Received July 31, 2020, accepted August 5, 2020, date of publication August 17, 2020, date of current version August 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016937

Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges

TEKLAY GEBREMICHAEL[1], LEHLOGONOLO P. I. LEDWABA[2], (Graduate Student Member, IEEE), MOHAMED H. ELDEFRAWY[3], GERHARD P. HANCKE[2], (Senior Member, IEEE), NUNO PEREIRA[4], (Member, IEEE), MIKAEL GIDLUND[1], (Senior Member, IEEE), AND JOHAN AKERBERG[5], (Senior Member, IEEE)

[1]Department of Information Systems and Technologies, Mid Sweden University, 852 30 Sundsvall, Sweden
[2]Department of Computer Science, City University of Hong Kong, Hong Kong
[3]School of Information Technology, Halmstad University, 301 18 Halmstad, Sweden
[4]Polytechnic Institute of Porto, 4200-465 Porto, Portugal
[5]ABB Corporate Research, 722 26 Västerås, Sweden

Corresponding author: Gerhard P. Hancke (gp.hancke@cityu.edu.hk)

This work was supported in part by the STINT Foundation under Grant IB2017-7022, and in part by the Partnership Research Program through the Industrial Technology Commission under Grant PRP/036/19FX.

ABSTRACT The Internet of Things (IoT) is rapidly becoming an integral component of the industrial market in areas such as automation and analytics, giving rise to what is termed as the Industrial IoT (IIoT). The IIoT promises innovative business models in various industrial domains by providing ubiquitous connectivity, efficient data analytics tools, and better decision support systems for a better market competitiveness. However, IIoT deployments are vulnerable to a variety of security threats at various levels of the connectivity and communications infrastructure. The complex nature of the IIoT infrastructure means that availability, confidentiality and integrity are difficult to guarantee, leading to a potential distrust in the network operations and concerns of loss of critical infrastructure, compromised safety of network end-users and privacy breaches on sensitive information. This work attempts to look at the requirements currently specified for a secure IIoT ecosystem in industry standards, such as Industrial Internet Consortium (IIC) and OpenFog Consortium, and to what extent current IIoT connectivity protocols and platforms hold up to the standards with regard to security and privacy. The paper also discusses possible future research directions to enhance the security, privacy and safety of the IIoT.

INDEX TERMS Industrial Internet of Things, IIoT, industrial networks, security and privacy.

I. INTRODUCTION

The adoption of the Internet of Things (IoT) technologies in industrial domains – termed as the Industrial IoT (IIoT) [1] – is enabling businesses to gain a competitive edge by enabling smart manufacturing, better decision making and data analytics [2]. The IIoT is mostly used to monitor and control critical infrastructures that are potentially exposed to various kinds of attacks [3]. Fig. 1 shows various Industrial IoT applications, covering, smart cities, healthcare industry, intelligent transportation system, and device-to-device communication. In order to maintain a safe and reliable operation, it is important that proper security and privacy-ensuring mechanisms are put in place [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

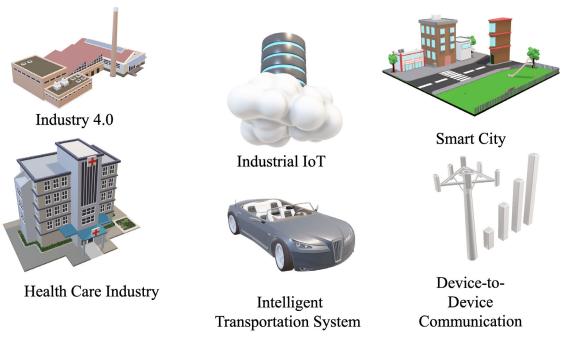

FIGURE 1. Overview of the industrial IoT applications [5].

The IIoT is characterized by stringent deadline requirements and operations with serious safety and/or economic loss implications in the event of a security breach. Even

though the type of security attacks that could be targeted against the IIoT are similar to those targeted against consumer IoT in nature, there is a difference in the degree of severity when an attack is successful. For example, whereas authenticating an illegitimate device to a consumer IoT network may cause some damage such as invasion of privacy or data theft, a similar attack on a typical IIoT could cause a huge disaster, such as disrupting the network, or forcing the network to take a hazardous action. As a result, the IIoT requires a higher-grade security mechanism that takes into account deadline requirements, nature of devices in the network, recovery mechanism in the event of an attack, and similar factors [6]. Privacy in the IIoT is made even more tricky due to the fact that data storage and processing is typically delegated to third-party cloud services, opening another attack dimension [7], [8].

A variety of industry standards and frameworks for device production, communication protocols, and security services and solutions have been proposed which detail mechanisms on how to best integrate the IIoT into industrial processes with strict safety guidelines. This work attempts to present an overview of the status of security and privacy within IIoT communications architectures with regards to industry framework requirements and current connectivity technologies. The work focuses on the current state of IIoT security from an industry perspective, and is not intended to be an overview of academic research in this area, or cover all possible security solutions for IIoT.

Summary of our contributions:

- We provide a taxonomic overview of the IIoT infrastructure; present standards for security requirements; and analyze relevant security protocols at various layers with regards to the said standards.
- We discuss how secure connectivity can be achieved in the IIoT by outlining a holistic picture of the IIoT, analysing how various protocols communicate with each other; what security vulnerabilities could potentially arise at various points; and what needs to be done to address such vulnerabilities.
- We outline research directions to address research gaps that we have identified.

The paper is organized as follows: Section II presents a taxonomic overview of the IIoT. Section III discusses the current state of various security protocols in the IIoT. Section IV discusses secure connectivity in the IIoT in the light of industry standards. Section V discusses privacy in the IIoT. Section VI discusses open problems and research directions. Section VII concludes the paper.

II. A TAXONOMIC OVERVIEW OF THE IIoT AND SECURITY REQUIREMENTS

We start our discussion by first providing a three-tiered architecture of the IIoT that we believe would capture the main components of most IIoT deployments (see Fig. 2).

The edge tier consists of end-points and edge-based gateway devices all making up a proximity-based network, which connects sensor devices, actuators and control systems together. The gateway devices provide a clustering point for the network, enabling bridged communications to the other network tiers. Connecting the edge tier to the platform tier is an access network. The access network is intended for data and control flow between the edge and platform tiers and may be implemented as an internet-based or mobile-network connectivity.

The platform tier contains service-based applications and middle-ware such as those used for network analytics and data transformation. This tier is connected to the tier above it by the service network. The service network allows for connectivity between the platform and enterprise tiers in the network and is typically Internet-based. The enterprise tier is used to host domain-based applications with business rules. It is also at this level that end users are able to interact with the network through specially designed interfaces.

Next we give a brief discussion of security requirements at each layer from two standardization bodies: Industrial Internet Consortium and OpenFog Consortium.

A. INDUSTRIAL INTERNET CONSORTIUM

The Industrial Internet Consortium (IIC) reference architecture provides detailed insight into the roles that cyber-physical technologies play at various tiers of the IIoT. Technology deployed at the network edge are classified under the functional view-point while bridging connectivity technologies form part of the implementation and information view-points. The implementation view-point gives the architectural patterns for the IIoT which describe network layouts and how information is transported in the network.

It can be seen from Fig. 2 that security services are required through all tiers of the architecture, from edge through to enterprise. This means data travelling though the various tiers also need to be secured continuously against malicious attacks and eavesdropping. According to the IIC's best practise recommendations, an IIoT network should be able to [11]:

- Support authentication protocols providing non-repudiation at endpoint levels
- Allow cryptographically protected edge-to-cloud connectivity
- Allow cryptographically protected endpoint-to endpoint connectivity
- Provide trusted data transport with the use of quantum resistant cipher suites
- Use hardware security modules for secure key store
- Provide interoperability across multi-vendor systems
- Complete transport and connectivity protocol suite support

The IIC security framework expands upon the requirements defined within the reference architecture. As part of a security risk assessment on the communications and

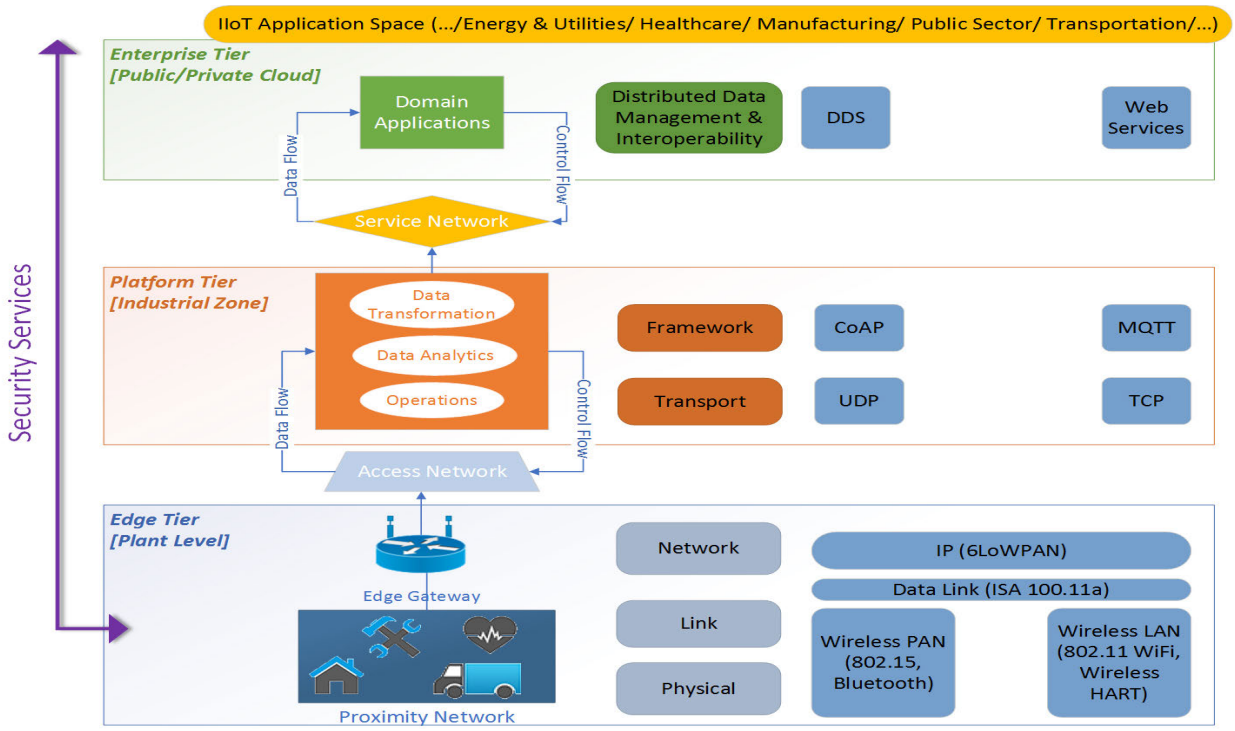

FIGURE 2. Three-tier architecture of IIoT connectivity and communications standards [9], [10].

connectivity infrastructure, network owners should consider the physical security of the connections, the protection of the communications infrastructure, information flow and cryptographic protection, the monitoring and analysis of the network communications, the configuration and management of the network communications and the development of security policies regarding communications and connectivity protection in the IIoT network [9], [10]. As part of guaranteeing these protections mechanisms such as authorization techniques, intrusion detection mechanisms, capacity planning, load-balancing and caching could be employed within the various tiers [10].

B. OpenFog CONSORTIUM

As a mechanism of bringing processing capability closer to the edge, fog-based IIoT networks introduce additional endpoint devices with larger processing and memory resources. Fog nodes often provide proxy and aggregation services to cloud servers on behalf of front-end devices [12]. As fog nodes may also be vulnerable to various IIoT security attacks, security mechanisms such as firewalls, secure remote access, anomaly detection and intrusion prevention systems are necessary to ensure the continued availability, integrity and confidentiality of an industrial network [12].

The Openfog Consortium's architecture defines three layers, i.e., communications, services and applications security, and two operational planes, i.e, security provisioning and monitoring and management, at which connectivity security is required to be able to guarantee secure end-to-end communications. This architecture design aids in establishing interoperability between security solutions designed for the fog and security solutions designed for the general IIoT communications networks as the same device capabilities and connectivity protocols can be considered at each level of the provisioning architecture [12].

The communication security layer is used to govern the communications that are established between entities forming the Device-Fog-Cloud network hierarchy [12]. As part of the requirements, data and traffic flow confidentiality, integrity with recovery and detection, anti-replay protection, data origin and peer entity authentication and access control should be provided between node-to-cloud communication, node-to-node communication and node-to-endpoint communication. Non-repudiation of origins and destination may also be provided as an optional security service. Table 1 provides a condensed list of implementation requirements needed for secure communication at the communication security layer. The diversity in device communication protocols makes it more difficult to establish effective standards for node-to-device connectivity security across industry although adaptation of Internet protocol suites such as TCP, UDP and IP is slowly growing for wireless communications. All the security services defined previously, excluding non-repudiation, may be implemented over wired or wireless communication infrastructures through the use of well-established security protocols. Endpoint devices establish authentication using security credentials issued to the device at the inception of the

TABLE 1. Summary of the OpenFog consortium security services and implementation requirements for IIoT connectivity and communications.

Security services	Implementation requirements		
	Node-to-Cloud	Node-to-Node	Node-to-Endpoint
Authentication	HRoT security credentials	HRoT security credentials	Device-allocated security credentials
Non-repudiation	HRoT security credentials	HRoT security credentials	X
Data confidentiality	Cryptography	Cryptography	Cryptography
Traffic flow confidentiality	Cryptography	Cryptography	Cryptography
Access control	Service provider security policy	Fog manager security policy	Fog provider security policy
Data encryption	HW accelerators	HW accelerators	Crypto-enabled embedded processor
Communications protocols	SOAP, COAP with WSS, TLS or DTLS	SOAP, COAP with WSS, TLS or DTLS(client-server); MQTT, AMQP or RTPS with TLS or DTLS (publish-subscribe)	IEEE 802.15, 802.11, 6LowPAN, WiFi, Bluetooth, Zigbee, COAP, IPv6 TCP, UDP, IEEE 802.1AR, 802,1AE, 802.1X, IPsec and DTLS

IIoT network while access control is established according to the security policies defined by fog service providers. The crypto-enabled embedded processors used by the endpoint devices are to be used to provide cryptographic operations while cryptographic key management is once again delegated to the monitoring and management operational plane. On devices with stricter resource constraints, manually installed keys are to be used in addition to symmetric cipher algorithms. However, such nodes must be installed in physically protected environments and connected through wired connections to fog nodes that are able to provide the larger suite of security services. A wide range of communications protocols, across multiple protocol stack layers, need to be supported to ensure interoperability between nodes and endpoints. Some of these protocols include IEEE 802.15, 802.11 and 6LowPAN for WLAN and WPAN structures; WiFi, Bluetooth and Zigbee for the wireless; COAP for publish-subscribe communications; IPv6, TCP and UDP for network layer communications; and LISP for routing [12]. For security, some protocols include IEEE 802.1AR, 802.1AE, 802.1X, IPsec and DTLS. A complete list of protocols requiring support for node-to-endpoint communications is given in [12], [13].

III. CURRENT SECURITY IN IIoT TECHNOLOGY

In Sect. II, we discussed a tiered-architecture of the IIoT and various security requirements at each tier. In this section, we present the state of security protocols deployed at each tier, highlighting important security aspects.

A. IIoT EDGE CONNECTIVITY PROTOCOLS

A large number of connectivity protocols are available to provide secure communication throughout the IIoT. Looking at the IIoT network edge, wireless technologies are highly favoured, with the most popular protocols establishing wireless PAN or wireless LAN networks.

1) BLUETOOTH [IEEE 802.15.1] (WPAN)

Bluetooth was developed as a low power communication protocol for short range (1m to 100m) communication, operating within the 2.4GHz frequency band [14]. Depending on the class of devices, various connectivity ranges could be achieved [14]. In its native state, Bluetooth provides four access security modes, with mode 1 being insecure, mode 2 enforcing service level security, mode 3 enforcing link level security and mode 4 enforcing service level security with encrypted key exchange [14]. Modes 1 and 3 do not provide specifications of security services that were required in implementation, exposing the protocol and devices to a large number of security threats such as malware, denial of service, sniffing and surveillance, while mode 2 specified basic services such as authentication, confidentiality and authorisation [14]. Mode 4 gave the most thorough security service definitions with hashing being provided by SHA256, AES-CCM being used for encryption and secure simple pairing being used for key generation [14]. From Bluetooth 2.1 beyond, mode 4 was made mandatory for any Bluetooth communications and connections [14].

A variant of Bluetooth, called Bluetooth Low Energy or BLE, was developed as a cost and power consumption reduction protocol for Bluetooth transceivers while still providing connectivity ranges equivalent to classic Bluetooth [15]. The low power, low rate wireless transmission can achieve ranges between 10m to 1000m depending on the network configuration and the operational environment. Transmission power consumption is set to a maximum 20dBm (100mW) [15]. One restriction seen in BLE is that a device may only connect to one central device at a time as a result of the ad hoc communication topology [15]. This is not the most ideal for IIoT connectivity where an edge node is required to have connectivity relationships with and broadcast messages to multiple fog and gateway nodes for forwarding through the communication infrastructure.

BLE adds to classic Bluetooth security services to address privacy, authenticity and integrity of endpoint data. Within the link layer, AES128 is implemented for encryption of over-the-air data transmissions. If AES is not supported, data integrity and authenticity are guaranteed using an AES128-based CMAC [15]. To allow for privacy, BLE devices may change their addresses frequently to achieve pseudo-identity anonymity outside of trusted peer devices. A pairing process allows for the optional creation of trusted relationships between devices during which identity information and cryptographic keys are exchanged to allow for future communication autonomously.

2) ZIGBEE 802.15.4 (WPAN)

A standard of the Zigbee Alliance, the Zigbee connectivity protocol is the most common enhancement of IEEE 802.15.4 in the IoT, WSN and IIoT space [16]. Zigbee offers two networking standards – Zigbee Pro and Zigbee RF4CE- at network level with varying service offers depending on the requirements of the network application. Additional features such as node authentication, and cryptographic services for communications security are implemented on top of the base 802.15.4 standard from the network layer up to the enterprise tier with some Zigbee versions providing support for energy harvesting to extend the functional energy lifetime of Zigbee nodes [16].

Zigbee RF4CE is designed to provide simple, low-cost wireless networks for consumer electronics devices [17]. The RF4CE protocol protects against passive eavesdropping and message tampering by employing cryptographic transmission security [17]. Security services such as data confidentiality, authenticity and replay protection are included as part of the protocol definition with 128-bit cryptographic keys being generated during pairing operations and stored in secured pairing tables [17].

Zigbee PRO is designed to provide network connectivity and interoperability to IoT implementations utilising Zigbee compatible edge devices and is subsequently implemented on both the network and application layers of the OSI protocol stack [18]. Low processing power is provided for applications requiring low power connectivity and support for large networks is guaranteed through the use of 802.15.4 radios. Security in the PRO network depends on the ability to safeguard symmetric keys, how protection mechanisms and cryptographic operations are employed and the development of adequate security policies [18]. Secure key generation and AES128 for transmission encryption for some of the security mechanisms which can be used as part of the secure network configurations detailed during the drafting of the security policy [18].

3) IEEE 802.15.4 (WPAN)

IEEE 802.15.4 provides various protocol sub-variants for meeting various application requirements although all use the base 802.15.4a/b technology and protocol [16]. The goal of the 802.15.4 standard is to provide a basic communication, which other protocols and technologies are capable of implementing within the upper layers of their protocol stacks [16].

802.15.4 provides numerous security techniques at the MAC layer. Data integrity and confidentiality are provided within the protocol description using AES128 and AES128-based message authentication codes (MAC) which may be generated as 32, 64 or 128 bit long codes [19]. The standard uses 128-bit keys that can be shared with the two partners in the communication channel. Some of the essential security factors provided at the MAC layer include:

- Confidentiality: As secrecy is an optional issue in the IEEE 802.15.4 standard, applications that need confidentiality for the exchanged data can use an AES encryption with 128-bit keys in the Counter (CTR) mode.
- Access control, Integrity, and Authenticity: Authentic and integrity applications can be achieved with the utilization of one of the security modes that adopts AES with the Cipher Block Chaining (CBC) approach to harvest a Message Integrity Code (MIC) or Message Authentication Code (MAC) concatenated to the exchanged data. The dual modes of CTR and CBC can be achieved using the encryption of CBC-MAC AES/CCM with a combined Counter to assure confidentiality, authenticity and integrity for the data link-layer
- Replay attack prevention: In a communications exchange, as long as a legitimate entity creates the message, it will concatenate with a correct MAC, which in turn will allow the destination to accept it. To prevent this kind of attack, the sender assigns a counter to each message to help the receiver reject packets with late order numbers.

One of the main challenges with 802.15.4 is in the establishment of an appropriate keying approach in order to prevent malicious attacks. The authors of [20] showed that the single shared session key approach cannot promise a defence from replay attacks in addition to the fact that the pairwise keying approach is not strongly supported. Moreover, they illustrated a scenario of a single-packet DoS attack over the AES-CTR approach. They also demonstrated that the IEEE 802.15.4 standard could not ensure confidentiality/integrity for acknowledgement packets.

4) NB-IoT (WWAN)

3GPP specified Narrowband IoT (NB-IoT), which is dedicated for low power and low data rate services that need good coverage and adaptable implementation. NB-IoT is based on LTE, which makes it compatible with the current LTE systems that utilize the advantages of the 4G network, such as long-range connectivity. In addition, NB-IoT offers end-to-end security, which leads to authentic and secure communications [21]. The NB-IoT efforts were launched by offering different proposals by several cellular vendors [22]. NB-IoT has three modes of operation [22];

- Standalone mode: A NB-IoT carrier is achieved over a GSM carrier by reusing the 900 MHz or 1800 MHz.
- In-band mode: Segment of an LTE carrier frequency band is assigned as a NB-IoT carrier. The service provider assigns this allocation then the IoT devices are adjusted correspondingly. Having several and dissimilar service providers without coordination can led to unmatching frequency distributions.
- Guard band mode: A NB-IoT carrier is fixed between the LTE or WCDMA bands, which in turn, requires synchronicity between LTE and NB-IoT frequency bands.

On the other hand, however, the fully open access nature of unlicensed bands generates security issues. Some malicious nodes can launch traffic offloading on unlicensed bands

to engender secrecy-outage for the corresponding IoT networks [23].

5) WirelessHART(WLAN)

Unlike the other protocols already considered, which all establish personal area networks, WirelessHART provides a local area network especially designed for industrial process control applications [24]. Proposed as an extension of the HART protocol and compatible with existing wired HART devices, WirelessHART allows a mesh topology to be used in industrial contexts and allows devices at the network edge to perform routing on data packets originating from neighbour devices through to gateway or fog devices [24]. Built upon IEEE 802.15.4, the protocol provides a platform for integrating wired devices in the industrial process into the wireless communications exchanged frequently within the IIoT [24].

To establish security within a HART network, information confidentiality and integrity, device authentication and information availability must be guaranteed. WirelessHART provides information integrity from mechanisms inherited from the 802.15.4 protocol [25]. Additionally, message integrity codes (MIC) and AES128 encryption are incorporated into the WirelessHART protocol to provide authentication and verification of layer information through the use of network and session keys [25]. Connectivity availability is threatened by interference with other wireless communication protocols although it has already been seen that WirelessHART employs multiple mechanisms to ensure coexistence within the frequency band with other network communications [25].

Two additional connectivity protocols may be used at the edge tier of the IIoT, operating at the link and network layers.

6) LoRaWAN(WWAN)

LoRaWAN is a higher layer protocol of LoRA that identifies the configuration and process of the complete edge system to transfer data to the Network Server (NS) over the Internet protocol [26]. LoRaWAN assures information secrecy by adopting AES128 [27] for encryption/decryption processes, MAC operations for data integrity and Over-The-Air-Activation (OTAA) to present the common ED authentication method.

Various security issues were discovered in LoRaWAN v1.0, [28], some of which were recovered in v1.1 [26]. Both LoRaWAN v1.0 or LoRaWAN v1.1 were shown to be vulnerable to complex jamming attacks, such as a selective-jamming attack in [29], as a result of wireless communication. Some remaining security vulnerabilities in LoRaWAN v1.1 were identified by the authors in [26] as:

- Cryptographic Primitives: Earlier researchers have showed some major flaws in AES using electronic codebook (ECB) mode [30], which is used to encrypt the join-accept message of LoRaWAN v1.1.
- Key Preloading: The key-control property assures that no partner in the network can fix the shared key to a predefined value with the intent to stop one party from having control over the other party [31]. The preloading process of the network and application keys in LoRaWAN v1.1 (NwkKey and AppKey) into the ED interrupts this anticipated feature.
- Infrastructure Trust: [32] illustrated some weaknesses of LoRaWAN v1.0 such as the bit-flipping attack, in which an adversary can change the content of a message over the connection between the network server and the application server. This attack is still applicable for v1.1 as declared in [27].
- Roaming: Roaming presents one of the main challenges for LoRaWAN v1.1. owing to the fact that it is vulnerable to bit-flipping attacks. The handover/roaming in v1.1 also creates more difficulties as it increases the risks for MITM attacks [33].

7) ISA100.11a (DATA LINK)

In September 2009, the International Society of Automation (ISA) introduced the industrial automation wireless system ISA100.11a [34]. ISA100.11a tries to achieve secure and reliable wireless communication for supervisory control applications and operates as a bridge between link and network layer protocols. In a similar way to WirelessHART, ISA100.11a uses AES symmetric encryption with a 128-bit key in the counter mode over a Cipher Block Chaining-Message Authentication Code (CBC-MAC). ISA100.11a can provide more direct connections in a peer-to-peer fashion than WirelessHART. The Security Manager in ISA100.11a has more precise roles than its peer in the WirelessHART; it includes device authorization for the joining phase as well as the key management process that includes re-keying, key archiving and key recovery. Dissimilar to WirelessHART, asymmetric keys is adopted for the joining phase in ISA100.11a. A similar WirelessHART end-to-end encryption is delivered at the Transport Layer. In 2014 new procedures have been introduced to improve ISA100.11a security in terms of sniffing, data falsification, spoofing, and replay attacks [35].

8) 6LoWPAN (NETWORK LAYER)

Some IIoT networks are being interconnected to the Internet using IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [36], [37], which defines IP communication for resource-constrained networks. IPSEC [38] is used to provide security services at the network level in the conventional Internet. The heavyweight and complex nature of IPSEC means that it is not feasible for deployment in IIoT environments. In [39], a mechanism has been proposed to integrate IPSEC to (Industrial) IoT networks by extending the original implementation in such a way that it is feasible for tiny devices. This research direction is appealing because it is in keeping with the standard recommendation that it is advisable to extend a well studied security solution rather than invent a new one. Moreover, the authors of [39] demonstrate that IPSEC customized for IoT scales better than link layer solutions as the size of data and number of hops increases. IPSEC in IIoT also makes it possible for the provision of End-to-End (E2E) encryption [40] which is not otherwise

possible using traditional 802.15.4 link-layer security mechanisms.

TABLE 2. Summary of wireless standard connectivity technologies for the IIoT edge network.

Protocol	Channel Bandwidth (MHz)	Power (mW)	Trans. Range (m)	Provided Security Services
Bluetooth Classic [IEEE 802.15.1]	2	1 [C3], 2.5 [C2], 100 [C1]	1-100	Hashing, data trans. encrypt. and pairing for secure key gen.
BLE	2	100	10-1000	Data trans. encryption, CMAC, pseudo identity anonymity, trusted pairings
Zigbee	5	Vary	10-100	Node authent. comms crypto, symmetric key gen.
IEEE 802.15.4	5	1	10-75	Data integrity using MAC, Data trans. encryption
Wireless HART	5	Vary	200	Authent. keys, message integrity codes, connectivity availability, data trans.encryption
ISA100.11a [41]	5	10	600	AES128 (CTR/CBC-MAC), Security manager, device authorisation, key management, asymmetric keys
LoRaWAN [42]	0.125-0.500	25	10^3 – 2×10^4	AES-128 encryption/symmetric key generation
SigFox [42]	10^{-4}	25	10^4 – 4×10^4	No encryption
NB-IoT [43]	0.2	200	10^3 – 10^4	LTE encryption

Table 2 depicts the differences and similarities present in the IIoT connectivity protocols. In all the analysed connectivity protocols, it can be seen that some form of security services has been provided as a part of the design specification. All the protocols analysed are capable of transmission within the 2.4 GHz band making anti-collision and interference protection an important consideration for the resulting IIoT network design in order to be able to sustain the availability of device transmissions. However, this also means that inter-device communication, and interoperability, are better achieved without requiring the introduction of frequency modulation to transform the transmissions into a common band. The direct relationship between the power consumption of transceivers and the achievable range of the protocol means that a detailed analysis will need to be made regarding the network design of the IIoT deployment. As the topology supported by the protocol also has an affect on the extensible transmission range; when selecting a connectivity protocol for use, the number of devices, the distance between them, the ability to extend that distance and the tolerable power consumption of the network must be given due consideration in order to be able to achieve an acceptable trade-off between cost and the effective operation of the network.

B. IIoT PLATFORM CONNECTIVITY PROTOCOLS

As with the edge tier, platform connectivity protocols are available to provide communications between enterprise tier applications, edger tier gateways and middle-ware solutions.

1) CoAP

In the conventional Internet (TLS) [44] is used to provide security services such as confidentiality and integrity to application-level protocols such as HTTP. CoAP [36], which is a stripped-down version of the HTTP protocol for IoT devices running on top of the UDP protocol, relies on DTLS [45] to provide security services. This version is termed secure CoAP (CoAPs).While DTLS supports a wide range of cryptographic primitives, it was originally designed for network environments where message length was not an issue. As a consequence, deploying native DTLS in IIoT environments presents two challenges [46]. First, a big message payload results in data fragmentation, forcing IIoT devices to handle the overhead associated with fragmentation and reassembling of data. Second, fragmentation opens up new possibilities for fragmentation related attacks [47].

Efforts are being made to develop a lightweight version of CoAPs by compressing the underlying DTLS protocol using 6LoWPAN header compression mechanisms [46]. Given that CoAP is projected to become ubiquitous in many IIoT enviornments [48], there is a need for making CoAPs suitable for various IIoT network contexts including those that do not rely on 6LoWPAN. A comprehensive analysis of various CoAP implementations for IIoT is presented in [49].

2) MQTT

MQTT is a publish/subscribe [50] based communication protocol that is fast becoming a standard in various IIoT applications due to it being lightweight. MQTT enables devices to exchange data by relying on an entity called a broker to which devices publish data, and from which devices retrieve data.

In the original design of MQTT, security was left to other protocols such as SSL/TLS. However, due to the inherent complexities involved in these protocols, they are not ideal for deployment in IIoT applications enabled by small devices. To remedy this, there has been efforts to design lightweight security protocols to augment the raw MQTT protocol. In [51], a secure version of MQTT, termed SMQTT, has been proposed that is based on the Attribute Based Encryption (ABE) mechanism [35]. In addition to SMQTT being lightweight owing to the fact that it is underpinned by lightweight elliptic curve based crytpo system, the ABE mechanism allows it to effect broadcast encryption - a desirable property in resource-constrained IIoT environments since broadcast reduces traffic and processing time at the sender's end. Problems such as key revocation, key renewal, and group publish/subscribe without a trust anchor remain unresolved. To the best knowledge of the authors, there are no other lightweight security solutions that attempt to address the various security aspects of MQTT, ranging from device

authentication to distributed trust on MQTT based applications.

IV. SECURE CONNECTIVITY IN THE IIoT

Secure communication in the IIoT requires a myriad of security protocols, hardware, and other components to work in harmony. The requirements for secure connectivity, as defined by the IIC and the OpenFog Consortium, show many similarities that allow for the two standards to be used as complementary documentation towards the development of a secure connectivity strategy for the IIoT. A high degree of overlap occurs in both the requirements and implementation technologies. This is summarised in Table 3. The use of similar or exact technologies to guarantee security services for edge devices [52] and connectivity security aid in highlighting connectivity security as an extension of edge device security and supports the need to guarantee strong edge device security from the inception of an IIoT network. The extension of these implementing technologies also allows for load sharing of the security requirements between the two network areas while building in redundancies that could serve as backup protections in the event of a security breach.

A. AUTHENTICATION

The IIC and OpenFog Consortium frameworks recommend establishing a root of trust from which credentials for authentication, non-repudiation and integrity checking can be derived. The root of trust is to establish initial confidence within the system operations, which then further supports the establishment of confidence in knowing that entities requesting network access are both authorised to access network resources and that they cannot access resources for which they do not have access permission [10]. The root of trust also aids with establishing network integrity by providing a baseline for identifying and preventing unauthorised access attempts [10]. Authentication mechanisms based on physical proximity of entities have also been proposed for the IIoT [53].

To create a secure network root of trust, the security framework recommends the use of a hardware root of trust (HRoT) mechanism such as a hardware security module (HSM), and a Trusted Platform Module (TPM) [10]. HSMs are Systems on Chip (SoC) solutions that can be used to provide minimum cryptographic functions, such as encryption, decryption, key generation, digital signing, and hashing, along with providing physical tamper resistance and physical isolation of security and cryptographic functions [54]. Some areas of very active research include recent work developing tamper-resistant/tamper-evident hardware, FPGAs with encrypted bitstreams [55], physically unclonable functions [56] or hardware-based Trusted Computing Bases (TCBs) for low power embedded devices [57].

As was seen in edge device security, using hardware security chips as the sole security solution can serve to shorten the effective security lifetime of the secure network as standards groups continually work to update existing standards. As the chips are hard-soldered into edge nodes, they would be difficult to replace and with large network deployments, such an operation would be highly expensive and infeasible. Also, the selection of an appropriate physical security protection mechanism and chip-to-chip communication protocol becomes highly important as additional care would need to be taken to protect the communication paths between the MCU and the crypto accelerator to ensure that no security information is leaked.

B. ACCESS CONTROL

Access control machinery is necessary to safeguard the IIoT systems. Recently, researchers have recognized that access control needs to be tailored to the specificities of the IoT [58], [59]. For instance, Jafarnejad *et al.* [60] has revealed a platform based on the Open Vehicle Monitoring System (OVMS)[1] that can achieve illegal access to the internal network of an all-electric car. Moreover, according to [58], attackers were successful to get access to millions of IoT nodes and exploited them as botnet zombies to start a DDoS attack to DNS servers run by Dyn Inc [61], [62].

Techniques implementing access control, network segmentation and data and communications isolation in the IIoT remain largely academic, meaning they are subject to a wide variety of short comings that are to be handled as future work and overall lack consensus on a standard methodology with which to provide the security service for general network applications. A larger push needs to be made towards the development and verification of usable, commercial, standard solutions based research efforts already concluded. However, this requires increased collaboration across various fields in engineering and computer science along with increased collaborative development efforts between academia, private and public sectors.

CP-ABE-based [63] encryption mechanisms can also be used to enforce access control rules. By grouping and configuring devices in various access groups, data can be encrypted in a such a way that only a device with a specified access right can decrypt it. These kinds of schemes help one achieve different objectives in simultaneously, in this case confidentiality and enforcing access control.

C. IDENTITY MANAGEMENT

Identity management solutions are required in order to deal with the problem of naming, addressing and discovery of IIoT devices. Identity management in IIoT assumes an elevated level of importance because a rogue device can force a system to take actions that are hazardous. Identity management is a multi-faceted problem that encompasses the following issues [64]:

- Having in place proper naming and addressing mechanisms
- Defining the identity of an entity
- Storing relevant information about entities

[1]OVMS website: http://www.openvehicles.com/

- Defining interfaces to access entities
- Defining roles and relationships among entities

One of the challenges with regards to naming and addressing is the sheer number of IIoT devices, which makes it hard or impossible to use conventional addressing and naming schemes such as IP and domain names. Other factors that potentially exacerbate the problem include managing mobility of devices and subsequent name or address changes, identity theft and having scalable device discovery mechanism [65]. There are many identity management solutions in the literature, such as OpenID [66] for identity management and Library Alliance [67] for trust management. Future identity management solutions need to solve problems related with managing identities of devices in proprietary networks, devising a naming and addressing mechanism that scales with the constantly growing number of devices, and a fast way of discovering devices to meet the often stringent timing requirement IIoT application demand.

Identity management solutions that are comprehensive in terms of being privacy-preserving, and encompassing related issues such as anonymity, zero-knowledge proofs and authentication have been proposed in [68]. Similar identity management solutions that are tailor-made for specific IIoT deployments and requirements would be desirable towards creating a more secure and privacy-preserving IIoT environment.

D. KEY MANAGEMENT

Secure key exchange and storage is a problem that manifests itself at various connectivity protocol layers in which cryptographic mechanisms are required to provide security services. This is made difficult given that devices in the IIoT are resource-constrained and that both data and devices are physically exposed to attackers. Key management solutions based on public cryptography are infeasible for the IIoT owing to the complex computations that are inherent to public key cryptography.

To tackle the problems related with the computationally limited nature of IIoT devices, key management solutions based on lightweight cryptography have been proposed. However, maintaining a certain security level and ensuring that key management primitives are computationally feasible for the smallest devices is difficult. The physical accessibility of devices also poses a new security challenge that is not common in the conventional Internet where computers are not physically reachable by an attacker. A key management scheme would need to include mechanisms to protect against tampering attacks and detection and recovery mechanism [69] for when such attacks succeed.

E. DATA FLOW CONFIDENTIALITY

The use of cryptography in connectivity architectures allows for the encryption of sensor data generated at and transmitted from the network edge. Cryptographic services for data and communications confidentiality may be implemented in either software or hardware with connectivity protocols already defining their support of specific crypto algorithms. As part of the requirements proposed by the OpenFog Consortium, devices and connectivity protocols that are intended for fog-enabled industrial internet networks need to be able to support a variety of open, vetted cryptographic algorithms [12], [70], [71]. Depending on the network tolerance for delay and the size constraints on the device, software, hardware acceleration or hybrid solutions may be used to provide cryptographic services.

F. DATA ISOLATION FOR IIoT COMMUNICATIONS

The use of isolation techniques can be used to shelter parts of the IIoT network to prevent the cascade of undesirable effects caused by a failure of some parts of the network [10]. Physical isolation techniques may also be used to provide security separately from operational devices by employing the use of a separate, security dedicated device. One such example, proposed within the IIC security framework, is a dedicated security gateway for communications security between legacy deployments and the wider IIoT network [10]. Isolation can be achieved through the use of the operating system to isolate business and operational processes from security processes (process isolation), or the use of boundaries as determined by hardware, software or a hybrid implementation (container isolation), or through a hypervisor configured to isolate each running instance on an endpoint device (virtual isolation) [10]. Isolation practices are implemented as part of solutions already highlighted. HSM provides physical isolation of security processes.

Currently, hyper-visor and container-based technologies remain mainly focused on securing traditional ICT technologies and operating systems. Solutions for the IIoT are slowly emerging with implementations focusing on the development of container technologies for IoT cloud services or Linux-based embedded operating systems designed to support gateway functions.

G. FILTERING AND ACCESS CONTROL IN THE IIoT

Three main models for access control have been proposed for the IIoT. In the centralised model, filtering operations are compared against the predefined security and authorisation policies with endpoint devices taking on the role of only being information providers [72]. In the hybrid approach, the centralised server accepts requests from end users, evaluates the current environment information provided from endpoint devices and makes the decision whether to allow or deny access; generating an authentication token for acceptances or rejection messages for refusals [72]. The main drawbacks of these models are the provision of a central point of failure, reduced efficiency, bottlenecks in the communications flow and the dependence on the timely arrival of contextual information from the endpoint devices to be able to make informed access right decisions [72]. The distributed approach to access control identifies endpoint devices as smart resources able to obtain, process and distribute access control information to other services and

devices [72]. Authorisation decisions are then based on the local area state information provided by collaborating neighbour nodes.

A popular distributed access control model is capability-based access control (CapBAC), which is based on the idea presented in [73] that a device presents a token or key that grants it permission for access to a resource or protected area [72]. To minimise the communication transactions needed during the authentication process, a requesting device attaches its token together with its request, detailing the permission rights allocated to the requesting device on reception by the receiver device [72]. While it presents as the most ideal solution for access control in the IIoT, CapBAC has several drawbacks. In its native implementation, CapBAC appears vulnerable to replay attacks of the device capability, does not fully solve the issues of containment of unauthorised information flows to restricted areas and resources specific access denial rules are not expressed and published to the wider network [74]. To solve this, Gong *et al.* [74] proposed a secure identity-based capability system (ICAP), in which access to a resource is granted only in events where the capability presented by a requesting device matches the token stored on an access management entity such as a fog node or gateway device [74]. However, the solution failed to define the security policy that is to be used for capability creation and propagation and failed to define what contextual information would be required for making access control decisions [75]. Another adaptation, proposed by Mahalle in [76], utilised public key cryptography to provide the device capability token to a capability based access control device which provides a verification interface for device tokens before allowing communications to be established between requested and receiver devices [76] however it too failed to adequately address the propagation and renovation of compromised capability access tokens and efficient network interoperability [75].

H. MANUFACTURER USAGE DESCRIPTION

One of the main standards that enforce behavioral security profiles is the Manufacturer Usage Description (MUD) model [77], which allows operators to particularize their devices' application to limit the attack surface of a particular system. MUD has been introduced as an Internet Engineering Task Force (IETF) model [78]. The MUD's primary goal is to restrict the attack surface of a particular machine by setting strategies or Access Control mechanisms to limit the interaction with other services or devices. Moreover, it is regarded as a promising technique to protect IoT networks against denial of service (DoS) attacks [77]. MUD is directed to the behavior of IoT devices with a particular or single purpose, as IoT devices usually interact by recognizable models [79]. Notably, the National Institute of Standards and Technology (NIST) acknowledged the MUD utilization to minimize IoT-based automated distributed threats [80].

I. SOFTWARE DEFINED NETWORKS AND NETWORK FUNCTION VIRTUALIZATION

The Software Defined Networks (SDN) and Network Function Virtualization (NFV) approaches provide organizational security features in the IoT systems [81]. NFV offers some benefits in delivering virtual appliances in the edge and remote cloud data centers [82]. Edge computing has close contact with sensors and actuators. The demand for cloud, fog, and edge computing architectures is enlarged with the evolution of the IIoT application [5]. Authentication, Access, and Authorization (AAA) are three factors required for the intended IIoT security. The demand for end-to-end communication in IIoT necessitates comprehensive data privacy as well [5]. SDN is needed to integrate the new virtualized services into the current structure to implement networking countermeasures to eliminate/reduce cyberattacks [81]. The SDN/NFV-based virtual AAA and virtual Channel-Protection solution for IoT networks presented in [81] offers a policy-aware approach to manage AAA and channel protection in SDN/NFV-enabled IoT networks. In which, the virtual AAA and Channel-Protection Network Security. Functions are dynamically operated at the edge to enhance the devices' bootstrapping and support the access control of IoT nodes to the network.

V. PRIVACY IN THE IIoT

IIoT applications are enabled by devices that generate, process and exchange vast amounts of data which, if not collected, processed and exchanged in a secure way, can compromise the user privacy required to maintain a competitive advantage. Ensuring privacy is a complex problem involving social, legal and technical challenges, e.g. Stankovic [83] discusses in detail why defining privacy policies and enforcing them is a difficult task in IoT in general. This section provides a brief overview of this area.

Privacy in IIoT generally has two aspects [84]: protecting data collected from unauthorized access and ensuring that the location of a sensor or actuator is kept secret, as exposing location information could be a security and safety risk. A wide variety of threats that could impact the secure operation of the IIoT network as a consequence of a lack of privacy preservation. Some of the threats identified by Seliem *et al* in [85] include: user identification, user tracking, profiling, utility monitoring and network control [85]. Ensuring privacy through the IIoT network requires consideration at various levels of the architecture. At the device layer, solutions providing access control, authentication mechanisms, data encryption and secure channels would be required to counter attacks that could compromise the privacy of the edge nodes such as side channel attacks, node capture, fake node insertion, replay or routing attacks [85]. Moving up towards the platform layer, more pre-processing operations are being handled making preventing attacks such as eavesdropping and MitM more significant towards ensuring continued privacy [85]. When considering the application layer, privacy

TABLE 3. Summary of connectivity and edge device security technologies.

Security services	IIC Security objectives			OpenFog implementation requirements			Available technologies [Edge and connectivity]
	A	I	C	Node-to-Cloud	Node-to-Node	Node-to-Endpoint	
Authentication		X	X	HRoT security credentials	HRoT security credentials	Device-allocated security credentials	software/hardware TPM
Non-repudiation		X		HRoT security credentials	HRoT security credentials	X	software/hardware TPM
Data confidentiality			X	Encryption	Encryption	Encryption	AES with at least 128-bit keys, 3DES, DH, RSA, DSA, ECDH, ECDSA, ECQV, SHA-2 to SHA-5, True RNG, CCM, GCM, GMAC, CMAC, HMAC
Traffic flow confidentiality			X	Encryption	Encryption	Encryption	See Data Confidentiality
Access control			X	Service provider security policy	Fog manager security policy	Fog provider security policy	CapBAC
Data encryption			X	HW accelerators	HW accelerators	Crypto-enabled embedded processor	See Data Confidentiality
Communications protocols	X	X	X	SOAP, COAP with WSS, TLS or DTLS	SOAP, COAP with WSS, TLS or DTLS(client-server); MQTT, AMQP or RTPS with TLS or DTLS (publish-subscribe)	IEEE 802.15, 802.11, 6LowPAN, WiFi, Bluetooth, Zigbee, COAP, IPv6 TCP, UDP, IEEE 802.1AR, 802,1AE, 802.1X, IPsec and DTLS	Bluetooth Classic [IEEE 802.15.1], BLE, Zigbee, IEEE 802.15.4, WirelessHART
Data isolation	X	X	X	Not covered within the OpenFog framework			Hardware isolation, TEE, process, container isolation, hypervisor
Segmentation	X	X	X	Not covered within the OpenFog framework			Firewalls, intrusion detection, autonomous segmentation based on zero trust

preservation will start requiring the inclusion of non-technical solutions such as thorough end user training and implementation of security management policies to reduce the risk that human interactions and interventions open new entryways in the security attack space for malicious attackers [85].

Given the multi-faceted nature of privacy in IIoT, independent efforts to address privacy in IIoT fall short of providing a comprehensive solution to all privacy issues that may potentially arise. Privacy preserving, computational models, such as (fully) homomorphic encryption [86], are generally good in theory, however they are currently not mature technologies [87]. Privacy enhancing techniques such as differential privacy [84] and local differential privacy [88] are considered as alternatives towards achieving location privacy; with privacy preserving data aggregation mechanisms, seen in smart grid applications, proposed in [89]. For hop-to-hop, physical layer privacy, standard solutions are to employ end-to-end encryption (E2E) mechanisms however, this is challenging to implement in the IIoT [90]. Blockchain-enabled IIoT [91], data anonymisation [92], content-oriented protection [93], privacy frameworks [94], [95] and distributed data privacy protections [96] are also being considered as potential solutions towards IIoT privacy preservation.

Maintaining privacy in the IIoT is made more challenging when data is stored and processed in a cloud service owned by third parties. A mechanism is required to ensure that the data in the hands of a third party is processed in such a manner that it does not compromise the privacy of the entity that owns the data [97]. The authors of [98] propose a privacy-preserving mechanism for an IIoT application to outsource computations to a cloud source provider. Privacy enhancing messaging protocols such as XMPP could be potential alternatives if they could be optimized for resource-constrained devices.

Solutions designed towards maintaining privacy in the IIoT domain need to consider various application domain and end user requirements going forward; including those highlighted in RFC7452 [99], which proposes the various architectural considerations that are required as part of smart object networking. As such, when designing privacy solutions for the IIoT, developers would need to focus on:

- Identifying business processes and operations which need to operate in a privacy-preserving manner. Following this, privacy policy statements need to be stated in a manner that is clear to understand and practically enforceable. This problem is complex in general, and it is even more complex in the IIoT due to fact that data is required to travel through sub-systems made up of heterogeneous software and hardware, sometimes owned by third-parties as in the case of cloud storage that the owner of the data cannot control. In such cases, inconsistencies in privacy policy might arise. Therefore, it is important that there is a mechanism in place for resolving such inconsistencies.

- Cryptographic mechanisms are generally employed to enforce privacy policies. The challenge is designing a privacy-enhancing crypto-system that is not computationally heavy to resource-constrained nodes in the IIoT network. Heavy-weight crypto in the IIoT could slow down computations resulting in processes not meeting strict deadline requirements. Non-crypto based privacy-enhancing solutions such as anonymizing data, developing data analyses tools that deal with aggregate data should be further explored.
- Delegating big-data processing tasks to a third-party cloud service provides an opportunity for fast and efficient data processing services but also presents a challenge with regards to privacy. Ensuring that data is processed by a third-party cloud service without it learning privacy-sensitive information is a critical privacy problem that many IIoT businesses must deal with.
- Ensuring transparency regarding the data collection, handling and processing operations of the network would need to be afforded to end users such that they are aware of the associated risks and the mechanisms that would be in place to mitigate them, the data which may be collected and for what purpose this data would be used in the network operations. This transparency would afford for additional accountability for network operations and would assist towards complying with international data protection laws [99].
- Limiting the amount of data collected by edge devices to the minimum data points that are required and relevant for network operations while continuing to employ anonymisation techniques on personally identifiable information as much as is feasible [99].
- Developing clear data access policies and implementing appropriate access control measures capable of defining to whom edge node data is accessible and under which pre-existing conditions such data access may occur [99].

VI. RESEARCH DIRECTIONS

The research required to address the challenges discussed so far is multi-faceted. In some respects, the IIoT is similar to the general IoT, and research problems in the IoT such as designing secure crypto-systems tailored towards resource-constrained devices; putting in place a mechanism for secure and reliable operation in the face of failures and successful attacks; and designing secure data analytics mechanisms are important in the IIoT as well. However, the IIoT is intended to support industrial systems, which rely on time-sensitive information, e.g., real-time sensor data and control commands, so any security mechanism would need to provide security services while also ensuring the continues timeliness of data communication.

Given the sheer size of the data most IIoT systems rely on, it is sensible to store data in a third-party data storage system. This raises an immediate concern regarding the confidentiality of the data in the hands of a third party, and with regard to maintaining privacy to keep important business assets away from competitors. Homomorphic encryption and searchable encryption mechanism has emerged as potential solutions to these problems, but further research needs to be done with regard to scaling, fast and secure delivery of data from the cloud in time-critical applications, and reliable recovery mechanisms when the data in third-party storage systems is compromised.

From a cryptographic perspective, another important research area is designing secure quantum-safe crypto-systems commensurate with resource-constrained devices. This is a concern about which different researchers have different views regarding priority and whether it is something researchers should invest their effort in [100]. We believe that given the enormous importance of the IIoT, and given the benefits of public-key cryptography in managing key material for a large amount of devices, that it is important that quantum-safe security mechanisms suitable for the IIoT are developed.

Another research challenge relates to the heterogeneous nature of the hardware and software employed in many IIoT deployments. Ensuring that required security services are guaranteed as data travels across multiple layers and a disparate set of hardware and software is a challenge. This is specially critical in contexts where end-to-end encryption needs to be provided as data travels across multiple hardware from various vendors, and with disparate software and implementations of security protocols.

For IIoT deployments where an attacker could physically tamper with a device, research into designing tamper-resistance hardware and maintaining operational safety in the face of such physical attacks needs to be considered. Designing a mechanism for detecting, and recovering from, device-capture-attacks [101] is an important problem in the IIoT where a successful attack on a single device (such as stealing a cryptographic key) could cause a huge damage to the whole network.

In safety-critical applications, implementing proper security and privacy mechanisms may not suffice. Certification authorities could demand that a proof that the system works as intended be presented. Demonstrating that an IIoT infrastructure meets a given set of security and safety requirements is a hard problem, as elaborated in [83], and further research needs to be done on how to show that a complex IIoT system provides a set of specific safety guarantees.

To enhance privacy, data collection and analytics should be done in a privacy-preserving manner. One way of achieving this is by anonymizing collected data. There could also arise a need for ascertaining the identities of devices by asking them to prove themselves without revealing anything. Therefore (pseudo)anonymization and and zero-knowledge proof techniques suitable for the IIoT should be studied and developed for the IIoT.

Finally, an important research direction concerns integrating the IIoT with other emerging technologies, such as 5G and blockchain technologies. There are some nascent efforts towards this end. In [102], how 5G can be employed for efficient management of energy in the IIoT has

been discussed. The authors of [103] have proposed how blockchain can be used for distributed data storage in the IIoT. We believe a more comprehensive framework and strategy for integrating the IIoT to other technologies is required. Such a framework would need to take into account the disparate nature of various IIoT deployments, specific requirement with regard to security, timeliness, scalability, compatibility and other similar factors [83].

VII. CONCLUSION

The IIoT is rapidly becoming an integral component in various industrial processes such as factories and safety-critical control applications. The IIoT is inherently complex, consisting of heterogeneous hardware and software, sub-systems interacting in complex ways, and stringent security, safety and privacy requirements. Guaranteeing security and privacy in the IIoT is hard in part because of the complexity of the systems and in part because it is hard to clearly specify security requirements and implement them in a manner that can be proved. The paper attempted to provide a holistic overview of security and privacy in the IIoT in relation to recommendations from well-known standardization bodies, so that researchers and practitioners alike could easily see where various security protocol at various layers fit in the bigger picture. A thorough analysis of various security protocols and solutions, with emphasis on pointing out security weaknesses and vulnerabilities has been provided. The paper also outlined possible directions for further research to bridge some of the security and privacy problems that the IIoT now faces. Finally, current research and implementation efforts that attempt to integrate the IIoT with emerging technologies like 5G have been pointed out, with suggestions for future work in that direction.

ACKNOWLEDGMENT

Any opinions, findings, conclusions or recommendations expressed in this material/event (or by members of the project team) do not reflect the views of the Government of the Hong Kong Special Administrative Region or the Innovation and Technology Commission.

REFERENCES

[1] D. Rawat, C. Brecher, H. Song, and S. Jeschke, *Industrial Internet of Things: Cybermanufacturing Systems*. Cham, Switzerland: Springer, 2017.

[2] S. Goudarzi, N. Kama, M. H. Anisi, S. Zeadally, and S. Mumtaz, "Data collection using unmanned aerial vehicles for Internet of Things platforms," *Comput. Electr. Eng.*, vol. 75, pp. 1–15, May 2019.

[3] L. P. I. Ledwaba, G. P. Hancke, H. S. Venter, and S. J. Isaac, "Performance costs of software cryptography in securing new-generation Internet of energy endpoint devices," *IEEE Access*, vol. 6, pp. 9303–9323, 2018.

[4] M. Gidlund, G. P. Hancke, M. H. Eldefrawy, and J. Åkerberg, "Guest editorial: Security, privacy, and trust for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 625–628, Jan. 2020.

[5] R. Basir, S. Qaisar, M. Ali, M. Aldwairi, M. I. Ashraf, A. Mahmood, and M. Gidlund, "Fog computing enabling industrial Internet of Things: State-of-the-art and research challenges," *Sensors*, vol. 19, no. 21, p. 4807, Nov. 2019.

[6] L. Zhou, K.-H. Yeh, G. Hancke, Z. Liu, and C. Su, "Security and privacy for the industrial Internet of Things: An overview of approaches to safeguarding endpoints," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 76–87, Sep. 2018.

[7] B. Leukert, T. Kubach, C. Eckert, K. Tsutsumi, M. Crawford, and N. Vayssiere, "IoT 2020: Smart and secure IoT platform," Int. Electrotechnical Commission, Geneva, Switzerland, White Papers, 2016, pp. 1–181. [Online]. Available: https://s3.amazonaws.com/midokura-marketing-materials/IIOT/iecWP-loT2020-LR.pdf

[8] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[9] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the Internet of Things in the future Internet architecture," *Future Internet*, vol. 9, no. 3, p. 27, Jun. 2017.

[10] S.-W. Lin *et al.*, "Industrial Internet reference architecture," Ind. Internet Consortium Technol., Needham, MA, USA, Tech. Rep., 2015.

[11] S. Hanna, S. Kumar, and D. Weber, "IIC endpoint security best practices," Ind. Internet Consortium, Needham, MA, USA, 2018.

[12] *OpenFog Reference Architecture for Fog Computing*, Archit. Work. Group, OpenFog Consortium, Fremont, CA, USA, 2017, pp. 1–162.

[13] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, *Problem Statement and Requirements for IPv6 Over Low-Power Wireless Personal Area Network (6LoWPAN) Routing*, document RFC 6606, 2012.

[14] A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, "Security vulnerabilities in Bluetooth technology as used in IoT," *J. Sens. Actuator Netw.*, vol. 7, no. 3, p. 28, Jul. 2018.

[15] A. F. Harris, III, V. Khanna, G. Tuncay, R. Want, and R. Kravets, "Bluetooth low energy in dense IoT environments," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 30–36, Dec. 2016.

[16] L. Frenzel, "What is the difference between IEEE 802.15. 4 and ZigBee wireless," *Electron. Des.*, vol. 22, 2013. [Online]. Available: https://www.electronicdesign.com/unused/article/21796046/whats-the-difference-between-ieee-802154-and-zigbee-wireless

[17] *Understanding ZigBee*, ZigBee Alliance, Davis, CA, USA, 2014.

[18] *The ZigBee Alliance*, ZigBee Alliance, Davis, CA, USA, 2018.

[19] D. Gascón, "Security in 802.15. 4 and ZigBee networks," Libelium World, Zaragoza, Spain, Tech. Rep., Apr. 2009, pp. 1–5, vol. 28. [Online]. Available: http://www.libelium.com/libelium-organized-the-4th-annual-conference-of-world-experts-of-the-internet-of-things-from-23-countries/

[20] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15. 4 networks," in *Proc. 3rd ACM Workshop Wireless Secur.*, 2004, pp. 32–42.

[21] S. Fuhrmann and L. Cavo, "Implementation and benchmarking of a crypto processor for a Nb-IoT SoC platform," Lund Univ., Lund, Sweden, Tech. Rep. LU/LTH-EIT 2018-649, 2018.

[22] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*, Cisco, San Jose, CA, USA, 2017.

[23] X. Yang, X. Wang, Y. Wu, L. P. Qian, W. Lu, and H. Zhou, "Small-cell assisted secure traffic offloading for narrowband Internet of Thing (NB-IoT) systems," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1516–1526, Jun. 2018.

[24] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proc. IEEE*, vol. 107, no. 6, pp. 944–961, Jun. 2019.

[25] M. S. Costa and J. Amaral, "Analysis of wireless industrial automation standards: ISA-100.11 a and wirelesshart," InTech Mag., Internation Soc. Automat., Research Triangle, NC, USA, Tech. Rep., 2012. [Online]. Available: https://isajobs.isa.org/standards-publications/isa-publications/intech-magazine/2012/december/web-exclusive-analysis-wireless-industrial-automation-standards-isa-100-11a-wirelesshart/

[26] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Comput. Netw.*, vol. 148, pp. 328–339, Jan. 2019.

[27] I. Butun, N. Pereira, and M. Gidlund, "Analysis of LoRaWAN v1. 1 security," in *Proc. 4th ACM MobiHoc Workshop Exper. With Design Implement. Smart Objects*, 2018, pp. 1–6.

[28] S. Zulian, "Security threat analysis and countermeasures for LoRaWAN join procedure," M.S. thesis, Univ. Padua, Padua, Italy, 2016. [Online]. Available: http://tesi.cab.unipd.it/53210/1/zulian_simone_tesi.pdf

[29] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. 3rd IEEE Int. Conf. Cybern. (CYBCONF)*, Jun. 2017, pp. 1–6.

[30] P. Rogaway, "Evaluation of some blockcipher modes of operation," Cryptogr. Res. Eval. Committees (CRYPTREC) Government Jpn., Univ. California, Davis, Davis, CA, USA, Tech. Rep., 2011. [Online]. Available: https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf

[31] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.
[32] X. Yang, "LoRaWAN: Vulnerability analysis and practical exploitation," M.S. thesis, Delft Univ. Technol., Delft, The Netherlands, 2017.
[33] T. C. M. Dönmez and E. Nigussie, "Security of join procedure and its delegation in LoRaWAN v1.1," *Procedia Comput. Sci.*, vol. 134, pp. 204–211, Jan. 2018.
[34] J. Akerberg, M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *Proc. 9th IEEE Int. Conf. Ind. Informat.*, Jul. 2011, pp. 410–415.
[35] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 89–98.
[36] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP)*, document RFC 7252, 2014.
[37] E. Kim, D. Kaspar, and J. Vasseur, *Design and Application Spaces for IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs)*, document RFC6568, 2012.
[38] N. Doraswamy and D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.
[39] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for 6LoWPAN," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2654–2668, Dec. 2014.
[40] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, vol. 3, 2012, pp. 648–651.
[41] J. Werb, "ISA100 wireless applications technology and systems a tutorial white paper," Wireless Compliance Inst., Research Triangle Park, NC, USA, Tech. Rep. ISA100, 2014.
[42] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. Skarmeta, "Performance evaluation of LoRa considering scenario conditions," *Sensors*, vol. 18, no. 3, p. 772, Mar. 2018.
[43] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
[44] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, document RFC 5246, The Internet Engineering Task Force, 2008.
[45] E. Rescorla and N. Modadugu, *Datagram Transport Layer Security Version 1.2*, document RFC 6347, Internet Engineering Task Force, 2012, p. 101, vol. 13.
[46] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.
[47] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2013, pp. 55–66.
[48] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar. 2012.
[49] M. Iglesias-Urkia, A. Orive, and A. Urbieta, "Analysis of CoAP implementations for industrial Internet of Things: A survey," in *Proc. ANT/SEIT*, 2017, pp. 188–195.
[50] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in *Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE)*, 2008, pp. 791–798.
[51] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2015, pp. 746–751.
[52] Q. Hu, J. Zhang, A. Mitrokotsa, and G. Hancke, "Tangible security: Survey of methods supporting secure ad-hoc connects of edge devices with physical context," *Comput. Secur.*, vol. 78, pp. 281–300, Sep. 2018.
[53] U. M. Qureshi, G. P. Hancke, T. Gebremichael, U. Jennehag, S. Forsstrom, and M. Gidlund, "Survey of proximity based authentication mechanisms for the industrial Internet of Things," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 5246–5251.
[54] J. Attridge, "An overview of hardware security modules," *SANS Inst., InfoSec Reading Room*, vol. 1, no. 1, pp. 1–10, 2002.
[55] K. Wilkinson, "Using encryption to secure a 7 series FPGA bitstream," Xilinx, San Jose, CA, USA, Tech. Rep. XAPP1239(v1.1), 2015, vol. 7.
[56] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "8.7 physically unclonable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Jan. 2016, pp. 158–160.
[57] J. Noorman, P. Agten, W. Daniels, R. Strackx, A. Van Herrewege, C. Huygens, B. Preneel, I. Verbauwhede, and F. Piessens, "Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *Proc. 22nd USENIX Secur. Symp. (USENIX Secur.)*, 2013, pp. 479–498.
[58] M. Alramadhan and K. Sha, "An overview of access control mechanisms for Internet of Things," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–6.
[59] J. B. Bernabe, J. L. H. Ramos, and A. F. S. Gomez, "TACIoT: Multidimensional trust-aware access control system for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016.
[60] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, "A car hacking experiment: When connectivity meets vulnerability," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2015, pp. 1–6.
[61] S. Hilton. (2016). Dyn analysis summary of friday October 21 attack. Dyn Blog. [Online]. Available: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack
[62] K. York, "Read Dyn's statement on the 10/21/2016 DNS DDoS attack," Dyn, Manchester, NH, USA, Tech. Rep., 2016. [Online]. Available: https://cyber-peace.org/wp-content/uploads/2016/10/Dyn-Statement-on-10_21_2016-DDoS-Attack.pdf
[63] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.
[64] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards Internet of Things (IoT): Roadmap and key challenges," in *Proc. Int. Conf. Netw. Secur. Appl.* Berlin, Germany: Springer, 2010, pp. 430–439.
[65] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
[66] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manage. (DIM)*, 2006, pp. 11–16.
[67] P. Fremantle, B. Aziz, J. Kopecky, and P. Scott, "Federated identity and access management for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 10–17.
[68] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, pp. 1–20, Aug. 2017.
[69] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet Things J.*, early access, May 6, 2020, doi: 10.1109/JIOT.2020.2991693.
[70] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4093–4100, Sep. 2018.
[71] B. Cheng, J. Zhang, G. P. Hancke, S. Karnouskos, and A. W. Colombo, "Industrial cyberphysical systems: Realizing cloud-based big data infrastructures," *IEEE Ind. Electron. Mag.*, vol. 12, no. 1, pp. 25–35, Mar. 2018.
[72] J. L. Hernández-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta, "Distributed capability-based access control for the Internet of Things," *J. Internet Services Inf. Secur.*, vol. 3, nos. 3–4, pp. 1–16, Nov. 2013.
[73] J. B. Dennis and E. C. Van Horn, "Programming semantics for multiprogrammed computations," *Commun. ACM*, vol. 9, no. 3, pp. 143–155, Mar. 1966.
[74] L. Gong, "A secure identity-based capability system," in *Proc. IEEE Symp. Secur. Privacy*, May 1989, pp. 56–63.
[75] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.
[76] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the Internet of Things," *J. Cyber Secur. Mobility*, vol. 1, no. 4, pp. 309–348, Oct. 2014.
[77] S. N. M. García, A. M. Zarca, J. L. Hernández-Ramos, J. B. Bernabé, and A. S. Gómez, "Enforcing behavioral profiles through software-defined networks in the industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 21, p. 4576, Oct. 2019.

[78] E. Lear, R. Droms, and D. Romascanu, *Manufacturer Usage Description Specification*, document RFC:8520, IETF, Fremont, CA, USA, 2017.
[79] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Characterizing and classifying IoT traffic in smart cities and campuses," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2017, pp. 559–564.
[80] T. Polk, M. Souppaya, B. Haag, Jr., and W. C. Barker, "Mitigating IoT-based distributed denial of service (DDoS)," Nat. Cybersecurity Center Excellence, Rockville, MD, USA, Tech. Rep., 2017. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/iot-ddos-project-description-final.pdf
[81] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Managing AAA in NFV/SDN-enabled IoT scenarios," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–7.
[82] J. G. Herrera and J. F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.
[83] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.
[84] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.
[85] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: A survey," *Wireless Commun. Mobile Comput.*, vol. 2018, Nov. 2018, Art. no. 1032761, doi: 10.1155/2018/1032761.
[86] C. Gentry and D. Boneh, *A Fully Homomorphic Encryption Scheme*, vol. 20, no. 9. Stanford, CA, USA: Stanford Univ. Stanford, 2009.
[87] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.
[88] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for IoT data analytics," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 20–25, Aug. 2018.
[89] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.
[90] R. Sanchez-Iborra and M.-D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors*, vol. 16, no. 5, p. 708, May 2016.
[91] V. Puri, I. Priyadarshini, R. Kumar, and L. C. Kim, "Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT," in *Proc. Int. Conf. Comput. Sci., Eng. Appl. (ICCSEA)*, Mar. 2020, pp. 1–7.
[92] S. Darwish, I. Nouretdinov, and S. Wolthusen, "A dynamic distributed architecture for preserving privacy of medical iot monitoring measurements," in *Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living*, M. Mokhtari, B. Abdulrazak, and H. Aloulou, Eds. Cham, Switzerland: Springer, 2018, pp. 146–157.
[93] K. Gai, K.-K.-R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3059–3067, Aug. 2018.
[94] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing Internet of Things applications and platforms," in *Proc. 6th Int. Conf. Internet Things (IoT)*. New York, NY, USA: Association for Computing Machinery, 2016, pp. 83–92, doi: 10.1145/2991561.2991566.
[95] C. Perera, M. Barhamgi, A. K. Bandara, M. Ajmal, B. Price, and B. Nuseibeh, "Designing privacy-aware Internet of Things applications," *Inf. Sci.*, vol. 512, pp. 238–257, Feb. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519309120
[96] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li, and Y. Ren, "Distributed data privacy preservation in IoT applications," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 68–76, Dec. 2018.
[97] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.
[98] Y. Zhao, L. T. Yang, and J. Sun, "A secure high-order CFS algorithm on clouds for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3766–3774, Aug. 2018.
[99] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, *Architectural Considerations in Smart Object Networking*, document RFC 7452, 2015. [Online]. Available: https://tools.ietf.org/html/rfc7452#section-7
[100] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 1–14.
[101] M. H. Eldefrawy, N. Pereira, and M. Gidlund, "Key distribution protocol for industrial Internet of Things without implicit certificates," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 906–917, Feb. 2019.
[102] L. Lyu, C. Chen, S. Zhu, and X. Guan, "5G enabled codesign of energy-efficient transmission and estimation for industrial IoT systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2690–2704, Jun. 2018.
[103] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

TEKLAY GEBREMICHAEL received the B.Sc. degree in information technology and engineering from the Mekelle Institute of Technology, Ethiopia, and the M.Sc. degree in computer science from the University of Trento, Italy. He is currently pursuing the Ph.D. degree with Mid Sweden University, Sweden. His main research interest includes designing cryptographic protocols for crypotographic key management in the Internet of Things.

LEHLOGONOLO P. I. LEDWABA (Graduate Student Member, IEEE) received the B.C.I.S. degree from Monash University, South Africa, in 2016, and the B.Sc. degree (Hons.) in computer science and the M.Sc. degree (Hons.) in applied science from the University of Pretoria, South Africa, in 2017 and 2018, respectively. She is currently pursuing the Ph.D. degree in computer science with the City University of Hong Kong, Hong Kong. She is currently a Candidate Researcher with the Council for Scientific and Industrial Research, Pretoria, South Africa. Her research interests include cyber-physical systems, wireless sensor networks and the industrial Internet-of-Things security, distributed ledger technologies and secure, and smart microgrid market trading.

MOHAMED H. ELDEFRAWY received the Ph.D. degree in electrical engineering from Alexandria University, Alexandria, Egypt, in 2014. He is currently an Assistant Professor with the School of Information Technology, Halmstad University, Halmstad, Sweden. Before joining Halmstad University, he was a Postdoctoral Researcher with the Department of Information Systems and Technology, Mid Sweden University, Sundsvall, Sweden. He was a Senior Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He is also an inventor of two U.S./PCT patents in cybersecurity. His research interests include network security, digital authentication, the IoT security and privacy, and digital forensics.

GERHARD P. HANCKE (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees from the University of Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree in computer science from the Computer Laboratory, Security Group, University of Cambridge, in 2009. He is currently an Associate Professor with the City University of Hong Kong, Hong Kong. His research interests include system security, embedded platforms, and distributed sensing applications related to the industrial Internet of Things.

NUNO PEREIRA (Member, IEEE) received the Ph.D. degree in computer science from the University of Minho, Braga, Portugal, in 2010. He is currently a Professor with the School of Engineering, Polytechnic of Porto (ISEP), Porto, Portugal. He was involved in numerous international (European) and national research projects, including as a Principal Investigator.

MIKAEL GIDLUND (Senior Member, IEEE) received the Lic.Eng. degree in radio communication systems from the Royal Institute of Technology, Stockholm, Sweden, in 2004, and the Ph.D. degree in electrical engineering from Mid Sweden University, Sundsvall, Sweden, in 2005. From 2006 to 2007, he was a Research Engineer and a Project Manager with Acreo AB, Kista, Sweden. From 2007 to 2008, he was a Project Manager and a Senior Specialist with Nera Networks AS, Bergen, Norway. From 2008 to 2015, he was a Senior Principal Scientist and a Global Research Area Coordinator of wireless technologies with ABB Corporate Research, Västerås, Sweden. Since 2015, he has been a Professor of computer engineering with Mid Sweden University. He holds over 20 patents (granted and pending applications) in the area of wireless communication.

JOHAN AKERBERG (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science and engineering from Malardalen University, Västerås, Sweden. He is currently a Principal Scientist and Global Research Area Coordinator of Embedded Systems and Electronics, ABB Corporate Research, Västerås. He is mainly working with communication for embedded real-time systems in industrial automation and is frequently invited to give talks to governmental bodies, international universities, and automation fairs. He has close to 20 years' experience within ABB in various positions, such as the Research and Development Project Manager, an Industrial Communication Specialist, and the Product Manager. He holds more than ten patents (granted and pending applications) in the area of wired/wireless industrial automation.