Towards a data provenance model for private data sharing management in IoT

Nouha Laamech, Manuel Munier, Cong-Duc Pham

Towards a data provenance model for private data sharing management in IoT

Nouha Laamech, Manuel Munier, Congduc Pham
LIUPPA
Universite de Pau et des Pays de l'Adour, E2S UPPA
Mont-de-Marsan / Pau, France
surename.name@univ-pau.fr

***Abstract*—Internet of Things (IoT) is one of the key technologies in the industry 4.0 era and promotes the interconnection of numerous data sources in several sectors such as ecology, agriculture, or healthcare. Meanwhile, each entity within these connected environments carries its unique requirements and individual goals. For connected environments to gain greater legitimacy among end users, service-oriented systems must adopt a new paradigm that allows end users to move from being passive consumers to actively participate in monitoring their own data at different stages of its lifecycle. In this context, a usage model based on ontological reasoning can be integrated within a data provenance mechanism to help create a trust worthy environment. In this paper, we introduce a vision for democratizing service-oriented systems. We discuss potential new directions that need to be pursued in the area of data management. Then, we review existing schemes applied in IoT data provenance and rely on the requirements to discuss their strengths and weaknesses. Finally, we summarize a number of potential solutions to direct future research.**

***Index Terms*—Data Provenance, Internet of Things, Rule Manager, Data Governance**

I. Introduction

With more than 500 billion objects connected to the Internet by 2030 according to Cisco [1], IoT represents an undeniable growth factor for both small and medium-sized enterprises (SMEs) and multinationals. Multiple common devices previously inactive will be able to communicate through sensors connected to the Internet. As a result, numerous new uses are emerging in diverse fields like industry, health, logistics and mobility. This IoT revolution impacts all sectors of activity and aims at facilitating decision-making in a wide range of fields such as intelligent diagnosis, predictive maintenance and asset optimization. In this context, multiple authorized parties, namely data producer, data requesters, and data brokers are involved in the process and each one of them aims to use the shared data in order to achieve its own goals. For instance, different entities can share their energy consumption to facilitate the energy provider's ability to forecast its production. Data owners and data requesters can be individuals, a group of individuals, or private/public organizations.

However, the distributed nature of IoT networks leads to the recognition of security and privacy as being among the key challenges in IoT domain. For instance, popular encryption protocols and privacy-preserving methods, such as ECDSA, have been shown to be highly expensive when run on devices with limited computing capabilities in IoT domain [2]. Moreover, due to the lack of IoT data management, data requesters don't have the ability to trace the source of the asset as well as its processing history to tailor it to their business needs. Furthermore, the data owner has little to no control over his IoT data once shared, and therefore quickly lose his ownership. All this creates a dysfunctional IoT environment that lacks mutual trust between its agents and can disrupt the envisioned services.

Despite data being rightfully recognized by the community as the essence of the future, only few consider it as an asset with a measurable economic value. To have a good management of the information system within an organization means to be able to control information in a context where various entities are interconnected and frequently exchange each other resources. It is then a priority to maintain control of the information possessed, even when it is shared in an external domain. In the context of risk management, three main criteria are used to evaluate data security: confidentiality, integrity and availability. In [3], authors define "controllability" as a new necessary criterion to add along the existing ones, and whose objective is to ensure an organization's control over the data it manipulates. An implementation of this new process is yet to be built and a combination of IT security mechanisms is to be considered.

Data provenance provides a potential solution to address the issues mentioned above by storing information about the origin of the data, the transactions performed on the data, and the history of the processing from its initial source to its current state. Thus, it allows:

a) Ascending traceability: data requesters to trace the origin of a data item and determine whether it meets the technical and legal requirements of a given activity and to assess its quality.

2325-6605/21/$31.00 ©2021 IEEE
DOI 10.1109/EDOCW52865.2021.00051

b) Descending traceability: data providers to be informed where their data is distributed and in which processes it's being involved, therefore not completely lose their ownership.

Current Data provenance solutions do not cover all the privacy demands, such as retention time, disclosure limitations, etc., which are set by the privacy standard [4] and legislation [5] to preserve the privacy of the users. In future work, the privacy obligations are to include the requirements that must be met by all concerned parties to ensure that privacy is maintained throughout the life cycle of IoT data.

Relying on the fundamentals set by the European General Data Protection Regulation (GDPR) [5], our goal is to ensure that privacy requirements are respected when dealing with shared data collected by IoT devices. The rest of this paper is organized as follows. Section 2 introduces Internet of things architecture and knowledge representation based on semantic modelisation. In section 3, current data provenance solutions are presented with the existing techniques and models. Several open issues are brought up in section 4 as well as future directions. Section 5 concludes the paper and presents a larger context.

II. BACKGROUND

A. Internet of things

Several architectures are proposed to model IoT, such as IoT-A [6] and IIRA [7]. We base our work on the architecture proposed by Wu [8], which splits IoT systems into 5 layers. As shown in figure 1, the Perception layer consists of physical objects that are controlled by sensor and actuator devices that aim to collect data. The sensor data is then transmitted to the Middleware layer through the Network layer using gateways and routers. Information analysis is realized in the Middleware using advanced data processing technologies. The analyzed data is represented in the Application layer featuring the interface between IoT system and users. Finally, Business layer provides management tools in order to control the overall IoT system. The primary purpose is to achieve an autonomous decision-making process, which returns commands for lower layers to carry out actions.

An information is the processed form of collected data. Well-known security and privacy techniques such as encryption, access control, and anonymization has been applied to ensure the preservation of raw data captured during the first layer of the architecture and avoid security attacks. At each stage of IoT data life cycle within those layers, conventional security mechanisms are implemented to preserve the efficiency and integrity of the service. Alshahrani in [9] summarize the existing techniques for data security used in each layer, namely authentification procedures, encryption mechanism, and usage control. However, much less work is targeted towards aspects regarding information quality and its governance. In this context, and as shown in figure 1, our approach aims to enhance existing works with mechanisms that allow the improvement of information management by introducing new components to manage information security,

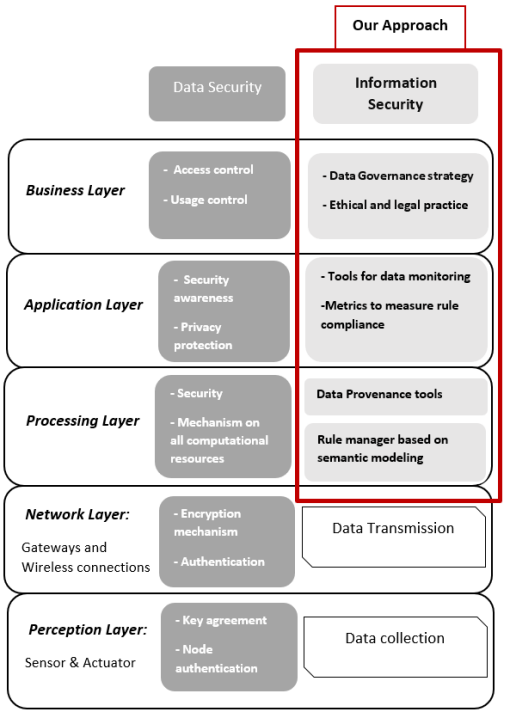

Fig. 1. Global IoT system architecture and security mechanisms

assess data quality and trustworthiness, and monitor data exploitation and data sharing by the various parties involved in the ecosystem. Therefore, we aim to complement existing practices by taking into account not only the transmission security aspects, but the preservation of information quality present in the collected data. In order to do this, we introduce in the processing layer semantics-based rule manager and data provenance utilities to be integrated in a decentralized global architecture. In the application layer, we propose a shared data monitoring mechanism based on these tools to allow IoT actors to monitor their shared data, as well as the data consumer to know where available data comes from and assess its relevancy.

B. Knowledge representation based on semantic modeling

Privacy threats and legislative constraints require both the data owner and the requester to maintain the confidentiality of shared data. For this purpose, and in a similar approach as a license, data owners set the requirements that other parties need to respect to be able to use their assets. However, matching the data owner's preferences with the requester's demand for access entails using the same vocabulary that describes the privacy requirements. This correspondence allows for the creation of a common policy that can be enforced to protect the privacy of the data owner of IoT environment. These challenges are not limited to private data but have a broader coverage and concerns any sensible data.

To express this vocabulary, various ontologies for preserving privacy in IoT have been built, namely semantic sensor

network ontology [10] that portrays IoT resources but fails to consider privacy policies, or privacy-aware access control [11] that concentrates solely on who can access the generated IoT resource data at the time of processing. Following this lead, constructing a unified knowledge representation based on semantic modeling is a necessity for the achievement of the creation of a common policy process.

Afterwards, from the moment the resource is requested and deployed, there is no way to guarantee the data owner will stay updated to whether its asset is correctly used or if the entity at the receiving end follows the established policies agreed on. In this case, the challenge is to guarantee that the external party behaves as expected when the resource is in her domain and that the mutual reliance on each entity is preserved. By recording data origins and the history of data generation and processing, data provenance can answer critical privacy issues and ensure "data quality" assertion.

III. DATA PROVENANCE IN IOT

Data provenance is defined as all the relevant information about the process of data production and evolution through time, and includes both the static and evolving origins of the data [12]. With the provenance information collected, we can determine the originating node that produced the data, the immediate node through which the data passed, agents involved in, and the operations performed on it. Sometimes we can even find out the time and location of the behaviors performed on the data. Thus, data provenance is widely applied in both scientific and business domains.

A. Models

[13] constructed a solution called PROV, based on five requirements that must be met to enable provenance composition. First, a minimal solution is identified by which a message identifier is shared by its sender and receiver, to enable a form of composition that meets the two first requirements. The minimal solution is then progressively enriched with bundles and topicIn property, attribution, and the pingback mechanism to satisfy the remaining requirements. Although the solution proposed here fills existing data traceability gaps, it still leaves open a number of practical issues, including system interoperability.

Along the same lines, [14] defines a comprehensive UML2PROV approach. First, a mapping strategy is established between class diagrams to models. Then, an improvement of the first prototype is proposed using a model-driven development based approach, which not only implements the global mapping patterns, but also provides a fully automatic way to generate the artifacts for provenance collection. However, the solution as presented cannot be applied to a distributed system. An ontology-based data provenance model is proposed in [15]. The model describes the context of the creation or modification of data points, including information about the agents involved, the execution context, time, and location. Furthermore, the model captures the dependency relationships between data points and does not depend on the execution models of IoT applications.

B. Architectures

Privacy preservation approaches can be categorized into three types of architectures.

1) Centralized architectures: Centralized schemes are based on one or more central nodes where data is kept to ensure privacy preservation before delivering the data to data consumers.

An anonymous privacy-preserving scheme called APPA [16] handles privacy-preserving data aggregation in the fog-enhanced IoT environment (fog computing). The APPA scheme consists of five entities, namely smart devices, a fog node, a public cloud server, a trusted certificate authority and a local certificate authority. The two authorities are independent organizations responsible for managing the certification of the system. The smart devices collect and send data to the fog node, which stores and aggregates the received data using the Paillier Cryptosystem system. Then, it transmitted the aggregated data to the public cloud server that processed the data to better serve the users. In addition, the anonymity and authenticity of the device is guaranteed by a pseudonym and a pseudonym certificate.

Data aggregation is also used for privacy preservation. Lu et al. proposed a lightweight aggregation scheme, called LPDA [17]. This uses one-way hash chain techniques to allow a fog node to filter out fake data by performing source authentication at the network edge. In addition, LPDA combines Paillier homomorphic encryption and Chinese remainder theorem to aggregate data from hybrid IoT devices into a single ciphertext. LPDA consists of four actors, namely IoT devices, a fog device, a control center, and a trusted authority. A set of IoT devices periodically report their data to a fog device, which aggregates the received data and forwards it to the control center, which can perform data analysis on the aggregated data. The role of the trusted authority is to assign and manage keys to all IoT devices, the fog node and the control center.

The main problem with centralized approaches is that all processing and privacy-preserving tasks are handled by a single node. Thus, if a node is compromised, all sensitive user data is impacted.

2) Distributed architectures: Dorri et al. proposes a lightweight blockchain optimized for resource-constrained devices [18]. The proposed solution eliminates mining and thus has no additional delays in processing the generated transactions. Under the proposed model, only authorized users can access and control home devices. In [19], the same authors applied their lightweight blockchain for a smart home. In each home, multiple IoT devices (e.g., smartphones, personal desktops, and sensors) are connected to the same network. In addition, each home is equipped with a powerful, online resource device known as the home miner. The latter is responsible for processing all transactions inside the house.

[20] introduces innovative techniques for IoT data privacy preservation, using multiple cloud data warehouses to protect the privacy of IoT data. The objective of the technique is to decompose IoT data, store it in multiple warehouses, and reaggregate it when a consumer requests it without exposing anything beyond what is allowed. The solution avoids the single point of attack/failure problem by distributing the system and using Paillier's Cryptosystem properties, which allows recovery of analyzed IoT data without exposing the raw data.

3) N-tier architectures: [21] proposes a lightweight and anonymous authentication scheme for wearable devices with the help of a cloud server. The scheme enables mutual authentication while keeping the anonymity of IoT devices. Only lightweight cryptographic operations including hash function and exclusive-or operations are employed. The proposed system can be divided into three phases: initialization, pairing, which allows the smartphone and wearable device to know about each other's existence, and authentication, which builds the session key for transmitting information after pairing. However, the authors consider that the cloud server was trustworthy due to its own security mechanism. Thus, the cloud server stores all critical identity information about both the user's mobile device and smartphone. In the same context, PrivTAM is a system for calculating Television Audience Measurement (TAM) indices while preserving their confidentiality thanks to SmartTV technology. PrivTAM [22] receives as input the viewing records of users' SmartTVs and produces TAMs by performing secure multi-party calculations. The smartTVs actually communicate over the Internet to compute the aggregated metrics. SSL/TLS sockets are used to secure the communication between the different entities. However, PrivTAM requires the intervention of a central third party, called a TAM aggregator, which coordinates the calculation of TAMs, verifies the validity of the records, collects the encrypted results, and provides the compensation to the participants.

C. Data provenance techniques

1) Semantic-based techniques: These mechanisms aim at representing a domain in a standard format using a common notation in order to overcome the problem of heterogeneity in a given domain. Two objectives can be ensured by ontological modeling techniques, namely domain description and reasoning by inference.

In order to enable information security and privacy for smart spaces, [23] proposed a security framework, which is composed of various components collaborating together to support different aspects of security, such as authentication, authorization and access control. In addition, a role-based and context-aware access control scheme is proposed, which is modeled using ontological techniques and the Web Ontology Language (OWL) and implemented by the C Language Integrated Production System (CLIPS) rules. In this model, roles are assigned to users by the administrator when they register in the system. At runtime, privacy rules are executed to grant or deny access based on the user's role and contextual information.

In another context, [23] proposes ORDM, an ontology based resource description model, to describe resources in IoT environment. These resources are described by the attribute, state, control, historical information, and privacy classes. The Attribute class defines information inherent to the device, such as device types, model, and range of sensed values. The data description is done in the State class, which provides the current data captured by the sensor with its associated data unit. The Privacy class protects the device from illegal access or control. A smart desktop application based on the ORDM is implemented for evaluation. However, both ORDM and the previously presented model do not provide flexible access control to the captured data. Indeed, the users who can access IoT resources are fixed in the proposed ontology without any clear reasoning or criteria. Moreover, the authors did not address the sharing of data resources during the data processing phase. In addition, only access and control permissions are considered as privacy requirements. The authors did not consider the rest of the confidentiality requirements, such as specifying the purpose, retention, and limiting disclosure.

2) Blockchain-based techniques: Based on the smart contracts, BlockPro [24] use each PUF (Physical unclonable function) to produce a single response for each device and uses it to identify the source of the data. Furthermore, a blockchain with two smart contracts is implemented to guarantee the reliability of the data. The first verifies the sourcing of the data to ensure the accuracy of the data origin. And the second is in charge of storing and collecting the data provenance in the blockchain. However, this framework does not provide the history of data processing. In counterparts, a cloud-centric secure provenance framework for IoT [25] is proposed to not only identifies the origin of data but also generates a periodic history of connected objects to overcome the limitations of BlockPro.

One of the main disadvantages of the blockchain is the time it takes for a transaction to actually take place. For example, it can take up to several hours on the Bitcoin platform due to the size of the Bitcoin network. Secondly, the consensus algorithms used in the blockchain, especially the PoW (Proof Of Work), are very greedy in terms of consumption. The same goes for data redundancy and computational redundancy, which are needed each time to decide whether or not a new block can be added to the blockchain. Finally, blockchain requires a complete model change, which means moving from a centralized to a decentralized network. This can lead to problems with the transition and integration of this technology by customers into existing ecosystems.

IV. DISCUSSIONS

Traceability approaches are appropriate solutions to address data sharing management. Ascending traceability provides the ability to trace the provenance of different data, and therefore allow users to reuse it with confidence in their own knowledge systems. On the other hand, descending traceability allows

entities to be informed where their data is distributed and in which processes it is being involved in. In order to align communication between involved IoT entities, it is necessary to define a formal semantic description using ontological modeling to describe the properties of the exchanged data in order to apply expression rule language such as control usage models, access control models, or Rule-Based Service Level Agreement [26].

The incorporation of data provenance into IoT can be effective in helping to overcome security and trust issues. However, little research has yet been carried out into that area and most of the suggested schemes converge towards direct applications of data provenance rather than the development of a general data provenance management system that can be embedded within various contexts for "data quality" assessment. Existing systems continue to face the following limitations :

- Legal requirements for IoT security in Europe are rarely considered through the building of IoT data management systems. In 2018, according to the GDPR, users are to be put at the core of the data prevention processing systems and be sufficiently informed in order to make autonomous choices, as well as to have the technical means to impose their requirements on the data requirers. More specifically, the right of informational self-determination consists of granting users the control over the uses that are made of their assets. Therefore, the goal is not only the protection of users's private data, but also to provide them the necessary tools to make autonomous choices and thus take decisions that they deem appropriate.
- Flexible data provenance management is expected if a data requester within the system does not adhere to the rules set by the data owner when using his assets. The system must remain loose enough not to shut down all access at once, which would lead to a disruption of the entire ecosystem. In this context, we need to provide an agile system that allows the user to be aware of whether their requirements are being met, but also gives the data requesters a chance to account if they violate the rules.
- In collaborative environments and multi-organizational structures, companies agree on common long-term goals such as customer satisfaction, economic growth and reputation preservation. Nevertheless, their operational objectives and strategic visions are different and vary from one organization to another, leading to a potentially biased quality of the produced data. In this context, the policy management system must have the ability to take into account the various sources of the collected data as well as their different levels of granularity, therefore providing a dynamic and adaptive security policy.

V. CONCLUSIONS AND FUTURE DIRECTIONS

Provenance metadata can answer critical questions for different use cases, especially challenges related to "Data Quality" and Data Governance: determining the origin of a data item allows us to ensure if it meets the technical and legal requirements of a given activity and to assess its quality.

Our research is a work in progress, and we are currently engaged with the technical foundation to conduct further evaluations to develop an ontology constructed based on existing models that propose a standard vocabulary for smart cities, and enrich it with our own specific requirements. Ontological reasoning, which relies mainly on the accurate definition of concepts and their relations, can take advantage of the general reusability of ontologies and gain further knowledge by going beyond a specified domain. A modeling formalization of the control of use of data based on the uniformed representation established before comes to build a sematic rule manager, that will in its turn be incorporated in a Data Provenance system in order to build a privacy mechanism.

This research work is in line with several large schemes aimed to provide efficient management within the digital world. From a quality management perspective, ensuring that data is consistent, up to date and conforms ensures that it is relevant to each entity's individual goals and organizational standards. From a legal point of view, a law-abiding IoT environment is a new challenge that the legislative community has to deal with. To comply with it, audit mechanism based on policies must be enforced on how a data should be controlled during its life cycle. On a parallel perspective, IoT main goal is to provide trusted high-quality services and innovative solutions to its users by transforming the captured data into meaningful information. In this context, it is in the best interest of the community to encourage entities within IoT environment to share their data, and therefore help contribute to overall public interest, generate technological progress, and build the next generation of services for greater convenience and value. The more data is made available, the more it boosts IoT ecosystems. In order to achieve this, it is essential to reassure all the agents implicated throughout the process about the credibility of their own knowledge systems. Merging data provenance mechanisms with a semantic model based on rules is an appropriate solution to address the data sharing management and build a civilized digital community in which data is the centerpiece.

Data-driven models are growing rapidly and becoming essential in all sectors. In this context, data governance has evolved from a privacy matter to a multidimensional issue with implications for various sectors including economics, law enforcement, and even geopolitics. Poor protection of citizens' data due to limited jurisdiction, lack of users's trust, and limited access to data are concerns that can be addressed by establishing a firm data management solution.

This paper aims to introduce data provenance and model based rule manager as a privacy preservation mechanism for IoT applications in various domains. Our broad analysis of existing research has allowed us to build a vision and identify guidelines in order to infer privacy and security coverage in IoT context. Our privacy ontology is being developed in an ongoing smart agriculture research project, we intend to build our inference system by proposing robust rules and integrate the result into a data provenance mechanism to achieve a privacy preserving system.

ACKNOWLEDGMENT

This work is supported by the Conseil Départemental des Landes (PhD grant to N.Laamech).

REFERENCES

[1] Cisco. (2016) Internet of things at-a-glance. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf?dtid=osscdc000283.

[2] A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. A. Yavuz, "Haa: Hardware-accelerated authentication for internet of things in mission critical vehicular networks," in *MILCOM 2015-2015 IEEE Military Communications Conference*. IEEE, 2015, pp. 1298–1304.

[3] M. Munier and V. Lalanne, "Data controllability for risk management in smart and intelligent systems," *Journal of Internet Technology and Secured Transactions (JITST)*, 2020.

[4] I. O. for Standardization: Information technology. (2011) security techniques privacy framework, iso/iec 29100.

[5] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, p. 3152676, 2017.

[6] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2015.

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

[8] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5. IEEE, 2010, pp. V5–484.

[9] H. M. Alshahrani, "Coll-iot: A collaborative intruder detection system for internet of things devices," *Electronics*, vol. 10, no. 7, p. 848, 2021.

[10] H. Neuhaus and M. Compton, "The semantic sensor network ontology," in *AGILE workshop on challenges in geospatial data harmonisation, Hannover, Germany*, 2009, pp. 1–33.

[11] S. Wang, Y. Hou, F. Gao, and S. Ma, "Ontology-based resource description model for internet of things," in *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, 2016, pp. 105–108.

[12] M. Gao, C.-Q. Jin, X.-L. Wang, X.-X. Tian, and A.-Y. Zhou, "A survey on management of data provenance," *Chinese Journal of Computers*, vol. 33, no. 3, pp. 373–389, 2010.

[13] P. Buneman, A. Gascon Caro, L. Moreau, and D. Murray-Rust, "Provenance composition in PROV," 2017.

[14] C. Sáenz-Adán, L. Moreau, B. Pérez, S. Miles, and F. J. García-Izquierdo, "Automating provenance capture in software engineering with uml2prov," in *International Provenance and Annotation Workshop*. Springer, 2018, pp. 58–70.

[15] H. Olufowobi, R. Engel, N. Baracaldo, L. A. D. Bathen, S. Tata, and H. Ludwig, "Data provenance model for internet of things (iot) systems," in *International Conference on Service-Oriented Computing*. Springer, 2016, pp. 85–91.

[16] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "Appa: An anonymous and privacy preserving data aggregation scheme for fog-enhanced iot," *Journal of Network and Computer Applications*, vol. 125, pp. 82–92, 2019.

[17] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[18] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2017, pp. 173–178.

[19] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[20] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Generation Computer Systems*, vol. 76, pp. 540–549, 2017.

[21] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[22] G. Drosatos, A. Tasidou, and P. S. Efraimidis, "Privacy-enhanced television audience measurements," *ACM Transactions on Internet Technology (TOIT)*, vol. 17, no. 1, pp. 1–29, 2017.

[23] S. Hosseinzadeh, S. Virtanen, N. Díaz-Rodríguez, and J. Lilius, "A semantic security framework and context-aware role-based access control ontology for smart spaces," in *Proceedings of the International Workshop on Semantic Big Data*, 2016, pp. 1–6.

[24] U. Javaid, M. N. Aman, and B. Sikdar, "Blockpro: Blockchain based data provenance and integrity for secure iot environments," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, 2018, pp. 13–18.

[25] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric internet of things via blockchain smart contracts," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2018, pp. 991–998.

[26] A. Paschke, "Rbsla: Rule-based service level agreements," Ph.D. dissertation, Technische Universität München, 2007.