2019-10-17

A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem

Rantos, Konstantinos

Wiley

Hindawi
Security and Communication Networks
Volume 2019, Article ID 1431578, 15 pages
https://doi.org/10.1155/2019/1431578

Research Article

A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem

Konstantinos Rantos,[1] **George Drosatos**,[2] **Antonios Kritsas**,[1] **Christos Ilioudis**,[3] **Alexandros Papanikolaou**,[3] **and Adam P. Filippidis**[4]

[1]*Department of Computer Science, International Hellenic University, Kavala, Greece*
[2]*Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece*
[3]*Department of Informatics and Electronic Engineering, International Hellenic University, Thessaloniki, Greece*
[4]*Department of Computer, Informatics and Telecommunications Engineering, International Hellenic University, Serres, Greece*

Correspondence should be addressed to Konstantinos Rantos; krantos@teiemt.gr

Received 10 December 2018; Revised 9 April 2019; Accepted 16 May 2019; Published 17 October 2019

Academic Editor: Bela Genge

In the Internet of Things (IoT) ecosystem, the volume of data generated by devices in the user's environment is continually increasing and becoming of particular value. In such an environment the average user is bound to face considerable difficulties in understanding the size and scope of his/her collected data. However, the provisions of the European General Data Protection Regulation (GDPR) require data subjects to be able to control their personal data, be informed, and consent to its processing in an intelligible manner. This paper proposes ADVOCATE platform, a user-centric solution that allows data subjects to easily manage consents regarding access to their personal data in the IoT ecosystem. The proposed platform also assists data controllers to meet GDPR requirements, such as informing data subjects in a transparent and unambiguous manner about the data they will manage, the processing purposes, and periods. The integrity of personal data processing consents and the immutable versioning control of them are protected by a blockchain infrastructure. Finally, the paper provides a prototype implementation of the proposed platform that supports the main consents management functionality.

1. Introduction

A significant proportion of Internet of Things (IoT) devices, which according to published reports will be more than 75 billion by 2025 [1], will soon surround users and will collect data that are likely to threaten users' privacy. These data can be used to monitor users, create users profiles, evaluate certain personal aspects related to the data subject, i.e., for profiling, and make automated decisions with questionable technical and organizational measures to protect user rights and freedoms [2, 3]. It is evident that most of the users will not be able to cope with this vast amount of data, sufficiently understand the scope of the data collected and the different processing methods, and have control over their personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) [4]. Even if GDPR compliance is secured, users should be aware of it. This will facilitate trust establishment among users, their IoT devices, and the corresponding services, which is considered as one of the success factors of the IoT. Users expect these devices to respect their privacy and keep data safe.

The need to provide users with the ability to control their personal data generated by smart devices in their environment is widely recognised [5]. The European Research Cluster on the Internet of Things (IERC) also highlights this need with an additional emphasis on the GDPR [6]. However, the extensive research work that has been carried out in the field of user-centric privacy solutions does not address privacy requirement in the IoT ecosystem [7] in light of the GDPR. The latter defines the conditions under which data processing is lawful, which include processing (a) on the basis of a data subject's consent, (b) for the needs of a contract, (c) for

compliance with a legal obligation, (d) to protect the vital interests of the data subject, (e) for the needs of the public interest, and (f) for the legitimate interests of the controller.

In the IoT ecosystem, and especially in segments like smart health and smart homes, processing will be accomplished not only for the needs of a contract and for protecting the vital interests of the data subject but also on the grounds of users' consents, for data that are not covered by a contract, or where there is no contract. This is likely for manufacturers, vendors, or service providers which might already have a contractual relationship with the data subject but also by third parties which, without having a contractual relationship with the data subject, will be very keen to gain access to smart devices for their own business or governmental needs. For instance, the local energy provider or the government might want to have access to the power consumption of the deployed air-conditioning units in a city for statistical purposes. The local fire department might want to have access to deployed smoke detectors to minimize response times. The local police might want to gain access to a security camera during an emergency call. In such and similar situations, consents should be given only as a result of a declaration provided by the data controller in an easily accessible manner for the data subject. According to the GDPR, the data controller should use clear and plain language and allow separate consents to be given to different data processing operations.

In this paper, which is an extended version of work published in [8, 9], we present ADVOCATE, a platform that aims to provide an environment that facilitates data controllers' interaction with data subjects and, more importantly, provide more control to data subjects on their consents, in line with the GDPR requirements. In particular, following a user-centric approach to the development of IoT solutions [10], this framework covers the main principles of GDPR according to which data controllers will, among others, be able to inform the user in a transparent and unambiguous manner about

(i) any personal data they are about to manage and their sources of origin

(ii) the entity(ies) that will process it and recipients or categories of data recipients

(iii) any personal data they are about to manage and their sources of origin

(iv) the purposes, time periods, and legal basis of the processing

(v) the existence of automated decision making, including profiling, as well as possible further processing for purposes other than the one for which they were collected

Similarly, data subjects will

(i) be immediately and comprehensively informed about requests for processing their personal data

(ii) be able to provide their consents

(iii) be able to withdraw their consents in a straightforward and unambiguous manner

(iv) be able to create privacy preferences and define specific data processing rules

(v) be aware of the security and quality of the consents they have given

All provided consents handled by the system will be authenticated and integrity-protected using digital signatures and blockchain technology. Apart from the integrity of consents, blockchain is used to ensure consents versioning so that the corresponding competent authority or a court of law will be able to easily resolve any disputes between a data controller and a data subject with regard to lawful processing of personal data, should the need arise. The provided immutable versioning control identifies the latest consents as well as periods that specific consents were valid, in an undisputable manner, as all consents' updates are logged and historical data are secured. As a result, both the consents' integrity and validity periods are secured, thus protecting the user from a data controller and vice versa, which might attempt to present to the court an altered consent or a consent that was valid during another period. Note that monitoring of data controller's adherence to a consent is out of the scope of this paper, although it is in the authors' plans to investigate in the future, i.e., provide policy-based access control to personal data with the support of a blockchain infrastructure [11, 12].

The remainder of this paper is organized as follows. Related Work describes the related work. ADVOCATE Architecture specifies the proposed framework and its components. Choosing the Most Appropriate Blockchain Infrastructure presents an analysis regarding the deployment of an internal blockchain as opposed to using external to ADVOCATE services, and Reference Implementation presents a reference implementation of the proposed framework. This last section concludes the paper with suggestions for future work.

2. Related Work

Several research efforts have been made in the direction of developing suitable protocols for security and privacy in the IoT, which is not considered an easy task [13]. The framework proposed in [14] allows users to set their privacy preferences for the IoT devices they interact with. Communications are performed via a central gateway, which ensures that the transmitted data is in accordance with the set user preferences. Furthermore, blockchain technology is employed to both protect and manage the privacy preferences that each user of the system has set, thus ensuring that no sensitive data has been accessed without their consent. The framework, however, does not consider GDPR requirements and the much-needed interaction with data controllers for providing consents.

The use of blockchain gateways is also proposed in [15], where the setup is tailored for use with IoT scenarios, and, more specifically, with legacy devices. In particular, the user can use the same account for connecting to different blockchain-enabled gateways rather than having to register to each gateway, thus enhancing practicality. These gateways

effectively play the roles of mediators, handling the various requests/responses to/from the devices accordingly.

There are also ongoing research efforts regarding user-centric security and privacy in IoT, such as the UPRISE-IoT project [16], where the user's behaviour and context are taken into consideration, so as to elevate security and privacy in a privacy-preserving manner. Apart from enabling the users to fine-tune the level of privacy, it makes them aware of what information is being protected as well as the value of the aforementioned information. Good practices to be considered for obtaining user consent for IoT applications in the healthcare domain are also proposed in [17].

The work presented in [18] involves the use of a semi-autonomous context-aware agent, which takes decisions on behalf of the user. The agent takes into consideration context, behavior, and a community-based reputation system in order to reach a decision. Despite the fact that the system allows the user to retain control, it may be the case that it may fail to choose the intended privacy options in cases that fall outside the observed behaviour.

Another approach for providing informed consents is presented in [19]. The proposed framework enables users to have a clear understanding about the exact way their personal data will be used by the system. The specific solution targets only Cooperative Intelligent Transport Systems though. A policy-based approach is followed, where the data owners specify a priori the rules for accessing and using their data.

The authors in [20] propose a protocol suitable for smart homes, where a central controller is used for handling key management and all underlying secured communications in a centralised manner. Any communication among devices is only feasible through this controller, which also has the ability to configure the network's devices for ensuring the preservation of privacy. Furthermore, the authors present detailed protocols for smart agents to communicate with the central controller that ensure message integrity and authentication.

In [21], attribute-based encryption is employed and is combined with the well-known μTESLA protocol [22] for real-time user authentication so as to offer location privacy to the participating devices.

A lightweight RFID medical privacy protection scheme is proposed in [23]. Its authors claim that it requires low computing resources and give extensive proofs regarding its ability to satisfy the security requirements of anonymity, replay attack resistance, synchronisation, forward security, and mutual authentication as well as nondenial of service.

In [24], the authors present a robust data access mechanism that ensures the confidentiality of the access policy against all unauthorised entities in a multiauthority scenario, even the attribute authorities. The scheme is adapted for use-cases where outsourced data needs to be accessed through smart watches and IoT devices, which usually collect sensitive personal information in such scenarios. The scheme was implemented on contemporary embedded devices (smartphone, smartwatch, and a Raspberry Pi B+) and the evaluation results were quite promising.

The EnCoRe project [25] has also developed mechanisms in which subjects can set consent policies and manage them. However, EnCoRe was not designed for the IoT ecosystem. Instead it was centred on employees' data on an organizational context and on how user's privacy policy is enforced within the organization. The framework proposed in the present work borrows certain aspects of the EnCoRe solution, adapted to the IoT environment, while adopting enhanced GDPR-compliant ontologies to provide a solid mechanism for managing data subjects' consents.

ADVOCATE addresses the challenges related to privacy protection in the IoT, especially with regard to the management of consents, as GDPR requires and tries to fill a significant gap in this area. It allows users to manage their consents and formulate their personal data disposal policies. Similarly, it provides data controllers with a useful tool for being GDPR-compliant. In contrast to the majority of previous works where a gateway is needed to implement users' privacy policy, ADVOCATE takes a more dynamic and technology neutral approach of requesting and providing consents and therefore focuses on establishing an interoperable environment to facilitate interaction between data subjects and controllers.

3. ADVOCATE Architecture

The ADVOCATE approach assumes an IoT ecosystem where sensors deployed on devices that operate in the user's environment collect and exchange data related to the data subject. Such environments include a smart home, a patient health monitoring system, or activity monitoring sensors. The use of a portable device, such as a mobile phone, is considered a key component that provides a focal point for controlling IoT devices and a user-friendly environment for data subjects to interact and manage their personal data disposal policy and consents. It also provides the means and a central point by which a data controller interacts with data subjects and obtains the necessary consents. The proposed architecture focusing, for the sake of simplicity, on smart cities and health ecosystems, is depicted in Figure 1.

ADVOCATE is a trusted cloud-based service that acts as an intermediary among data subjects and controllers. It is responsible for relaying data access requests issued by data controllers and obtaining the corresponding consents from the data subjects, in a predefined format that will ensure interoperability among them. It is also responsible for maintaining the user's policy and protecting the consents' integrity and versioning, based on a blockchain, which will ensure that no unauthorized modifications will be made to the consents provided by data subjects. Note that ADVOCATE does not intervene in data exchanges and does not have any access to data collected by data subject's IoT devices as also depicted in Figure 1. Data acquired by IoT devices are made available to data controllers either directly or through the user's mobile phone. The functional components of ADVOCATE are described in the following sections.

3.1. Consent Management Component. In the core of ADVOCATE is the *consent management component*, which is responsible for managing users' personal data disposal policies and the corresponding consents, including generation, updates, and withdrawals. Utilising this component, data

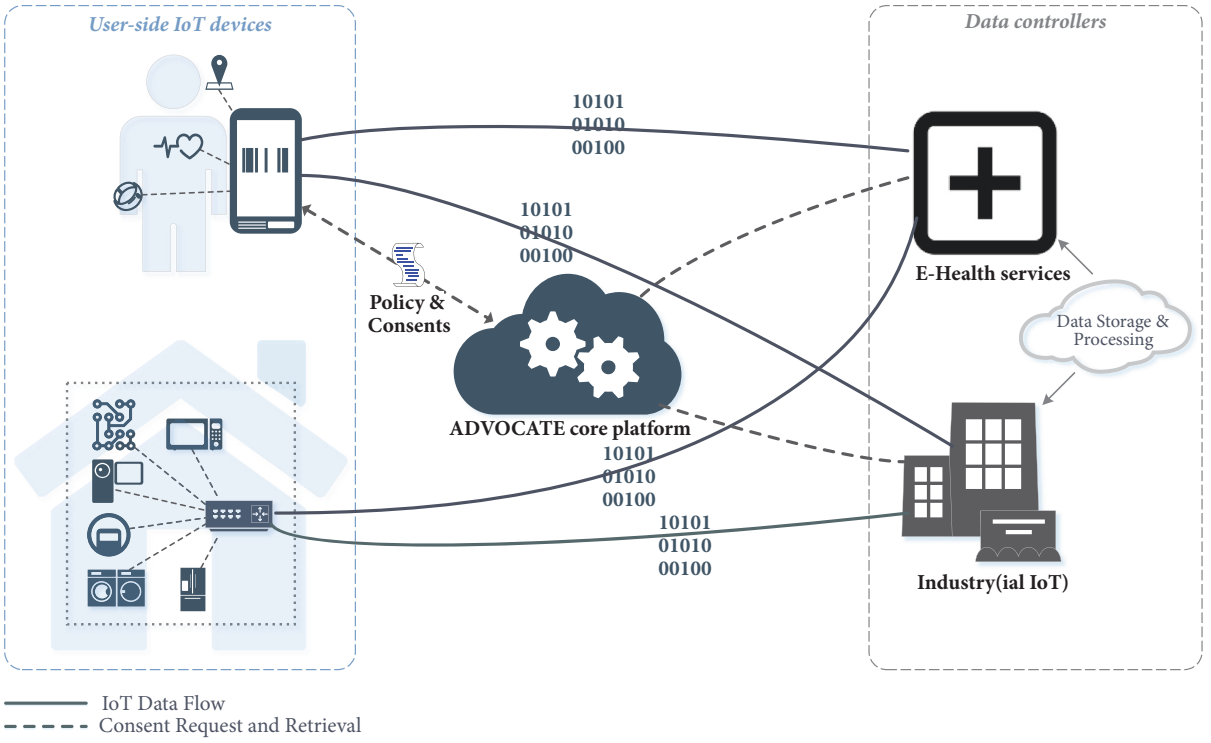


Figure 1: ADVOCATE conceptual architecture.

subjects are able to create generic, domain-specific, or context-based privacy policies comprising a set of rules that correspond to data subjects' consents. The latter is the result of requests placed by data controllers for access to specific IoT data, for definite processing purposes and periods, in line with the GDPR requirements.

Having an interoperable mechanism for placing requests, granting permissions, and formulating policies requires relying on common rules for defining data sets, as well as the meaning and the use thereof. This ensures that (JSON formatted) data controller access requests are projected to data subjects in a unified, clear, and unambiguous manner. The process of creating a new consent for access to data subject's data as shown in Figure 2 consists of the following steps:

(1) Prior to creating any consents, the data subject has to register his/her IoT device with the platform. This process will typically be accomplished using a controlling device at the data subject's environment, such as his mobile phone. Specific characteristics of the IoT device are recorded to ensure that the IoT device is easily searchable by the platform based on its type or the sets of data it acquires. Registered devices together with the types of data they acquire might be searchable through the platform for all third parties wishing to have access to such data, under data subject agreement and without disclosing any private information about the data subject at this stage. Optionally, the device can also be registered, through the platform, with the data controller. Such registration with the data controller is a quite common situation if the data controller is the device manufacturer or vendor. Note that this step is not necessary for the services provided by the ADVOCATE platform.

(2) A data controller wishing to gain access to data acquired by a registered IoT device can place a request through the platform specifying the details with regard to the GDPR requirements, such as the sets of data and the access period, as well as the types and purposes of processing.

(3) The request is properly formatted and presented to the data subject (e.g., using his mobile phone app, or the web-based interface) to review and decide about giving his consent or denying access. The data subject will be able to modify the details of the request, such as excluding specific data sets, or altering the access period. His decision is sent to the platform.

(4) Assuming a positive response, the platform sends the consent to both entities to be signed.

(5) The signed responses are sent back to the platform and are used for preparing the appropriate input values that would be inserted in the blockchain via a smart contract (see Consent Notary Component).

(6) Finally, the smart contract's input values are stored to the blockchain and the user's access policy is updated.

The foundation of this interoperable mechanism is the adoption of an appropriate ontology. Ontologies solve in principle the IoT device heterogeneity problem, contributing to the

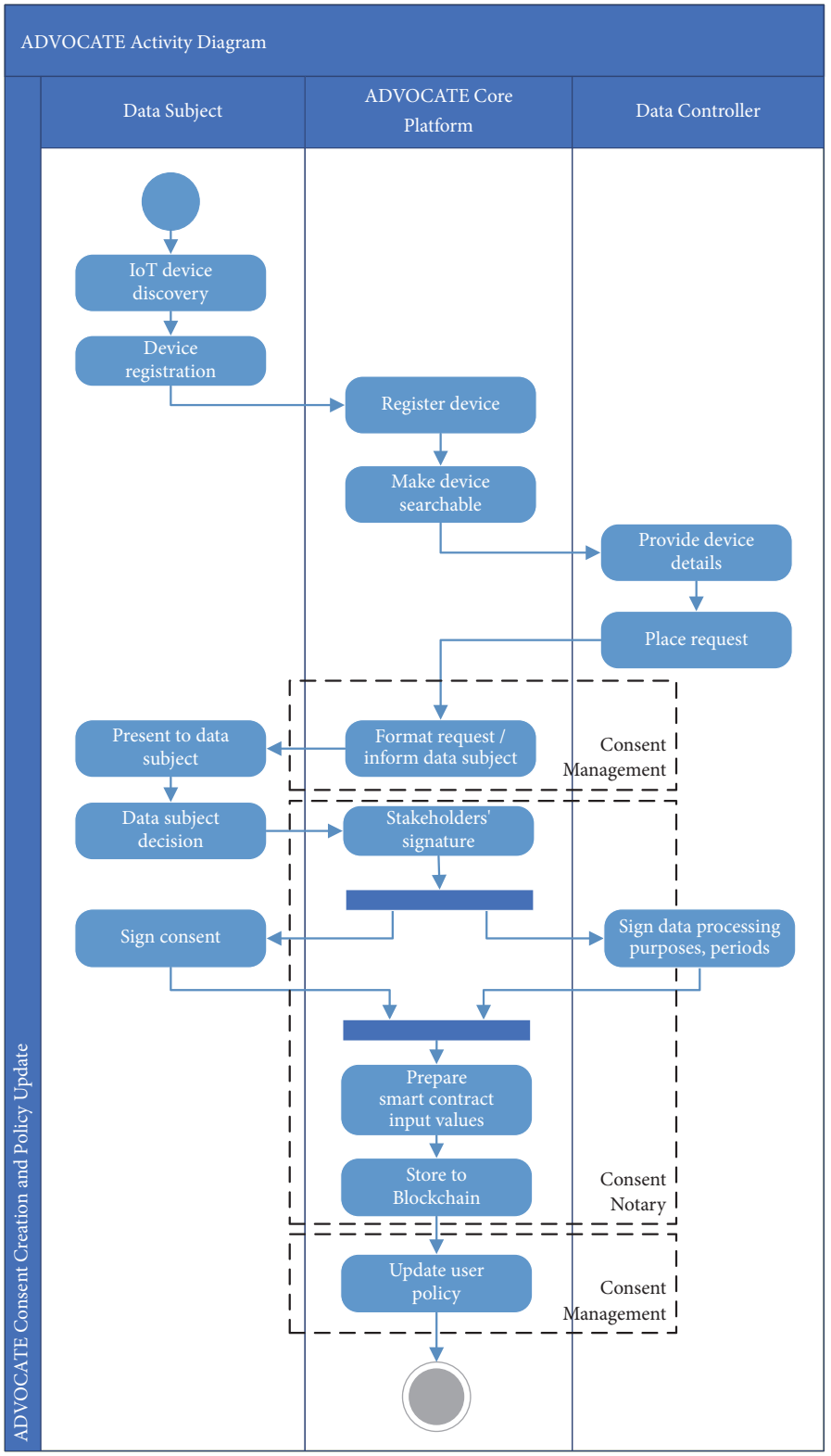


Figure 2: Interaction of ADVOCATE components during the introduction of new consents.

safety and privacy of users [5]. They also facilitate semantic heterogeneity in the field of Internet security with user-defined rules [26]. Moreover, they contribute to the description of threats, attacks, impacts, controls, and vulnerabilities and the definition of relationships among them, with many important advantages [27].

Several ontologies have been defined to support privacy and allow users to express access control rules for sharing Resource Description Framework (RDF) or W3C Web Ontology Language (OWL) modelled data. The authors in [28] observe that protecting data does not merely mean granting access or not to the full RDF data, but in most cases users require more fine-grained privacy preferences that define access privileges to specific data.

The ontology that is close to the needs of ADVOCATE is proposed in [29]. Although being a work in progress, the proposed model considers an early version of GDPR and defines an ontology to model data protection requirements to facilitate data controllers in achieving the desired GDPR compliance. By utilizing the above ontology, JSON schemas for placing requests and formatting consents are defined. The schema used by ADVOCATE for placing requests for consents is listed in Data Structure 1.

Adopting an appropriate ontology for data privacy also facilitates the specification of enforceable privacy policies. This implies that the description of policies is based on well-defined policy languages, such as the eXtensible Access Control Markup Language (XACML), to assist in the decision-making process. In [30] the authors use W3C OWL to propose an ontology for sharing and processing sensitive patient data. They also highlight the advantage of having policies that conform to a widely adopted policy language standard. EnCoRe [25] has also adopted XACML for enforcing policy-based access control. The transformation of consents to XACML based privacy policies that will be deployed in the user's environment is one of the issues that will be further investigated by the authors.

3.2. Consent Notary Component. The *consent notary component* constitutes an important and structural component of the proposed architecture responsible for providing integrity, versioning control, nonrepudiation, and validity of data subjects' consents and data controllers' commitments. To ensure these security features for the given consents, we adopt digital signatures and the usage of blockchain technology [31]. Blockchain technology was firstly introduced to secure transactions in Bitcoin cryptocurrency [31] and nowadays has a wide range of applications to IoT [32], to smart contracts and digital content distribution [33], and even to the biomedical domain [34, 35]. The consent notary component acts as a mediator between the consent management component and a blockchain infrastructure. Additionally, it assures that the generated consents (and the corresponding policies) are up-to-date and protected against malicious or unauthorized attempts to repudiate or alter them. Apart from that, the usage of blockchain infrastructure ensures the immutability of all the given consents and acts as a logger that captures all the changes on them in a distributed manner, thus avoiding the risk of making ADVOCATE a single a point of failure.

In ADVOCATE, we focus on the concept of smart contracts that have been introduced by Ethereum [36], which defines the rules and penalties around an agreement in a similar fashion that a conventional contract does, but also automatically enforces these obligations. In public blockchains, such as Bitcoin [31] and Ethereum [36], all the transactions are public and there is no direct link to the actual user identities. However, in applications that require nonrepudiation, identities should be irrevocably maintained; this can be ensured by the appropriate use of public key infrastructure solutions [37, 38]. In ADVOCATE, the consents are digitally signed by the contracting parties to provide the nonrepudiation. Moreover, in order to ensure their anonymity, only the consents' hashed version is deployed to a blockchain infrastructure.

The steps followed by this component to secure a consent are presented in Figure 3 and are described as follows. As a first step, the consent notary component takes as input the agreed consent from the consent management component. This consent might be a new one, an update following changes occurred in the corresponding policies among the parties, or a withdrawal notice. Subsequently, a request is sent to both the data controller and the data subject to independently sign the data consent. These signatures can be later used in a dispute, if necessary, while versioning can demonstrate the exact time periods that this consent was valid, to cover any consent updates or withdrawal. Afterwards, the hash only (e.g. SHA-256 or Keccak-256 hash algorithm used by the Ethereum [36]) of both digital signatures is submitted to the blockchain infrastructure using an interaction process with the blockchain infrastructure.

Overall, the smart contract represents a specific IoT device of a data subject and manages all the given consents (initial, updated, or withdrawal) for this device for all data controllers to whom access is granted to the data acquired by this device. Also, it is only deployed in the blockchain once, with the first given consent. Each update on the initial consent or even its final withdrawal is managed by the smart contract and each data contract represents a different version of the consent for a data controller. This structure of the smart contract allows verifying whether a specific consent is the last version of it. Thus, the usage of a blockchain infrastructure, apart from the consents' integrity, ensures the versioning and the withdrawal notice of consents. The workflow of this interaction process is shown in Figure 4 and considers the following cases:

(1) *No consent has been given for the* IoT *device.* In this case, the consent notary component deploys in the blockchain infrastructure a new smart contract that will be responsible to manage all subject's consents for this IoT device. The hash value of the initial consent and the hash value of the data controller identification are added using the smart contract.

(2) *The data controller has not received a prior consent.* The hash value of the data controller identification and the hash value of this initial consent provided to this data controller are added to the smart contract.

```
{
"$schema": "http//...",
"$id": "http://...",
"title": "ConsentRequest",
"description": "Placing a request to a data subject for a consent",
"type": "object",
"properties": {
  "Controller": {
   "description": "Defines the controller's identity as this is displayed in Certificate's
   common name",
    "type": "string"
  },
  "DataSubject": {
   "description": "Defines the data subject's identity",
   "type": "object",
   "properties": {
    "firstName": {
     "description": "The person's first name.",
     "type": "string"
    },
    "lastName": {
     "description": "The person's last name.",
     "type": "string"
    },
    "age": {
     "description": "Age in years which must be equal to or greater than zero.",
     "type": "integer",
     "minimum": 0
    }
   }
  }
 },
 "PersonalData": {
 "description": "Defines the kind of personal data collected for processing",
 "type": "array",
 "items": {
   "type": "string"
 },
 "minItems": 1,
 "uniqueItems": true
 },
"SensitiveData": {
 "description": "Defines the data are sensitive",
 "type": "boolean"
 },
 "ChildData": {
 "description": "Defines whether the data are related to a child",
 "type": "boolean"
 },
 "DataProcessing": {
 "description": "Details about the type of processing",
"type": "object",
 "properties": {
   "Purposes": {
     "description": "Lists the processing purposes",
     "type": "string"
   },
   "ProcessingActivity": {
     "description": "The kind of activity related to personal data processing",
     "type": "string"
```

Data Structure 1: Continued.

```
60      },
61      "ProcessingMode": {
62        "description": "Defines whether processing is automated",
63        "type": "boolean",
64      },
65      "Profiling": {
66        "description": "Defines whether automated processing includes profiling",
67        "type": "boolean"
68      },
69      "Recipient": {
70        "description": "Defines whether data are sent to third parties",
71        "type": "object",
72        "properties": {
73          "EURecipient": {
74            "description": "Identifies the European third parties that receive the personal data",
75            "type": "array",
76            "items": {
77              "type": "string"
78            },
79            "minItems": 0,
80            "uniqueItems": true
81          },
82          "NonEURecipient": {
83            "description": "Identifies the non-European third parties that receive the personal data",
84            "type": "array",
85            "items": {
86              "type": "string"
87            },
88            "minItems": 0,
89            "uniqueItems": true
90          }
91        }
92      }
93    }
94  },
95  "Retention": {
96    "description": "Defines the retention period for these data",
97    "type": "object",
98    "properties": {
99      "startDate": {
100     "description": "The starting date.",
101     "type": "string"
102     },
103     "endDate": {
104     "description": "The end date.",
105     "type": "string"
106     }
107   }
108 },
109 "required": ["Controller","DataSubject","PersonalData","SensitiveData","ChildData",
"     DataProcessing"]
110 }
```

Data Structure 1: Consent request schema.

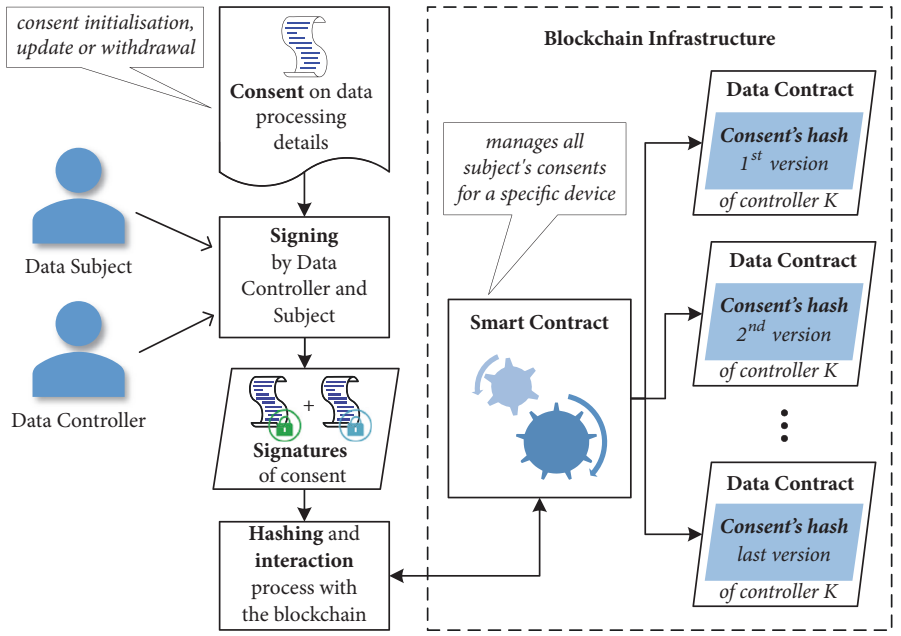


Figure 3: The steps followed by the consent notary component to submit consents' hashed version in the blockchain infrastructure.

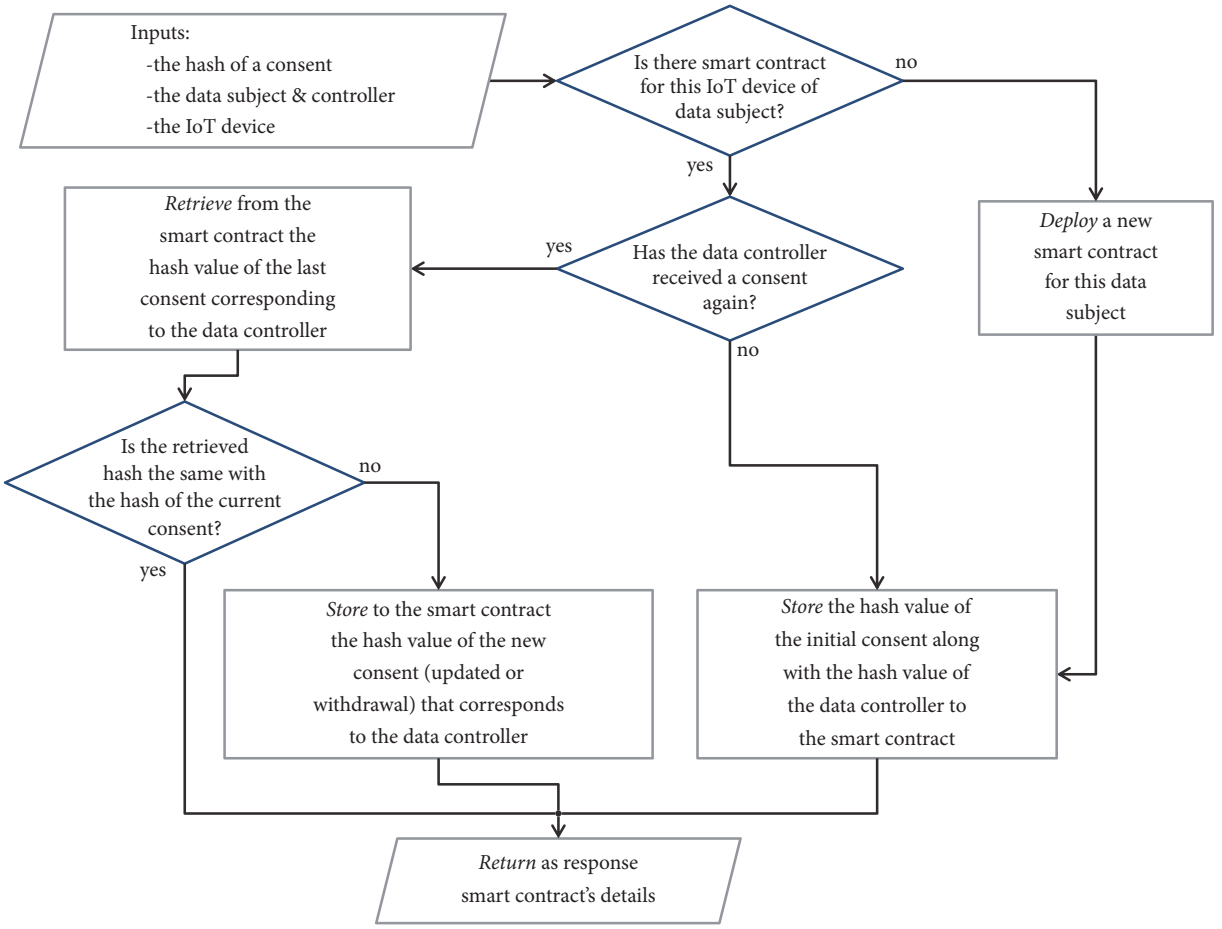


Figure 4: The workflow of interaction process between the consent notary component and the blockchain infrastructure.

```
01: pragma solidity ^0.4.23;
02: contract ConsentPerDataSubjectDevice{
03:   mapping (bytes32 => ConsentVersion) controller;
      //the address of the ADVOCATE platform
04:   address private ADVOCATE = 0x583031d1113ad414f02576bd6afabfb302140225;
05:   bytes32 subjectHash = 0xd35f61ad141d7b92f4c17e609ef394292ca0e9341942c55...;
06:   bytes32 deviceHash = 0xa018a0957ed590aeb053fa0561ea90453e260eca1846f...;
07:   struct ConsentVersion{
08:     bytes32[ ] consentHash;
09:     mapping (bytes32 => uint256) timeStamp;
10:   }
      //Function 1: add new consent for a data controller
11:  function addConsent(bytes32 _ctlhash, bytes32 _csthash) public{
12:     require(msg.sender == ADVOCATE); //only the owner can add new values
13:     controller[_ctlhash].consentHash.push(_csthash);
14:     controller[_ctlhash].timeStamp[_csthash] = now;
15:   }
      //Function 2: return the hash of the last consent for a data controller
16:   function getLastConsent(bytes32 _ctlhash) view public returns (bytes32){
17:     if (controller[_ctlhash].consentHash.length == 0) return 0;
18:     else return controller[_ctlhash].consentHash[controller[_ctlhash].consentHash.length - 1];
19:   }
      //Function 3: return the time of consent for a data controller
20:   function getTime(bytes32 _ctlhash, bytes32 _csthash) view public returns (uint256){
21:     return controller[_ctlhash].timeStamp[_csthash];
22:   }
      //Function 4: return all the consents for a data controller
23:   function getAll(bytes32 _ctlhash) view public returns (bytes32[ ]){
24:     return controller[_ctlhash].consentHash;
25:   }
26: }
```

Contract 1: Smart contract of a consent per device of data subject.

(3) *The data controller has received a prior consent.* The consent notary component interacts with the smart contract (by calling the appropriate function) that will return the hash value of the last consent to this data controller. The notary component compares the hash value that is retrieved from the smart contract with the hash value of the current consent. In this case, there are two subcases:

   (a) *The hash values of consents are not the same.* The consent notary component interacts with the smart contract and for the specific data controller adds the hash value of the new consent (updated or withdrawal). In this way, the smart contract contains all the hash values of the consents to a data controller and it can identify their last version.

   (b) *The hash values of consents are the same.* In this case, the notary component does not need to add any information to the smart contract.

Finally, the consent notary component returns the current version of the signed consent with the corresponding signatures to the consent management component, accompanied by the smart contract's address on the blockchain.

The source code of the smart contract that is shown in Contract 1 is written in Solidity language (https://solidity.readthedocs.io) and represents what is deployed to the Ethereum blockchain infrastructure. More specifically, this contract supports four basic functions: the first one adds new consents (initial, updated, or withdrawal) for a data controller, the second function returns the hash of the last consent for a specific data controller, the third returns the time that a specific consent was given to a data controller, and the fourth function returns all the consents that are given to a specific data controller over the time.

At any time, the data controller and the data subject (or any other authorised third-party) can verify the validity of the consent: (1) by validating the digital signatures on the consent and (2) by retrieving the respective data contract, i.e., the last version, from the blockchain infrastructure via the smart contract and comparing the retrieved hash with a new hash of the consent digital signatures. The usage of a blockchain infrastructure is crucial for our platform to secure the provided consents and validation of all versions thereof, in a distributed and publicly verifiable way without a single trusted third-party. The digital consents with the corresponding signatures are stored for each contracting party on ADVOCATE platform, while the blockchain infrastructure

```
# ADVOCATE Device:
    "Owner":"5af3a64f2848d418c425e80f",
    "DeviceID":"5c804c0f2f64c7100ce1b31423",
    "Vendor":"VendorA",
    "DeviceType":"Lamp",
     "PersonalData":["deviceworkinghours","lightcolor","location"]
```

Data Structure 2: Registered device information stored on the database.

only manages their hashes. Moreover, the generated hashes (especially of data subject and controller) are appropriately salted per smart contract to avoid any linkability issues among different smart contracts that correspond to the same data subject or data controller. The smart contracts are deployed using the private key of the platform for digitally signing the transactions in the blockchain. The privacy of data subjects is preserved by utilising this information distribution among the parties. Only the contracting parties know the data subjects' identity, thus preventing any leaks from the blockchain infrastructure.

4. Choosing the Most Appropriate Blockchain Infrastructure

In a public blockchain, like Ethereum, substantial amounts of electric power are drawn as a consequence of the consensus mechanism [39]. This is mainly because the distributed consensus is achieved via Proof-of-Work (PoW), a computationally intensive hashing-based challenge [40]. Indicatively, in ADVOCATE, if we use the actual publicly available Ethereum blockchain infrastructure, the cost of Contract 1 in our solution is as follows: deployment cost: 1.03€; initial consent to a data controller: 0.22€; and updating or withdrawing consent: 0.18€. These prices were calculated on 19 September 2018 (1 Ether = 179.78€) and using as average price of 'gas' 14 Gwei (1 Gwei = 1 M Nanoether). It becomes evident that this cost for a big number of IoT devices and corresponding consents per year will most likely be not affordable for data controllers (and/or data subjects), especially when the prices of cryptocurrencies are not fixed and also depend on the computational cost of PoW consensus algorithm.

Thus, our proposal in ADVOCATE is to use a different approach as a blockchain infrastructure where a consortium (or federated) blockchain would be maintained by a partially distributed network which includes nodes provided by selected entities/organizations. In this approach, it is not needed to use PoW as consensus algorithm. A Proof-of-Authority (PoA) algorithm, which requires less messages exchanges and offers better performance [41], is acceptable for this usage. In PoA, the transactions and blocks are validated by approved accounts known as validators. Due to the number of transactions and the nature of the PoA algorithm, only one typical server per data controller, with no special specifications, could be enough for this scenario. These servers could be maintained by the data controllers and their total number could be equal to the number of data controllers (i.e., IoT providers). In this way, the same data controllers can guarantee the integrity of provided blockchain and consequently the security of the given consents. This approach is still secure against malicious data controllers, if the majority of them (> 51%) are honest, something that is reasonable in our case.

Finally, it is possible to perform an accurate cost analysis of both approaches based on variables extracted from the literature, such as the IoT growth [1], the GDPR market growth, and the energy consumption growth. However, this analysis is out of scope of this work and it is in our plan to perform it as a research work to a different scientific audience.

5. Reference Implementation

A reference implementation for the device registration and consent management component of the proposed architecture based on cutting edge technologies, such as Node.js (https://nodejs.org) and MongoDB (https://www.mongodb.org), and the ontology defined in [1] can be found in https://github.com/AnthonyK95/adplatform. For the needs of the reference implementation, the data controller is considered to be the vendor of a device.

The platform allows registered users to register new personal devices by providing the device name, serial number, and type of device. The platform stores the provided information to the database using a prebuilt schema shown in Data Structure 2, while the registered device is assigned by the platform a unique id.

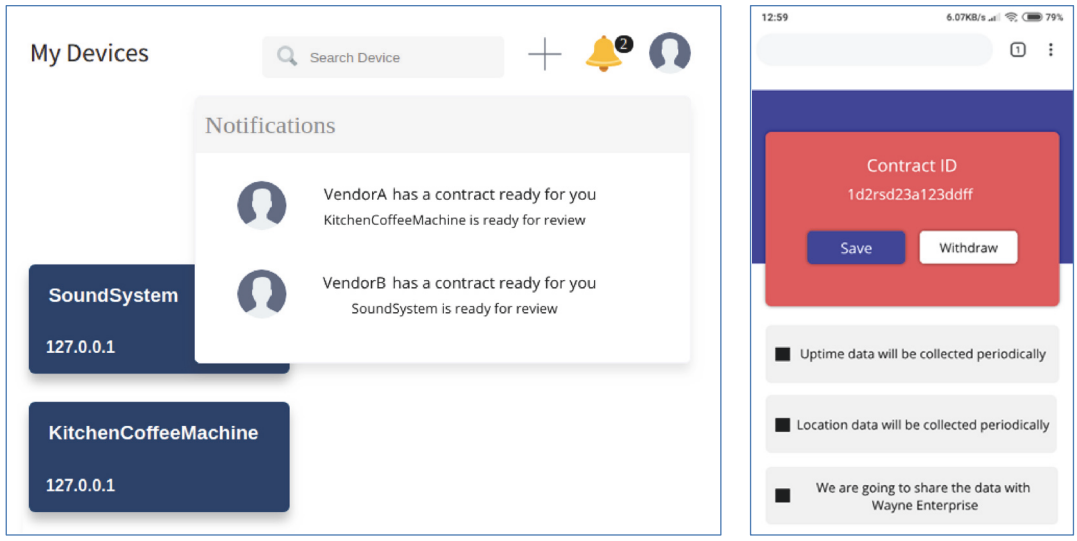
After the successful registration of a new device, the vendor gets a notification about it with the corresponding device id, namely, "deviceID." The vendor's id, namely, "vendorID," located at the serial number of the device, allows the platform to identify the corresponding vendor.

The vendor creates a contract request with all the necessary data privacy information and sends it to the user. Note that this will most likely be an automated process for the vendor. Moreover, this functionality can be expanded to allow any company or organization to request access to IoT devices, e.g., of a specific type. The extract of the JSON-formatted request contains the information shown in Data Structure 3. The data subject gets notified for incoming requests as shown in Figure 5(a).

The data subject can provide his/her consent on certain aspects of processing. An example of options that can be

```
{
  "Controller":"VendorB",
  "DeviceID":"5c804c0f2f64c7100ce1b31423",
  "DeviceType":"Lamp",
  "DataSubject":{
    "Firstname":"",
    "Lastname":"",
    "Age": ""
  },
    "PersonalData":["firstname","lastname","age","deviceworkinghours"],
   "SensitiveData":false,
   "ChildData":false,
   "DataProcessing":{
     "ProcessingActivity":"For maintenance purposes",
     "ProcessingMode":true,
     "Profiling":false,
     "Recipient":{
       "EURecipient":"Company XYZ",
       "NonEURecipient":" Company WA"
     }
   }
}
```

Data Structure 3: JSON-formatted request.



(a) Notification for incoming consent request

(b) Mobile app consent request

Figure 5: Representative snapshots of reference implementation.

provided to the data subject is depicted in Figure 5(b) for mobile app.

The user's response initiates the creation of an instance of a contract which will keep all the requested data and the data subject's consent in a database entry shown in Data Structure 4. Finally, the data subjects have the ability to update their consents, view any changes made on the consents supporting consent versioning, and ask to withdraw his/her consent.

6. Conclusions

In this paper we presented ADVOCATE, a platform that addresses a significant emerging need regarding users' privacy protection in the IoT. It lays the foundations for the establishment of trust relationships among data subjects and controllers towards a GDPR-compliant IoT ecosystem. The platform provides an interoperable mechanism for data

```
{
    "ContactID":"5c804c23420f2f231456164c7100ce1b314",
    "Controller":"VendorB",
    "DeviceID":"5c804c0f2f64c7100ce1b31423",
    "DeviceType":"Lamp",
    "Status":"Confirmed",
    "DataSubject":{
        "Firstname":"John",
        "Lastname":"Doe",
         "Age":25
    },
     "PersonalData":["firstname","lastname","age","deviceworkinghours"],
     "SensitiveData":false,
     "ChildData":false,
     "ControllerSignature":"5c804c23420f2f23...",
     "SubjectSignature":"2f64c7100ce1b314...",
     "DataProcessing":{
         "ProcessingActivity":"For Maintaining Purposes",
         "ProcessingMode":true,
          "Profiling":false,
         "Retention":"Data will be collected until August 5 2020",
         "Recipient":{
             "EURecipient":"Company XYZ",
             "NonEURecipient":"Company WA"
             }
         }
    }
```

Data Structure 4: Data subject's consent.

controllers to place data access requests in a user-friendly and unambiguous manner and get the corresponding consents. It also gives data subjects the ability to manage their consents and therefore establish their personal data access policy. Consents versioning and their integrity are secured by the use of digital signatures and the deployment of a consortium blockchain network maintained by the participating data controllers, a solution that minimizes the deployment cost. As expected, running ADVOCATE on the public blockchain is expensive. Also, for higher volumes of consensus PoW algorithms would make it economically impossible to run such a service. PoA usage is the alternative solution that is proposed in this paper.

As future work, we intend to explore further issues that can significantly enhance the quality of services provided by ADVOCATE such as the development of an intelligence component. This can assist users in making the right decisions prior to providing their consents by analysing incoming requests and identifying policy rules conflicts regarding personal data disposal. As a result to this analysis, it can provide recommendations to data subjects to further protect them from unwittingly exposing their personal data. Furthermore, we aim to consider the use of policies, generated by the proposed system, in policy-based access control systems using blockchain technology [11], which will complement a personal data management solution in the IoT ecosystem. Finding appropriate ways for applying policy management access control has been identified as an essential research opportunity by IERC and other researchers in the field [7, 42].

Data Availability

The historical data about the price of "gas" and the price of "Ether," as well as for the other variables used to support the findings of this study, are included within the article.

Disclosure

Preliminary parts of this work were presented at the 15th International Conference on Security and Cryptography (SECRYPT 2018) and the 11th International Conference on Innovative Security Solutions for Information Technology and Communications (SecITC 2018).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] S. Lucero, "Iot platforms: enabling the internet of things. white paper," *IHS Technology*, 2016.

[2] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *The Computer Journal*, vol. 44, no. 9, Article ID 6017172, pp. 51–58, 2011.

[3] D. Mendez Mena, I. Papapanagiotou, and B. Yang, "Internet of things: survey on security," https://arxiv.org/abs/1707.01879 .

[4] 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*, 2016.

[5] B. Russell, C. Garlat, and D. Lingenfelter, "Security guidance for early adopters of the Internet of Things (IoT)," *White paper, Cloud Security Alliance*, 2015.

[6] IERC, *European Research Cluster on the Internet of Things, Internet of Things: IoT Governance, Privacy and Security Issues*, 2015, http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf .

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[8] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain based consents management for personal data processing in the IoT ecosystem," in *Proceedings of the 15th International Conference on Security and Cryptography*, pp. 572–577, SCITEPRESS, Porto, Portugal, 2018.

[9] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, and A. Kritsas, "ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology," in *Innovative Security Solutions for Information Technology and Communications*, vol. 11359 of *Lecture Notes in Computer Science*, pp. 300–313, Springer International Publishing, Cham, 2019.

[10] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[11] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, vol. 520, pp. 523–533, 2017.

[12] X. Zhang and S. Poslad, "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)," in *Proceedings of the IEEE International Conference on Communications (ICC '18)*, pp. 1–6, IEEE, Kansas City, Mo, USA, 2018.

[13] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *Proceedings of the 7th IEEE International Conference on Service-Oriented Computing and Applications (SOCA '14)*, pp. 230–234, IEEE, Matsue, Japan, November 2014.

[14] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[15] S. Cha, T. Tsai, W. Peng, T. Huang, and T. Hsu, "Privacy-aware and blockchain connected gateways for users to access legacy IoT devices," in *Proceedings of the IEEE 6th Global Conference on Consumer Electronics (GCCE '17)*, pp. 1–3, Nagoya, 2017.

[16] M. Musolesi, "UPRISE-IoT: user-centric privacy & security in IoT," *UK Research and Innovation*, 2017.

[17] Y. O'Connor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by design: informed consent and internet of things for smart health," *Procedia Computer Science*, vol. 113, pp. 653–658, 2017.

[18] B. Copigneaux, "Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the internet of things," in *Proceedings of the 2014 IEEE World Forum on Internet of Things, (WF-IoT '14)*, pp. 411–416, Republic of Korea, 2014.

[19] R. Neisse, G. Baldini, G. Steri, and V. Mahieu, "Informed consent in Internet of Things: The case study of cooperative intelligent transport systems," in *Proceedings of the 23rd International Conference on Telecommunications, (ICT '16)*, pp. 1–5, Greece, 2016.

[20] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," in *Proceedings of the International Conference on Identification, Information and Knowledge in the Internet of Things, (IIKI '16)*, pp. 519–524, IEEE, Beijing, China, 2016.

[21] S. Zebboudj, R. Brahami, C. Mouzaia, C. Abbas, N. Boussaid, and M. Omar, "Big data source location privacy and access control in the framework of IoT," in *Proceedings of the 5th International Conference on Electrical Engineering - Boumerdes, (ICEE-B '17)*, pp. 1–5, IEEE, Algeria, 2017.

[22] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[23] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656–1665, 2018.

[24] M. Jahan, S. Seneviratne, B. Chu, A. Seneviratne, and S. Jha, "Privacy preserving data access scheme for IoT devices," in *Proceedings of the 16th IEEE International Symposium on Network Computing and Applications, NCA '17*, pp. 1–10, IEEE, USA, 2017.

[25] E. A. Whitley and N. Kanellopoulou, "Privacy and informed consent in online interactions: evidence from expert focus groups. In: Icis 2010 Proceedings," *Association for Information Systems*, vol. 126, pp. 1–22, 2010, ISBN 9780615418988.

[26] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for internet of things," *IEEE Access*, vol. 5, pp. 21046–21056, 2017.

[27] T. Pereira and H. Santos, "An ontology based approach to information security," in *Metadata and Semantic Research*, F. Sartori, M. Ã. Sicilia, and N. Manouselis, Eds., vol. 46 of *Communications in Computer and Information Science*, pp. 183–192, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[28] A. Passant, P. Laublet, J. G. Breslin, and S. Decker, "A uri is worth a thousand tags: From tagging to linked data with MOAT," *International Journal on Semantic Web and Information Systems*, vol. 5, no. 3, pp. 71–94, 2009.

[29] C. Bartolini, R. Muthuri, and C. Santos, "Using ontologies to model data protection requirements in workflows," in *New Frontiers in Artificial Intelligence*, M. Otake, S. Kurahashi, Y. Ota, K. Satoh, and D. Bekki, Eds., vol. 10091 of *Lecture Notes in Comput. Sci.*, pp. 233–248, Springer International Publishing, Cham, 2017.

[30] H. B. Rahmouni, T. Solomonides, M. C. Mont, and S. Shiu, "Privacy compliance in european healthgrid domains: an ontology-based approach," in *Proceedings of the 22nd IEEE International Symposium on Computer-Based Medical Systems (CBMS '09)*, pp. 1–8, IEEE, Albuquerque, NM, USA, 2009.

[31] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf .

[32] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the internet of things: a systematic literature review," in *Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA '16*, pp. 1–6, IEEE, Agadir, Morocco, 2016.

[33] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, and H. Song, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PLoS ONE*, vol. 11, no. 10, Article ID e0163477, 2016.

[34] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A blockchain-based notarization service for biomedical knowledge retrieval," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 288–297, 2018.

[35] G. Drosatos and E. Kaldoudi, "Blockchain applications in the biomedical domain: a scoping review," *Computational and Structural Biotechnology Journal*, vol. 17, pp. 229–240, 2019.

[36] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[37] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile, RFC 2459, RFC Editor (Jan 1999)," https://doi.org/10.17487/rfc2459 .

[38] S. Matsumoto and R. M. Reischuk, "IKP: turning a PKI around with decentralized automated incentives," in *Proceedings of the IEEE Symposium on Security and Privacy, SP '17*, pp. 410–426, IEEE, San Jose, Calif, USA, 2017.

[39] J. Ullrich, N. Stifter, A. Judmayer, A. Dabrowski, and E. Weippl, "Proof-of-blackouts? how proof-of-work cryptocurrencies could affect power grids," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, vol. 11050 of *Lecture Notes in Computer Science*, pp. 184–203, Springer International Publishing, Cham, 2018.

[40] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain," in *Proceedings of the 2nd Italian Conference on Cyber Security, ITASEC '18*, Italy, 2018.

[41] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: a framework for analyzing private blockchains," in *Proceedings of the ACM SIGMOD International Conference on Management of Data, SIGMOD '17*, pp. 1085–1100, 2017.

[42] A. J. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.