Collaborative approaches to secure the IIoT: a survey

Léo Lavaur
IMT Atlantique, Cyber CNI
leo.lavaur@imt-atlantique.fr

Marc-Oliver Pahl
IMT Atlantique, Cyber CNI
pahl@cybercni.fr

Yann Busnel
IMT Atlantique
yann.busnel@imt-atlantique.fr

Fabien Autrel
IMT Atlantique, Cyber CNI
fabien.autrel@imt-atlantique.fr

***Abstract*—The continuous merging of IT and OT infrastructures introduces a new set of threats. OT security already lacks collaboration and actionable threat intelligence. Federated approaches have been proposed to solve similar problems, especially improving detection accuracy and confidentiality, but also preserving trust and accountability between parties. This paper surveys different collaborative approaches to secure IT and OT in the literature, and identifies open issues that require further research.**

***Index Terms*—federated learning, IIoT, collaborative sharing, cyber threat intelligence, automation**

I. Introduction

The Internet of Things (IoT) has begun to spread over a variety of domains, including industry and finance. It represents an increasing threat for both Information Technology (IT) and Operational Technology (OT). Over the years, multiple attacks have been reported to aim the consumer IoT devices, but also Industrial Control System (ICS) [1]. Stuxnet [2] introduced in 2010 a new threat paradigm in which attacks cannot be detected with known features or Indicators of Compromise (IoCs). Security in the Industrial Internet of Things (IIoT) is therefore a major concern [3].

On one side, Threat Intelligence (TI) sharing is required to acquire a thorough understanding of large-scale cyberattacks like Mirai [4] or Hajime [5]. On the other, collaborative Artificial Intelligence (AI) allows dealing with the constraints of the IIoT, like its sporadic traffic generation which complicates the training of accurate Machine Learning (ML) models [6]. Anomaly detection is globally used to detect intrusions [7]. This paper shows the developments of collaboration to cope with threats against the IIoT.

Therefore, this work answers the following questions:

- What are the most important attacks over the past 10 years that could have been tackled with collaboration?
- What are the topics covered by the academic literature over that time?
- Where was the literatures published?
- Which groups are active in this area?
- What are open questions according to existing surveys?

The contributions of this paper are twofold. First, it reviews the collaborative approaches which apply to the security of the IIoT. To do so, it firstly reviews the literature in the associated subtopics, and then put these approaches in perspective of the existing taxonomies on IoT threats. The second contribution is the proposal of a reference architecture in the context of which the reviewed works are placed.

Section II presents the related works and provides a comparison with this survey. Section III introduces the domain and details our reference architecture. In Section IV, we present our methodology, provide an analysis of the existing surveys, and review the selected works. Quantitative analysis of the reviewed papers is provided to answer the research questions.

II. Related Work

While several surveys already exist in the literature [1], [3], [7]–[19], they tend to address wider challenges or, on the contrary, specific ones that overlap with this work without covering it. To the best of our knowledge, no existing work address both the collaborative aspects of cybersecurity and its application to the IIoT.

The reviewed works can be categorized in four subtopics – see section III: (a) information sharing, (b) IoT and IIoT security, (c) anomaly detection, (d) collaborative AI.

Topic (a) is addressed by [8]–[11]. They discuss the advantages and limitations of information-sharing, especially Cyber Threat Intelligence (CTI). The authors emphasize on the need of standardization, automation, and incentives, in order to achieve efficient collaboration. This work differs by focusing on the technical aspects of automated collaboration. On the other hand, abstract concepts like context and regulation dictates how technologies behave. Hence, their presence in this work is necessary to put the outcomes in perspective.

The authors of [1], [3], [12]–[14] address topic (b). They review the threats induced by IoT and IIoT devices, and discuss the technologies available in the literature. In contrast to this work, the collaboration is however barely addressed.

Topic (c) is addressed by [7], [15], [16], especially ML algorithms suitable for anomaly detection. They also discuss the usage of blockchain technologies to support collaborative Intrusion Detection System (IDS). Using the blockchain and its features is related to the research presented in this paper. However, it has a broader approach, where the blockchain is only one of the considered solutions.

Finally, the authors of [17]–[19] cover topic (d). They discuss Federated Learning (FL) approaches to work with distributed architectures. Its security is also heavily addressed to point out security threats like communication bottleneck, poisoning, and Distributed Denial of Service (DDoS) attacks.

Those three papers are close to the goal of this meta-survey in their topics but does not focus on the IIoT. The results are expected to be different since working with the IIoT implies specific systems, protocol and network configurations — see section III-B.

Table I shows a summary of the selected papers, sorted according to their topic of dominance. A more in-depth overview of each survey is available in section IV-C. The topic coverage of a paper in the table is defined as follows:

- a topic is considered *covered* (●) when several references around the topic are cited and their outcomes are discussed;
- a topic is considered *partly covered* (◐) if at least one reference is cited and its outcomes are explained;
- a topic is considered *not covered* (○) if the topic is only mentioned or not spoken of at all.

Some surveys have been chosen for their number of citation, the others because they represent the only related survey in their domain, to the best of our ability. Finally, in some domains such as CTI or IoT security, multiple surveys have been selected for the sake of completeness. This list is not exhaustive but covers each identified topic. The list has been modified throughout the entire writing process to reflect the content of the survey at best.

III. The Domain

Info: This section currently reflect the order in which the parts have been researched, but not the canonical order in which they should be presented. The *right* order is the following: IIoT (the domain), threat sharing and collaborative AI (the two main approaches), and anomaly detection (the most important technique).

This section defines the concept of collaborative security and overviews its limitations. It details the subtopics (a) to (d) and identifies the corresponding challenges that collaboration faces. Finally, it presents our approach to collaboration in IIoT security and the corresponding reference architecture on which is based the remaining of this survey.

A. Information sharing

As noticed by [9], the index terms "information sharing" in academic search engines first led to information-sharing in an organizational and industrial context, used to improve production. In cybersecurity however, the primary objective of information-sharing is to achieve situation *cyberawereness* among stakeholders about threats and vulnerabilities to improve the security of a system [8]. Collaboration is important to share findings and insights on encountered threats before they hit anyone else. In fact, malwares like Mirai [4] or Hajime [5] have been seen attacking several organizations using the same mechanics before their operation is characterized, and actionable threat intelligence can be shared.

There are multiple types of CTI depending on what it contains and who it is intended for. In their report, Chismon and Ruks [20] devise CTI in four types: strategic CTI, operational CTI, tactical CTI, and technical CTI. The first two are the more abstract types, consumed by decision-makers and high-level security staff; the last two deal with Techique, Tactic, and Procedure (TTP), and IoCs, respectively. Because it is based on technical features, technical threat intelligence (TTI) is the easiest to share and, more importantly, the easiest to automate. Wagner *et al.* [8] states that current (in 2019) sharing methods heavily rely on human input, which lead to a slowdown in processing and sometimes errors. Consequently, as the size of threat data grows, automated mechanisms are required to cope with the proliferation of cyberattacks [10].

Challenge 1. *Human interaction adds slowdown and potential errors to the information-sharing process.*

To be of use in an operational context, CTI must also be actionable. The ENISA [21] defines the actionability of CTI as the fulfillment of five criteria: relevance, timeliness, accuracy, completeness, and ingestibility. Relevancy depends on the context of the recipient. Accuracy and completeness depend on the emitter, which is assumed to be exemplary in this context. Timeliness and ingestibility however are mostly provided by the supporting architecture. Consequently, CTI needs to be shared *machine-to-machine*, even if human interaction is required afterward [21].

Challenge 2. *Information must be distributed in a timely manner.*

Challenge 3. *Information must be easily processable by the recipient.*

A lot of other factors can impede collaboration. For instance, stakeholders are often reluctant to share their information, fearing confidentiality and privacy issues, as well as reputation loss [9]. Cultural and language barriers can negatively affect the accuracy of the shared information, even though international collaboration is push by regulation, such as the NIS directive in Europe [22]. Existing platforms also require the information-sharing to be centrally verified, which negatively affect the timeliness of the information [11]— see challenge 2. The authors consequently state that there is a need for new sharing standards allowing direct sharing without the need of centralized validation. Finally, the balance between anonymity and trust must be taken into consideration to protect the participants without sacrificing the quality of the information [23].

B. IoT and IIoT Security

The IoT adds a lot of constraints to the traditional IT to be properly secured. They have little performance, poor patching capabilities, often weak encryption and authentication mechanisms [1].

1) Context and differences: The industrial context adds further constraints that need to be managed [24]:

- **priority**: whereas the securing the IoT focuses mainly on the data confidentiality and privacy, the IIoT needs first and foremost to be available. Any failure can have

TABLE I: Related works, their topics and number of citation according to Google Scholar – Avr. 2021

Domain		Reference	Topics: Security	Privacy	Attacks & Vulnerabilities	Trust	Automation	Detection	Cyber Threat Intelligence	Information sharing	Law & Regulation	Standardisation	Cultural impact	Fog/Edge-computing	Internet of Things	Industrial IoT	Industrial Control System	Cyber-Physical Systems	Blockchain	Deep Learning	Federated Learning	Decision-making	Cited
Domain	(a)	Wagner *et al.* [8]	●	●	●	○	◐	○	●	●	●	○	◐	○	○	○	○	○	○	○	○	○	15
		Pala and Zhuang [9]	●	○	●	○	○	○	●	●	○	○	●	○	○	○	○	○	○	○	○	○	6
		Tounsi and Rais [10]	○	○	◐	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	111
		Skopik, Settanni, and Fiedler [11]	○	○	○	○	○	○	●	○	●	●	●	○	○	○	○	○	○	○	○	○	150
	(b)	Lin *et al.* [12]	●	●	◐	○	○	○	○	○	○	○	○	○	●	●	○	●	●	○	○	○	1300
		Sha *et al.* [13]	●	●	○	○	○	◐	○	○	○	○	○	○	●	●	○	●	○	○	○	○	20
		Neshenko *et al.* [1]	●	○	○	●	○	○	○	○	○	○	○	○	○	●	○	○	◐	○	○	○	139
		Sengupta, Ruj, and Das Bit [14]	●	●	◐	●	○	○	○	○	○	○	○	○	○	●	●	○	◐	●	○	○	76
		Panchal, Khadse, and Mahalle [3]	●	○	○	●	○	○	○	○	○	○	○	○	○	◐	●	○	○	○	○	○	17
	(c)	Chaabouni *et al.* [16]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	●	○	○	●	○	148
		da Costa *et al.* [7]	○	○	○	○	○	●	○	○	○	○	○	○	○	●	●	●	○	○	●	○	93
		Meng *et al.* [15]	○	○	●	○	○	●	●	○	○	○	○	○	○	○	○	○	○	●	○	○	236
	(d)	Aledhari *et al.* [17]	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	20
		Mothukuri *et al.* [18]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	7
		Lyu, Yu, and Yang [19]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	30
		Lavaur et al.	●	●	●	◐	●	●	●	◐	○	○	○	○	○	●	●	●	●	◐	◐	●	●	-

● covers topic; ◐ partly addresses topic; ○ does not cover topic;

disastrous impact on production and induce physical harm.

- **interruption**: in case of a threat, a typical IoT device can be disconnected or shut down. Some industrial devices just cannot be stopped without causing damages, and standard shutdowns are scheduled.
- **lifecycle**: typical IoT devices have a short life, forcing them to be frequently upgraded to a more modern system. Industrial devices, on the other hand, can be used for at least ten years, meaning that a security flaw will probably not be patched quickly.

Challenge 4. *IIoT devices are subject to more constraints than their consumer counterparts.*

Over the years, multiple attacks have been reported to aim IoT devices or ICS. The Mirai botnet stands above the crowd for its efficiency and its worldwide spread [25]. In 2016, the botnet have been used for multiple large-scale DDoS campaigns, like the one targeting the DNS provider Dyn and responsible for downtime at some of the biggest websites, including – but not limited to – Twitter, Netflix, GitHub and Reddit [4], [25]. Other botnets have since been seen using the same attack model as Mirai, like Hajime or BrickerBot [25].

Botnets are not the only threats against the IIoT. In 2010, the malware Stuxnet (latter attributed to American and Israeli services) was part of an Advanced Persistent Threat (APT) targeting the Iranian nuclear program [26]. It targeted Siemens PLC and was able to alter their operation, namely causing rotors to change their programmed speed without anyone noticing [2]. Apart from being the most advanced from its time, Stuxnet also introduced a new threat model where computer-based attack can affect the real world, and the attack is not detectable with shared IoCs.

2) Collaboration approach to the taxonomies: Several taxonomies have been proposed to allow easier classification of security events [1], [14], [27], [28]. It can be particularly useful in detection systems to propose appropriate countermeasures depending on the attack. Common dimensions are the target architecture layer, the impact and the method of operation. The definition of those do change however, and each term does not always imply the same thing. In the context of collaborative detection systems, we focus on the following:

- **layer**: sometimes referred to as *level* – the layer a simplification of the OSI model specification. Three layers are commonly identified [1], [14], [27], [29]:
  - the *physical* layer, also called *device* or *perception*, is the lowest layer and concerns the physical devices (e.g. Cyber-Physical System (CPS)) and any measurements or alteration that can be done without access to the communication protocol;
  - the *network* layer includes all attack that are performed on the communication between the devices, such as *eyes dropping* or *Denial of Service (DoS)*;
  - the *application* layer concerns the attack targeting the software running on the devices or its operating system; a fourth category is proposed by [14] where the attacks target *data*, but data attacks are mostly related to the *network* or *application* layers.

  The detection on the *physical* layer require specific information and context, and are difficult to generalize.

TABLE II: Common datasets according to [7], [16]

Dataset	Type	Reference
KDD Cup 99	Labelled TCPdump data	**kdd99**
NSL-KDD	Improved version of KDD99	[35]
AWID	Captured 802.11 packets	[36]
CIDDS-001	Labelled NetFlow data	[37]
CIDDS-002	Labelled NetFlow data	**Ring2017b**
UNSW-NB15	Labelled TCPdump data	[38]

Collaborative detection systems will focus on the upper layers.

- **impact**: it represents how the attack affect the target. The Confidenciality, Integrity, Availability (CIA) triad has defined the impact of attacks since the 2000s [30]. In their taxonomy, the authors of [1] add the *Accountability* to the triad to cover the aspects of repudiation and traceability. Other types of impact include *Utility*, *Authenticity* and *Possession* as proposed by [31], as well as *Privacy* [3].
- **method**: the method covers how the attack is performed. In [27], the method is described with four categories: *Technique*, *Mechanism*, *Executability* and *Focus*. The method used by an attacker can be also described as a list of techniques he deployed to achieve his goals. The MITRE ATT&CK® framework for ICS [32] provides an extensive taxonomy of techniques used by an attacker toward ICS.

Some attack mitigation will particularly well benefit of collaboration and information sharing. Mostly, attacks that have a reproducible *modus operandi* can easily be countered once they have been observed and studied. Mirai's source code, for instance, has been known since late 2016 and its recognizable behavior can be detected [4]. The botnet and its variants are still active today, which shoes that countermeasures are not always deployed [33].

C. Anomaly detection

To protect organizations, security systems often rely on signature-based attack detection like IDS to detect known attacks. This approach is however inefficient against novel or zero-day attacks and APTs, like Stuxnet in 2016. Furthermore, the heterogeneity and low traffic of the IoT make IDS be less efficient and/or inadequate [6], [16].

Hence, the research community started to explore anomaly detection as a solution to improve detection systems. Anomaly-based detection systems compare a normal profile trained upon nominal traffic with the observed events to determine if they are malicious [34]. To that end, researchers started to AI and especially ML as a way to identify the abnormal behavior. Most ML algorithms need data to train upon. Table II sums up the most used datasets.

In real world however, algorithms must be trained on relevant data in order to perform well. It is an issue in the IT, but more importantly in the OT. IoT devices tend to generate less traffic and make the training less efficient [6]. Consequently, the siloed architecture of detection systems is an obstacle to their effectiveness [17] and detection systems need to be federated.

Challenge 5. *The siloed architecture of ML-based detection systems is an obstacle to their effectiveness.*

D. Collaborative AI

Modern AI in the context of cybersecurity can mostly be divided in two approaches. The first one is decision-making, which is intended to assist or automate the human process. The second one is the ML, which is designed to recognize patterns or behavior in the input data. Multi-Agent Systems (MAS) are studied to deal with heavily distributed architectures like the IoT. MAS are composed of multiple independent smart systems which act as a whole. Each device has its own sensing, computing, and decision-making capabilities [39]. Recent research focus on how to reach consensus among a fleet of agents in a fixed time [40] and keep consistency in their behavior.

Konečný *et al.* [41] introduced FL in 2016, originally to reduce the communication overhead induced by the data sharing; the technology has since been studied intensely—see section IV-D, notably to improve IDS. FL works by aggregating the models resulting of on-device training to benefit from the experience of each participant without compromising the local data. The aggregation can be performed by a trusted server [6], [42]–[44], but the research tends toward the use of distributed ledgers such as the blockchain [45], [46] to improve availability and robustness.

E. Reference architecture

This section presents the reference architecture for this survey, as depicted in Figure 1. This architecture is a generic approach to the architectures considered in the selected works.

IoT devices have constrained resources [13] which prevents the use of on-device operation, also called edge computing. Consequently, we consider an IoT gateway through which all traffic is directed [6], [47]. The gateway embeds enough computing power to perform real-time anomaly detection against ML models. It is also capable of training its own model based on captured traffic.

Each gateway is also independent and follows the principles of autonomic systems defined by IBM in 2001 [48]. The architecture is referred to as Monitor-Analyze-Plan-Execute plus Knowledge (MAPE-K); the knowledge being shared among all agent in this case. To support knowledge-sharing, the reference architecture considers a federation entity which aggregates models and redistributes them among the participants. We do not specify the nature of this federation entity, as it can be implemented in different ways depending on the use case and the objectives, as noticed in section III-D.

IV. The survey

A. Methodology

The first objective of this paper is to conduct a meta-survey of existing related survey papers. This process allows both to identify the related works as depicted in section II,

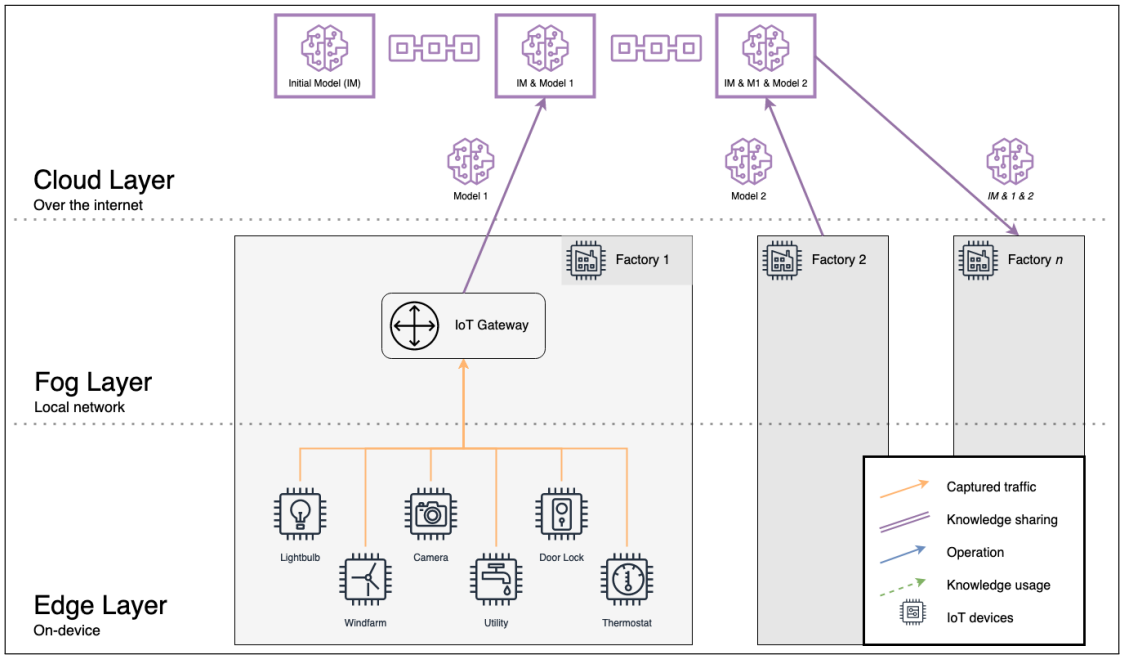


Fig. 1: The reference architecture

and to extract the relevant subtopics detailed in section III. This classification allowed the selection of more precise *query strings* for the used search engines (Google Scholar, Semantic Scholar, Microsoft Academic, Lens.org). Here are the query strings for topics for topics (a) to (d) respectively:

(a) `(information OR threat intelligence) AND (sharing OR collaboration);`
(b) `(IIoT OR industrial IoT) AND security;`
(c) `(anomaly OR intrusion) AND detection;`
(d) `federated learning OR distributed machine learning OR collaborative AI.`

It should be noted that some words have variations or acronyms that may not lead to the same results. For instance, collaborat*ion* and collaborat*ive*, or MAS for Multi-Agent Systems. Furthermore, some search engines do not support boolean operators and only yield results that contains all terms. In that case, several requests must be made to reflect the `OR` logic. In addition to the search engines, the following sources have been used:

- recommendations from supervisors and coworkers;
- natural (or intuitive) research: ideas that are connected to the domain;
- snow ball effect: notably from the surveys.

To select the relevant papers among the others, the following exclusion criteria have been considered. They were used at different reading phases, depending on the amount of information they require. They are threefold: (1) title and abstract; (2) introduction, conclusion and findings; (3) full article.

- *out-of-scope*—papers that do not match the identified subtopics and challenges;
- *missing citations*—papers that state facts without proper sourcing, or show numbers that are not proved;
- *old* and *not cited*—papers that do not contribute to the research.

The challenges identified in section III restrict the contributions of the selected papers. For instance, challenge 1 identifies the human interaction as a source of errors and slowdowns, so the selection is restricted to automated systems.

B. Surveys

As introduced in section II and depicted in table I, this work come after 15 identified surveys that cover one part or another of the subject. The following sections present the considered surveys and with their contributions.

1) Information sharing: The authors of [8] discuss threat-sharing and the challenges it faces in a survey analysis of about one hundred papers, patents and technical reports. The authors emphasize the topic of trust, trust management and how anonymity can be an obstacle. The authors analyze the current collaboration status of CTI, especially the sharing standards and platforms available. They highlight the need for incentives for stakeholders to make the community reactive.

The authors analyze the regulation around the CTI sharing and how it can impact the implication of organizations. Differences between countries laws can indeed impede the international collaborations of organizations. The authors of [9] review the same topic through their research framework and compare the quantitative and qualitative approaches seen in the literature. They highlight the use of the game-theory which prominent in their findings. CTI platforms and tools are also discussed in [10], where the authors propose a classification of TI in four distinct types: strategic, operational, tactical, and technical. Then, focusing on the technical TI, they

emphasize the need of standardization to improve the quality of the CTI.

The authors of [11] detail the implications of collective cyber defense in five dimensions: cooperation, law and regulations, standardization, geographical differences, and technology integration. They highlight the importance of having an efficient cooperation to preserve the timeliness of the information. They emphasize on the value of taking the new SCADA-targeting threats—and more generally the ICS—into consideration.

2) IoT and IIoT: The work of Lin *et al.* [12] surveys the topic of the IoT, which is deeply tied with the ICS nowadays. In this paper, the authors detail the concept of fog/edge computing, its relation with the IoT and CPS industries, as well as its security and privacy implications. The authors of [13] discuss real-world applications to securing the IoT on the edge layer.

In [1], the authors survey the existing vulnerabilities that affect the IoT and provide a taxonomy for these vulnerabilities, alongside their attack vector and potential impact. The findings of the paper are accompanied by the analysis of a dataset collected using a network telescope monitoring 2^{24} IPv4 addresses. They finally emphasize on the possible research directions, namely large-scale identification of IoT devices. These works [1], [12], [13] does focus neither on the collaboration aspects, nor the industrial world.

The authors of [14] review the security of the IIoT, thus extending the work of [1] by focusing on the industrial aspects. They discuss the current security issues and then focus on the study of blockchain-related solutions. The authors of [3] also address the security of the IIoT but focus their work on known attacks and their counter-measures. Though both works are dedicated to the security IIoT, they barely address the subject of collaboration.

3) Anomaly detection: Meng *et al.* [15] introduces the concept of blockchain as an opportunity for collaborative intrusion detection networks, where multiple IDSs could share their information to enhance the detection capabilities. They review both the intrusion detection and the blockchain literatures and highlight challenges in intrusion detection that can be solved by blockchain, such as trust computation and data sharing. Using the blockchain and its features is close to the research presented in this paper. However, it has a broader approach, where the blockchain is only one of the considered solution.

Both [16] and [7] review the applicability of IDS to the IoT. They review different IDS solution and strategies and compare their efficiency. da Costa *et al.* [7] focuses on techniques backed by ML while Chaabouni *et al.* [16] review both traditional and ML techniques. Comparisons show that ML-based IDS have higher success rate. Both work also compare the existing datasets and emphasize the lack of proper dataset dedicated to the IoT.

Our work exclusively focuses on the federated approaches on IoT security. However, several contributions have proposed federated detection systems, often by sharing the parameters of ML-based IDS. Hence, we considered including this section as a requirement.

4) Collaborative AI: Behind the AI term are mostly two concepts in this case: machine learning and decision-making. The authors of [17] detail numerous applications of FL which remedies the shortcomings of ML when working with distributed or decentralized architectures. Security aspects of FL are addressed in several reviews [18], [19], where the authors identify security threats like communication bottleneck, poisoning and DDoS attacks.

More generally, decision-making in distributed systems has been heavily researched over the years [49] and several surveys address it. Notwithstanding its numerous applications in cybersecurity, no survey regarding decision-making has met the criteria for this selection. Those three papers [17]–[19] are close to the goal of this meta-survey in their topics but does not focus on the IIoT. The results are expected to be different since working with the IIoT implies specific systems, protocol and network configurations.

C. Overview on relevant existing works

This section reviews the selected literature. The selected works are presented, sorted by their topic of dominance. Figure 2 summarizes the information and helps identify the differences between works.

1) Federated learning: The authors of **McMahan2016** propose a model aggregation method based on the iterative averaging of the models called `FederatedAveraging`. The evaluation is performed on several families of ML algorithms, and shows that the proposition is a practical solution for FL model aggregations. `FedAvg` is at the base of other works at Google [44], [50].

Konečný *et al.* [41] introduce two FL techniques allowing to drastically reduce the communication overhead of centralized model training, by modifying the type of update that is shared. The first one is called structured update. It works by limiting the structure of the trained model by reducing the number of parameters beforehand. The second, sketched updates, compresses the models loosely after training. With enough clients, the authors show that their methods allow decreasing the communication cost by two orders of magnitude without sacrificing the accuracy of the training. With fewer clients, however, the cost in terms of accuracy is too big.

The authors of [43] present DeepFed, a deep federated learning detection system tailored to deal with CPSs. The proposed scheme is three-fold. First, they use a machine learning algorithm based on Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) to detect attacks. Then, the parameters of the algorithm are shared with a centralized cloud server where model aggregation is performed. The connection between the agent and the server is secured by a Paillier public-key cryptosystem they also proposed. Their comparison with the state-of-the-art shows better results in the firsts rounds of computation. While using a federated approach, the proposed scheme maintains a centralized architecture.

	Paper	Year	Architecture	Algorihms	Aggregation	Dataset	Use cases	Sharing	Information shared	Cryptographic scheme	Notes
FL											
	McMahan2016	2016	-	CNN, LTSM	FederatedAveraging	MNIST, CIFAR-10	-	-	Models		
	Konecny2016	2016	-	LTSM	FederatedAveraging	CIFAR-10, Google BigQuery	-	-	Models (compressed/truncated)		
	Bonawitz2017	2017	-	-	SecureAggregation	-	-	-	Models (encrypted)		
	Bonawitz2019	2019	centralized, distributed	-	-	-	-	-	Models	Diffie-Helman key exchange, t-out-of-n Secret Sharing	
FL-based systems											
	Li2020	2020	centralized, independant trust authority	CNN, GRU	Homomorphic addition	custom (gas pipelining system, unpublished	CPS attack detection	P2CS	Models (encrypted)		
	Zhang2020	2020	centralized, distributed		dynamic, FederatedAveraging	COVID-CT, Covid radiography database, Covid chestxray	Covid-19 detection in medical images	P2CS	Models		
	Zhang2020a	2020	centralized, decentralized storage		CWD_FedAvg	custom (air-conditioner sensors), unpublished	Failure detection in IoT	P2CS	Models		incentives
	Majeed2019	2019	decentralized	-	DANE	-	-	P2CS	Models		
	Nguyen2019	2019	centralized, distributed	GRU	FederatedAveraging	custom, unpublished	Attack detection in IoT	P2CS	Models		
	Li2019	2019	centralized, distributed	SGD	Homomorphic multiplication	custom, unpublished	-	P2CS	Models (encrypted)	Homomorphic (Pallier)	"tradeoff between security, efficiency and functionality"
	Fereidooni2021	2021	-	-	SAFELearn	-	-	P2CS	Models (encrypted)	Homomorphic (Pallier)	
	Dong2020	2020	decentralized	-	Homomorphic addition	MNIST, SVHN	-	P2CS	Models (encrypted)	Homomorphic (Pallier)	
	Nguyen2021	2021	centralized	-	FederatedAveraging	Google BigQuery Reddit Dataset, CIFAR-10, DÏoT @Nguyen2019, UNSW-Benign @Sivanathan2019	Text prediction, Image classification, NIDS	P2CS	Models		poisoning-resilient FL
	Katevas2020	2020	centralized, distributed	-	FederatedAveraging	Google BigQuery	-	P2CS	Models		policy-enforcing system
	Ren2019	2019	local, distributed	DRL	custom	-	-	P2CS	Models		
Archi											
	HaddadPajouh20	2020	centralized	-	-	-	IoT security	-	-		
	Rathore2019	2019	centralized, distributed	GD	score fusion / feature fusion	NSL-KDD	Attack detection in IoT	P2P/C	Models		
	Leo2014	2014	decentralized	-	-	-	Home IoT security	P2P	Security events, metadata		
Detection											
	Thanigeaivelan2(	2016	local, distributed	N/A	-	-	Anomaly detection for IoT	P2S	Anomalies		
	Zhang2019	2019	local	SVM	-	Undisclosed	IoT	-	-		
	Schneider2018	2018	local	SDA	-	SWaT	ICS	-	-		Unsupervised
	Rosa2021	2021	local, distributed	Decision tree, Ra	-	Live HEDva	ICS	-	-		
	Charyyev2020	2020	local	-	-	Generated, unpublished	IoT	-	-		
	SafaeiPour2019	2019	local	PCA	-	Generated	IoT / botnets	-	-		
	Sivanathan2017	2017	local	K-means, Rando	-	-	Device classification in IoT	-	-		
	Hamza2019	2019	local	PCA	-	Generated	Volumtry attack detection in IoT	-	-		
	Doshi2018	2018	local	KN, LSVM, DT, R	-	Generated, unpublished	DDoS detection in IoT	-	-		
	Pahl2018	2018	distrinuted, middleware-based	BIRCH, K-mean	-	Generated	Anomaly detection for IoT	-	-		
	Sivanathan2020	2020	local	Random forest	-	Generated	Device classification in IoT	-	-		
	Kang2019	2019	distributed	-	-	Real (San Fransisco Yellow Cab dataset	Smart vehicles	P2P	Vehicular data		Detection of abnormal behavior using reputation
Sharing											
	DeFuentes2017	2017	publish-subscribe	-	-	-	Security incident sharing	P2S	Security information (STIX)	Homomorphic (Pallier), format-preserving	
	Gong2020	2020	decentralized	-	-	-	Security incident sharing	P2P	Security information (STIX)		
	Cha2020	2020	centralized, disitributed	-	-	-	CTI information sharing	P2S	TTI	-	Sybil-resilent
	Badsha2019	2019	centralized, disitributed	ID3	-	Apache's Spamassassin	CTI information sharing	P2CS	extracted features (encrypted)	Homomorphic encryption (ElGamal)	Classification of spam emails
	Lautert2020	2020	centralized, disitributed	-	-	-	Data provenance	P2P/CS	unspecified data	-	
	Vakilinia2017	2017	centralized	-	-	-	Information sharing	P2CS	unspecified data	-	
	Vakilinia2017a	2017	centralized	-	-	-	Information sharing with access-control	P2S	Security information (STIX)	Attribute-based encryption	
	Vakilinia2017b	2017	centralized	-	-	-	Information sharing	P2S	unspecified data	Aggregable blind signature (BBS+)	Anounymous ssharing and rewards
	Kokkonen2016	2016	undefined	-	-	-	Information sharing	P2P	Security information (STIX)	-	
	Wu2019	2019	decentralized	-	-	-	CTI nformation sharing	P2P	unspecified data	-	
	Badsha2020	2020	centralized, disitributed	-	-	-	-	P2S	unspecified data	Attribute-based encryption (CP-ABE)	

Fig. 2: Table of the reviewed literature

The authors of [51] used federated learning to improve Covid-19 detection by using dynamic fusion of the models. Health data cannot be shared because of privacy reasons, which is also true for most IoT applications. Federated Learning can be used to share models without sharing the data itself, which allows improving machine learning models significantly. Too many participants in the model fusion can cause important resource overhead. To help solve this issue, this work introduces dynamic fusion of the models, which allows selecting models both on their accuracy and their performance. Results show that the proposed implementation improves detection rate compared to the default parameters. It is also more fault tolerant as the dataset has been corrupted without having too much impact on the performance.

In their work, the authors of [46] present a federated learning algorithm capable of detecting failure in IIoT. The scheme is distributed and makes use of the Ethereum blockchain to preserve security and integrity of the shared data, where each the client stores its sensor data using a Merkel tree. The federation is made using the Centroid Distance Weighted (CDW) average between the two detection classes (failure or normal behavior). Tests show that their algorithm meet their expectation while being less accurate that more standard approaches like centralized federation or local training. The federated learning allows, however, to reduce the communication overhead when compared to centralized learning. Finally, the use of CDW is showed to be slightly better than standard aggregation (FedAvg, proposed by Google **McMahan2016**) depending on the dataset used.

The authors of [45] propose FLchain, a blockchain-enabled FL algorithm tailored for MEC networks, where the mobile devices rely on dedicated nodes on the edge to update the global model. They use a Merkle Patricia tree to store the model as the blockchain global state. Their proposed ecosystem is built upon Ethereum [52] and Hyperledger Fabric [53], the latter introducing the concept of channels on which FLchain's proposal rely. The contribution is evaluated by comparing its features with the ones of state-of-the-art alternatives. FLchain is stated to be more robust by means of its distributed architecture. An implementation still need to be reviewed.

The authors of [6] present DÏoT, the first federated detection systems for IoT devices to the author's knowledge. The system can train itself without human intervention in consequence of its architecture. The system leverages a classifier to detect clusters of devices and create device types. A GRU model is then trained on each type of device and aggregated in

a centralized server, allowing the system to be trained in less epochs while conserving good accuracy. DÏoT has been measured to produce zero false positives and has a detection rate of 95.6% on novel attacks using a dataset they generated. As far as we know, this dataset is not yet available.

In their work, the authors of [54] present a novel poisoning attack against federated learning approaches that cannot be prevented with the current techniques. They consider that the attacker compromised IoT devices but not the edge nodes which analyze the traffic, unlike other proposed attacks [55], [56] which need the nodes to be controlled by the attacker. Using their previously published federated learning system and dataset [6], they demonstrated that by injecting only ten percents of crafted traffic during the training phase, they are able to make malicious traffic labeled as benign.

The authors of [57] introduce `PoliFL`, a policy enforcement system for federated learning. The solution is meant to define how the models are trained and shared. They provide a decentralized platform built upon the `policile` framework, which provide the enforcement features. Model computation is performed by edge-devices, which are orchestrated via the `PoliFL` server. Evaluation has been performed on three use cases using Raspberry Pi devices. While the results show little overhead for the model aggregation, the initial model distribution observe a bandwidth saturation which causes slowdown.

Ren *et al.* [42] propose to exploit federated learning to optimize the training of deep reinforcement learning (deep RL) in the IoT. The authors consider IoT devices which rely on deep RL to make decisions, but cannot train the models themselves due to the heavy computation required by deep RL algorithms. Edge nodes are introduced to run the deep RL algorithms, but this setup induces communication overhead. Thus, the authors propose to use FL to train parts of the model, and send only the parameters. Their solution is showed to be as effective as a centralized approach, while lifting the communication constraint. However, the results of the evaluation also showed that the system is less effective on heterogeneous IoT devices, as they do not require the same amount of information at the same time; counter this disadvantage is identified as future work.

In [58], the authors propose a novel approach for employing federated learning at scale. Their work is based on the proposition of a protocol allowing the training of models without saturating the central server in centralized architectures. In the considered use case, the models are trained on mobile devices that report back to the server for each round. A round starts with the devices fetching the training information (e.g. current model). The server selects at the same time the devices on which the model will be trained. This way, not every device work on every round, which release bandwidth and computation resources.

Faced with the possibilities introduced by federated learning of poisoning the training, Shen, Tople, and Saxena [55] propose `Auror`, a defense systems against poisoning attacks in FL systems. Their approach relies on the identification of malicious contribution by detecting abnormal distributions in the shared features. The system is evaluated on two datasets: MNIST for handwriting recognition, and GTSRB for self-driving vehicles. The results are convincing, with only a 3% accuracy lost when compared to a model trained without poisoning.

To improve the privacy of FL, Bonawitz *et al.* [44] the authors propose a secure aggregation protocol which prevents the aggregating server of accessing the model updates of a specific user. The protocol is supported by cryptographic operations allowing to compute the model aggregation only if enough users have participated. The protocol is found to be quite communication-efficient, as it expends the data by a factor of two, in the worst case. This work inspired subsequent papers that focused on the security of FL, such as EPPS [59], SAFELearn [60], EaSTFLFy [61], or more recently FLGUARD [62].

2) Security Architectures: The authors of [29] propose an AI-enabled architecture to secure the physical layer (they call edge) of the IoT. Their model is based on a modular architecture with modules specifically tailored for one layer. A secured communication protocol, an AI-based Web Application Firewall (WAF) and a threat attribution module are dedicated to the application layer. The network layer includes a firewall module and an IDS. Finally, the perception (or edge) layer is secured by a threat hunting and a CTI module. Their approach is evaluated using comparisons with other works and a scoring formula they are providing.

The authors of [47] proposed an Software-defined networking (SDN)-based detection system using blockchain-based federated learning on a three-layer architecture. On the edge layer are monitored the devices via SDN-enabled switches which allow measuring traffic and quickly deploy effective counter-measures. The fog layer is made of SDN controllers that analyze the traffic and manages the flow rules of a cluster of switches. Each fog node trains a deep learning model on the traffic collected at the edge. All fog nodes then share their model via an Ethereum blockchain using a smart contract providing the model fusion. A last SDN controller in the cloud layer provides large-scale monitoring and allows deploying rules globally. This architecture removes the single point-of-failure induced by a cloud server and allows accurate detection fast mitigation thanks to being close to the devices. The authors compared their solution to centralized and distributed ones using the NSL-KDD dataset [35]. Their results show that their architecture outperforms the others on both the accuracy and the detection time, while only inducing a small computing overhead due to the blockchain.

Leo *et al.* [63] propose a generic security architecture for IoT network management. Their proposal relies on a middleware introduced by the same team [64] which allows the communication between gateways called Secure Mediation Gateway (SMGW). Each local network is monitored by a SMGW which provides Authentication, Authorization, and Accounting (AAA). Then, gateways are federated over the internet in a domain to exchange data.

3) Anomaly detection: The authors of [65] succinctly present a theoretical architecture for a distributed detection system. The proposal is built upon RPL — the IPV6 routing protocol for wireless lossy networks — in which the author propose to implement a control message, allowing nodes to report detected anomaly to the edge router. Each node monitors the characteristics of its 1-hop neighbors on the network and apply a non-specified machine learning algorithm to detect anomalies. The root node is in charge of making the decision to block the device or not. While not evaluated, the system is promised to solve common issues, especially the scalability.

This paper [66] leverages the concept of Social IoT (SIoT) to predict potential IoT threats. They analyze the relations between users, and especially account behavior, to identify malicious accounts. They train a SVM model on 6400 samples containing examples of zombie account, spam, or relationship mutation to identify malicious activity. Upon detection, the behavior prediction module output predications that could be used as input to a defense mechanism.

Schneider and Böttinger [67] present a deep learning-based detection system for CPS. Their solution is based on stacked denoising autoencoders (SDA) to perform anomaly detection on network packets. This approach requires a lot of data to properly train the model. Thereby, after trying to train their model on Modbus data, the authors evaluated their solution on the 300 GB Secure Water Treatment (SWaT) dataset. Their approach yields significant results, detecting over 99% of scenarios in long-lasting attacks. The detection is less efficient with short sequences and leads to some attacks being filtered out.

In [68], the authors introduce a novel holistic approach to anomaly detection where, instead of proposing an alternative detection system, they propose to mutualize and correlate different sources. The Intrusion and Anomaly Detection System (IADS) framework is built around three main parts: CPS probes with a configuration agent, event stream processing using Apache Kafka, and Apache Spark acting as a Security Information Management System (SIEM). They evaluate the solution on the HEDva testbed [69], and show significant results due to the use of multiple algorithms.

In [70], the authors propose a detection mechanism which doesn't require any feature extraction. Instead, it relies on the Nilsimsa hash [1] of the device's network traffic. It works by generating a set of signatures for each device during a training phase, and then comparing each new device's signature with the existing set. The system is proven to be effective, with 90% accuracy on the dataset created by the authors.

Hamza *et al.* [72] present a detection system for volumetric attacks toward IoT devices based on SDN monitoring. They analyze the devices' MUD profiles and translate it into a flow table which will later be used as a reference to identify malicious flows. The traffic features are then passed through a clustering algorithm and an outlier detector to identify anomalies. Upon evaluation, the system is shown to be effective, with an 89.7% true positive rate.

The authors of [73] address the issue of- high-dimensional vectors for machine learning. The paper introduces a novel data dimensionality reduction technique based on L1-norm Principal Component Analysis (PCA). They apply their technique on a dataset collected using a network telescope monitoring 2^{24} IPv4 addresses, also used in [1]. Their analysis identified 140 probing campaigns affecting 120,000 devices.

In [74], the authors do preliminary exploration on DDoS detection in home network. They analyze different local machine learning algorithms on a dataset containing emulated Mirai traffic. Packet-level feature extraction is performed for both stateless and stateful features, the former being the more lightweight. In the evaluation, all algorithm performed well with an F1-score of 0.99, except the Linear Support Vector Machine (LSVM) at 0.92, due to the nature of the dataset. Detection based on stateless feature outperformed the stateful one, suggesting that an integration in light-resource devices such as home routers may be possible.

Pahl and Aubet [75] study anomaly detection in microservices (μSs). Using Virtual State Layer (VSL) [76] to abstract the μS' interfaces, they use ML to model the behavior of IoT devices based on their communications. Models can be merged using a federation service allowing to improve anomaly detection. Evaluation is performed using a dataset they generated by motoring connections between seven devices over 24 hours. The solution is shown to be accurate at 99%, with only 0.2% of false positive. The dataset has been published to allow reproducibility.

In [77], the authors focus on traffic characterization for IoT devices. As operators often do not have a full grasp on their assets, Sivanathan *et al.* [77] propose a system capable of characterizing and classifying devices based on their traffic. Clustering is performed by using K-Means algorithm. Then, they evaluate their approach using a Random Forest (RF) classifier and obtained a 95% accuracy on new data. Their approach is further developed in [78], where they introduce specialized classifiers able to identify the operational state of a device (e.g. booting, idle).

Kang *et al.* [79] study the use of consortium blockchain (by opposition to private and open blockchains) to support data sharing in vehicular edge-networks, preventing sharing without authorization. They also introduce a reputation model designed to ensure the quality of the information. Their system is based on the use of smart contract for data storage and information sharing, with cryptographic operations to guaranty the system's security. The computing nodes are called roadside units and operate on the edge network. The system is evaluated on the San Francisco Yellow Cabs dataset (C Projects. (2013). [Online]. Available: http://www.yellowcabsf.com/) and shows a 100% detection rate of abnormal vehicles in 60 minutes.

4) Information sharing: The authors [80] present PRACIS, a Structured Threat Information Expression (STIX)-based secure information sharing system. The system provides pri-

[1]Hashing mechanism which produces similar hashes for similar inputs, originally used for spam detection [71].

vate information forwarding and aggregation. To that end, PRACIS leverages format-preserving and homomorphic encryption primitives: the messages are encrypted but allows the system to verify attributes, such as the incident type, and the incidents are aggregated without accessing the data itself. The performance of the system has been measured, and appears to be suitable for real-world usage.

Gong and Lee [81] present BLOCIS, a Sybil-resilient blockchain-based information sharing framework. The implementation relies on smart-contract to manage users, validate information, share alerts, and thus offer traceability and privacy through encryption. Sybil-resilience is assured a penalty system that increase the cost (in cryptocurrencies) for the process of conducting Sybil attacks.

In [82], the authors propose another blockchain-based CTI sharing system. They focus their approach on sustainability, with a proposed model which save 15% of storage when compared to the other network resources. In their architecture, the blockchain provides contribution validation and rewards, as well as data integrity. A third-party cloud server is used to process the data shared by the different feeds over the blockchain.

Badsha, Vakilinia, and Sengupta [83] introduce a privacy preserving information sharing system which takes advantage of a decision tree-based learning classification algorithm to share information about the participant without accessing the data itself. To allow operating on the data, they leverage the ElGamal homomorphic encryption scheme [84]. They test their algorithm by training the decision-tree on a dataset of spam emails, they then use the algorithm to classify an email sample between spam and non-spam. The same protocol could theoretically be applied to other kind of data as long as the features are numerical values.

The authors also propose BloCyNfo-Share [85], a blockchain-based information sharing platform which includes access control. They therefore leverage attribute-based encryption, preventing anyone not meeting the condition to decipher the message. Using the Ethereum blockchain, they provide integrity and traceability to their system. Proxy re-encryption has been studied in other works, such as [86], which has however a centralized cloud-based approach.

In [87], the authors propose a blockchain architecture to share information while attesting of its provenance. The system relies on fog nodes to achieve data-spread and distributed storage. Any uploaded information is associated with a cryptographic proof of authenticity in the blockchain, allowing provenance tracking without accessing itself. The proposed architecture is evaluated in comparison with a cloud-based one on three criteria: time per request, system load, and blocked threads. The fog architecture obtained better results in all three.

Developing incentives for organizations to share their information is a major research question in the field of information sharing. Vakilinia and Sengupta [88] propose to apply game theory to information sharing to motivate the organizations to participate, and get a reward. According to their simulation, game-theoretic approaches allow a better distribution of the benefits of the sharing, as well as a better participation rate. The problematic of incentives in information sharing has been discussed by other papers [89]–[91] but applying game-theory is quite a novel approach. The authors also presented two other systems the same year, the first one is focused on attribute-based encryption for access control [92], while the other addresses privacy-preserving information-sharing [93].

The authors of [94] propose a risk-based model to share situation awareness with the lowest impact possible. Their model relies on the STIX and Trusted Automated eXchange of Indicator Information (TAXII) standards, and has for objective to calculate the sharing opportunities with the lowest risk. To that end, the model identifies the participants (and potential partners), and associates a risk level with each one.

In [95], the authors introduce the TITAN framework to address trust issues in peer-to-peer (P2P) reputation systems. They use the blockchain and Trusted Execution Environment (TEE) to provide security, integrity, and privacy. On the contrary of other works, the blockchain here is solely used as an immutable database, not for its distributed properties. To the best of our knowledge, TITAN has yet to be validated.

D. Evolution of the topic

The topic of anomaly detection is an old topic, which started to rise in the early 2000' as depicted in fig. 3c. The topics gained interest in 2015, with the increasing of the research on IoT and IIoT devices [16], [74], as shown with fig. 3b. IIoT security has appeared recently, due to the proliferation of connected devices in modern industries.

On the topic of collaboration, the sharing of threat-related information is also an old topic which regained interest in 2017—see fig. 3a, with a focus on the topics of privacy-preserving sharing [80], [87], [93]. With the introduction of FL by **McMahan2016**, the community started to apply distributed learning approaches to anomaly detection around 2019, with works like [6].

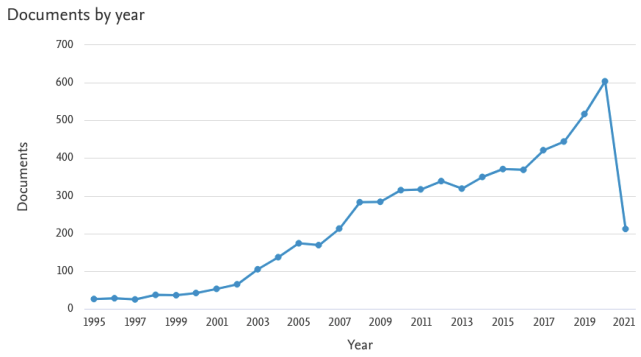
E. Relevant venues

Venues vary a lot, partly because of the wide spectrum that this work addresses. *Computer & Security* is the most represented venue (journals and conferences combined). Close after comes *arXiv* as Google published multiple papers in it. Most publications are made in IEEE journals, notably *IEEE Transactions on Industrial Informatics* and *IEEE Internet of Things Journal*. This shows how spared the publications concerning the IoT are.

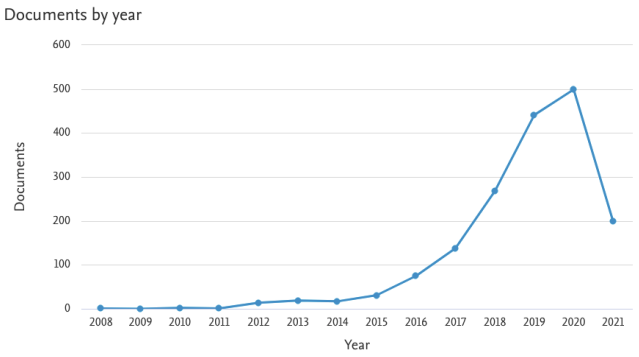
Figure 4 shows the relevant venues in the literature.

F. Most active groups

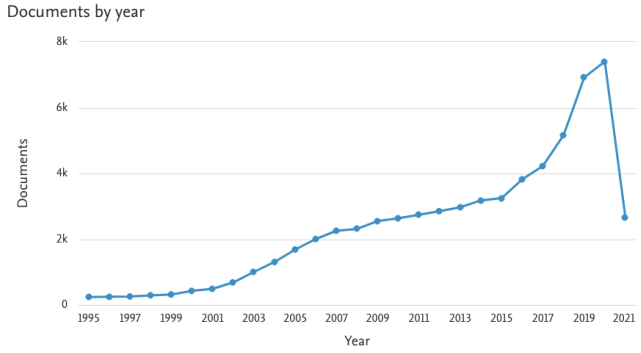
Since they introduced the topic of FL in 2016, the team at Google Research has been a big influence for the research community **McMahan2016**, [41], [44], [50], [58]. They mostly work on the primitives behind FL, such as model aggregation with the FedAvg algorithm **McMahan2016**. The team of TU Darmstadt (Germany) is contributing to the field with DÏoT [6] and an analysis of FL poisoning attacks.



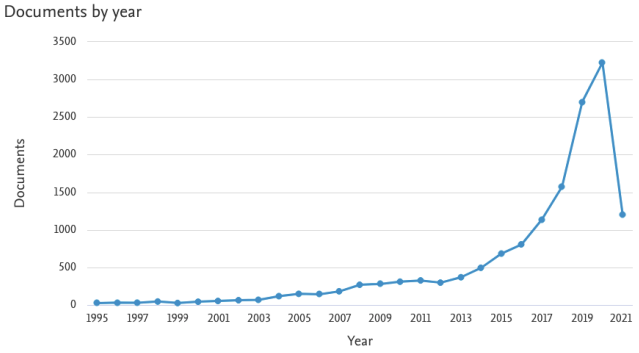
(a) Threat intelligence sharing—query (a)



(b) IIoT security—query (b)



(c) Anomaly detection—query (c)



(d) Distributed ML—query (d)

Fig. 3: Evolution of the topics using queries (a) to (d), according to Scopus

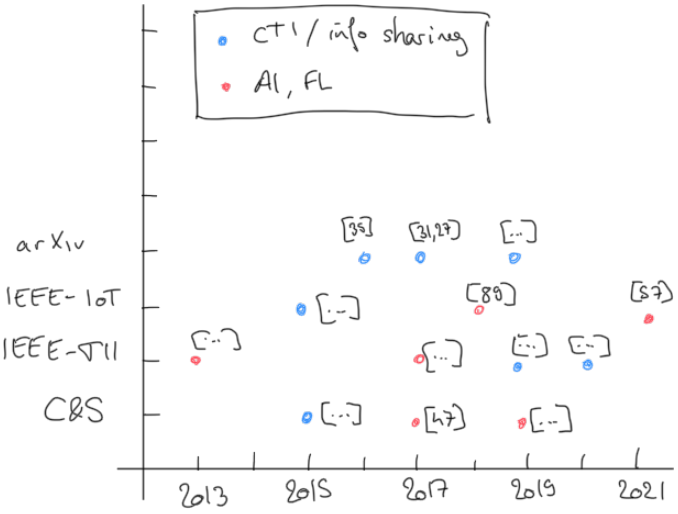


Fig. 4: Relevant venues

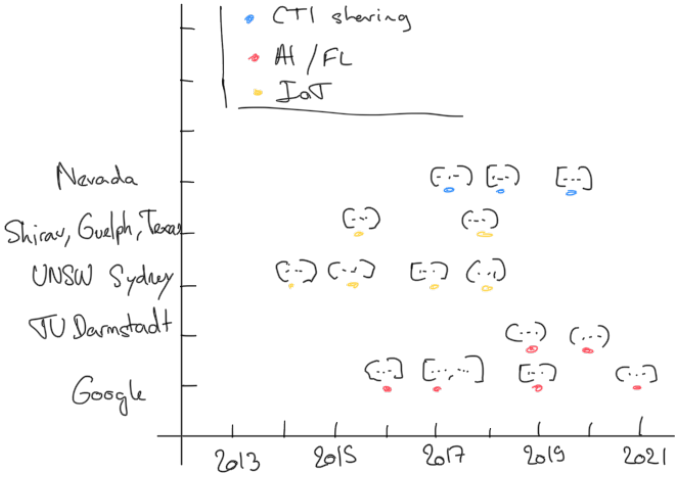


Fig. 5: Relevant venues

UNSW Sydney is very invested in the IoT security, mostly traffic analysis [72], [77], [78]. The universities of Shiraz (Iran), Guelph (Canada), and Texas collaborated on multiple occasion to provide papers about IoT security [29], [73], [86], proposing a security architecture of the edge layer [29].

On the subjects of information-sharing, the *Department of Computer Science and Engineering* of the University of Nevada has produced multiple papers in the past years [83], [85], [88], [92], [93]. They notably propose the use of blockchain technologies to support the information-sharing while preserving privacy and efficiency [85].

Figure 5 shows the most active groups in their topic.

G. Open Issues

Depending on the underlying domain, several questions are yet to answer. On the topic of information sharing, future works are required to improve automation of the sharing systems. Furthermore, as a lot of work are trying to improve the security of sharing mechanisms by implementing different cryptographic scheme **DeFuentes2017d**, [83], [85], the security of such proposals deserves future work. Improving the efficiency of such complex systems is also considered [61].

As FL starts to become mature, its security begins to be assessed by several works [6], [56], [62]. Further works may be required to extensively discuss the security and privacy of federated learning. Since this work particularly focuses on the application of federated learning to security and anomaly detection, research question also include the selection of algorithms that are (i) efficient to classify and group devices, (ii) and have models that can be easily aggregated.

V. Conclusion

This paper presented automated collaborative security approaches for the IIoT. A selection of relevant papers are presented in the fields of information sharing and collaborative AI. In contrast to the existing surveys presented in section II, this work focused on the application of these approaches to the IIoT.

Section III gave an overview of the identified subtopics and provided a reference architecture to put the selected works in context. Sections IV-D to IV-F identified the major venues, the most active research groups, and the evolution of the topic. Both FL and MAS are relatively new research fields, but their application to the IIoT has yet to be thoroughly studied.

In section IV-C, this work reviewed the selected papers along the different parts of the reference architecture as depicted in fig. 1: anomaly detection algorithms, FL model aggregation, secured information-sharing, and distributed ledgers.

We hope that this paper will help fellow researchers to acquire an efficient overview of this domain, and eventually improve the security of the IIoT.

References

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, ISSN: 1553-877X. DOI: 10.1109/COMST.2019.2910750. [Online]. Available: https://ieeexplore.ieee.org/document/8688434/.

[2] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy Magazine*, vol. 9, no. 3, pp. 49–51, May 2011, ISSN: 1540-7993. DOI: 10.1109/MSP.2011.67. [Online]. Available: http://ieeexplore.ieee.org/document/5772960/.

[3] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, IEEE, Nov. 2018, pp. 124–130, ISBN: 978-1-5386-5201-5. DOI: 10.1109/GCWCN.2018.8668630. [Online]. Available: https://ieeexplore.ieee.org/document/8668630/.

[4] B. Herzberg, I. Zeifman, and D. Bekerman. "Breaking Down Mirai: An IoT DDoS Botnet Analysis." (2016), [Online]. Available: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/?redirect=Incapsula (visited on 03/12/2021).

[5] S. Edwards and I. Profetis, "Hajime: Analysis of a decentralized internet worm for IoT devices," *Cs.Umd.Edu*, pp. 1–18, 2016.

[6] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, vol. 2019-July, IEEE, Jul. 2019, pp. 756–767, ISBN: 978-1-72812-519-0. DOI: 10.1109/ICDCS.2019.00080. [Online]. Available: https://ieeexplore.ieee.org/document/8884802/.

[7] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, Mar. 2019, ISSN: 13891286. DOI: 10.1016/j.comnet.2019.01.023. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.01.023.

[8] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101 589, 2019, ISSN: 01674048. DOI: 10.1016/j.cose.2019.101589.

[9] A. Pala and J. Zhuang, "Information Sharing in Cybersecurity: A Review," *Decision Analysis*, vol. 16, no. 3, pp. 172–196, Sep. 2019, ISSN: 1545-8490. DOI: 10.1287/deca.2018.0387. [Online]. Available: http://pubsonline.informs.org/doi/10.1287/deca.2018.0387.

[10] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, Jan. 2018, ISSN: 01674048. DOI: 10.1016/j.cose.2017.09.001. [Online]. Available: https://doi.org/10.1016/j.cose.2017.09.001.

[11] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol. 60, pp. 154–176, 2016, ISSN: 01674048. DOI: 10.1016/j.cose.2016.04.003.

[12] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2683200. [Online]. Available: https://ieeexplore.ieee.org/document/7879243/.

[13] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, ISSN: 23528648. DOI: 10.1016/j.dcan.2019.08.006. [Online]. Available: https://doi.org/10.1016/j.dcan.2019.08.006.

[14] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102 481, April 2019 Jan. 2020, ISSN: 10848045. DOI: 10.1016/j.jnca.2019.102481. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.102481.

[15] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2799854. [Online]. Available: http://ieeexplore.ieee.org/document/8274922/.

[16] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, ISSN: 1553-877X. DOI: 10 . 1109 / COMST . 2019 . 2896380. [Online]. Available: https://ieeexplore.ieee.org/document/8629941/.

[17] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Access*, vol. 8, pp. 140 699–140 725, 2020, ISSN: 2169-3536. DOI: 10 . 1109 / ACCESS . 2020 . 3013541. [Online]. Available: https : / / ieeexplore . ieee . org / document/9153560/.

[18] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Generation Computer Systems*, vol. 115, pp. 619–640, Feb. 2021, ISSN: 0167739X. DOI: 10.1016/j.future.2020.10.007. [Online]. Available: https://doi.org/10.1016/j.future.2020.10.007.

[19] L. Lyu, H. Yu, and Q. Yang, "Threats to Federated Learning: A Survey," *arXiv*, Mar. 4, 2020. [Online]. Available: http://arxiv.org/abs/2003.02133.

[20] D. Chismon and M. Ruks, "Threat Intelligence: Collecting, Analysing, Evaluating," *Cert-Uk*, p. 36, 2015.

[21] ENISA, "Actionable Information for Security Incident Response," 2014, pp. 1–79.

[22] *Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, in collab. with The European Parliament and The Counsil, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[23] S. Murdoch and N. Leaver, "Anonymity vs. Trust in Cyber-Security Collaboration," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, New York, NY, USA: ACM, Oct. 12, 2015, pp. 27–29, ISBN: 978-1-4503-3822-6. DOI: 10 . 1145 / 2808128 . 2808134. [Online]. Available: https://dl.acm.org/doi/10.1145/2808128.2808134.

[24] V. Sklyar and V. Kharchenko, "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 2, IEEE, Sep. 2019, pp. 1046–1049, ISBN: 978-1-72814-069-8. DOI: 10.1109/IDAACS.2019.8924452. [Online]. Available: https://ieeexplore.ieee.org/document/8924452/.

[25] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, ISSN: 0018-9162. DOI: 10.1109/MC.2017.201. [Online]. Available: http://ieeexplore.ieee.org/document/7971869/.

[26] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 28, 2011, ISSN: 0039-6338. DOI: 10.1080/00396338.2011.555586. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00396338.2011.555586.

[27] S. Berger, O. Bürger, and M. Röglinger, "Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy," *Computers & Security*, vol. 93, p. 101 790, Jun. 2020, ISSN: 01674048. DOI: 10.1016/j.cose.2020.101790. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101790.

[28] L. Wustrich, M.-O. Pahl, and S. Liebald, "Towards an Extensible IoT Security Taxonomy," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, vol. 2020-July, IEEE, Jul. 2020, pp. 1–6, ISBN: 978-1-72818-086-1. DOI: 10.1109/ISCC50000.2020.9219584. [Online]. Available: https://ieeexplore.ieee.org/document/9219584/.

[29] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things," *Neural Computing and Applications*, vol. 32, no. 20, pp. 16 119–16 133, Oct. 25, 2020, ISSN: 0941-0643. DOI: 10.1007/s00521-020-04772-3. [Online]. Available: https://doi.org/10.1007/s00521-020-04772-3.

[30] D. Coss and S. Samonas, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security.," *Journal of Information System Security*, vol. 10, no. 3, pp. 21–45, 2014. [Online]. Available: www.jissec.org.

[31] D. B. Parker, "Toward a New Framework for Information Security?" In *Computer Security Handbook*, Hoboken, NJ, USA: John Wiley & Sons, Inc., Sep. 12, 2015, pp. 3.1–3.23. DOI: 10.1002/9781118851678.ch3. [Online]. Available: http://doi.wiley.com/10.1002/9781118851678.ch3.

[32] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK for Industrial Control Systems : Design and Philosophy," 2020.

[33] Anonym. "Mirai Tracker." (2019), [Online]. Available: https://mirai.security.gives/ (visited on 03/12/2021).

[34] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18–28, Feb. 2009, ISSN: 01674048. DOI: 10.1016/j.cose.2008.08.003. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404808000692.

[35] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, Jul. 2009, pp. 1–6, ISBN: 978-1-4244-3763-4. DOI: 10.1109/CISDA.2009.5356528. [Online]. Available: http://ieeexplore.ieee.org/document/5356528/.

[36] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2016, ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2402161. [Online]. Available: http://ieeexplore.ieee.org/document/7041170/.

[37] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS)*, pp. 361–369, 2017, ISSN: 20488610.

[38] S. A. V. Jatti and V. J. Kishor Sontif, "UNSW-NB15: A Comprehensive Data set for Network Intrusion Detection Systems," *International Journal of Recent Technology and Engineering*, vol. 8, pp. 3976–3983, 2S11 Nov. 2, 2019, ISSN: 2277-3878. DOI: 10.35940/ijrte.B1540.0982S1119.

[39] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021, ISSN: 2329-9266. DOI: 10.1109/JAS.2021.1003820. [Online]. Available: https://ieeexplore.ieee.org/document/9317716/.

[40] Z. Zuo, Q.-L. Han, B. Ning, X. Ge, and X.-M. Zhang, "An Overview of Recent Advances in Fixed-Time Cooperative Control of Multiagent Systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2322–2334, Jun. 2018, ISSN: 1551-3203. DOI: 10.1109/TII.2018.2817248. [Online]. Available: https://ieeexplore.ieee.org/document/8322314/.

[41] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," pp. 1–10, Oct. 18, 2016. [Online]. Available: http://arxiv.org/abs/1610.05492.

[42] J. Ren, H. Wang, T. Hou, S. Zheng, and C. Tang, "Federated Learning-Based Computation Offloading Optimization in Edge Computing-Supported Internet of Things," *IEEE Access*, vol. 7, pp. 69 194–69 201, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2919736. [Online]. Available: https://ieeexplore.ieee.org/document/8728285/.

[43] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics*, vol. 3203, no. c, pp. 1–1, 2020, ISSN: 1551-3203. DOI: 10.1109/TII.2020.3023430. [Online]. Available: https://ieeexplore.ieee.org/document/9195012/.

[44] K. Bonawitz *et al.*, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 30, 2017, pp. 1175–1191, ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3133982. [Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3133982.

[45] U. Majeed and C. S. Hong, "FLchain: Federated Learning via MEC-enabled Blockchain Network," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, Sep. 2019, pp. 1–4, ISBN: 978-4-88552-320-5. DOI: 10.23919/APNOMS.2019.8892848. [Online]. Available: https://ieeexplore.ieee.org/document/8892848/.

[46] W. Zhang *et al.*, "Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT," *IEEE Internet of Things Journal*, pp. 1–1, Sep. 6, 2020, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3032544. [Online]. Available: https://ieeexplore.ieee.org/document/9233457/.

[47] S. Rathore, B. Wook Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications*, vol. 143, pp. 167–177, December 2018 Oct. 2019, ISSN: 10848045. DOI: 10.1016/j.jnca.2019.06.019. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.06.019.

[48] J. Kephart and D. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003, ISSN: 0018-9162. DOI: 10.1109/MC.2003.1160055. [Online]. Available: http://ieeexplore.ieee.org/document/1160055/.

[49] K. S. Decker, "Distributed problem-solving techniques: A survey," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 17, no. 5, pp. 729–740, Sep. 1987, ISSN: 0018-9472. DOI: 10.1109/TSMC.1987.6499280. [Online]. Available: https://ieeexplore.ieee.org/document/6499280/.

[50] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," pp. 1–38, Oct. 8, 2016. [Online]. Available: http://arxiv.org/abs/1610.02527.

[51] W. Zhang *et al.*, "Dynamic Fusion based Federated Learning for COVID-19 Detection," *arXiv*, vol. 14, no. 8, pp. 1–9, Sep. 22, 2020, ISSN: 23318422. [Online]. Available: http://arxiv.org/abs/2009.10401.

[52] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Nov. 2014.

[53] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, New York, NY, USA: ACM, Apr. 23, 2018, pp. 1–15, ISBN: 978-1-4503-5584-1. DOI: 10.1145/3190508.3190538. [Online]. Available: https://dl.acm.org/doi/10.1145/3190508.3190538.

[54] T. D. Nguyen, P. Rieger, M. Miettinen, and A.-r. Sadeghi, "Poisoning Attacks on Federated Learning-based IoT Intrusion Detection System," in *The Network and Distributed System Security Symposium (NDSS) 2020*, 2020, ISBN: 1-891562-64-9. [Online]. Available: https://dx.doi.org/10.14722/diss.2020.23003.

[55] S. Shen, S. Tople, and P. Saxena, "Auror: Defending against poisoning attacks in collaborative deep learning systems," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, New York, NY, USA: ACM, Dec. 5, 2016, pp. 508–519, ISBN: 978-1-4503-4771-6. DOI: 10.1145/2991079.2991125. [Online]. Available: https://dl.acm.org/doi/10.1145/2991079.2991125.

[56] C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Mitigating Sybils in Federated Learning Poisoning," *arXiv*, Aug. 14, 2018, ISSN: 23318422. [Online]. Available: http://arxiv.org/abs/1808.04866.

[57] K. Katevas *et al.*, "Policy-Based Federated Learning," Mar. 14, 2020. [Online]. Available: http://arxiv.org/abs/2003.06612.

[58] K. Bonawitz *et al.*, "Towards Federated Learning at Scale: System Design," *arXiv*, Feb. 4, 2019. [Online]. Available: http://arxiv.org/abs/1902.01046.

[59] Y. Li, H. Li, G. Xu, S. Liu, and R. Lu, "EPPS: Efficient Privacy-Preserving Scheme in Distributed Deep Learning," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, USA: IEEE, Dec. 2019, pp. 1–6, ISBN: 978-1-72810-962-6. DOI: 10.1109/GLOBECOM38437.2019.9013395. [Online]. Available: https://ieeexplore.ieee.org/document/9013395/ (visited on 05/18/2021).

[60] H. Fereidooni *et al.*, "SAFELearn: Secure Aggregation for private FEderated Learning," p. 8, 2021.

[61] Y. Dong, X. Chen, L. Shen, and D. Wang, "EaSTFLy: Efficient and secure ternary federated learning," *Computers & Security*, vol. 94, p. 101 824, Jul. 2020, ISSN: 01674048. DOI: 10.1016/j.cose.2020.101824. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820300985 (visited on 05/18/2021).

[62] T. D. Nguyen *et al.*, "FLGUARD: Secure and Private Federated Learning," Jan. 21, 2021. arXiv: 2101.02281 [cs]. [Online]. Available: http://arxiv.org/abs/2101.02281 (visited on 05/18/2021).

[63] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *2014 Euro Med Telco Conference (EMTC)*, IEEE, Nov. 2014, pp. 1–5, ISBN: 978-88-87237-20-7. DOI: 10.1109/EMTC.2014.6996632. [Online]. Available: http://ieeexplore.ieee.org/document/6996632/.

[64] M. Castrucci *et al.*, "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 2, pp. 86–97, Jul. 2012, ISSN: 18745482. DOI: 10.1016/j.ijcip.2012.04.001. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874548212000194 (visited on 05/19/2021).

[65] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2016, pp. 319–320, ISBN: 978-1-4673-9292-1. DOI: 10.1109/CCNC.2016.7444797. [Online]. Available: http://ieeexplore.ieee.org/document/7444797/.

[66] H. Zhang, Y. Yi, J. Wang, N. Cao, and Q. Duan, "Network attack prediction method based on threat intelligence for IoT," *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 30 257–30 270, Nov. 20, 2019, ISSN: 1380-7501. DOI: 10.1007/s11042-018-7005-2. [Online]. Available: http://link.springer.com/10.1007/s11042-018-7005-2.

[67] P. Schneider and K. Böttinger, "High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks," in *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, New York, NY, USA:

ACM, Jan. 15, 2018, pp. 1–12, ISBN: 978-1-4503-5992-4. DOI: 10.1145/3264888.3264890. [Online]. Available: https://dl.acm.org/doi/10.1145/3264888.3264890.

[68] L. Rosa *et al.*, "Intrusion and anomaly detection for the next-generation of industrial automation and control systems," *Future Generation Computer Systems*, vol. 119, pp. 50–67, Jun. 2021, ISSN: 0167739X. DOI: 10.1016/j.future.2021.01.033. [Online]. Available: https://doi.org/10.1016/j.future.2021.01.033.

[69] C. Foglietta *et al.*, "From Detecting Cyber-Attacks to Mitigating Risk Within a Hybrid Environment," *IEEE Systems Journal*, vol. 13, no. 1, pp. 424–435, Mar. 2019, ISSN: 1932-8184, 1937-9234, 2373-7816. DOI: 10.1109/JSYST.2018.2824252. [Online]. Available: https://ieeexplore.ieee.org/document/8352138/ (visited on 05/19/2021).

[70] B. Charyyev and M. H. Gunes, "IoT Traffic Flow Identification using Locality Sensitive Hashes," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, vol. 2020-June, IEEE, Jun. 2020, pp. 1–6, ISBN: 978-1-72815-089-5. DOI: 10.1109/ICC40277.2020.9148743. [Online]. Available: https://ieeexplore.ieee.org/document/9148743/.

[71] E. Damiani, "An Open Digest-based Technique for Spam Detection," p. 6, 2004.

[72] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman, "Detecting Volumetric Attacks on loT Devices via SDN-Based Monitoring of MUD Activity," in *Proceedings of the 2019 ACM Symposium on SDN Research*, New York, NY, USA: ACM, Apr. 3, 2019, pp. 36–48, ISBN: 978-1-4503-6710-3. DOI: 10.1145/3314148.3314352. [Online]. Available: https://dl.acm.org/doi/10.1145/3314148.3314352.

[73] M. Safaei Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. A. Pados, and K.-K. R. Choo, "Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns," *Digital Investigation*, vol. 28, S40–S49, Apr. 2019, ISSN: 17422876. DOI: 10.1016/j.diin.2019.01.014. [Online]. Available: https://doi.org/10.1016/j.diin.2019.01.014.

[74] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 29–35, Ml Apr. 11, 2018. DOI: 10.1109/SPW.2018.00013. [Online]. Available: https://ieeexplore.ieee.org/document/8424629/.

[75] M.-O. Pahl and F. X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," *14th International Conference on Network and Service Management, CNSM 2018, 1st Workshop on Segment Routing and Service Function Chaining*, pp. 72–80, 2018.

[76] M.-O. Pahl, G. Carle, and G. Klinker, "Distributed smart space orchestration," in *Network Operations and Management Symposium 2016 (NOMS 2016) - Dissertation Digest*, May 2016.

[77] A. Sivanathan *et al.*, "Characterizing and classifying IoT traffic in smart cities and campuses," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, May 2017, pp. 559–564, ISBN: 978-1-5386-2784-6. DOI: 10.1109/INFCOMW.2017.8116438. [Online]. Available: http://ieeexplore.ieee.org/document/8116438/.

[78] A. Sivanathan, H. Habibi Gharakheili, and V. Sivaraman, "Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 60–74, Mar. 2020, ISSN: 1932-4537. DOI: 10.1109/TNSM.2020.2971213. [Online]. Available: https://ieeexplore.ieee.org/document/8981946/.

[79] J. Kang *et al.*, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019, ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2875542. [Online]. Available: https://ieeexplore.ieee.org/document/8489897/.

[80] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez, "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing," *Computers & Security*, vol. 69, pp. 127–141, Aug. 2017, ISSN: 01674048. DOI: 10.1016/j.cose.2016.12.011. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2016.12.011.

[81] S. Gong and C. Lee, "BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance," *Electronics*, vol. 9, no. 3, p. 521, Mar. 21, 2020, ISSN: 2079-9292. DOI: 10.3390/electronics9030521. [Online]. Available: https://www.mdpi.com/2079-9292/9/3/521.

[82] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing," *Sustainability*, vol. 12, no. 16, p. 6401, 2020, ISSN: 2071-1050. DOI: 10.3390/su12166401.

[83] S. Badsha, I. Vakilinia, and S. Sengupta, "Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2019, pp. 0708–0714, ISBN: 978-1-72810-554-3. DOI: 10.1109/CCWC.2019.8666477. [Online]. Available: https://ieeexplore.ieee.org/document/8666477/.

[84] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985, ISSN: 0018-9448. DOI: 10.1109/TIT.1985.1057074. [Online]. Available: http://ieeexplore.ieee.org/document/1057074/ (visited on 05/20/2021).

[85] S. Badsha, I. Vakilinia, and S. Sengupta, "BloCyNfo-Share: Blockchain based Cybersecurity Information Sharing with Fine Grained Access Control," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2020, pp. 0317–0323, ISBN: 978-1-72813-783-4. DOI: 10.1109/CCWC47524.2020.9031164. [Online]. Available: https://ieeexplore.ieee.org/document/9031164/.

[86] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," *Pervasive and Mobile Computing*, vol. 28, pp. 122–134, Jun. 2016, ISSN: 15741192. DOI: 10.1016/j.pmcj.2015.06.017. [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2015.06.017.

[87] F. Lautert, D. F. Pigatto, and L. Gomes, "A fog architecture for privacy-preserving data provenance using blockchains," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, vol. 2020-July, IEEE, Jul. 2020, pp. 1–6, ISBN: 978-1-72818-086-1. DOI: 10.1109/ISCC50000.2020.9219724. [Online]. Available: https://ieeexplore.ieee.org/document/9219724/.

[88] I. Vakilinia and S. Sengupta, "A coalitional game theory approach for cybersecurity information sharing," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, vol. 2017-Octob, IEEE, Oct. 2017, pp. 237–242, ISBN: 978-1-5386-0595-0. DOI: 10.1109/MILCOM.2017.8170845. [Online]. Available: http://ieeexplore.ieee.org/document/8170845/.

[89] M. Abouzahra and J. Tan, "The Effect of Community Type on Knowledge Sharing Incentives in Online Communities: A Meta-analysis," in *2014 47th Hawaii International Conference on System Sciences*, IEEE, Jan. 2014, pp. 1765–1773, ISBN: 978-1-4799-2504-9. DOI: 10.1109/HICSS.2014.224. [Online]. Available: http://ieeexplore.ieee.org/document/6758821/.

[90] ENISA, "Incentives and Challenges for Information Sharing in the Context of Network and Information Security," 2010, p. 52. [Online]. Available: http://www.google.com/#sclient=

psy & hl = en & safe = off & q = literature + review + information + sharing+law+enforcement&aq=f&aqi=&aql=&oq=&gs_rfai=&pbx=1&fp=9bef8cda26d1a6ec.

[91] D. Fernández Vázquez, O. Pastor Acosta, C. Spirito, S. Brown, and E. Reid, "Conceptual framework for cyber defense information sharing within trust relationships," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, Jun. 2012, pp. 1–17, ISBN: 978-9949-9040-8-2.

[92] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Attribute based sharing in cybersecurity information exchange framework," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, vol. 49, IEEE, Jul. 2017, pp. 1–6. DOI: 10.23919/SPECTS.2017.8046770. [Online]. Available: http://ieeexplore.ieee.org/document/8046770/.

[93] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, vol. 49, IEEE, Jul. 2017, pp. 1–7. DOI: 10.23919/SPECTS.2017.8046783. [Online]. Available: http://ieeexplore.ieee.org/document/8046783/.

[94] T. Kokkonen, J. Hautamaki, J. Siltanen, and T. Hamalainen, "Model for sharing the information of cyber security situation awareness between organizations," in *2016 23rd International Conference on Telecommunications (ICT)*, IEEE, May 2016, pp. 1–5, ISBN: 978-1-5090-1990-8. DOI: 10.1109/ICT.2016.7500406. [Online]. Available: http://ieeexplore.ieee.org/document/7500406/.

[95] Y. Wu, Y. Qiao, Y. Ye, and B. Lee, "Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, IEEE, Oct. 2019, pp. 474–481, ISBN: 978-1-72812-949-5. DOI: 10.1109/IOTSMS48152.2019.8939192. [Online]. Available: https://ieeexplore.ieee.org/document/8939192/.