Forensic Science International: Reports 5 (2022) 100257

Contents lists available at ScienceDirect

Forensic Science International: Reports

journal homepage: www.sciencedirect.com/journal/forensic-science-international-reports

Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0

Victor R. Kebande [a,*]

[a] Department of Computer Science (DIDA), Blekinge Institute of Technology, Karlskrona, 37179, Sweden

ARTICLE INFO

Keywords:
IIoT
Cybersecurity
Industry 4.0
Digital
Forensics

ABSTRACT

Advances in Industrial Internet of Things (IIoT), inter-connectivity, continuous rise of smart ecosystems, and the quintessential need of process automation has not only opened formidable opportunities, but it has also extended the cyber-threat and attack landscape. Predominantly, this has been witnessed even as industries race towards aligning themselves with the on-demand industry 4.0 goals. Notably, it has become apparent that the convergence and amalgamation of Industrial Operational Technology (OT) with Information Technology (IT) brings about sophiscation, IIoT ecosystem complexities, paradigm shift and overall changes in security and digital forensic investigation architectures. Consequently, as the cybersecurity threat landscape also becomes more complicated in this context, with a widened attack surface, emergent and diverse system behaviors, the digital forensic perspective of IIoT is hardly integrated or addressed as many industries race to realize industry 4.0 objectives at the time of writing this paper. It is based on this premise, that this paper puts an argument that, at the time of writing this paper, there still lacks methodologies, standards, processes or maturity models that have a focus on IIoT forensics as the rat-race towards achieving Industry 4.0 persists. Based on these dimensions, the author explores the scope of IIoT forensics and posits the need of exploring and incorporating forensic standards and methods in IIoT. It is the authors' opinion that the suppositions fronted herewith may provide fundamental building blocks for future IIoT-centered investigative frameworks.

1. Introduction

The fourth industrial revolution dubbed Industry 4.0 has ushered in a significant new era that has seen diversification in sensing, process automation, and a race towards creating smart manufacturing ecosystems. These revolutions among others have seen a paradigm shift and a change of industrial ecosystems, processes and rather increased operational efficiency. Consequently, this has led to the creation of Industrial Internet of Things (IIoT) technology where Operational Technologies (OT) like Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) and Distributed Control Systems (DCS) that used to be stand-alone have been able, to not only converge with ICT-based technologies but also have led to automation of smart ecosystems that consist of a multitude of networked devices, applications and embedded systems that have shared intelligence [1].

Currently, the global forecast for IIoT in terms of market size is projected to be around USD 950 billion by the year 2025 [2]. This implies that OT and the need for Machine to Machine (M2M) based systems is projected to be a norm that will see IIoT thrive based on the data generated from the convergence of OT and IT.

While this wave takes the world by a storm, it is worth to mention that unprecedented cybersecurity issues and challenges seems to be the weak link that may hinder achieving the full potential of industry 4.0, and IIoT especially considering the integration of cross-cutting vulnerable technologies. Apart from that, attribution, incident detection and Incident Response Procedures (IRP) in IIoT are techniques that have not been explored to the full potential in the race towards industry 4.0′s process automation. At the time of writing this paper, this concept is still seen from a very narrow perspective mainly due to the absence of forensic methodologies, processes and application-specific standards that have a focus on IIoT with key forensic application requirements [3].

The key objective of this paper is presented in two-folds: Firstly, the author assess the cross cutting vulnerable trends, from IoT to IIoT technologies to what is realized in the quest for process automation, owing to how IoT is able to generate the exchange of large amount of secure and safety critical data [4]. After this, the author assess how the complexity of these systems may end up having an impact in the wake of a cybersecurity attack, and the need for attribution as a result.

* Correspondence to: Department of Computer Science, Blekinge Institute of Technology, Karlskrona, Sweden.
E-mail address: victor.kebande@bth.se.

https://doi.org/10.1016/j.fsir.2022.100257
Received 17 April 2021; Received in revised form 1 January 2022; Accepted 11 January 2022
Available online 19 January 2022

Therefore the contributions of this paper are summarized as follows:

- Highlight the need for digital forensic investigation processes, standards and methods in IIoT.
- Provide a contextual evaluation of the study.
- Identify open and future challenges.

The remainder of this paper is organized as follows: In Section 2, a Related Literature is given. This is followed by Research Gap in Section 3 which is then followed by the Cross-cutting Vulnerable technologies in Section 4. The Need for IIoT Forensics is givend in Section 5, followed by a discussion in Section 6. A Conclusion and a mention of future work is ultimately given in Section 7.

2. Related Literature

2.1. IIoT and Industry 4.0

Digitization and the need for smart manufacturing processes has led to the emergence of IIoT, where it has become possible to integrate OT and IT domains, as many industrial processes are being automated. Currently, this has been projected as the most suitable way of achieving operational efficiency. Consequently, IIoT has more relevance on machine-to machine communication and mission critical systems that have a high volume of data. Fig. 1 shows the relationship between IoT, IIoT, industry 4.0 and Cyber Physical Systems (CPS).

According to [6], industrial internet comprise of IoT, machines, and people that enables effective and successful intelligent industrial operations while leveraging data analytics process. Notably, industry 4.0 is presented as a collection of terminologies and concepts for value chains that enhances smart factories, CPS and the real time monitoring of physical processes. Fundamentally, the notion of industry 4.0 represents an emerging trend aimed at achieving the fourth industrial revolution while leveraging computation and communication resources [7]. On the other hand, CPS, is highlighted as a set of interactions of distributed physical and digital components, like sensing, computations, control and networking [8]. The foundation of IIoT has in diverse contexts been attributed to the integration of sophisticated processes into production systems in order to control and monitor the systems in real-time.

2.2. Digital forensics

Relatively, digital forensics is still an emerging discipline that has a focus on utilizing scientifically prescribed methodologies for purposes of electronic discovery. While forensics itself carries a legal connotation, it is also envisioned as a precursor to litigation on matters of post-event response. NIST Special Publication 8006–86 [9] highlights the essence and need by industries or organizations in establishing a digital forensic capability. A variety of tasks are identified as follows: For purposes of operational troubleshooting, log monitoring, data recovery, data acquisition while organizations are able to have due diligence and compliance. Nevertheless, the importance of enforcing this capability is to be able to forensically collect, examine, analyse and report the existence of artifacts in a digital environment. Also, ISO/IEC 27043 international standard [10], which exists as an umbrella standard for high-level investigation concepts opens the scope for incident investigation techniques by suggesting strategies that are relevant for pre-incident and post-incident identifications in organizations. Apart from that, research by [11] has also portrayed the need for incorporating forensic models in connected environments based the adoption of the classes of digital investigation processes-which is more relevant in maximizing the potential use of digital forensic evidence for purposes of litigation.

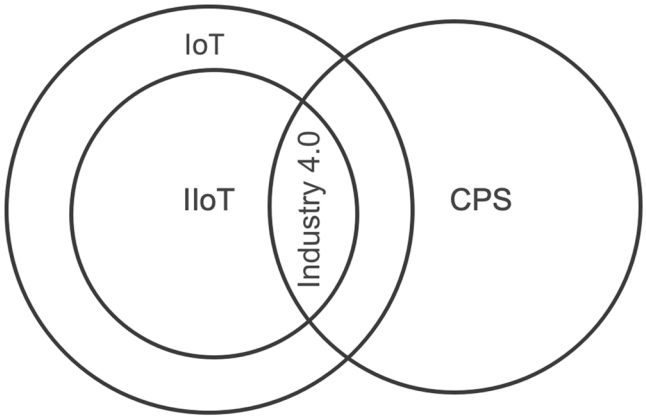

Fig. 1. Relationship between IoT, IIoT and Industry 4.0 [5].

3. Research gap

The significance of realizing the fourth industrial revolution shows technological and operation disruptions across diverse areas. Following the remarkable and continuous success of 5G and 6G fabric, the current and next generation IoT and IIoT technologies provides a promising and a wide-range of capabilities; ranging from effective inter-communication, process integration, interoperability and the need for creating smart ecosystems. IIoT attempts to provide an integration of smart environments (M2M, people together with analytics) through interconnection. In addition, it promotes exchange of data, monitoring of activities for purposes of efficiency. Currently, IIoT ecosystem faces complexity and with the incorporation and integration of OT with IT there is an extended cyber-threat and attack landscape, which also lacks application-specific standards on what is acceptable or not. Discounting that, digital forensics which attempts to provide post-event response strategies is a concept that has hardly been explored in this context. While from the authors' opinion this is seen as an inadvertent omission, the author postulates the lack standards, methodologies, maturity models or specific guidelines that can be employed in this discourse at the time of writing this paper.

4. Cross-cutting IoT/IIoT vulnerable technologies

A concise overview of vulnerable IoT and IIoT segments whose processes are being automated are explored in this section. The current penetration of IIoT has been realized in many areas like the cloud, data analytics, mobile technology etc., as a result of sensorial escalation and advancements. While in the last decade this had been regarded as an emerging technology [12] its prevalence and penetration has already outlived this narrative due to the explosion of devices, ubiquity, increased number of devices and rapid technological changes. The author of this paper explores a number of IoT based application areas that have witnessed advances that have motivated and influenced an expansion to IIoT, which in this context has been referred with the term "smart". Smart in this context is used to denote an aspect that utilizes ICT to make an influence to critical and operational infrastructure components [13]. Additionally, smart IoT serves as a reflection of application areas that have a plethora of things that are able to collect, process, sense and share the collected data from operational and integrated-based set-ups [14]. Table 1 shows a summary of the cross-cutting IoT vulnerable trends that have propelled the quintessential rise of IIoT.

- *Smart Cities*: Based on smart-oriented trends, IoT has been positioned as a technology that facilitates a number of processes that can help in monitoring and integrating operational industrial critical infrastructure processes within a city, like air travel, railway, seaport, bridges road transport etc [15]. Due constant monitoring, automating smart city processes makes this a highly susceptible process to security and privacy.

Table 1
Distinctions on the Cross-Cutting IoT/IIoT Vulnerable Technologies, Consequences and Relevance.

IoT	IIoT	Consequences	Relevance
Smart Cities Trends	manufacturing 4.0 processes/ strategies	Extended threat & attack landscape/ DoS/Spoofing/ Replay Attacks	-Device attribution -Perpetrator/ suspect linkage to potential digital crime -Attack Prevention through profiling
Smart-IoT Transport trends	Efficient intelligent & smart production processes	Threats on OT and IT integration points, IoT-related attacks, data integrity attacks	At OT & IT intersection, there lacks forensic standards and methodologies or maturity models -May be impossible to conduct forensic activities
IoT health /IoMT (Medical of Things)	Smart IoMT integrated and intelligent processes	Ransomware threats/Process/ Data-related attacks	-potential detection of ransomware paths-Attribution of digitally propagated crimes
Smart living spaces/ homes	dynamic Integration and interconnecting processes that can realize smart environments	Intrusion/privacy violations/process hijack and corruption	-Monitoring privacy invasion beacons
Internet of vehicles (IoV) Autonomous Vehicles	Incorporate OT and IT operations for IoV support	Communication-based attacks (V2V, V2S, V2R,V2D, V2I), DoS, Spoofing, masquerading attacks	Attack detection through providing proof of possession of past data
Unmanned Aerial Vehicle (UAVs)	Dynamic process integration (Focus on intelligent UAV-production processes	fault data injection, spoofing, Sensor-based attacks, channel interference	-Forensic attribution and threat intelligence gatherinbg based on UAVs traversals
Big data analytics	IIoT decision making-based on data	data availability attacks, authentication-based attacks, comouflage attacks, tampering, Replay Attacks	Profiling generic data-related attacks through digital forensic activities

- *Smart Transport*: It is relative to intelligent transport techniques, which in the-recent past has gained more attention. Research by DEMO has showed a demonstration using a feasible technique and an intelligent vehicle initiative that are mainly focused on creating a smart transport ecosystem [16]. Basically, the perception behind smart transportation relies on the influence of people, road networks and intelligent ICT techniques, which is a critical area that presents vulnerable surfaces as a result of process integration.
- *Smart Health*: The IoT-based medical sector, healthcare centers and hospitals form an ecosystem that provisions healthcare-based services using infrastructures and technologies that are provided by smart cities. This has accelerated the formation of ubiquitous healthcare system “Smart health" [17], and IIoT plays a significant role in this integration. Intelligent IoT technology allows predictive techniques, intelligent prescription approaches and medical diagnosis. These techniques are more personalized in a fashion that allows data to be collected using sensor-based devices based on the interconnection between users and infrastructures [18].
- *Smart Homes/Smart Living spaces*: The topology of smart homes relies on intelligent sensor networks and the interconnection of IoT devices in order to establish an effective and reliable communication channel. Generally, smart homes are structured in a way that allows them to rely on an array of data in order to form some behaviors either defined or pre-defined [19,20,21]. This involves a consideration of some learning patterns and agent-based behaviors to make some decisions [19]. Additionally, the context of smart homes attempts to generate context-based information that has a capability of being processed in an intelligent approach by providing effective serves over reliable infrastructures. Smart homes are basic building blocks of the smart city concept with an advantage of sharing a pool of resources through machine to machine interconnection and human to machine [22].
- *Autonomous Vehicles*: Autonomous Vehicles (AV) or self-driving cars technology has witnessed quite substantially novel designs, implementations and integration with IIoT technologies with the sole aim of providing efficient transportation experiences that. The concept of AV is basically been a revolution that allows vehicles to intelligently operate with minimal human intervention [23]. This is possible through the ability of self-configuration in diverse areas like navigation, road movement based on the dynamic environment. Furthermore, they are supported by communication systems and infrastructures that allow VtoV communication, and also utilize sensing technologies to discover the surrounding and environment using vehicle control systems [24]. In this context, as an IoT based approach, AVs are able to fit in an IIoT ecosystem by way of utilizing sensors that are able to collect data, where real-time analysis of the collected data is used to improve the models used in Vehicular technologies.
- *Unmanned Aerial Vehicles*:Unmanned Aerial Vehicles/drones have been propelled as a very useful technology in the last decade, across different application areas. UAVs are able to archive their objectives by relying on the connectivity between the users and the environment by collecting useful data using sensor-based approaches. UAVs generally are able to utilize a variety of emerging technologies like 5G, 4G, LTE, edge computing in order to effectively deliver IIoT services. [24]. UAV and IoT works in tandem given that UAV/drones are mostly embedded with IoT-based devices that allow co-existence-by allowing IoT-based technology to collect useful data based on the events that UAV acts on. Existing research has also shown that UAVs can accomplish image processing techniques in order to detect/locate specific targets, altering this processes during automation can lead to undesirable effects. The integration of UAV with IIoT environment positions it as a critical aspect that could be explored from a digital forensic perspective [25].
- *Big data analytics*: Increased number of devices and communication techniques has not only reinforced monitoring of events by IIoT applications but also in the collection of information and data from sensor controlled environments. Advances in big data analytics techniques plays a significant role by showing how the data that is collected from IoT ecosystems can be used to shape how business situations can be used to bring valuable insights [26]. Existing big data frameworks have mainly suggested approaches that can be used in overcoming the existing huge amount of data that is stored from IIoT ecosystems through utilizing sensors in order to enable real-time detection [27].

5. Need for IIoT forensics

It is imperative to develop digital forensic models and systems that are able to support future investigative technologies. This, is owing to the fact that during incident response, an attack, a disaster or a potential security incident has to be attributed to a potential perpetrator. The notion of digital forensics in IIoT suffers from lack of accepted standards methodologies, policies and procedures that can define what a digital

forensic environment constitutes and how potential incidents can be handled in the wake of an attack. While the traditional ICS, SCADA and OT environments were thought to be disconnected from other internet-based environments, it has become apparent with the race to industry 4.0 that the convergence of OT and IT environments underpins different critical infrastructure sectors like healthcare, manufacturing and transport etc, and the threat and attack landscape has widened tremendously as a result. Therefore, this paper posits an argument on why it might be important to incorporate forensic strategies that are inclined towards incidental planning and preparation in IIoT environment. The core objective of exploring this notion, is based on the fact that, process automation and manufacturing processes currently utilizes OT/IT-based technologies and services, and the cost of a cyber attack may have adverse effects to industries if they are not forensically attributed to a given source. Also, this is based on assertions that rely on the fact that the current projections for industry 4.0 initiatives are expanding, and as a result it is worth incorporating the legal connotations when such ramifications are experienced for future planning and saving the costs of reactive processes. Additionally, the need for exploring digital forensics in diverse fields has also been necessitated by the persistent need of electronic discovery of new content and artifacts that are previously unknown to digital forensics practitioners-which is a core motivating factor for conducting comprehensive investigations [28].

5.1. Scope of IIOT forensics

Pre-incident planning and preparation is a vital process in any digital ecosystem, therefore, the scope of IIoT forensics opines to the same forensic logic. Digital forensic processes in IIoT have in the past been aligned towards in SCADA systems, where diverse aspects like live forensics [32] and maintaining the forensic soundness of collected potential evidence has been positioned as a core technical challenge. In essence, this challenge can easily be overcome if a device-specific forensic method and techniques are actualized that can go just beyond collecting and analysing network-forensic data [33]. Fig. 2, shows how the current relationship between IoT, IIoT, CPS-that have an expanded cyber attack surface needs digital forensics as the projection for fully achieving industry 4.0 is envisioned.

Additionally, integrating open-source tools for purposes of network forensic analysis as a way of ensuring resiliency in the wake of industrial-based attacks, is a significant approach for industrial processes. Notably, existing frameworks or models lacks significant evaluation approaches. The existing work/technologies are presented from a very high-level perspective and as a result, this hinders key investigation approaches [34], especially with OT and IT convergence.

5.2. Need for forensic standards, methodologies and processes in IIoT

The continuous realization of IIoT faces a critical hurdle of standardization given that at the time of writing this article, still there lacks acceptable standards and methodologies that entirely have a focus on IIoT. Despite this, IIoT still currently faces an exponential growth albeit

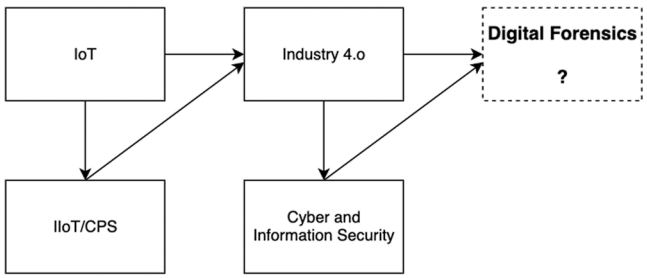

Fig. 2. The figure shows the scope and the need for incorporating IIoT forensics.

with an extended and increased threat and attack landscape, complexity and the need for post-event response strategies. Existing standards like the ISO/IEC 27043 do not explicitly have a focus in IIoT spectrum and integrating some or all of these processes may hamper the chances of digital evidence being admitted as credible evidence during litigation. Also, IIoT technical challenges [35] that have been highlighted in the industrial internet architecture include data sharing, security and privacy, interoperability, safety, OT and IT convergence, reliability and resiliency, however, digital forensics in IIoT environments is hardly mentioned in this context.

As a result, an expanded attack surface and increased potential security incidents implies that there is a need for developing common acceptable standards [36] with key benefits to IIoT ecosystems in order to guarantee seamless investigation processes. The key benefits of developing such holistic standards and methodologies are as follows:

- Incidental planning and preparation in a digital forensic readiness approach in IIoT: This action would allow industries to be able to identify potential risks, sources of attacks and potential digital evidence that can allow forensic planning and preparing for incident detection processes.
- Generating processes that would allow initializing digital forensic investigation process through incident response and by identifying first responders while planning for attribution.
- Acquiring and locating potential digital evidence by way of identifying, collecting and digitally preserving potential evidence, for example using triage [37].
- Maximizing the potential use planning and preparation phases as a way of saving the cost of conducting digital forensic evidence during incident response.

That notwithstanding, industry 4.0 advances are currently more dependent on automation of processes and the real time data that is collected from highly connected smart processes. With this interconnection there is an increase in security challenges given that a majority of industrial processes needs to run continuously.

Generally, it takes great strides to set up an Incident Detection and Response (IDR) mechanism, in an IIoT ecosystem given the sophiscation, complexity and constant change of the cyber-attack landscape of IIoT architecture. An IDR would allow forensic practitioners and the legal experts to develop a major understanding of the IIoT forensic ecosystem and how it can be mapped or aligned to forensic practices. A key aspect of consideration that can be embedded in IIoT forensics by design [38, 39,40] manufacturers is the need for forensic by design technique, which is positioned as an effective way for developing automated forensic tools/systems. In this context, an ideal IIoT forensic tool or a process model would be focused on addressing the following strategies: Potential risks, preparation of IIoT environments for incident detection strategies(proactive-based processes), using automated forensic tools for potential incident identification, digital evidence collection and forensic analysis process.

Furthermore, existing research has shown the limitations that exists in IIoT forensics, given the absence of forensic standards, methods and process models as is shown in Table 2. The study infers from Table 2 that there is no specific existing industrial standard that has an inclination towards digital forensics, however, standards like ISA/IEC 62443 family are able to address security risks, threat and vulnerabilities, information security and cybersecurity strategies.

International standard like ISO/IEC 27043 [10] which in its entirety has a foundation on incident investigation techniques is generic, and not application specific to IIoT. This is a perennial challenge to IIoT environment and it is the authors opinion that a core IIoT investigative model should incorporate the following aspects: .

- Devices that are designed to support automated digital forensics (forensic by design)

Table 2
Existing Security Standards for Industrial Processes/Systems and Automation of Devices.

Reference	Standard	Focus	Security risks	Threat/ Vulnerability	Infosec	Digital forensics	Cybersecurity
[29]	ISA/IEC 62443	Security for control system components	✓	✓	X	X	✓
[29]	ISA/IEC 62443–4–2	Security for Industrial Automation	✓	✓	✓	X	✓
[29]	ISA/IEC 62443–3–3	System Security Requirements	✓	✓	✓	X	✓
[29]	ISA/IEC 62443–4–1	Product Security Development	X	X	X	X	✓
[29]	ISA/IEC 62443–3–2	Security Risk Assessment	✓	✓	✓	X	✓
[30]	NIST-IIoT	Security for IIoT	✓	✓	✓	X	✓
[10]	ISO/IEC 27043	Incident Investigation Principles	✓	X	✓	✓	✓
[31]	NIST-SP800–82	Industrial control system security	✓	X	✓	X	✓
[29]	ISA/IEC 62443–4–2	Technical requirements for IACS components	✓	X	✓	X	✓
[29]	IEC 62351–4	Security for any profiles including MMS - Authentication for MMS - TLS for TCP/IP	X	✓	✓	X	✓
[29]	IEC 62351–5	TLS for TCP/IP profiles and encryption for serial profiles	X	✓	✓	X	✓
[29]	IEC 62351–7	Security through network and system management	✓	✓	✓	X	✓
[29]	IEC62351–8	Role Based Authentication Control	✓	✓	✓	X	✓

- Industrial network forensics support where different clients are able to communicate over different protocols. Through this communication, forensic techniques can be supported by collecting digital data at industrial network level
- Given data that is generated from IIoT environments like SCADA is processed in the cloud, it is needful for IIoT environment to support cloud forensics strategies
- IIoT support for digital forensic readiness, which is a crucial phase of incidental planning and preparation

Fundamentally, given that the essence of IIoT is to enable smart manufacturing, IIoT ecosystems need to conform to digital forensic processes that can alleviate the perennial challenge of attribution by incorporating standards, methods and process as is shown in Fig. 3. Fig. 3 shows different level through which forensics could be incorporated in IIoT. SCADA forensics, network forensics, cloud and live forensics could be incorporated at the lowest level, followed by digital forensic readiness that should be implemented based on the existing standards, methods and processes.

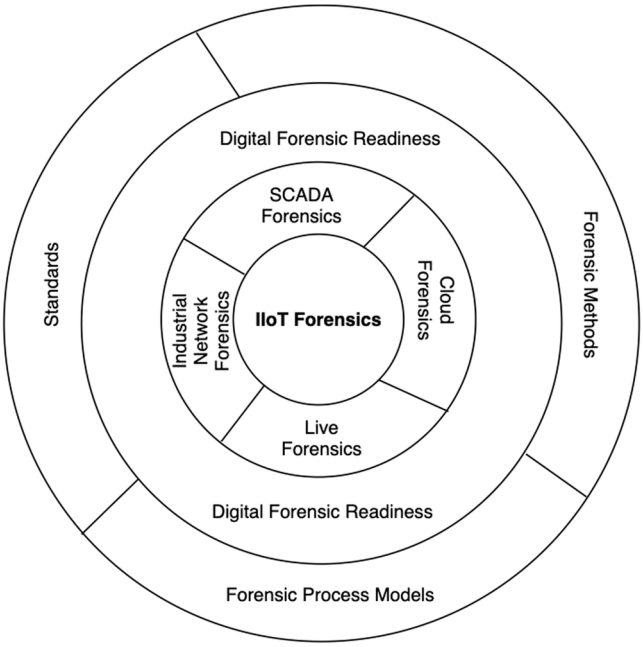

Fig. 3. Incorporating digital forensics, standards, models and methods in IIoT.

6. Discussions

As industry 4.0 advances and technologies are being accepted worldwide, key vulnerabilities keep increasing too and data seems to play the central role on how major operations are being conducted. As a result, it is important to be able to measure IIoT parameters whether they are able to dynamically produce accurate outputs and to be able to continuously run even in the wake of potential attacks or security incidents. While it is imperative to mention that IIoT environments require real-time monitoring of constantly communicating devices, the key concerns are mainly the cost that can be incurred to organizations if potential threats and attacks are not mitigated, while it is important to emphasize that the security of data and safety of human life could in this context be a key subject of focus.

It is the authors' opinion that attributing a potential incident to a perpetrator could play a key role of future incident detection and mitigation and that incorporating strategies of pre-incident and post-incident detection in industry 4.0 could have an impact on real-time incident detection strategies. For example, standards like ISO/IEC 27000 [41] family highlights special guidelines that can be used in managing digital information and assets in organizations, however still, ISO/IEC 2700 is not inclined to IIoT. Precisely, if the ISO/IEC 2700 guidelines are adopted they could play a special role of conducting real-time monitoring. Also, ISA/IEC 62443 has set a precedent for the frameworks that are able to address security vulnerabilities in industry 4.0/industrial automation and control systems. Also, ISA-62243 family [29] also highlights a range of guidelines, for example, on cybersecurity requirements for components, system security requirements for components, mitigating threats and vulnerabilities. Apart from that, ISO/IEC 27043 [10] which is a standard on information security, incident investigation principles and processes has outlined guidelines that are meant to expedite digital investigations, however, this cannot be translated and fit in the current IIoT environments given the complexity in IIoT architectures, functionalities and ecosystem. Notably, based on the existing standards, there is currently no digital forensic based standard that has a focus to IIoT or industry 4.0 strategy at the time or writing this paper. Table 2 as has been shown explores some of the existing standards that have a focus on industrial automation, industrial control and the standards, that are measured against security risks, threats and vulnerabilities, information security, digital forensics and cybersecurity.

In view of the foregoing, industry 4.0 advancements are influenced

by many factors like advanced 5G networks, resource optimization and constantly the functionalities of these environments keeps alternating, which creates threats and vulnerable end points. Predominantly, this becomes an easy target for adversaries, given the cross-cutting technologies. Important to note is the fact that standard forensic investigations are paramount to any emerging ecosystem. To achieve this, an IIoT ecosystem should primarily have a key focus on the dynamicity and the ever changing IIoT landscape, diverse sources of data, need for compliance, attribution, anti-forensics and the absence of standardized forensic tools. The notion behind having standardized tools that have a focus on IIoT forensics is to incorporate mechanisms that allows reliable testing of tools [42] in order to aid in the acquisition and interpretation of digital data-this increases the chances of admissibility given the complexity of IIoT ecosystems.

7. Conclusion and future work

From a cybersecurity perspective, the integration of OT and IT extends and opens the attack surface, owing to the nonexistence of acceptable strategies (Standards and methodologies) for conducting proactive and reactive forensic processes in IIoT on the fly. As a result, this paper identifies the following as open and future problems: .

- While OT has relevance to IIoT-based functions like SCADA and ICS, its integration with IT from a security perspective is seen to be orthogonal. This, is owing to the fact that IT concentrates on the communication side as opposed to OT. Monitoring functions (from IT perspective) at their integration opens a new complex attack surface. In addition, from a forensic perspective, solutions that are centered to IIoT are hardly identified at the time of writing this paper.
- As IoT-based devices keep increasing, so does the processes of achieving IIoT (Complexity due to device proliferation, process integration and technology evolvement). This means that the changing IIoT ecosystem are devoid of accepted digital forensic investigation approaches. While the ISA/IEC 62443 family (Table 2) points out a number of security-related aspects, they are generic from the authors opinion and forensics is hardly mentioned.
- As OT and IT integration persists major decisions are seen to be made based on the data that is being generated. From the context of analysing these data, it would be important to stipulate the baseline techniques that can take processing models close to the integrating points given that sometimes it is a case of distributed systems.
- Explicitly, it is worth mentioning that there is no accepted digital forensic approach centered for IIoT or future manufacturing 4.0 still-this hinders attack detection, attribution and lowers changes of digital evidence admissibility if a potential security incident is detected.

This paper has concentrated on exploring how in the race of achieving industry 4.0- smart manufacturing and process automation has forgotten the concept of IIoT forensics. The paper mainly identifies key cross-cutting vulnerable IoT technologies that are identified as catalysts that have accelerated the birth of IIoT, the scope and the need for digital forensics standards, methodologies and processes in IIoT. This paper shows the relevance and also highlights perrenial open and future. problems As a continuation of this work, future work aims at developing a generic IIoT forensic framework that is compliant with existing standards that can support current future investigative processes.

References

[1] K. Tange, M. De Donno, X. Fafoutis, N. Dragoni, A systematic survey of industrial internet of things security: requirements and fog computing opportunities, IEEE Commun. Surv. Tutor. 22 (2020) 2489.

[2] GrandReview, Iiotmarketsize: Industrial iot market size worth usd949.42 billion by 2025 – cagr: 29.4 per cent, GrandReview Research 1, 1 2019.

[3] V.R. Kebande, S.O. Baror, R.M. Parizi, K.-K.R. Choo, H. Venter, Mapping digital forensic application requirement specification to an international standard, Forensic Sci. Int. Rep. 2 (2020), 100137.

[4] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things. Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE,, 2015, pp. 1–6.

[5] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (2018) 4724.

[6] I. internet, Industry internet consortium, what is the industrial internet, (2018).

[7] D. Serpanos, M. Wolf, Industrial internet of things. Internet-of-Things (IoT) Systems, Springer,, 2018, pp. 37–54.

[8] H. Boyes, A Security Framework for Cyber-Physical Systems, University of Warwick,, Coventry, 2017.

[9] K. Kent, S. Chevalier, T. Grance, H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication, 2006.

[10] ISO/IEC,27043: 2015 international standard, information technology - security techniques - incident investigation principles and processes, ISO.org 1, 1 (2015).

[11] V.R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (iot). Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2016, pp. 356–362.

[12] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (2013) 1645.

[13] J. Bélissent, et al., Getting Clever about Smart Cities: New Opportunities Require New Business Models, Cambridge, Massachusetts, USA, 2010, p. 244.

[14] P. Punithavathi, S. Geetha, M. Karuppiah, S.H. Islam, M.M. Hassan, K.-K.R. Choo, A lightweight machine learning-based authentication framework for smart iot devices, Inf. Sci. 484 (2019) 255.

[15] R.E. Hall, B. Bowerman, J. Braverman, J. Taylor, H. Todosow, and U. Von Wimmersperg, The vision of a smart city, Tech. Rep. (Brookhaven National Lab., Upton, NY (US), 2000).

[16] Z. Xiong, H. Sheng, W. Rong, D.E. Cooper, Intelligent transportation systems for smart cities: a progress review, Sci. China Inf. Sci. 55 (2012) 2908.

[17] G. Peng, D. Dey, A. Lahiri, Healthcare it adoption: an analysis of knowledge transfer in socioeconomic networks, J. Manag. Inf. Syst. 31 (2014) 7.

[18] G. Muhammad, S.M.M. Rahman, A. Alelaiwi, A. Alamri, Smart health solution integrating iot and cloud: a case study of voice pathology monitoring, IEEE Commun. Mag. 55 (2017) 69.

[19] K.E. Skouby, P. Lynggaard, Smart home and smart city solutions enabled by 5g, iot, aai and cot services. Proceedings of the International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2014, pp. 874–878.

[20] J. Bugeja, A. Jacobsson, R. Spalazzese, On the analysis of semantic denial-of-service attacks affecting smart living devices, In: Proceedings of the Science and Information Conference, Springer. 2020, pp. 427–444.

[21] J. Bugeja, A. Jacobsson, P. Davidsson, Prash: a framework for privacy risk analysis of smart homes, Sensors 21 (2021) 6399.

[22] T.K. Hui, R.S. Sherratt, D.D. Sánchez, Major requirements for building smart homes in smart cities based on internet of things technologies, Future Gener. Comput. Syst. 76 (2017) 358.

[23] N. Kumar, A.-S.K. Pathan, E.P. Duarte, R.A. Shaikh, Critical applications in vehicular ad hoc/sensor networks, Telecommun. Syst. 58 (2015) 275.

[24] B.V. Philip, T. Alpcan, J. Jin, M. Palaniswami, Distributed real-time iot for autonomous vehicles, IEEE Trans. Ind. Inform. 15 (2018) 1131.

[25] G. Horsman, Unmanned aerial vehicles: a preliminary analysis of forensic challenges, Digit. Investig. 16 (2016) 1.

[26] A. Nieto, R. Rios, J. Lopez, Iot-forensics meets privacy: towards cooperative digital investigations, Sensors 18 (2018) 492.

[27] C. Meffert, D. Clark, I. Baggili, F. Breitinger, Forensic state acquisition from internet of things (fsaiot) a general framework and practical approach for iot forensics through iot device state acquisition, In: Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017, pp. 1–11.

[28] G. Horsman, Raiders of the lost artefacts: Championing the need for digital forensics research, Forensic Sci. Int. Rep. 1 (2019), 100003.

[29] ISA/IEC, 62443: 2020 standard specifies security capabilities for control system components, ISA.org 1, 1 (2020).

[30] NIST, Nist: 2019 securing the industrial internet of things, NIST.gov 1, 1 2019.

[31] NIST, Nistsp800-82: 2015 guide to industrial control systems (ics) security, NIST.gov 1 1, 2019.

[32] V.R. Kebande, R.A. Ikuesan, N.M. Karie, S. Alawadi, K.-K.R. Choo, A. Al-Dhaqm, Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (eco) in iot environments, Forensic Sci. Int. Rep. 2 (2020), 100122.

[33] R. A. Awad, S. Beztchi, J. M. Smith, B. Lyles, and S. Prowell, Tools, techniques, and methodologies: A survey of digital forensics for scada systems, In: Proceedings of the 4th Annual Industrial Control System Security Workshop. 2018. pp. 1–8.

[34] C. Valli, Snort ids for scada networks. Secur. Manag. (2009) 618–621.

[35] S.-W. Lin, B. Miller, J. Durand, R. Joshi, P. Didier, A. Chigani, R. Torenbeek, D. Duggal, R. Martin, G. Bleakley, et al., Industrial internet reference architecture, Industrial Internet Consortium (IIC), Tech. Rep (2015).

[36] N.M. Karie, V.R. Kebande, H. Venter, K.-K.R. Choo, On the importance of standardising the process of generating digital forensic reports, Forensic Sci. Int. Rep. 1 (2019), 100008.

[37] G. Horsman, C. Laing, P. Vickers, A case-based reasoning method for locating evidence during digital forensic device triage, Decis. Support Syst. 61 (2014) 69.

[38] N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.-K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. 3 (2016) 50.
[39] N.H. Ab Rahman, N.D.W. Cahyani, K.-K.R. Choo, Cloud incident handling and forensic-by-design: cloud storage as a case study, Concurr. Comput.: Pract. Exp. 29 (2017), e3868.
[40] B. Zawali, R.A. Ikuesan, V.R. Kebande, S. Furnell, et al., Realising a push button modality for video-based forensics, Infrastructures 6 (2021) 54.
[41] ISO/IEC, Iso/iec2700: Key international standard for information security, ISO.org 1, 1 2018.
[42] G. Horsman, Tool testing and reliability issues in the field of digital forensics, Digit. Investig. 28 (2019) 163.