# *IoTCrawler: Browsing the Internet of Things*

Antonio F. Skarmeta, José Santa
Department of Information and Communication Engineering
University of Murcia
Murcia, Spain
{skarmeta, josesanta}@um.es

Juan A. Martínez
Odin Solutions S.L
Alcantarilla, Spain
jamartinez@odins.es

Josiane X. Parreira
Department of Corporate Technology
SIEMENS
Wien, Austria
josiane.parreira@siemens.com

Payam Barnaghi, Shirin Enshaeifar
Department of Electrical and Electronic Engineering
University of Surrey
Guildford, United Kingdom
{p.barnaghi, s.enshaeifar}@surrey.ac.uk

Michail J. Beliatis, Mirko A. Presser
Department of Business Development and Technology
Aarhus University, Birk Center park 15, 7400
Herning, Denmark
{mibel, mirko.presser}@btech.au.dk

Thorben Iggena, Marten Fischer, Ralf Tönjes
University of Applied Sciences Osnabrück
Osnabrück, Germany
{t.iggena, m.fischer, r.toenjes}@hs-osnabrueck.de

Martin Strohbach
AGT International
Darmstadt, Germany
mstrohbach@agtinternational.com

Alessandro Sforzin, Hien Truong
NEC Laboratories Europe
Heidelberg, Germany
{alessandro.sforzin, hien.truong}@neclab.eu

***Abstract*— The Internet of Things (IoT) offers an incredible innovation potential for developing smarter applications and services. However, today we see solutions in the development of vertical applications and services reflecting what used to be the early days of the Web, leading to fragmentation and intra-nets of Things. To achieve an open IoT ecosystem of systems and platforms, several key enablers are needed for effective, adaptive and scalable mechanisms for exploring and discovering IoT resources and their data/capabilities. This paper discusses our work in the EU H2020 IoTCrawler project. Its focus is on the integration and interoperability across different platforms, through dynamic and reconfigurable solutions for discovery and integration of data and services from legacy and new systems. This is complemented with adaptive, privacy-aware and secure solutions for crawling, indexing and searching in distributed IoT systems. IoTCrawler targets IoT development and demonstrations with a focus on Industry 4.0, Social IoT, Smart City and Smart Energy use cases.**

***Index Terms*—Internet of Things, crawling, discovery, indexing, ranking, Cyber-physical systems, security.**

## I. Introduction

Efficient and secure access to Big IoT Data will be a pivotal factor for the prosperity of European industry and society. However, today data and service discovery, search, and access methods and solutions for the IoT are in their infancy, like Web search in its early days. IoT search is different from Web search because of dynamicity and pervasiveness of the resources in the network. Current methods are suited for static or available resource repositories. There is yet no adaptable and dynamic solution for effective integration of distributed and heterogeneous IoT data and support of data reuse in compliance with security and privacy needs, thereby enabling a true digital single market. Previous reports show that a large part of the developers' time is spent on integration[1]. In general, the following issues limit the adoption of dynamic IoT-based applications:

- The heterogeneity of various data sources hinders the uptake of innovative cross-domain applications.
- Data records without embedded metainformation lack of utility for expending its usefulness across platforms.
- Missing security and neglected privacy present the major concern in most domains and are a challenge for constrained IoT resources.
- The large-scale, distributed and dynamic nature of IoT resources requires new methods for crawling, discovery, indexing, physical location identification and ranking.
- IoT applications require new search engines, such as bots that automatically initiate search based on user's context. This requires machine intelligence.

[1] https://www.gartner.com/doc/3221917/iot-data-proliferation-elevates-data

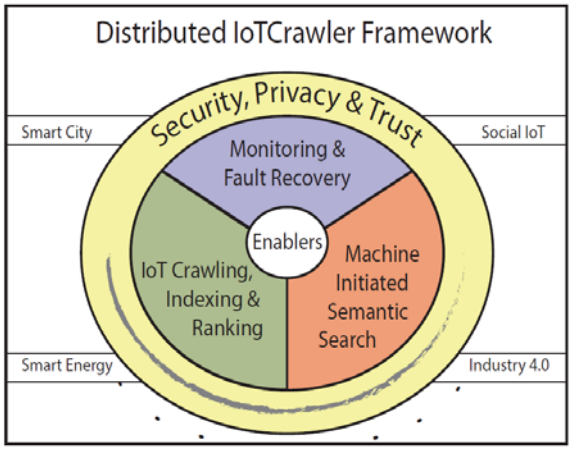


Fig. 1. Key concepts of the IoTCrawler proposal

- The complexity involved in discovery, search, and access methods makes the development of new IoT enabled applications a complex task.

Some ongoing efforts, such as Shodan[2] and Thingful[3] provide IoT searching solutions, but they rely mainly on a centralised indexing and manually provided metadata. Moreover, they are rather static and neglect privacy and security issues. To enable the use of IoT data and to exploit the business potential of IoT applications an effective approach needs to provide:

- An adaptive distributed framework enabling abstraction from heterogeneous data sources and dynamic integration of volatile IoT resources.
- Security, privacy and trust by design as integral part of all the processes from publication, indexing, discovery, and subscription to higher-level application access.
- Scalable methods for crawling, discovery, indexing and ranking of IoT resources in large-scale cross-platform and cross-disciplinary systems and scenarios.
- Machine initiated semantic search to enable automated context dependent access to IoT resources.
- Monitoring and analysing the Quality of Service (QoS) and Quality of Information (QoI) to support fault recovery and service continuity in IoT environments.

IoTCrawler is an EU H2020 project that addresses the above challenges by proposing efficient and scalable methods for crawling, discovery, indexing and ranking of IoT resources in large-scale cross-platform and cross-disciplinary systems and scenarios. It develops enablers for secure and privacy-aware discovery and access to the resources, and monitors and analyses QoS and QoI to rank suitable resources and to support fault recovery and service continuity. The project evaluates the developed methods and tools in various use-cases, such as Smart City, Social IoT, Smart Energy and Industry 4.0. The key elements of IoTCrawler are shown in Fig. 1.

The project aims to create scalable and flexible IoT resource discovery by using meta-data and resource descriptions in a dynamic data model. This means that searching actions could result in non-optimal results that could fit the user expectations.

For this, the system should understand the user priorities (which are often machine-initiated queries and search requests) and provide the results accordingly by using adaptive and dynamic techniques.

The rest of the paper is organised as follows. Section II describes the main architecture of the framework proposed in IoTCrawler. Section III details the use cases where the system is being validated. Section IV addresses the state of the art in the main areas of the project, identifying also its key innovations. Finally, Section V concludes the paper and presents the next activities to cover.

## II. Architecture of IoTCrawler

IoTCrawler provides novel approaches to support an IoT framework of interoperable systems including security and privacy-aware mechanisms, and offers new methods for discovery, crawling, indexing and search of dynamic IoT resources. It supports and enable machine-initiated knowledge-based search in the IoT world. Fig. 2 depicts the IoTCrawler framework and highlights its key components, which are detailed next.

### *A. IoT Framework of Interoperable (Distributed) Systems*

The diversity of the market has resulted in a variety of sophisticated IoT platforms that will continue to exist. However, to evolve and enable the full benefits of IoT, these platforms need access to data, information and services across various IoT networks and systems within an integrated ecosystem of IoT systems and platforms. IoTCrawler envisions a cooperation of platforms and systems to provide smart integrated IoT based services. Instead of defining an overarching hyper-platform on top, IoTCrawler aims at integrating the platforms and systems by proposing a common interface enabling cooperation and interconnection of various platforms through making their data and services discoverable and accessible by other applications and services. An IoTCrawler enabled platform can internally be implemented in different ways; it only has to support the common and open interfaces to join the ecosystem. The open IoT interfaces are split in two planes that are called control and data planes (analogous to OpenFlow in software defined networks). The control plane will coordinate and control the data and information processing in the platforms (monitoring and quality analysis). The data plane will allow for IoT data flow exchange between platforms (crawling, indexing and search).

### *B. Holistic Security, Privacy and Trust*

An ecosystem of IoT platforms brings immense benefits but also potential risks for users and stakeholders. The very principle that makes the IoT so powerful - the potential to share data instantly with everyone and everything - creates huge security and privacy risks. Since IoT systems are, by their nature, distributed and operate often in unprotected environments, the maintenance of security, privacy, and trust is a challenging task.

[2] http://www.shodan.io/

[3] http://thingful.net/

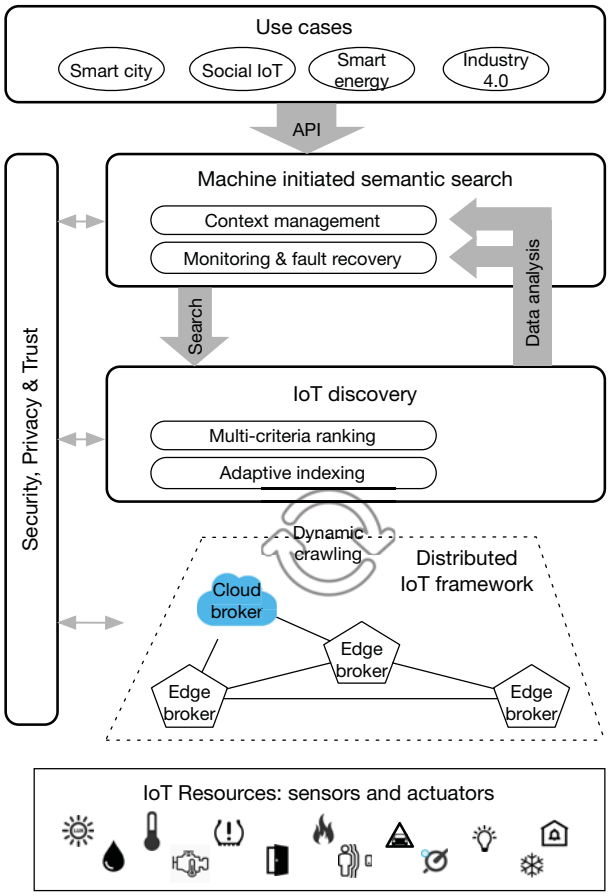


Fig. 2 Overall architecture of the IoTCrawler framework

IoTCrawler addresses quality, privacy, trust and security issues by employing a holistic and end-to-end approach to the data and service publication to search and access workflow. Device and connectivity management will ensure that the end devices only connect to trusted access networks. IoTCrawler develops solutions for mitigating privacy intrusion and data correlation based on data collected from multiple sources. Both technical and information governance procedures and guidelines are defined and implemented. This makes sure that the technical solutions are in place for avoiding the security and privacy risks, and also appropriate information governance procedures and best practices and measures are followed in development, deployment and utilisation of the use-cases and third-party applications.

### *C. Crawling, Discovery and Indexing of Dynamic IoT Resources*

Information access and retrieval on the early days of the Internet and the Web mainly relied on simple functions and methods. For example, Yahoo's first search engine was simply based on the "grep" function in Unix or the AltaVista search engine initially did not have a ranking mechanism. The Internet and the Web have gone a long way in the past two decades to improve the way we access the information on the Web. There are several sophisticated methods and solutions that provide crawling, indexing, ranking and search and retrieval of extremely large volumes of information on the Internet. The new generations of Web search engines have now focused on information extraction and personalised and customised knowledge and extraction techniques and solutions. Some early works are demonstrated by Google's knowledge graph, Wolfram Alpha and Microsoft Bing. The current information access and retrieval methods on the IoT are still at the same stage that the Web and the Internet were in their early days. Information retrieval on the large-scale IoT systems is currently based on the assumption that the sources are known to the devices and consumers or it is assumed that opportunistic methods will send discovery and negotiation messages to find and interact with other relevant resources in their outreach (e.g. Google's recent Physical Web project is designed based on this assumption). Overall, IoT systems have more ad-hoc resources that do not comply with document and URL processing and indexing norms; the resources, such as mobile phones and sensing devices, can publish data and then move to another location or disappear. Service and data crawling and discovery for smart connected devices and services will also involve automated associations and integration to provide an extensible framework for information access and retrieval in IoT. IoTCrawler focuses on providing reliable, quality and resource-aware and scalable mechanisms for data and services publishing, crawling, indexing in very large-scale distributed dynamic IoT environments.

### *D. Machine-Initiated Semantic Search*

In the past, search engines were mainly used by human users to search for content and information. In the newly emerging search model, information is provided depending on the users' (human user or a machine) context and requirements (for example, location, time, activity, previous records, and profile). The information access can be initiated without the user's explicit query or instruction but used on its necessity and relevance (context-aware search). This will require machine interpretable search results in semantic forms. Moreover, social media, physical sensors (numerical streaming values), and Web documents must be better integrated, and the search results should become more machine interpretable information rather than remaining as pure links (e.g. the Web search engines mainly return a list of links to the pages as their results; with some exceptions on popular questions and topics).

IoTCrawler enables context-aware search and automated processing of data by semantic annotation of the data streams, thus making their characteristics and capabilities available in a machine processable way. There are several existing works that provide methods and techniques for semantic annotations and description of the IoT devices, services and their messages and data. However, most of these methods rely on centralised solutions and complex query mechanisms that hinder their scalability and wide scale deployment and use for the IoT. IoTCrawler supports an ecosystem of multiple platforms and develops dynamic semantic annotation and reasoning methods that will allow continuous and seamless integration of new devices and services by exploiting and adapting existing annotations based on similarity measures.

The automatic discovery has to consider the current context. Context-awareness requires the integration and analysis of social, physical and cyber data. IoTCrawler develops enablers for context-aware IoT search. Hence the requirements of the different applications are mapped to the solutions by selecting resources considering parameters such as security and privacy level, quality, latency, availability, reliability and continuity. IoTCrawler improves reliability and robustness by fault recovery mechanisms and mitigation of malfunctioning devices using device activation/deactivation in the associated area. The fault recovery also requires mechanisms to support communication among networked IoT resources located in diverse locations and across different platforms, and to provide secure and efficient re-distribution of information in case of failure.

## III. Use Cases

IoTCrawler is currently evaluating its technologies in four real world use-cases: Smart Cities, Social IoT, Smart Energy, and Industry 4.0. Further use-cases will be identified and ranked in co-creation workshops with the relevant stakeholders within the project.

### *A. Smart City*

The city of Aarhus has been considered as a target smart city deployment in the project. IoTCrawler helps to overcome the negative perceptions of Internet of Things and Smart Cities by smart city experimentation tools for Aarhus' City Lab that can make citizens and companies engaged and be curious about smart city solutions. IoTCrawler also provides the enabling technologies to discover new data sources in Aarhus for Open Data platforms and has the potential to become a reference platform supporting IoT data and service sharing as part of the sharing economy. To track the performance of a smart city, IoTCrawler develops enablers for monitoring activity and quality of the sensors. This can be used to set up KPI's for City Labs and to track its performance. The smart city deployment of Murcia is also considered in IoTCrawler, exploiting the large sensor platform installed.

An especial application for smart city is improving well-being of citizens, supporting the treatment of mental health conditions with IoT. IoTCrawler tackles this challenge by creating a safe route planner that can guide individuals with social anxiety around the city to avoid large crowds by utilising different data sets e.g. big events in the city, big crowds at public places, traffic, and incoming tourists or to help expose them to crowds as part of their treatment. This use case could also be turned into a route planner that could help citizens navigate home safely at night by planning a route in crowded areas/paths and by avoiding areas with high crime rates.

### *B. Social IoT*

Social IoT relates to using sensors deployed at sports and entertainment events in order to quantify the performance of professionals or experience of participants. This enables participants to engage in events beyond simply watching, thus creating a unique personal record of their experience, and in combination with social and digital media allows event manager to create new insights and content for their audience. IoTCrawler has access to over 800 events, including fashion events (e.g. New York Fashion week), culinary events, sports events (e.g. Basketball Final Four), or events such as Miss Universe. For each event, sensors are deployed at local venues and participants and spectators are equipped with wearables. This results in a range of diverse data sets that are collected, analysed, stored, and used, e.g. for content creation. Discovering and semi-automatically describing existing sensors, data sets and streams using IoTCrawler technologies has the potential to significantly increase the overall value of the dataset access and their integration, making it accessible to a larger group of people and enabling new applications. As described above, the data sets include raw sensor data and processed analytic results. However, data processing often involves data from other third-party sources, for instance play-by-play data is used to correlate analytical results to match events and social media sources can be used to link to user generated content. IoTCrawler's discovery, indexing and search enablers have the potential to significantly reduce the effort associated with the integration of sensor technologies, and other external data sources.

### *C. Smart Energy*

Smart Buildings play an important role in distributed energy systems as they turn from energy consumers to the so-called energy prosumers. In future energy systems, Smart Buildings actively interact with the Smart Grids in order to stabilise the Smart Grid or participate in energy trading as well as for structural condition monitoring and proactive maintenance. For this purpose, buildings offer semantically annotated properties of the technical equipment within buildings especially energy flexibilities (i.e. for shifting electrical and thermal loads). In this frame, this use-case employs the technologies developed in IoTCrawler to dynamically discover the flexibilities of Smart Buildings and analyse their potential as well as their demand for applications that are necessary to manage and offer energy to the Smart Grid or the energy market. This information can be used by energy retailers or grid operators to deploy best fitting applications to individual buildings. The project uses semantic enrichment of grid data and data analytics to enhance smart grid applications to reduce the need for manual engineering and setup of systems.

### *D. Industry 4.0*

Industry 4.0 includes advances such as predictive maintenance, energy prediction, or human-robot collaboration. The results of IoTCrawler will be used to improve predictive maintenance planning for horizontal machining centres in aerospace and Die&Mould industries. Currently data integration often consumes more than 80% of the time. IoTCrawler has the potential to significantly accelerate the development and deployment of Industry 4.0 analytics solutions by discovering and semi-automatically integrating machine metadata, sensor data provided by the machines and information stored in related enterprise databases. Extending the discovery to actuator services (e.g. air conditioning, heating, and machine operation) allows to link actions for avoiding load peaks to energy analytics pipeline.

IoTCrawler also increases the workers' safety by identifying critical conditions (e.g. gas exposition) in the permanent sensor data stream of drones and forward such condition markers to monitoring teams and production management subsystems.

## IV. Main Innovations in the Areas of Research

The literature within key areas of the IoTCrawler proposal is reviewed next, indicating the main innovations of the work within the general framework described in Section II.

### *A. Search and Discovery*

Being essential for any network architecture, one of the key components of the proposed architecture is the search and discovery operation. In the domain of IoT there are proposals that have passed the standardisation pipeline and others still maturing in the research literature [1]. Providing high scalability degree in the storage as well as flexible support for query and update operations, is offered by the Distributed Hash Table (DHT), which is a totally decentralised system that stores data objects for easy and quick access (query) and update (store). DHTs are built on top of overlay networks into which network objects are spread and identified with unique keys, e.g. the well-studied overlay network and DHT Chord mechanism [2], which is the direct ancestor of Kademlina [3] (BitTorrent's DHT). Overlay networks and DHTs are well suited to form the basement of a proper discovery mechanism, such as the Overlay Management Backbone (OMB) approach [4]. To add suitable schema evolution to the information/content discovery, description mechanisms such as the Resource Description Framework (RDF) and JSON-LD [5] are needed. Combining a DHT mechanism with RDF, it can be found, for example, RDFPeers [6], which proposes to use an adapted version of RDQL [7] to perform the queries. The main problems of this approach are that it consumes a lot of storage space and that it is not efficient for simple searches. SPARQL [8] is the de facto query language for RDF by providing a coherent and simple search mechanism.

The IoTCrawler approach exploits the remarkable qualities of the overlay network and DHT described above to build the base components of the IoTCrawler discovery and using its nodes to build the distributed infrastructure. However, the nodes are deployed in separate administrative or network domains to distribute both the storage/finding load and the management of information access.

### *B. Security for IoT*

There are international initiatives in recent years to cover security aspects in IoT, such as IERC, ITU-T SG20, IEEE IoT Initiative4 or IPSO Alliance. However, there is not a unified vision on security and privacy in the domain. In the IoT, data confidentiality and authentication, access control within the networks, privacy and trust among users and things are among some of the key issues [9].

IoTCrawler explores the use of advanced cryptographic techniques based on Attribute-Based Encryption (ABE). Specifically, it analyses the application and extension of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as a flexible and promising cryptographic scheme in order to enable information to be shared while confidentiality is still preserved. In CP-ABE, the cipher-text embeds the access structure to describe which private-keys can decrypt it and the private-key is labelled with descriptive attributes. IoTCrawler addresses the integration of CP-ABE with different signatures schemes to provide end-to-end integrity to the information that is shared for anticipatory purposes. Users are given means to define how their personal information is shared and under which circumstances using a policy-based approach. Additionally, IoTCrawler investigates the integration of this solution within the search and discovery process for IoT.

The Blockchain paradigm [10] is also included in IoTCrawler. A Blockchain is a distributed database that maintains a growing set of transactions in a way that is designed to be secure, transparent, highly resistant to outages, auditable, and efficient, at the same time it is distributed. However, despite the benefits that Blockchain technologies offer, we still need to overcome two major challenges in IoTCrawler: privacy: since transactions tend to be public, and encryption still allows the remaining nodes in the system to learn about the occurrence of a particular exchange in the system; and scalability, because existing permission-less blockchains such as Bitcoin are only able to scale to a considerable number of nodes at the expense of attained throughput.

Moreover, IoTCrawler will leverage Trusted Execution Environments (TEEs) to enhance the security primitives deployed in the proposed framework, given that existing TEEs suffer from a number of shortcomings, especially with respect to their security and privacy provisions.

In the area of Authentication, Authorisation and Accounting (AAA), IoTCrawler proposes a lightweight access control scheme for IoT as presented in [11,12]. We propose a mechanism for interoperability of different authentication and authorisation solutions based on a bridge to third party elements such as the standard stacks as LDAP and FIWARE Service Enablers to support a lightweight federation-like approach.

### *C. Data Validation and Quality Analysis*

The assessment of Quality of Data can basically be evaluated in five common dimensions: Completeness, Correctness, Concordance, Plausibility and Currency. In [13] the authors provide a table of different terms used to describe one of the dimensions of data quality. Furthermore, they provide a mapping between data quality dimensions and data quality assessment methods. In [14] Sieve is introduced, a framework to flexibly express quality assessment methods and fusion methods. The STAR-CITY project [15] describes a system for semantic traffic analytics. Based on various heterogeneous data sources (e.g., Dublin bus activity, events in Dublin city) their system is able to predict future traffic conditions with the goal to make traffic management easier and to support urban planning.

One of the major challenges in the assessment of a quality metrics to sensory IoT data is the lack of ground truth. The authors of [16] and [17] developed and evaluated a concept for the assessment of node trustworthiness in a network based on data plausibility checks. They propose that every node performs a plausibility check to identify malicious nodes sending faulty data. Similar to this work, they use similar data sources in order

to find "witnesses" for a given sensor reading. The authors in [18] propose three different approaches to deal with a missing ground truth in social media: spatiotemporal, causality, and outcome evaluation. Their concept to use spatiotemporal evaluation to predict future behaviour of humans is similar to the proposed IoTCrawler approach, disregarding that we evaluate past events. Prior work of the authors emphasised the importance of an appropriate distance model reflecting infrastructure, e.g., roads, and physics, i.e. traffic or air movements [19]. The approach in IoTCrawler refines the state of the art by utilising sensor and domain independent correlation and interpolation models whilst incorporating knowledge of the city infrastructure to evaluate data stream plausibility.

## V. Conclusions

This paper presents the key ideas and the architecture of a crawling and discovery engine for the Internet of Things resources and their data. We describe our work in the context of the H2020 project. IoTCrawler proposes a framework to make possible the effective search over IoT resources. The system goes beyond the state of the art through adaptive, privacy-aware and secure algorithms and mechanisms for crawling, indexing and search in distributed IoT systems. Innovative technological developments are proposed as enablers to support any IoT scenario. We discuss four use cases of the platform, which are presented in the areas of Smart Cities, Social IoT, Smart Energy and Industry 4.0. The project is currently implementing the envisaged framework, at the same time the main interoperability issues are considered to support the real-life uses cases identified.

## Acknowledgment

This work has been sponsored by the European Commission, through the IoTCrawler project (contract 779852), and the Spanish Ministry of Economy and Competitiveness through the Torres Quevedo program (reference PTQ-15-08073).

## References

[1] A. Broring, S. K. Datta and C. Bonnet, "A Categorization of Discovery Technologies for the Internet of Things," in Proceedings of the 6th International Conference on the Internet of Things, (Stuttgart, Germany), pp. 131-139, ACM, 2016.

[2] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, (New York, NY, USA), pp. 149–160, ACM, 2001.

[3] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in Proceedings of the First International Workshop on Peer-to-Peer Systems, (London, UK), pp. 53–65, Springer-Verlag, 2002.

[4] L. Cheng, et al., "Self-organising management overlays for future internet services," in Proceedings of the 3rd IEEE International Workshop on Modelling Autonomic Communications Environments, (Berlin, Germany), pp. 74–89, Springer-Verlag, 2008.

[5] G. Klyne and J. J. Carroll, "Resource Description Framework (RDF): Concepts and Abstract Syntax," 2004. http://www.w3.org/TR/rdf-concepts/.

[6] M. Cai, M. Frank, B. Yan, and R. MacGregor, "A subscribable peer-to-peer RDF repository for distributed metadata management," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 2, no. 2, pp. 109–130, 2004.

[7] A. Seaborne, "RDQL - A Query Language for RDF," 2004. http://www.w3.org/Submission/RDQL/.

[8] E. Prud'hommeaux and A. Seaborne, "SPARQL Query Language for RDF," 2008. http://www.w3.org/TR/rdf-sparql-query/.

[9] Jan Henrik Ziegeldorf, Oscar García Morchon, Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges," Security and Communication Networks 7(12): 2728-2742, 2014.

[10] S. Nakamoto, "Bitcoin: A P2P Electronic Cash System," 2009.

[11] Hernandez-Ramos, J.L.; Pawlowski, M.P.; Jara, A.J.; Skarmeta, A.F.; Ladid, "L. Toward a Lightweight Authentication and Authorization Framework for Smart Objects," IEEE J. Select.Areas Commun., 33, 690–702, 2015.

[12] José L. Hernández-Ramos, Antonio J. Jara, Leandro Marín, and Antonio F. Skarmeta Gómez, "DCapBAC: embedding authorization logic into smart things through ECC optimizations," International Journal of Computer Mathematics, 93(2):345-366, 2014.

[13] N. G. Weiskopf and C. Weng, "Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research," Journal of the American Medical Informatics Association, vol. 20, no. 1, pp. 144–151, 2013.

[14] P. N. Mendes, H. Muhleisen, and C. Bizer, "Sieve: Linked data quality assessment and fusion," in Proceedings of the 2012 Joint EDBT/ICDT Workshops, ser. EDBT-ICDT '12. New York, NY, USA: ACM, 2012, pp. 116–123.

[15] F. Lecue, S. Tallevi-Diotallevi, J. Hayes, R. Tucker, V. Bicer, M. Sbodio, and P. Tommasi, "Smart traffic analytics in the semantic web with star-city: Scenarios, system and lessons learned in dublin city," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 27, pp. 26–33, 2014.

[16] N. Bissmeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in Vehicular Networking Conference (VNC), 2012 IEEE, Nov 2012, pp. 78–85.

[17] N. Bissmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications, ser. VANET '12. New York, NY, USA: ACM, 2012, pp. 73–82.

[18] R. Zafarani and H. Liu, "Evaluation without ground truth in social media research," Communications of the ACM, vol. 58, no. 6, pp. 54–60, 2015.

[19] R. Toenjes, D. Kuemper, and M. Fischer, "Knowledge-based spatial reasoning for IoT-enabled smart city applications," in 2015 IEEE International Conference on Data Science and Data Intensive Systems. IEEE, 2015, pp. 736–737.