Securing Things in the Healthcare Internet of Things

Áine MacDermott[1], Phillip Kendrick[1], Ibrahim Idowu[1], Mal Ashall[2], Qi Shi[1]
[1]Department of Computer Science
[2]Department of Built Environment
Liverpool John Moores University
Liverpool, UK
{a.m.macdermott, p.g.kendrick, i.o.idowu, m.c.ashall, q.shi}@ljmu.ac.uk

***Abstract*—The Internet of Things (IoT) has had a positive impact on e-health, assisted living, human-centric sensing and wellness. Recently this interconnection has been referred to as Healthcare IoT (H-IoT). Real-time monitoring based on the information gathered from the connected 'things' provides large scale connectivity and a greater insight into patient care, individual habits and routines. While the benefits of introducing this paradigm into healthcare are conspicuous, the underlying security vulnerabilities and threats of the infrastructure and devices cannot go unaddressed. H-IoT is set to impact society significantly, and with attackers already exploiting the IoT in a myriad of ways, it is inevitable that the IoT will become the most vulnerable area of cyber security. Securing these 'things' in H-IoT requires a multi-faceted approach. A multi-agent approach to advanced persistent threat detection is conveyed with the use of machine learning for predictive analytics: identifying security vulnerabilities, identifying patterns in order to make predictions and identify outliers.**

***Index Terms*—Healthcare, Cyber Security, Internet of Things, IoT, H-IoT, Network Security, Cloud Computing, Fog Computing.**

I. Introduction

The Internet of Things (IoT) is not a new paradigm; the technological capabilities of society have enabled its immense progression and increased utilisation. The Industrial Internet of Things (IIoT) describes industrial 'things' where the end devices typically comprise sensors, actuators, industrial processes, used for automation and data collection. In short, the IoT and IIoT are commonly used to describe collections of Internet-enabled 'things' or smart devices, increasingly interconnected with other 'things' in a mass ecosystem. Similarly, H-IoT (Healthcare Internet of Things) [1]–[4] is a relatively newer term, but describes IoT devices/smart devices for monitoring patients health and wellness – they collect and transmit patient-centric information such as health status (depending on the purpose of monitoring) and medical devices used by them. The IoT can facilitate automation of many day-to-day operations. Increasingly, there are applications of these varying Internet-enabled 'things' in everyday life including agriculture, healthcare, data analytics, smart buildings, and wearable technology. Worryingly, with IoT devices, practically anything can be connected to the Internet or to another 'thing'– in many instances we are creating our own problems and a larger attack surface with inherent underlying security issues. While H-IoT may seem in its infancy, the fundamental functionality of real-time monitoring based on information gathered from the connected things is the key similarity in each domain. Inspired by [5], the concept of H-IoT comprises four key elements: people, process, things, and data. In the context of 'people', we can consider the data observed and collected from the participant, as well as human-generated data and applications. We define the 'things' as physical sensors, devices, actuators, and other processes, generating data or receiving information from other sources. Observing H-IoT from the perspective of these four elements clearly conveys H-IoT as an ecosystem involving devices and humans, but also acknowledges the services, context, environments, and intelligence [5]. H-IoT can help practitioners monitor patients to gain a greater insight into patient care, manage diseases and improve treatments. While the applications can vary, this human-centric sensing and collection of data contributes to e-health, assisted living and e-wellness.

Data is collected from individual's habits and routines through their interaction with the things, analysed and processed to create useful information for intelligent decisions and to control mechanisms. Big data analytics is imperative for dealing with the volume of generated data. With large quantities of 'thing' data, there could be duplication of data and communication overheads. In terms of historical logging of data and predictive analytics, how much collected data is too much data? The remainder of the paper is as follows: Section II details H-IoT security – both in terms of securing the devices, and the associated security vulnerabilities and threats. In Section III we look at related research. Section IV details our experiments using Weka for feature selection with network datasets to understand machine learning in this domain. In Section V we highlight our solution to securing H-IoT, and conclude and identify future work in Section VI.

II. Security in H-IoT

The rapid connectivity of control processes in critical systems opens Internet-enabled devices and processes to a wide attack landscape and increases likelihood and risk of vulnerabilities and threats. For security, "one size fits all" does not work for the complex IoT ecosystem - interoperability issues are important. Secure by Design, Default and in Deployment is imperative in future implementations of such interconnected 'things'.

IoT security is twofold: security considerations in terms of keeping the devices secure and protected pre utilisation, in addition to security in terms of device vulnerabilities and attacks. Often vulnerabilities are not deliberate - they are down to ignorance, or connecting a 'thing' to other 'things' which had risks not initially considered as an individual entity. The IoT is an umbrella term for many devices, and in the case of H-IoT these devices may have socioeconomic implications, so the reach of these threats and exploits is phenomenal. As shown in Table 1, there are many threats per layer of the typical H-IoT architecture. While there are hardware, software, and application considerations, network DoS/Distributed Denial of Service (DDoS) remain a significant problem as availability of data and services is vital in H-IoT. Examples of availability attacks against IoT devices include a local DoS attack to prevent the timely transmission of data or availability of service, or a DDoS attack affecting the operations of the device or other interdependent attributes. A critical H-IoT process may rely on accurate and timely collection of data. The interconnection of IoT devices to other 'things' can often map to other vulnerable devices.

The IoT and artificial intelligence (AI) combined together will transform healthcare through smart devices. While this integration has many enrichments, the many underlying security concerns still need to be addressed. Securing data in the IoT can be challenging so a clearer understanding of the underlying architecture is essential. Figure 1 illustrates IoT interconnected networks and layers. Consider how each attribute introduces a potential vulnerability and entry points. This could be the 'thing' that interacts with the user via input (an application collecting health related statistics) or a sensor collecting data about a

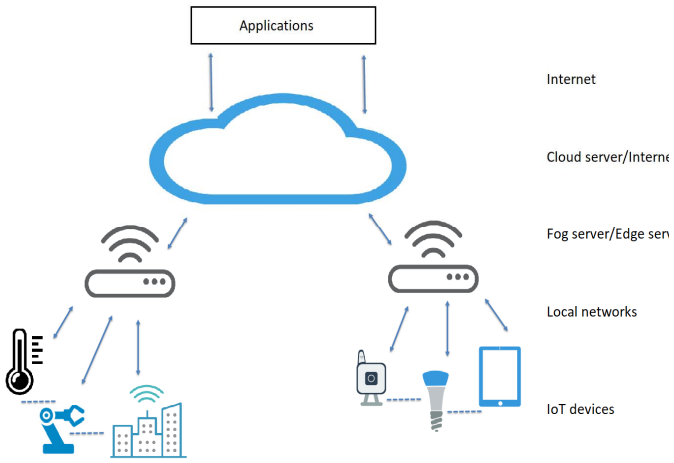

Fig 1. IoT inter-connected networks and layers

TABLE I. SECURITY THREATS IN IOT ARCHITECTURE

Layer	Description	Threats
Cloud	Data centre cloud layer/cloud network host applications that are critical providing IoT services.	Data interruption DDoS Buffer overflow Impersonation Remote code execution
Core	The function of this layer is to carry and exchange data and network information between multiple subnetworks.	Data interruption Man-in-the-middle (MITM) attacks Impersonation/Spoofing Modification of data at rest and in transit Relay attack Confidentiality attack Jamming/Congestion Data exchange issues: data privacy, access control, and disclosure of information
Edge	Endpoint devices with both wired and wireless connectivity. This scalable layer supports Zigbee, IEEE 802.11, 3G and 4G.	Connection flooding Data interruption DoS Eavesdropping Impersonation Jamming attack Modification of data at rest and in transit Misconfiguration Network protocol vulnerability and exploit Packet manipulation Physical attack/tampering Rogue access points
Things	Embedded systems and sensors. Small devices with varying OS, CPU types, memory, network capability.	Authenticity Device end-point attack Counterfeiting attacks Eavesdropping Hardware interruption/theft/modification Jamming attack Resource exhaustion Privacy Spyware Repudiation Device specific vulnerabilities, i.e. OS vulnerabilities, malware, weak authentication, etc.

situation, e.g. temperature, usage, transmitted data. This could also be securing the data transmitted between these 'things', to the edge/fog, and to the Cloud respectively. In the H-IoT, integrity and available of the healthcare data is essential also. Previously unconnected things are now generating exabytes of data per day, requiring vast bandwidth and strong analytic techniques. According to Cisco [6], current cloud models are not designed for the volume, variety and velocity of IoT generated data. Fog computing is an appropriate model for analysing such data – a fog-based approach analyses data at the network edge, close to where it is generated, instead of sending it directly to the cloud. Additionally, selected data can be sent to the cloud for historical analysis.

As stated, securing the H-IoT requires a multi-faceted approach. The first step is "device awareness". The IoT has introduced many new types of devices and endpoints on corporate networks. Attacks against the lower level 'things' in the network can open up a larger attack surface or reveal the bigger threat network. IoT devices are generally cheap with limited computing and storage capabilities. Many IoT devices leverage similar architectures even though their manufacturer may vary and they may provide a number of different functions. Secondly, "understanding network boundaries, access control, and collection of data" is imperative when utilising IoT/H-IoT. An IoT device should be segmented into its own network and have network access restricted – least privileges and access policies. The network segment should then be monitored to identify potential anomalous traffic, and action taken if there is a problem [7] - monitoring tools and technologies with forensic logging capabilities are key. Scalability and management of a large number of entities in the IoT ecosystem can often create a domino effect if one or many devices become corrupt. Every communication type must be secured, providing users with the confidence that their information and communication channels are properly safeguarded [8]. Thirdly, "monitoring network transmission" is essential. Current approaches to secure IoT devices attempt to leverage communication protocol-based mechanisms, such as encryption for data-in-transit. This is not sufficient if the endpoints themselves are vulnerable to modification by either local access or remote connections [9]. Additionally, encryption algorithms need higher processing power than many of the devices possess.

Data security issues are an increasing concern due to the wealth of data collected, stored, and processed on H-IoT-based devices. Depending on the nature of the device, this information can be personalised, location specific, or patient-centric information. As highlighted, Table 1 presents security threats in each H-IoT architecture layer. Many devices possess known vulnerabilities in their components or do not have strong security measures in place. HP, in a recent study, analysed a range of commonly used IoT devices (webcams, door locks, home alarms, and thermostats) and found that an alarming 70% of the devices used unencrypted network services. Also, the majority failed to encrypt data in transit [11].

While functions and activities may differ, commonality among IoT devices include [6]:

- Most IoT devices used a flash-based storage device.
- Many IoT devices are built on proprietary hardware.
- Some IoT devices store their data in the Cloud.
- Analysis of the interaction between IoT devices is necessary to collect data.
- Much of the evidence collected on IoT devices comes from network traffic analysis.

Device specific vulnerabilities are published in relevant literature but these are often overlooked. In a similar manner, increasing use of default Wi-Fi and router passwords, or insecure passwords is a key issue. OWASP [7], highlight weak or hardcoded passwords as the top IoT device vulnerability. Users often fail to change the default passwords on IoT devices, or do not follow practices to create good and secure passwords. Even if the H-IoT promises socioeconomic growth and health-related wellness, the security implications are equally significant.

III. Related Research

Securing IoT and specifically H-IoT can be explored from different avenues. Overall, the main aim of research in this area focuses on IoT protection [3], [12], [13], broadly focusing on the 'things' in the scenario and the exchange of information between the varying components. A context-based security and privacy approach for H-IoT is proposed in [1]. Their security architecture applies separation of concerns between end point 'things' in the H-IoT, and external 'things' who manage or use the services. The use of an Intelligent Trusted Authority (ITA), with similar characteristics to a broker, applies security and privacy policies modelled by the supervisory system and big data elements, with external flows screened by an authorisation unit. Access and flow conditions via authentication and least privilege per entity of the architecture are proposed, though no implementation details are provided. Fog assisted secure De-duplicated data dissemination in smart healthcare IoT is conveyed in [4]. The work details secure data exchange between sensor nodes, using fog servers at the edge of the network. The issue of duplicate and redundant data generation is highlighted. In the scheme an adaptive chunking algorithm is explained and tested using NS2 in a H-IoT-based scenario. Transmission of data is secured using symmetric key based encryption.

Application of machine learning algorithms into the field of cyber security has improved the accuracy of intrusion detection systems, by determining trends, signatures and in reducing the effect these malicious software have on devices. In [14], the focus of the study is on network feature selection for infiltration detection via dataset analysis using Weka [15]. They highlight that varying network architectures result in different normal patterns which can complicate the training phases for supervised learning. Their work highlights some commonality and trends in feature extraction but conveys how they should be taken lightly when applying to an IoT environment due to the scale and dynamic nature. In [16], Anthi et al. detail their adaptive intrusion detection approach for IoT, using machine learning. Similar to [14], their training and experimentation utilises Weka. They use a supervised approach to train their data, and the collection of historical logs to improve the accuracy of their detection. The addition of a rule-based engine to the approach is the main focus of future work, in addition to being able to

distinguish specific devices on the network. In [17], Meidan et al. detail their machine learning approach for IoT device identification based on network traffic analysis. The approach can be used to automatically and accurately recognise connections of IoT devices to an enterprise's computer network, mitigating policy violations and unauthorised access. While promising, it seems to focus on detecting connections rather than security threats or violations – however, it shows the merits of machine learning being applied broadly to network traffic analysis. Machine learning for improved maintenance and predictiveness of IoT sensor data is detailed in [18]. Their models can be used for prognostics and forecasting, improving production process runs efficiently with minimal costs incurred for maintenance and reduce product quality degradation. In terms of H-IoT, their approach using the sensor data analysis would have great benefits for e-health and wellness.

Multi agent systems have proven to be a valuable tool in the areas of cyber security, distributed networks and legacy systems because of their scalable and flexible architecture. Agent-based monitoring as evidenced in [14], [19] applied to a Cloud and IoT based environments are suitable for coping with dynamic environments, interdependent systems, and varying connections/requests. In [14], a multi agent architecture for IoT is presented with agents collecting information both locally on the network and remotely on a server. Local and global observations are communicated via agents shared amongst participants. Coalitions are used within the system to increase the speed at which agents can be consulted during the decision making process, however the weighting during the voting process assumes that all evidences should be treated equally. In [19], similarly the issue of equal weighting in collaborative intrusion detection is highlighted. Distributed collaboration among heterogeneous components within and across independent domains, in this case H-IoT will contribute to better incident detection and prevention, via cooperation of threat knowledge, both known attacks and unknown threats.

IV. Feature Selection Experiments

Related research identified the merits and wide applications of machine learning to the IoT domain. The H-IoT environment is a dynamic and unpredictable environment based on its varying usage. We applied machine learning classifiers to determine the best approach to detecting faults and attacks within such an environment. Feature selection can improve the learning performance of classifiers, lower computational complexity, and building better models in machine learning. The dynamic nature and invaluable advantages of feature selection in the field of pattern recognition, statistics, machine learning and data mining is highly commendable [20]. Experiments were performed using Weka [15], with a network attack dataset. The dataset was small in scale and represented a LAN, with similar characteristics to an H-IoT edge/fog environment. The dataset[1] consists of a wide variety of intrusions simulated in a military network environment.

Each connection is labelled as either normal or as an attack with exactly one specific attack type. Each connection record consists of a 100 bytes. For each TCP/IP connection, 41 quantitative and qualitative features are obtained from normal and attack data (3 qualitative and 38 quantitative features). While it is recognized that not all IoT networks use TCP/IP – many instead make use of UDP or proprietary protocols, machine learning techniques would require re-training for each protocol. As such, this paper presents the results for one protocol with a view to conducting further experiments on other protocols in the near future. The class variable has two categories: Normal and Anomalous. Four experiments were conducted in total, details of which are provided below:

Correlation-Based Feature (CSF) Subset Evaluation

This assesses the worth of a subset of attributes by considering the predictive ability of each feature, along with the degree of redundancy between them. Information on 41 features were found, and Table II below presents the top ten features from the experiment:

TABLE II. Predictive Features

Attribute Rank	Attribute Name
1	duration
2	protocol_type
3	service
4	flag
5	src_bytes
6	dst_bytes
7	land
8	wrong_fragment
9	urgent
10	hot

Subsets of features that are highly correlated with the class while having low inter-correlation are preferred. This experiment shows that based on the dataset that those attributes would be the most predictive. However, different algorithms produce slightly different results, rather than showing a clear best feature.

Gain Ratio Attribute Evaluation

Our next focus was on Gain Ratio Attribute Evaluation, where our understanding was the higher the 'average merit' the more predictive the feature is – the top selection from this is presented in Table III. From our analysis, we observe how this feature drops off quite quickly.

[1] Available from https://www.kaggle.com/sampadab17/network-intrusion-detection

TABLE III. GAIN RATIO ATTRIBUTE EVALUATION

Average Merit	Attribute Name
0.42	logged_in
0.37	srv_serror_rate
0.35	serror_rate
0.34	flag
0.33	dst_host_srv_serror_rate
0.32	dst_bytes
0.30	diff_srv_rate
0.28	dst_host_serror_rate
0.28	src_bytes
0.26	same_srv_rate

Interestingly, the most predictive feature "logged_in" is a host-based feature that in practice would require an agent to go and investigate since it is not visible from the network layer. Mobile agent technologies capable of autonomously and independently collecting and sharing information have proven to be a valuable tool for gathering evidence from non-traditional transient networks such as at the 'things' layer. These attributes are hard to collect based on a machine learning approach alone, and most of the more predictive features look like they would require some further investigation.

Information Gain Attribute Evaluation

Information gain attribute evaluation is a similar approach as the variation on gain ratio algorithm but the results are marginally different. This experiment evaluates the worth of an attribute by measuring the information gain with respect to the class – as shown in Table IV.

TABLE IV. INFORMATION GAIN ATTRIBUTE EVALUATION

Average Merit	Attribute Name
0.80	src_bytes
0.67	Service
0.63	dst_bytes
0.52	Flag
0.52	diff_srv_rate
0.51	same_srv_rate
0.47	dst_host_srv_count
0.44	dst_host_same_srv_rate
0.42	dst_host_diff_srv_rate
0.40	dst_host_serror_rate

K-means clustering analysis

K-means clustering is an unsupervised learning algorithm that classifies a given data set into a number of clusters, defined by the letter "k" which is fixed beforehand. The clusters are then positioned as points and all observations or data points are associated with the nearest cluster, computed, and adjusted until a desired result is reached. Running this clustering algorithm returns an error rate of: within cluster sum of squared errors: 57481.24. This error rate is quite a bad result. This shows that there are no 'clean' distinctions between the attack class and the normal class, which are visible from the feature analysis. Clearly a newer smarter approach is required. Upon further scrutiny of the dataset there appears to be an even class distribution (13,449 normal and 11,743 attack) – which is good for machine learning as inevitably it will improve the result and help with classification, however these conditions are unlikely to occur in a live environment where the 'normal' data vastly outnumbers the attack data – so machine learning would not produce as good results in practice on a larger scale dataset. Deep Learning would be an appropriate method for improved analysis, as it can learn and make intelligent decisions given certain inputs and intelligence. Additionally, some of the features (root_shell, num_root, num_shells, etc.) are host-based and are not easily collectable from the network layer. This will require an agent-based approach to provide dynamic, scalable and hierarchical collection.

V. MULTI-AGENT APPROACH TO ADVANCED PERSISTENT THREAT DETECTION FOR H-IOT

Intelligence awareness is the capability of automated intelligence sharing and alerting across a myriad of security systems. One key benefit of such an approach is the ability for the intelligence to adapt, based on contextual or situational awareness – as conveyed in the related works section. A challenge for H-IoT is that the low memory and sensing capabilities of these 'things' cannot support simply 'adding on security'. A multi-agent approach to threat detection for H-IoT is proposed as a scalable and lightweight solution. Agent-based monitoring utilises multiple agents to achieve different requirements depending on the detection unit – for H-IoT this could be targeted local and global monitoring of the lower level 'things', communication at the edge/fog layer, and communication between the core and cloud. Agent-based approaches reduce the computational load on the system by dividing it into hosts. Hierarchical based monitoring via agent based clustering can provide lightweight local and global monitoring. Similarly, collaborative intrusion detection in federated cloud environments as conveyed in [19] can be applied to the H-IoT environment. Agents deal with issues on a local level and communicate with their neighbours regarding systems states and signatures, in a similar communication structure as evidenced in [14].

For protecting healthcare data and services in a H-IoT infrastructure, time criticality is an important monitoring requirement. This includes both the responsiveness aspect of the system and the timeliness of any relevant data being delivered in its designated time period. In the proposed solution, the monitoring hierarchy is comprised of several agents $G = \{g_1 ..... g_i\}$ assigned data collection and analysis tasks for a particular service. A set of features F represent information about an activity monitored from the services, e.g., high traffic

volume. Agents are placed close to the source they monitor (i.e., on the same network, fog/edge or device) to give them access to the required data stream.

Each feature *(f ∈ F)* describes the type of information, while the value set *V* defines the range of possible values of the feature. Given an event and agent identity, a local report R_{Local} is defined as a tuple consisting of *<eid, ts, g, (f, v), p>* where: *eid* is a unique event identifier; *ts* is the events timestamp; g ∈ G is the agent's identity; *(f, v)* is a feature-value pair corresponding to the output of the data collection action performed by agent *g*; p ∈ [0, 1] is the agent's analysis of the suspicious activity; i.e. the probability of the suspicious activity being malicious [21]. The system is faced with the task of aggregating the different agent's outputs into a single final result, making a decision about the observed events.

Our current investigation is the appropriate voting approach for this collaborative decision making process. As outlined in [19], an issue with voting schemes is that each agent is given the same weighting or confidence value as their neighbour. Agents with higher responsibility or hierarchy may resultantly possess a higher influence, this is not always the case. Imbalance between influence weightings, confidence values, and normalisation that can occur when calculating the group decisions is the current focus of our work to ensure accurate and fair collaborative decisions.

VI. Conclusions

H-IoT can help gain a greater insight into patient care, manage diseases and improve treatments via collection and transmission of human-centric data. In this paper we explored feature selection for detecting network layer attacks in the H-IoT architecture. Attribute analysis and predictiveness of commonly used features were performed to help determine the feasibility of an unsupervised machine learning approach for protecting things in the H-IoT architecture. While there are merits for application of machine learning to understand and parse the H-IoT data, an agent-based monitoring approach could cope with the dynamic nature of 'things', edge/fog devices, and cloud applications – improving accuracy and adaptability through deep learning. Future work involves implementing our approach to securing H-IoT architecture and evaluating and refining our chosen algorithms, providing details on the decision making element of collaborative intrusion detection.

References

[1] V. Alagar, A. Alsaig, O. Ormandjieva, and K. Wan, "Context-based security and privacy for healthcare IoT," Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018, pp. 122–128, 2018.

[2] A. Djenna and D. E. Saidouni, "Cyber Attacks Classification in IoT-based-Healthcare Infrastructure," in 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 7471–7474.

[3] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 30–35, 2017.

[4] A. Ullah, I. Sehr, M. Akbar, and H. Ning, "FoG assisted secure De-duplicated data dissemination in smart healthcare IoT," Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018, pp. 166–171, 2018.

[5] C. Maple, "Security and privacy in the internet of things," J. Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[6] J. Muniz and A. Lakhami, "Investigating the Cyber Breach," in The Digital Forensics Guide for the Network Engineer, Cisco Press, 2018, pp. 207–210.

[7] OWASP, "Top 10 2018," OWASP Internet of Things (IoT) Project, 2018. .

[8] F. Alaba, M. Othman, I. Hashem, and F. Alotaibi, "Internet of Things security: A survey," J. Netw. Comput. Appl., vol. 88, pp. 10–28, 2017.

[9] W. M. S. Stout and V. E. Urias, "Challenges to Securing the Internet of Things," in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2020, pp. 1–8.

[10] S. Millar, "Network Security Issues in The Internet of Things (IoT)," in Queen's University Belfast, 2016, pp. 1–7.

[11] K. Rawlinson, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," Hewlett Packard, 2014. .

[12] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things Forensics: Challenges and Approaches," Proc. 9th IEEE Int. Conf. Collab. Comput. Networking, Appl. Work., 2013.

[13] Á. Macdermott, T. Baker, and Q. Shi, "IoT Forensics: Challenges for the IoA Era," in 9th IFIP International Conference on New Technologies Mobility and Security (NTMS), 2018, pp. 1–5.

[14] P. Kendrick, A. Hussain, N. Criado, and M. Randles, "Multi-agent systems for scalable internet of things security," in Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing, 2017, pp. 88–93.

[15] E. Frank, M. A. Hall, and I. H. Witten, "The WEKA Workbench. Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques," 2016.

[16] E. Anthi, L. Williams, and P. Burnap, "Pulse: An Adaptive Intrusion Detection for the Internet of Things," in PETRAS - Living in the Internet of Things Conference, 2018, pp. 1–4.

[17] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, N. O. Tippenhauer, and Y. Elovici, "ProfilIoT : A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis," in Proceedings of the Symposium on Applied Computing, 2017, pp. 506–509.

[18] A. Kanawaday and A. Sane, "Machine Learning for Predictive Maintenance of Industrial Machines using IoT Sensor Data," in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2017, pp. 87–90.

[19] Á. MacDermott, Q. Shi, and K. Kifayat, "Collaborative Intrusion Detection in Federated Cloud Environments," J. Comput. Sci. Appl. Big Data Anal. Intell. Syst., vol. 3, no. 3A, pp. 10–20, 2015.

[20] P. Fergus, I. Idowu, A. Hussain, and C. Dobbins, "Advanced artificial neural network classification for detecting preterm births using EHG records," Neurocomputing, vol. 188, pp. 42–49, 2016.

[21] P. Kendrick, N. Criado, A. Hussain, and M. Randles, "A self-organising multi-agent system for decentralised forensic investigations", Expert Systems with Applications, 102, pp.12-26, 2018.