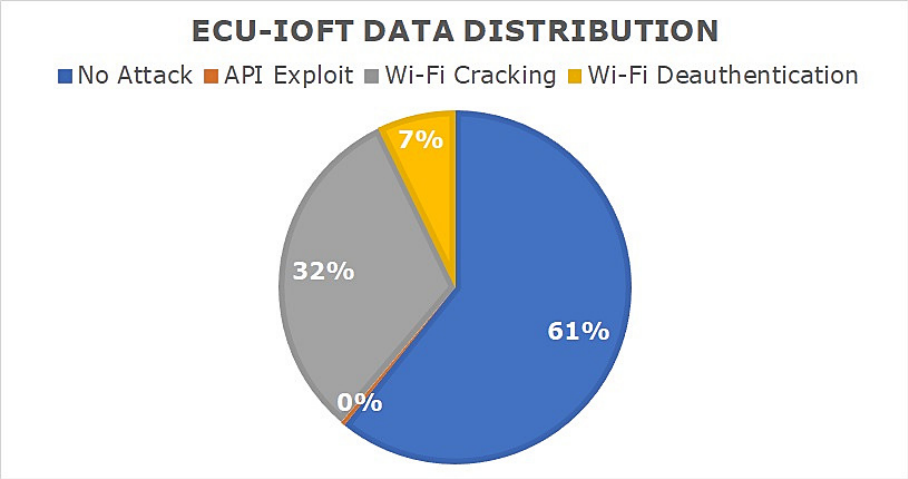

Figure 5. ECU-IoFT data distribution.

4. Anomaly Detection Using ECU-IoFT Dataset

Anomaly detection is an important data analysis task in the realm of cyber security [30,31]. In the last few decades, the artificial intelligence research community have developed a plethora of algorithms to analyse the data better and identify patterns of interest [32]. These algorithms are widely used to detect cyberattacks and to examine their efficacy, newer datasets are required. Therefore, in this section, ECU-IoFT dataset is used to analyse the performance of five most popular anomaly detection algorithms. Since, supervised and semi-supervised algorithms require a set of data for training and unable to

identify zero-day attacks, we have excluded them for the analysis. For evaluation purpose, we have used the *Hit Rate* metric, also known as *True Positive Rate*. Figure 6 showcases the anomaly detection techniques used for analysis. The details of these algorithms are available in [8,33,34].

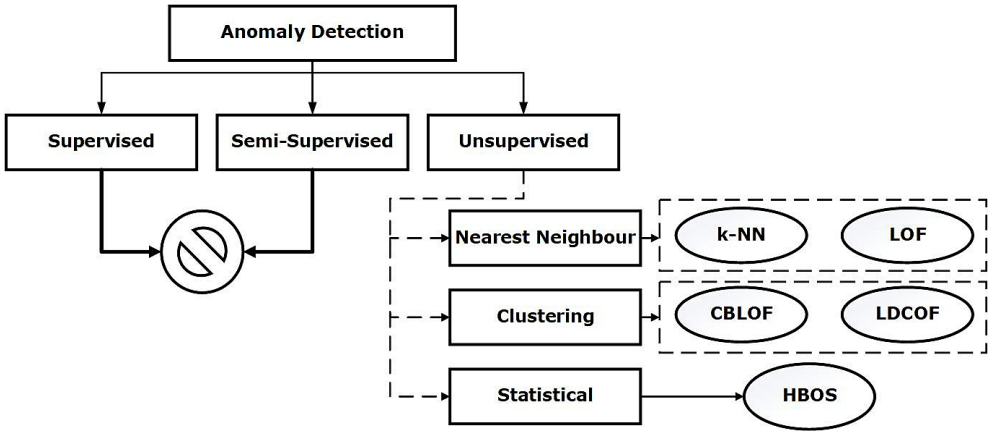

Figure 6. Anomaly detection algorithms.

In Table 5, the performance of these algorithms is showcased in identifying individual attacks from the ECU-IoFT dataset (the green color is a reflection of best performance and the red color is for worst performance). It is clear that each of the algorithms is successful in identifying the API exploits, whereas the majority of algorithms (k-NN, LOF, and HBOS) struggled to detect the deauthentication attacks. The cracking attacks are fairly identifiable by the algorithms and k-NN shows superior performance. Figure 7 showcases the overall performance in identifying attacks from the dataset. It is evident that, among these five popular algorithms, clustering-based techniques are more suitable for identifying the three types of attacks in IoFT environment, i.e., API exploit, Wi-Fi cracking, and deauthentication. In future instances, the endeavor will be taken towards other types of cyberattacks and the effectiveness of other algorithms will be investigated. At present in the given circumstances of ECU-IoFT dataset, the *CBLOF* technique [35] outperforms the rest of the techniques to identify the three attacks showcased in this paper.

Table 5. Hit rates of anomaly detection algorithms.

Algorithm	API Exploit	Deauthentication	Cracking
k-NN	100%	2.83%	100%
LOF	100%	0%	37.83%
CBLOF	100%	100%	81.07%
LDCOF	100%	100%	63.72%
HBOS	100%	0%	37.53%

Based on the signature analysis of deauthentication attacks, it is observed that these attacks do not require the attacker to be a member of the Wi-Fi network. The attackers can launch attacks just being within the vicinity of Wi-Fi Access Point. To address such attacks, the Wi-Fi network administrators can set some access control mechanisms to hinder such attacks. The drone manufacturers can also incorporate more strong authentication policies to ensure the safety and security of the drone users. Since these low-cost drones are mostly used in the education sector, the compromised drone ecosystem will jeopardize the original objectives. We are hopeful that, this paper will reinforce the need for robust cyber security in low-end drones and create awareness for the users.

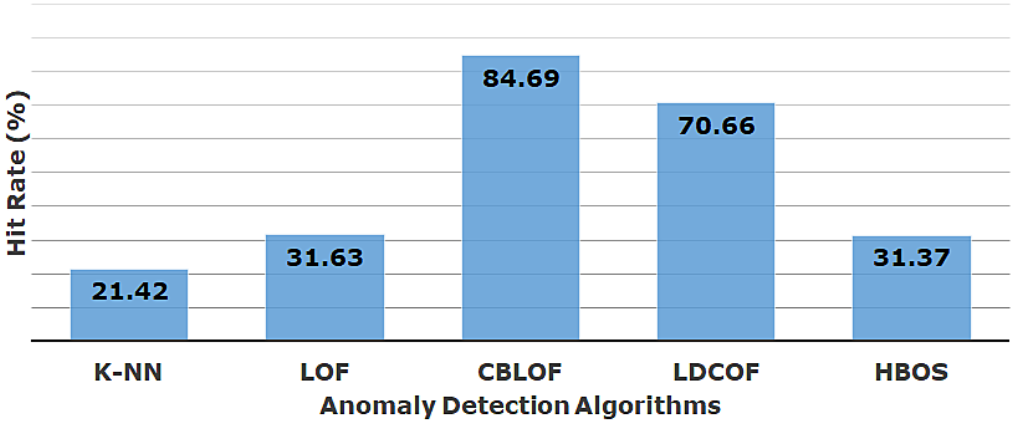

Figure 7. Overall performance comparison.

5. Findings

Based on the test and attacks used against the Ryze Tello Drone, it can be concluded that the Tello lacks the basic security that many other flight control systems produced by DJI contain. By default, the Tello does not contain a password on the Wi-Fi network it broadcasts, nor does it prompt the user for a password on the first connection. This would allow any user that is in range of the drone to connect to the Wi-Fi network and have the ability to control, view the camera and execute code on the drone.

Secondly, there is an overall lack of security on Tello's API. The API lacks any form of authentication, simply relying on the trust based on the connection to the UAV's Wi-Fi network, given that the default configuration of the Wi-Fi network broadcast by the Tello does not contain a password this level of security cannot be trusted. Device registration on the app to generate an API token or a physical button before the API can be communicated with should be implemented to prove control and ownership, as is seen in high-end UAVs [36].

In commencing the research into producing a dataset of state-of-the-art cyber-attacks, the authors commenced their research using the DJI Mavic Pro 2; however, no notable vulnerabilities were discovered. The Mavic Pro 2 is a high-end UAV that costs more than two thousand Australian dollars. This drone implements OcuSync 2.0 for communication between the controller and the UAV. OcuSync 2.0 built upon and improved the original implementation of OcuSync used in the original Mavic Pro. This new version allows for video streaming in 1080p and control of the drone up to 8 Km away, this was achieved through its use of dual-band broadcasting [37].

Targeting the communication between the UAV and the controller was where the authors first began researching possible attacks. If a radio frequency (RF) receiver such as the HackRF One was used to detect the UAV, it was hypothetically proposed to be possible to broadcast a stronger signal fundamentally blocking the communication from the UAV and the controller. Upon further research, it was discovered that DJI had mitigated this type of attack within the implementation of OcuSync 2.0. OcuSync 2.0 utilizes automatic band switching, if the signal is weak on one frequency it will switch to a stronger frequency that offers a stronger signal to provide the best connection [37]. This made this form of attack improbable. The authors pivoted their research to the Android mobile application DJI Go v4. A vulnerability was documented in 2020 targeting the auto-update mechanism for the application available for direct download from the DJI Website [38]. This version of the app contained the ability to self-update from DJI servers instead of downloading the update from the Google Play Store. When downloading the update, the traffic was able to be intercepted using a man-in-the-middle attack (Burp Suite). This could have allowed an attacker to change the URL of the update and execute any arbitrary code due to the elevated permissions (Contacts, Camera, Storage, Microphone).

When the authors attempted to execute the man-in-the-middle attack, they were unable to find any success with the application [38]. The authors attempted to use older APK versions of the application, without success. Upon further research, it was discovered that DJI mitigated the vulnerability within the application in addition to removing all backend infrastructure. Based on the discoveries from the research conducted on the DJI Mavic Pro 2 the authors concluded that they were not able to produce a dataset using the Mavic Pro 2, and hence pivoted their research to low-end consumer drones used in the education domain, such as the Ryze Tello where a greater scope of vulnerabilities exists. For more details, interested readers can study the dataset and the attacks launched. All this information is publicly available.

6. Conclusions and Future Works

The lack of cybersecurity awareness surrounding IoFT within the educational context can contribute to vulnerabilities to IoFT Devices that can cause potential harm or breach students' privacy. Therefore, it is essential to better understand and detect the potential attacks that a cyber-criminal may use. This paper is a first step in addressing this problem by creating a dataset of known attacks targeting the Ryze Tello Drone. Future research needs to be conducted to apply this dataset to detect attacks on Educational IoFT Devices. Additionally, attack samples from a greater selection of education UAVs should take place to achieve a more comprehensive dataset. In addition, it is also evident that the artificial intelligence research community can analyse the data better to understand the attack characteristics and develop more sophisticated countermeasures. In recent times, there have been some novel approaches in securing the distributed and smart systems [39–45]. We are optimistic that, the ECU-IoFT dataset will bring forth several new directions in UAV and cuber security research.

Author Contributions: Conceptualization, M.A.; methodology, D.C.; software, B.S., A.A. and D.C.; validation, M.A.; formal analysis, D.C. and M.A.; investigation, B.S. and A.A.; resources, M.A., D.C., B.S. and A.A.; data curation, M.A.; writing—original draft preparation, D.C., B.S., A.A. and M.A.; writing—review and editing, M.A.; visualization, M.A.; supervision, M.A.; project administration, M.A.; funding acquisition, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: No funding was specifically available for this work.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data and materials are shared using GitHub https://github.com/iMohi/ECU-IoFT (accessed on 18 January 2022).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

IoFT	Internet of Flying Things
STEM	Science, Technology, Engineering and Mathematics
IDS	Intrusion Detection Systems
CASA	Civil Aviation Safety Authority
API	Application Programming Interface
PTES	Penetration Testing Execution Standard
PSK	Pre-Shared Keys
UAV	Unmanned Aerial Vehicles

References

1. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]
2. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]

3. Review of Aviation Safety Regulation of Remotely Piloted Aircraft Systems by Australian Civil Aviation Safety Authority. 2018. Available online: https://consultation.casa.gov.au/regulatory-program/ (accessed on 3 January 2022).
4. Zaidi, S.; Atiquzzaman, M.; Calafate, C.T. Internet of Flying Things (IoFT): A Survey. *Comput. Commun.* **2021**, *165*, 53–74. [CrossRef]
5. Amazon Prime Air. 2021. Available online: https://www.amazon.com/Amazon-Prime-Air/ (accessed on 3 January 2022).
6. Meet The Entrepreneurs Bringing Drones to STEM Education. 2020. Available online: https://www.forbes.com/sites/forbestechcouncil/2020/12/08/meet-the-entrepreneurs-bringing-drones-to-stem-education (accessed on 3 January 2022).
7. Aerial Threat: Why Drone Hacking Could Be Bad News for the Military. 2019. Available online: https://theconversation.com/aerial-threat-why-drone-hacking-could-be-bad-news-for-the-military-124588 (accessed on 3 January 2022).
8. Ahmed, M.; Byreddy, S.; Nutakki, A.; Sikos, L.F.; Haskell-Dowland, P. ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. *Ad Hoc Netw.* **2021**, *122*, 102621. [CrossRef]
9. Ring, M.; Wunderlich, S.; Scheuring, D.; Landes, D.; Hotho, A. A survey of network-based intrusion detection data sets. *Comput. Secur.* **2019**, *86*, 147–167. [CrossRef]
10. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6. [CrossRef]
11. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018). 2018. Available online: https://registry.opendata.aws/cse-cic-ids2018 (accessed on 3 January 2022).
12. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. UAV Attack Dataset. Available online: https://ieee-dataport.org/open-access/uav-attack-dataset (accessed on 3 January 2022).
13. Incorporating Drones into STEM Education. RobotLAB Blog. 2020. Available online: https://www.robotlab.com/blog/incorporating-drones-into-stem-education (accessed on 3 January 2022).
14. Micro-Drones for STEM Education. 2019. Available online: https://sites.rmit.edu.au/cyber-physical-systems/2019/01/10/micro-drones-for-stem-education/ (accessed on 3 January 2022).
15. National STEM School Education Strategy 2016–2026. Australian Goverment. 2020. Available online: https://www.dese.gov.au/australian-curriculum/support-science-technology-engineering-and-mathematics-stem/national-stem-school-education-strategy-2016-2026 (accessed on 3 January 2022).
16. What Is DJI Doing for STEAM Education Around the World? DroneDJ. 2020. Available online: https://dronedj.com/2020/08/17/what-is-dji-doing-for-steam-education-around-the-world/ (accessed on 3 January 2022).
17. Yamamori, K. Classroom practices of low-cost STEM education using scratch. *J. Adv. Res. Soc. Sci. Humanit.* **2019**, *4*, 192–198. [CrossRef]
18. Adventures with DJI Ryze Tello: Controlling a Tello Swarm. 2018. Available online: https://medium.com/@henrymound/adventures-with-dji-ryze-tello-controlling-a-tello-swarm-1bce7d4e045d (accessed on 3 January 2022).
19. Agrafiotis, I.; Nurse, J.R.C.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J. Cybersecur.* **2018**, *4*, tyy006. [CrossRef]
20. Privacy Act 1988. Available online: https://www.legislation.gov.au/Details/C2021C00139 (accessed on 3 January 2022).
21. Australian Goverment Australian Law Reform Commission. 2010. Available online: https://www.alrc.gov.au (accessed on 3 January 2022).
22. Viswanathan, S.; Baig, Z. *Digital Forensics for Drones: A Study of Tools and Techniques*; Springer: Singapore, 2020; pp. 29–41. [CrossRef]
23. Yousef, M.; Iqbal, F.; Hussain, M. Drone Forensics: A Detailed Analysis of Emerging DJI Models. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 066–071. [CrossRef]
24. Yaqoob, I.; Hussain, S.; Mamoon, S.; Naseer, N.; Akram, J. *Penetration Testing and Vulnerability Assessment*; EverScience Publications: Tamil Nadu, India, 2017.
25. Rubbestad, G.; Söderqvist, W. *Hacking a Wi-Fi Based Drone*; DiVA Portal: Stockholm, Sweden, 2021.
26. Agarwal, M.; Biswas, S.; Nandi, S. Detection of De-authentication Denial of Service attack in 802.11 networks. In Proceedings of the 2013 Annual IEEE India Conference (INDICON), Mumbai, India, 13–15 December 2013; pp. 1–6. [CrossRef]
27. Radivilova, T.; Hassan, H.A. Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise. In Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 11–15 September 2017; pp. 1–4.
28. Abo-Soliman, M.A.; Azer, M. A study in WPA2 enterprise recent attacks. In Proceedings of the 2017 13th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 27–28 December 2017; pp. 323–330.
29. Ryze User Guide. 2018. Available online: https://dl-cdn.ryzerobotics.com/ (accessed on 3 January 2022).
30. Ahmed, M.; Barkat Ullah, A.S. Infrequent pattern mining in smart healthcare environment using data summarization. *J. Supercomput.* **2018**, *74*, 5041–5059. [CrossRef]
31. Rashid, A.N.M.B.; Ahmed, M.; Sikos, L.F.; Haskell-Dowland, P. Anomaly Detection in Cybersecurity Datasets via Cooperative Co-Evolution-Based Feature Selection. *ACM Trans. Manage. Inf. Syst.* **2022**, *13*, 1–39. [CrossRef]

32. Ahmed, M.; Choudhury, S.; Al-Turjman, F. Big Data Analytics for Intelligent Internet of Things. In *Artificial Intelligence in IoT*; Al-Turjman, F., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 107–127.
33. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
34. Ahmed, M.; Mahmood, A.N.; Islam, M.R. A survey of anomaly detection techniques in financial domain. *Future Gener. Comput. Syst.* **2016**, *55*, 278–288. [CrossRef]
35. He, Z.; Xu, X.; Deng, S. Discovering cluster-based local outliers. *Pattern Recognit. Lett.* **2003**, *24*, 1641–1650. [CrossRef]
36. Garg, H.; Dave, M. Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–6. [CrossRef]
37. Edström, V.; Zeynalli, E. *Penetration Testing a Civilian Drone: Reverse Engineering Software in Search for Security Vulnerabilities*; DiVA Portal: Stockholm, Sweden, 2020.
38. DJI Android GO 4 Application Security Analysis. 2020. Available online: https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html (accessed on 3 January 2022).
39. Abid, R.; Iwendi, C.; Javed, A.R.; Rizwan, M.; Jalil, Z.; Anajemba, J.H.; Biamba, C. An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Pers. Ubiquitous Comput.* **2021**, 1–14. [CrossRef]
40. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W., Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283. [CrossRef]
41. Kumar, P.; Tripathi, R.P.; Gupta, G. P2IDF: A Privacy-Preserving Based Intrusion Detection Framework for Software Defined Internet of Things-Fog (SDIoT-Fog). In Proceedings of the Adjunct Proceedings of the 2021 International Conference on Distributed Computing and Networking, Nara, Japan, 5–8 January 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 37–42.
42. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Comput. Commun.* **2021**, *166*, 110–124. [CrossRef]
43. Kumar, P.; Gupta, G.P.; Tripathi, R. Design of anomaly-based intrusion detection system using fog computing for IoT network. *Autom. Control. Comput. Sci.* **2021**, *55*, 137–147. [CrossRef]
44. Kumar, P.; Gupta, G.P.; Tripathi, R. Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks. *Arab. J. Sci. Eng.* **2021**, *46*, 3749–3778. [CrossRef]
45. Kumar, P.; Gupta, G.P.; Tripathi, R. A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *12*, 9555–9572. [CrossRef]