Privacy-preserving solutions in the Industrial Internet of Things

George Drosatos*, Konstantinos Rantos†, Dimitris Karampatzakis†, Thomas Lagkas†, Panagiotis Sarigiannidis‡

*Institute for Language and Speech Processing, Athena Research Center, Xanthi, Greece
gdrosato@athenarc.gr

†Department of Computer Science, International Hellenic University, Kavala, Greece
{*krantos,dkara,tlagkas*}*@cs.ihu.gr*

‡Dept. of Electrical and Computer Engineering, University of Western Macedonia, Kozani, Greece
psarigiannidis@uowm.gr

***Abstract*—Industrial Internet of Things (IIoT) is a relatively new area of research that utilises multidisciplinary and holistic approaches to develop smart solutions for complex problems in industrial environments. Designing applications for the IIoT is a non trivial issue and requires to address, among many others, technology concerns, the protection of personal data, and the privacy of individuals. In this review paper, we identify privacy-preserving solutions that have been proposed in the literature to safeguard the privacy of individuals being part, or interacting with, the IIoT environment. As such, it considers two main categories of the analysed protocols, i.e., the privacy-preserving data management and processing solutions, and the privacy-preserving authentication methods.**

***Index Terms*—Industrial Internet of Things (IIoT), Privacy, Privacy-preserving solutions, Privacy-preserving authentication methods, Literature review.**

I. Introduction

The Industrial Internet of Things (IIoT) is a relatively new area of research and development, where well-established technologies and solutions are still missing [1]. The convergence of Information Technology (IT) and Operational Technology (OT) is an important issue for industries and common approaches for product and services development must be presented for a successful exploitation of IIoT technologies. In the shop floor, implementing IIoT applications is a systems engineering problem and a multidisciplinary and holistic approach is required to develop solutions for complex problems comprising hardware, software, data, machinery and personnel.

The design of IIoT applications requires addressing new requirements including those related to edge and fog computing, efficient communication architectures, cyber security, privacy, scalability, protocol support and cognitive computing. The adoption of open IIoT standards, specifications, and architectures will also help IIoT dominate the industry. In the last years the following two organisations have been promoting the IIoT:

- *Industrial Internet Consortium* (IIC – https://www.iiconsortium.org), which follows a cross-domain approach to accelerate the development, adoption and widespread of the IIoT.
- *Plattform Industrie 4.0* (https://www.plattform-i40.de), which focuses on the concepts of efficient manufacturing and the smart factory (in Germany).

Both groups have developed reference architectures, the Industrial Internet Reference Architecture (IIRA) [2] and the Reference Architectural Model Industry 4.0 (RAMI 4.0) [3], respectively, to help streamline the standardization and adoption of IIoT technology.

Related to security and privacy issues, in 2016, IIC released the Industrial Internet Security Framework (IISF) technical report [4] initiating a procedure to create broad industry consensus on how to secure and increase trustworthiness of IIoT systems. The framework considers functional and implementation viewpoints, as well as technologies and practices that affect the security and privacy of IIoT systems. Also, it emphasizes the fact that security and privacy must be a fundamental part of the IIoT system architecture during all phases (design, implementation and operation). Furthermore, it suggests enhancements in IIoT privacy while still allowing data analytics using techniques, such as homomorphic encryption.

Privacy, in the physical world, is a vague concept that cannot be easily defined, and might be affected by the individual's perception on the protection of its own personal environment. Privacy is also sometimes related to anonymity, the desire to remain unnoticed or unrecognized in public. In information technology, it is known as information or data privacy, refers to the development of relationships between technology and the legal right to, or public expectation of, privacy in the collection and sharing of personal data [5].

Privacy concerns exist wherever uniquely identifiable data relating to an individual is collected and processed. In other cases the issue is how personal data is collected and who has access to it. Additionally, another issue is whether an individual has any ownership rights to his/her personal data, and the right to view, verify, delete and challenge that information. From a legal point of view, privacy enforcement typically comes from the applicable legal framework in each country, such as the General Data Protection Regulation (GDPR) [6]

in the European Union that gives citizens control over their personal data.

In this review paper, we focused, via a literature search process, on the identification of privacy-preserving solutions that try to address various privacy issues in the IIoT, such as anonymity and personal data processing. The list of solutions presented here is not meant to be an exhaustive list for the domain. Various other solutions, typically proposed for the more generic IoT environment, could also apply. However, in this paper the authors only analyse those that were specifically proposed for the IIoT and therefore address the peculiarities of the industrial environment. To the best of our knowledge, this is the first work that discovers explicitly privacy techniques for the IIoT, except for [7] which, however, covers both security and privacy issues without differentiating its analysis to each one of these issues.

The rest of this review paper is structured as follows. Section II describes the methodology used in conducting this research. Section III presents privacy-preserving solutions for data management and processing focused on the IIoT domain, while Section IV presents schemes that have been proposed to protect the privacy of the users that access IIoT data. Finally, Section V concludes the paper.

II. Research Methodology

The methodology that we followed to identify the relevant privacy-preserving solutions in the IIoT consists of two main steps:

1) Extensive search in the research publications performed in Scopus search engine (www.scopus.com), a well-known search engine for many sciences. The aim of our search was to identify papers that are most related to the research question which is to identify *"privacy-preserving solutions that have been proposed specifically for the IIoT environment"*. As such, we searched for the related keywords of "IIoT" and "privacy" in the title, abstract and keywords of publications. The exact query that was used in April 2020 and returned us 220 relevant papers, was the following:

```
TITLE-ABS-KEY((IIoT OR "Industrial
Internet of Things" OR "Industrial
IoT" OR "Industry 4.0") AND Privacy)
```

2) By studying the list of publications that was returned by Scopus we were able to narrow down even more the relevant, to our subject, papers. In this step, we considered solutions that were proposed specifically for the IIoT. As such, we also excluded mechanisms that aim to solve other issues, yet one of their properties is to safeguard privacy or satisfy, among others, privacy issues.

Figure 1 shows (i) the yearly distribution of publications that deal with privacy solutions in the IIoT, and (ii) the percentage of these publications in the total number of IIoT publications (specified by the first part of our query). This illustrates the increasing interest of the research community

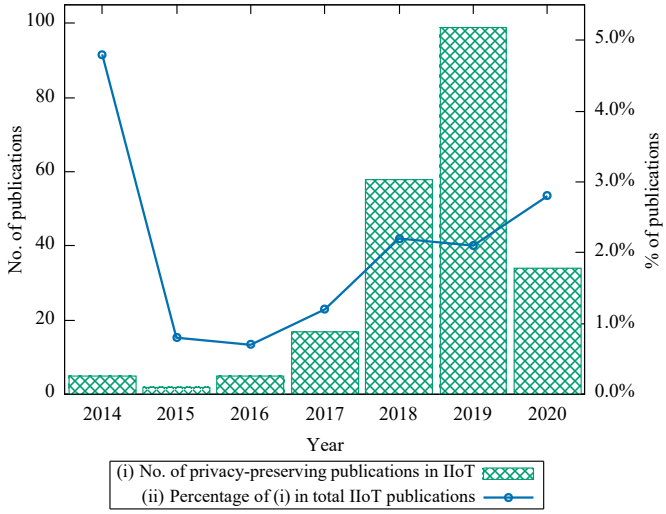

Fig. 1. Number and percentage of IIoT privacy-preserving publications per year in Scopus.

to propose privacy-preserving solutions in the IIoT. Based on these statistics, we infer that the IIoT interest in this kind of solutions shows a mean increase in the number of published papers of approximately 15% per annum during the last 6 years. Also, we should mention that the high percentage of privacy-preserving solutions in the IIoT in 2014 was the result of the low number of the total IIoT publications and after that this number increases by an average of 116% per year.

The analysis conducted on these papers revealed that they can be categorised under two main categories, i.e., the ones that focus on applying privacy-protection on data generated and managed in the IIoT, presented in Section III, and the ones which protect the privacy of the entity that accesses this data, presented in Section IV. The papers are presented in chronological order. A comparative analysis of privacy-related properties of the analysed papers is presented in Table I.

III. Privacy-Preserving Data Management and Processing Solutions in IIoT

In this section, we present solutions that have proposed to protect and manage personal data in the IIoT.

A. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in IIoT (LPT-DP-k)

LPT-DP-k, proposed by Yin et al. [8], is a location privacy protection algorithm that utilises a differential privacy strategy to preserve location data in sensor networks and maximise the utility of data in IIoT. In the proposed solution, the authors introduce a tree structure to model the location data, called location privacy tree (LPT). This structure mitigates any difficulties, such as characteristics of low density and high dispersion, to express the location data.

The differential privacy utilised in the proposed method achieves privacy protection using Laplace and index mechanism. The index mechanism is used to select data according to the accessing frequency of the tree node and the Laplace

TABLE I
COMPARISON OF PRIVACY-PRESERVING SOLUTIONS IN THE IIOT.

Proposed Solution	Privacy-Preserving Provided Service	Utilised Technologies/Architectures	Underlying Privacy Mechanisms	Security Analysis	Implementation
Privacy-preserving data management and processing solutions (Section III):					
LPT-DP-k [8]	Location data publishing and sharing	Laplace noise	Location privacy tree (LPT) & Differential privacy	–	Experimental
PPTMC [9]	Multiple clustering	Public/Private cloud computing, TMC	Paillier homomorphic encryption & Perturbation	Informal	Experimental
HKFS-KM [10]	Information retrieval & Key management	Cloud computing, Keyed hash tree (KHT), TFIDF	Searchable encryption (XTS-AES)	Formal	Experimental
HTPF [11]	Trust and privacy framework	–	Privacy checkpoints and guidelines	–	–
Xyreum [12]	Multi-factor authentication & Key establishment	Blockchain, REMME protocol	T-ZKPK & Authenticated encryption	Informal	Experimental
DeepPAR & DeepDPA [13]	Distributed machine Learning	Federated learning & Group key management	Additive homomorphic encryption	Informal	Experimental
BFL-PPDS [14]	Distributed machine learning	Permissioned blockchain, Federated learning	Differential privacy	Informal	Experimental
BIoE [15]	Task allocation	Ethereum blockchain, Edge computing	Differential privacy	Informal	Experimental
HI 4.0 [16]	Cross-border eHealth data exchange	RAMI 4.0, OpenNCP	Consent management & Data hiding tools	–	–
PDASH [17]	Privacy dashboard	HUMAN trust and privacy framework (HTPF)	Privacy by design	–	–
PPDSMP [18]	Data Sharing	–	Differential privacy & Data perturbation	–	Experimental
LDA-EPP [19]	Data aggregation	Cloud & fog computing, Hash chain, CRT	Paillier homomorphic encryption	Informal	Experimental
Privacy-preserving authentication solutions (Section IV):					
P2SAP [20]	Anonymous entity authentication	Biometrics, ECC	Dynamic identities & Untraceability	Formal & Informal	Simulation (NS-3)
ALCMAKA [21]	Anonymous entity authentication	Biometrics, Smart cards, Passwords	Pseudo-identities & Untraceability	Formal & Informal	Simulation (NS-2)
BP2UA [22]	Anonymous entity authentication	Biometrics	Pseudo-identities & Untraceability	Formal & Informal	Simulation (NS-2)
HCPPA-KE [23]	Anonymous entity authentication	Passwords	Pseudonyms	Formal & Informal	–

mechanism adds appropriate noise to change this frequency. The experimental results showed that the proposed method protects users' privacy without significant negative effects in the utility of data and the processing efficiency.

B. Privacy-Preserving Tensor-Based Multiple Clusterings on Cloud for IIoT (PPTMC)

Zhao et al. in [9] proposed a privacy-preserving tensor-based multiple clustering method (PPTMC) on a hybrid cloud (public and private) in order to provide an efficient, scalable and secure solution discovering different, hidden data structures in IIoT big data. In this work, the authors present a privacy-preserving approach solving the problem of tensor-based multiple clustering (TMC) based on the Paillier homomorphic encryption. Apart from the development of the proposed PPTCM method, the following security protocols for computations over encrypted data have also been developed: secure exponentiation (SE), secure attribute weight ranking (SAWR), and secure selective weighted tensor distance (SSWTD).

All computational tasks are implemented on the cloud and users' privacy is preserved because data encryption and the required perturbations are performed on the client. An informal security analysis of PPTMC is also presented. Experimental results show that the presented scheme achieves 100% clustering accuracy compared to the plaintext TMC method, and is scalable when using more cloud servers, while no additional or private information is leaked.

C. Hybrid Keyword-Field Search with Efficient Key Management for IIoT (HKFS-KM)

HKFS-KM, proposed by Miao et al. [10], is an outsourced hybrid keyword-field search over encrypted data with efficient key management scheme in the IIoT (Figure 2). The hybrid keyword-field search includes both textual and digital keyword fields utilising term frequency-inverse document frequency (TFIDF) metric and specific range of numeric data score function, accordingly. Furthermore, the proposed scheme implements a key management functionality to reduce massive keys storage using a keyed hash tree (KHT).

Additionally, the proposed searchable encryption scheme is supported by the XTS-AES algorithm [24] for the encryption of IIoT data records. The authors provide a formal security analysis that proves that the proposed HKFS-KM scheme can guarantee keyword privacy and trapdoor unlinkability for known ciphertexts attack and known background attack. The experimental results demonstrate the feasibility and efficiency of the HKFS-KM scheme using real-world datasets.

D. A Trust and Privacy Framework for Smart Manufacturing Systems (HTPF)

In this work, Mannhardt et al. [11] present a trust and privacy framework for smart manufacturing systems that allows understanding the concepts of trust and privacy, when designing solutions, for the benefit of manufactures. This work highlights the need for considering privacy and trust in smart

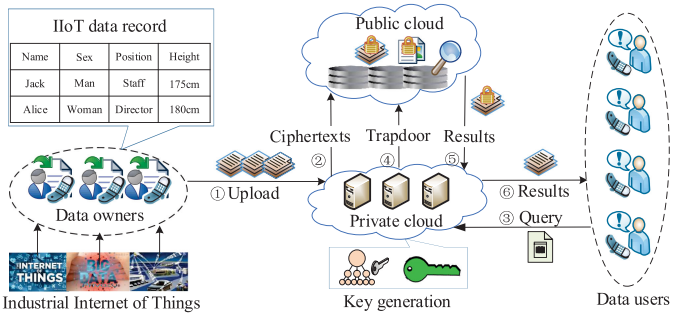

Fig. 2. HKFS-KM system model [10].

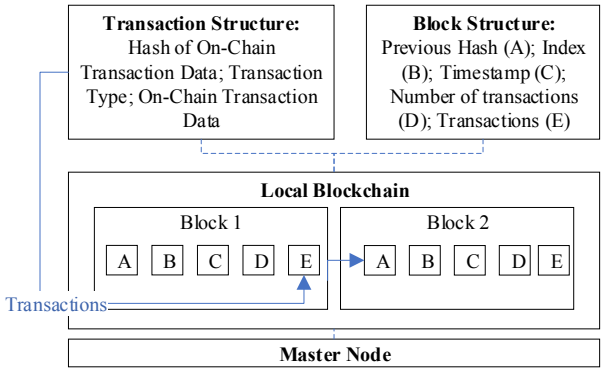

Fig. 3. Xyreum's local blockchain [12].

manufacturing environments particularly when humans are in the loop (operators, managers, etc.). The proposed framework integrates the trust and privacy perspectives, takes into account the data life-cycle in IIoT environments, covers technological and organisational issues limited to the legal framework of an organisation, in order to propose *privacy checkpoints with guidelines*. The applicability of this framework was instantiated in the context of a manufacturing environment in the HUMAN EU project (http://humanmanufacturing.eu) and evaluation results, regarding usefulness and privacy awareness, are presented by three studies. Although, this work is compared with other existing frameworks, the evaluation is only in academic context.

E. Xyreum: A High-Performance and Scalable Blockchain for IIoT Security and Privacy

Sani et al. [12], proposed Xyreum, a Mutual Multi-factor Authentication and Key Establishment (MMFA-KE) protocol which uses a Time-based Zero-Knowledge Proof of Knowledge (T-ZKPK) [25] scheme combined with authenticated encryption. Xyreum is a blockchain-based scheme that aims to provide privacy for the IIoT while overcoming high computational complexity problems found in blockchains, by the use of lightweight cryptographic mechanisms. It also addresses security concerns, such as latency challenges, which are considered inappropriate for the IIoT environment.

Node registration relies on Pedersen commitments [26], which supports homomorphic operations and can provide perfect hiding of real message with the same trapdoor. Xyreum authenticates nodes and derives session keys based on T-ZKPK. The T-ZKPK usage mitigates eclipse attacks where proof of work (PoW) and proof of stake (PoS) are vulnerable. Transactions are recorded on a local blockchain, which is managed by a master node, while participating nodes can access it for verification purposes. Xyreum allows the use of multiple such local blockchains in a distributed system, each with its own master node. Figure 3 depicts the block and transaction structures in a local blockchain. Nodes' privacy is preserved by the disclosure only of the transaction type only or transactions summary information.

The authors also provide an informal security and privacy analysis and give information on how to use their scheme to strengthen security and privacy of the REMME protocol (https://remme.io), a blockchain-based security protocol, which they use as a case study. The experimental results reveal that Xyreum has low computational complexity compared to existing relevant schemes and, in terms of latency, it meets the required IIoT latency target.

F. DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for IIoT

Zhang et al. [13] address the privacy concerns raised when utilising distributed datasets in IIoT in federated deep learning, by proposing two privacy-preserving mechanisms called DeepPAR (privacy-preserving and asynchronous deep learning via re-encryption) and DeepDPA (dynamic privacy-preserving and asynchronous deep learning). The aim is to protect participating users' privacy so that any personal data provided for deep learning will not be leaked to unauthorised parties.

DeepPAR (Figure 4) and DeepDPA (Figure 5) are based on proxy re-encryption and group dynamic key management, respectively. In DeepPAR, a proxy is responsible for re-encrypting ciphertexts provided by gradients in the deep learning network, from their different secret keys into ciphertexts encrypted using the same key.

The systems also provide forward secrecy for new participants in a learning group, who will not be able to have access to model parameters prior to joining, and backward secrecy for participants that leave the group, so that they won't be able to have access to model's parameters after leaving the group. In such dynamic environments, DeepDPA provides backward secrecy in a lightweight manner, by the use of group key management. Finally, the authors provide an informal security analysis for their schemes and also the results of a performance evaluation.

G. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in IIoT (BFL-PPDS)

Lu et al. proposed a differentially private multiparty data sharing model for machine learning purposes in IIoT applications, that is based on permissioned blockchain [14]. In their approach, the actual raw data is not directly shared among the

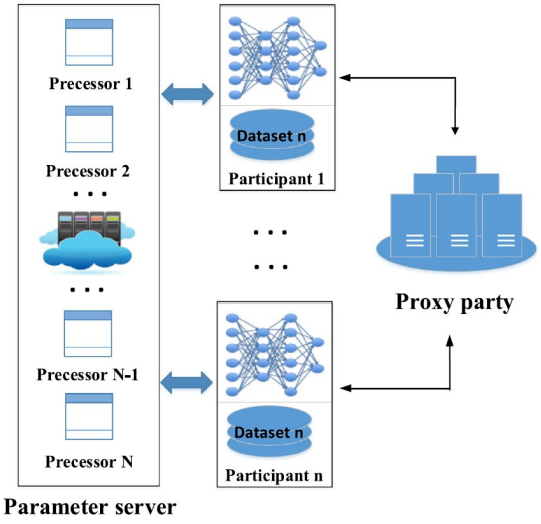

Fig. 4. DeepPAR system [13].

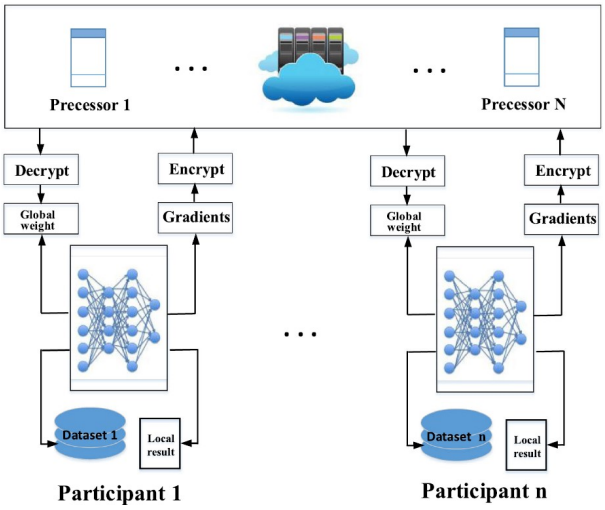

Fig. 5. DeepDPA system [13].

parties but used for building data models based on federated learning algorithms. In this way, the privacy concerns of data usage are addressed in the learning phase of algorithms via distributed training locally in the parties.

Additionally, the authors present a blockchain-based architecture that allows collaborative data sharing over the multiple parties located distributively in order to reduce data leakage risks. This decentralised architecture continues to support data owners to keep the control of their data and to provide selectively access to it. An overview of BFL-PPDS architecture is presented in Figure 6.

In order to enrich further the provided privacy, differential privacy methods [27] are integrated into federated learning by adding appropriate noise in the local raw data. Also, the proposed approach gives an informal security analysis and is evaluated for its effectiveness in two real-world datasets for data categorisation. The results show that the increase

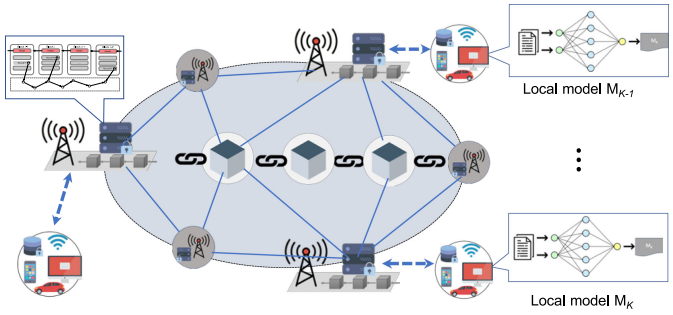

Fig. 6. Architecture of BFL-PPDS [14].

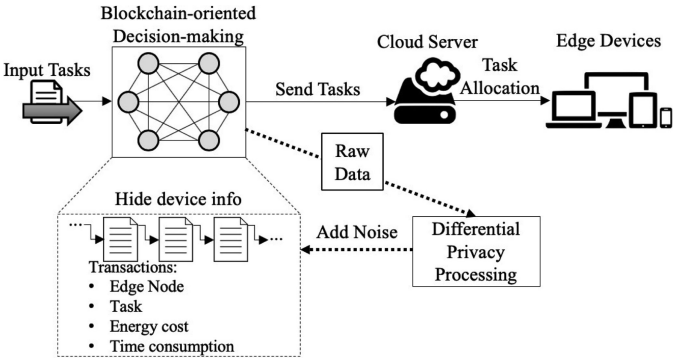

Fig. 7. Architecture of BIoE model [15].

in data providers has little effect on the accuracy, while the running time is obviously increasing. Nevertheless, the authors do not provide experiments with any custom or real blockchain infrastructure.

H. Differential Privacy-Based Blockchain for IIoT (BIoE)

BIoE model, introduced by Gai et al. [15], is a privacy-preserving scheme for implementing edge computing in IIoT utilising blockchain technology for task allocations. The architecture of the proposed approach is shown in Figure 7. This architecture provides a traceable mechanism for solving the task allocation problem in edge computing using features of blockchain technology. According to the authors, the proposed model is designed to support a controllable and scalable IIoT system while considering limitations, such as energy cost, apart from privacy preservation.

The required privacy is achieved using a differential privacy approach, by which noise is artificially added to those data stored in the blockchain, in order to prevent data mining-based attacks. Also, the authors provides an informal security analysis of their scheme. Experimental results are also provided, using Ethereum as a blockchain infrastructure, to evaluate the feasibility and the performance of the proposed BIoE model.

I. Towards a GDPR Compliant Way to Secure European Cross Border Healthcare Industry 4.0 (HI 4.0)

Larrucea et al. [16] proposed a Healthcare Industry 4.0 (HI 4.0) architectural model (Figure 8) that provides GPDR

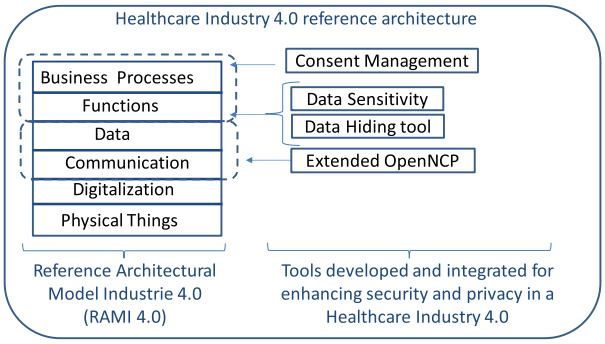

Fig. 8. Architectural model of HI 4.0 [16].

compliance for exchanging sensitive eHearth data cross different countries in Europe. This model extends the Reference Architectural Model Industry 4.0 (RAMI 4.0) [3] by adding a consent management process to satisfy GDPR requirements, a data sensitivity identification process, data hiding tools and OpenNCP [28], as a communication platform.

Additionally, the authors present a case study to illustrate the usage of the proposed HI 4.0 reference model. This case study aimed to determine the sensitive data of an individual, considering the GDPR, and integrate the consent management and data hiding tools, while giving users control over their personal data.

J. Designing a Privacy Dashboard for a Smart Manufacturing Environment (PDASH)

In [17], the authors describe the initial requirements and design process followed to develop a privacy dashboard for smart manufacturing environments. The aim of privacy dashboards is to capture what personal data is stored by a system and give the option to the users of the same system to manage what personal data is communicated to third parties. The design of privacy dashboard is based on a privacy by design approach, as promoted by the GDPR, following the guidelines of HTPF framework [11] proposed previously by the same authors in HUMAN EU project. As mentioned, currently, the design of the dashboard is in an early stage and requires to implement and compare it with other existing approaches.

K. Privacy-Preserved Data Sharing towards Multiple Parties in IIoT (PPDSMP)

Zheng and Cai [18] propose a framework for providing data consumers the ability to share their data in a privacy-preserving manner. The authors consider three main entities in their framework. The workers, or data providers (DPs), who (generate contents about different applications) share their data for profit with data consumers (DCs), aka subscribers, and the service providers (SPs), who coordinate data sharing among workers and subscribers. The proposed scheme tries to achieve a balance among user's privacy, profits of participating entities and data utilisation. The budgets provided by the data consumers are taken into account in the data sharing strategy.

The authors consider two scenarios and propose two algorithms. In the first scenario the DC has access to the same information as the SP, as the SP is only involved in fusing data received by DPs and making them available to DCs, and does not have access to the production system. A sharing strategy defines the scale of shared contents and the accuracy of the data provided by DPs. Privacy is preserved by the use of typical randomised responses.

In the other scenario, the service provider processes the information it gets from the data providers, and conceals some private business information, prior to making it available to subscribers. The SP, prior to sharing the data with the DCs, proceeds with the data perturbation, which is implemented with a second random response on the collected data, based on an agreed privacy factor.

The authors evaluate their work and measure the performance of the proposed algorithms using real Freight and Taxi datasets.

L. Layered Data Aggregation with Efficient Privacy Preservation for Fog-assisted IIoT (LDA-EPP)

LDA-EPP, as proposed by Li et al. in [19], is a layered data aggregation scheme with efficient privacy preservation in fog-assisted IIoT. The scheme comprises three layers (sensing layer, fog layer, and cloud layer) and mainly includes five entities (IIoT devices, fog nodes, industrial cloud, trusted management authority, and users). Figure 9 depicts the network architecture of the proposed solution. LDA-EPP preserves data privacy, confidentiality, and integrity, by employing a modified homomorphic encryption of Paillier cryptosystem, a simple hash chain mechanism and the Chinese Remainder theorem (CRT) for layered data aggregation. More specifically, the privacy of individual device is protected against the semi-trusted fog nodes and the cloud. Utilising the CRT, the cloud in the proposed solution can provide fine-grained services by acquiring aggregation data from smaller subareas.

Furthermore, the authors provide an informal security analysis of the proposed LDA-EPP scheme using honest-but-curious entities (fog nodes and industrial cloud) and focusing on the security and privacy preservation of data generation and transmission processes. Experimental results demonstrate advantages of the proposed scheme, over others, in terms of computation and communications costs.

IV. Anonymous Access to IIoT Data and Services

This section analyses schemes that have been proposed to address a different aspect of anonymity in IIoT, which is related to the privacy-preserving authentication for access to IIoT data and services. An example of a typical authentication model considered in these protocols is depicted in Figure 10.

A. A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for IIoT (P2SAP)

Li et al. [20] propose another biometrics-based authentication protocol for access to wireless-sensor networks in IIoT environment. The scheme is based on the use of elliptic-curve

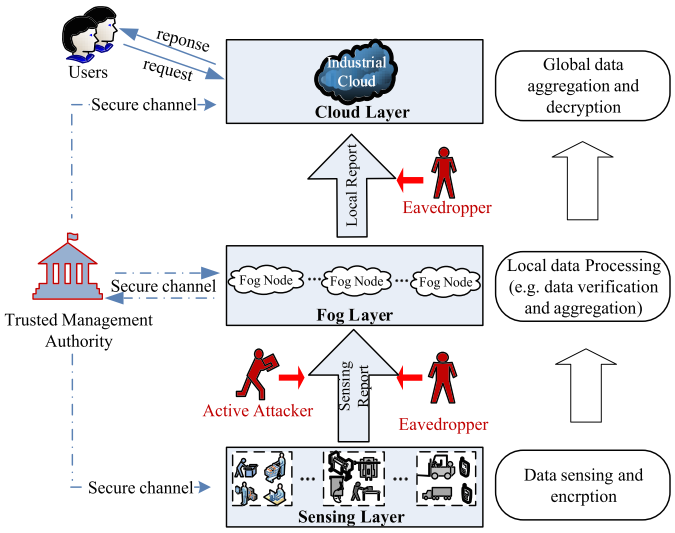

Fig. 9. Network architecture of LDA-EPP [19].

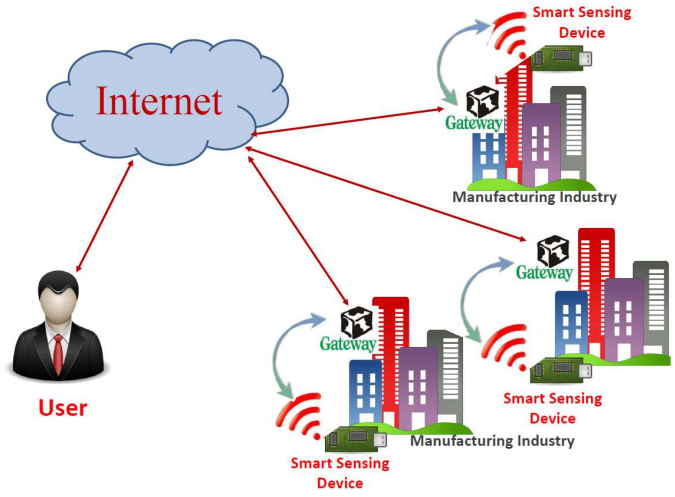

Fig. 10. IIoT Authentication Model [21].

cryptography (ECC) for the bi-directional authentication and key establishment that takes place among a user, the sensor gateway, and a sensor node.

P2SAP utilises the sensor gateway for the user's registration, while anonymity is preserved through the use of dynamic identities, instead of real identities, and untraceability. Sensor nodes' anonymity is also preserved, by not transmitting their identities via public channels. They are however identifiable by the gateway.

The authors provide a formal proof for their protocol, make a properties comparison analysis with other related protocols and provide the results of a performance comparison and benchmarks on a simulation conducted on NS-3.

B. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for IIoT (ALCMAKA)

The protocol proposed by Srinivas et al. [21], facilitates anonymous authorised access to nodes' services. The model utilised by the authors is depicted in Figure 10. The proposed protocol is a three-factor authentication and key establishment protocol which is based on the use of a smart card, biometrics, and a user password. Similarly to the previous scheme, a gateway, acts as a trusted entity and utilised for user and smart IoT device registration and facilitates their mutual authentication. The established secret session key is shared between the user and the smart IoT device. The protocol also provides provides user anonymity and untraceability.

The authors perform an informal and a formal security analysis based on Real-or-Random (RoR) oracle model and AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, a comparison with other protocols, and provide the results of a benchmarking on a simulation on NS-2.

C. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based IIoT Deployment (BP2UA)

BP2UA [22] is a two-factor authentication scheme which is based on the use of smart cards and biometrics to authenticate users prior to providing them access to personal data on cloud-based IIoT applications. The proposed method facilitates mutual authentication and key establishment between a smart device and a smart cardholder. This is accomplished with the help of the device's gateway (similarly to the P2SAP [20]), with which the device register during an offline registration phase. The use of pseudo-identities for the communicating parties and the untraceability property of the proposed protocol, provide the required user privacy. One of the main benefits of BP2UA is that it only requires bitwise Exclusive-OR and hash operations at the smart devices, which makes BP2UA a lightweight solution.

The authors provide an informal and a formal security analysis for the session key establishment method, using the real-or-random model. They also demonstrate their method's resilience against passive and active attacks. However, Hussain et al. [29] recently claimed that BP2UA is vulnerable to stolen verifier, stolen smart device, and traceability attacks which allow exposure of the session key. Moreover, it does not provide perfect forward secrecy.

The authors also make a comparative analysis with other similar schemes and provide some evaluation and performance results on a simulation on NS-2 (Network Simulator 2).

D. Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for IIoT (HCPPA-KE)

Paliwal [23] proposed a conditional privacy-preserving authentication and key exchange protocol. The proposed work is considered lightweight as it is mainly based on the use of hash functions. Similarly to the previously mentioned protocols, HCPPA-KE utilises the sensors gateway to perform the necessary user and sensor registration, authentication and key establishment. Anonymity is preserved with the use of pseudonyms which are updated in every session (the pseudonym for each session is provided with the messages of the previous session).

The protocol also provides perfect forward secrecy as the session keys depend on nonces and timestamps which are used only for a specific session.

The author provides an informal security analysis as well as a formal one based on AVISPA and Real-or-Random (RoR) oracle model simulations. The paper also provides some performance analysis results which are compared to similar works. The authors cost of the cryptographic operations is based on previous works. The author also performs a cryptanalysis on the Li et al. [20] proposed protocol and proves that the scheme is vulnerable to Denial-of-Service attacks and impersonation attacks.

V. Conclusions

In this review paper, we presented privacy-preserving solutions in the IIoT that try to address various privacy issues, such as anonymity and personal data processing, analysing those that were especially proposed for the IIoT and consequently address the peculiarities of the modern industrial environment. The conducted analysis of these solutions drove us to categorise them as, (1) those that focus on applying privacy-protection on data generated and managed in the IIoT, and (2) those that protect the privacy of the entity that accesses this data. Additionally, we compared them with regard to the privacy-preserving provided service, the utilised technologies in general, the utilised underlying privacy mechanisms, the presentation of a formal or informal security analysis, and the implementation level. The results of this review reveal that the privacy-enhancing technologies (PETs) is on the rise in the IIoT domain and we encourage researchers to continue their effort proposing even more advanced and innovative approaches.

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[2] Industrial Internet Consortium (IIC), "The Industrial Internet of Things – Volume G1: Reference Architecture v1.9," https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf (accessed on 29 Apr. 2020), 2019.

[3] K. Schweichhart, "Reference Architectural Model Industrie 4.0 (RAMI 4.0)," https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf (accessed on 29 Apr. 2020), 2016.

[4] Industrial Internet Consortium (IIC), "The Industrial Internet of Things – Volume G4: Security Framework v1.0," https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf (accessed on 29 Apr. 2020), 2016.

[5] G. Drosatos, "Utilization and protection of personal data in ubiquitous computing environments," Ph.D. dissertation, Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Xanthi 67100, Greece, July 2013.

[6] European Parliament and Council, "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, pp. 1–88, 2016.

[7] Y. Zhang and X. Huang, *Security and Privacy Techniques for the Industrial Internet of Things*. Cham: Springer, 2019, pp. 245–268.

[8] 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 Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2018.

[9] Y. Zhao, L. Yang, and J. Sun, "Privacy-Preserving Tensor-Based Multiple Clusterings on Cloud for Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2372–2381, 2019.

[10] Y. Miao, X. Liu, R. Deng, H. Wu, H. Li, J. Li, and D. Wu, "Hybrid keyword-field search with efficient key management for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3206–3217, 2019.

[11] F. Mannhardt, S. Petersen, and M. Oliveira, "A trust and privacy framework for smart manufacturing environments," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, no. 3, pp. 201–219, 2019.

[12] A. Sani, D. Yuan, W. Bao, P. Yeoh, Z. Dong, B. Vucetic, and E. Bertino, "Xyreum: A high-performance and scalable blockchain for iiot security and privacy," in *International Conference on Distributed Computing Systems*, vol. 2019-July, 2019, pp. 1920–1930.

[13] X. Zhang, X. Chen, J. Liu, and Y. Xiang, "DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2081–2090, 2020.

[14] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[15] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential Privacy-Based Blockchain for Industrial Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2020.

[16] X. Larrucea, M. Moffie, S. Asaf, and I. Santamaria, "Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0," *Computer Standards and Interfaces*, vol. 69, 2020.

[17] F. Mannhardt, M. Oliveira, and S. Petersen, "Designing a Privacy Dashboard for a Smart Manufacturing Environment," *IFIP Advances in Information and Communication Technology*, vol. 573 AICT, pp. 79–85, 2020.

[18] X. Zheng and Z. Cai, "Privacy-Preserved Data Sharing towards Multiple Parties in Industrial IoTs," *IEEE Journal on Selected Areas in Communications*, 2020.

[19] Y. Li, S. Chen, C. Zhao, and W. Lu, "Layered data aggregation with efficient privacy preservation for fog-assisted IIoT," *International Journal of Communication Systems*, vol. 33, no. 9, 2020.

[20] X. Li, J. Niu, M. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-Based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[21] J. Srinivas, A. Das, M. Wazid, and N. Kumar, "Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[22] A. Das, M. Wazid, N. Kumar, A. Vasilakos, and J. Rodrigues, "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, 2018.

[23] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things," *IEEE Access*, vol. 7, pp. 136 073–136 093, 2019.

[24] L. Martin, "XTS: A mode of AES for encrypting hard disks," *IEEE Security & Privacy*, vol. 8, no. 3, pp. 68–69, 2010.

[25] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology — CRYPTO' 86*, A. M. Odlyzko, Ed. Berlin, Heidelberg: Springer, 1987, pp. 186–194.

[26] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology — CRYPTO '91*, J. Feigenbaum, Ed. Berlin, Heidelberg: Springer, 1992, pp. 129–140.

[27] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*, M. Agrawal, D. Du, Z. Duan, and A. Li, Eds. Berlin, Heidelberg: Springer, 2008, pp. 1–19.

[28] M. Fonseca, K. Karkaletsis, I. A. Cruz, A. Berler, and I. C. Oliveira, "OpenNCP: A novel framework to foster cross-border e-health services," in *26th Medical Informatics in Europe Conference (MIE)*, vol. 210. IOS Press, 2015, pp. 617–621.

[29] S. Hussain and S. Chaudhry, "Comments on 'Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment'," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 936–10 940, 2019.