ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology

Konstantinos Rantos[1(✉)], George Drosatos[2], Konstantinos Demertzis[1], Christos Ilioudis[3], Alexandros Papanikolaou[3], and Antonios Kritsas[1]

[1] Department of Computer and Informatics Engineering, Eastern Macedonia and Thrace Institute of Technology, Kavala, Greece
{krantos,kdemertzis,ankrits}@teiemt.gr
[2] Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece
gdrosato@ee.duth.gr
[3] Department of Information Technology, Alexander Technological Educational Institute of Thessaloniki, Thessaloniki, Greece
iliou@it.teithe.gr, alxpapanikolaou@gmail.com

Abstract. The value of personal data generated and managed by smart devices which comprise the Internet of Things (IoT) is unquestionable. The EU General Data Protection Regulation (GDPR) that has been recently put in force, sets the cornerstones regarding the collection and processing of personal data, for the benefit of Data Subjects and Controllers. However, applying this regulation to the IoT ecosystem is not a trivial task. This paper proposes ADvoCATE, a user-centric solution that allows data subjects to easily control consents regarding access to their personal data in the IoT ecosystem and exercise their rights defined by GDPR. It also assists Data Controllers and Processors to meet GDPR requirements. A blockchain infrastructure ensures the integrity of personal data processing consents, while the quality thereof is evaluated by an intelligence service. Finally, we present some preliminary details of a partial implementation of the proposed framework.

Keywords: Privacy · Internet of Things · GDPR · Consents management · Blockchain · Policy-based access control · Data privacy ontology

1 Introduction

The rapid growth of the number of deployed Internet of Things (IoT) devices that collect personal data from the user's environment is bound to threaten users' privacy. These devices share data that can be used to monitor users activities, status and characteristics, create user profiles – with or without their consent

J.-L. Lanet and C. Toma (Eds.): SecITC 2018, LNCS 11359, pp. 300–313, 2019.
https://doi.org/10.1007/978-3-030-12942-2_23

– and make automated decisions. Most of the users will experience significant challenges regarding the protection of their personal data in the IoT ecosystem, which mainly originate from the fact that the average user does not understand how these data are being collected and used. At the same time, the majority of the IoT users are particularly concerned about the exposure of their personal data, they consider privacy an important issue in the IoT and want to have personal control of their personal data. These concerns have also been highlighted in a global survey contacted by Fortinet regarding key issues pertaining to the Internet of Things (IoT) [11].

The General Data Protection Regulation (GDPR) [10], which has recently set new rules for how companies can share EU citizens' personal data, significantly addresses the above concerns and influences user-centric privacy solutions and research directions regarding privacy in the IoT ecosystem [21]. Compliance with the GDPR requirements in the IoT world, and especially in applications related to smart health and smart homes, typically requires data controllers to obtain and manage appropriate users' consents[1].

ADvoCATE aims to provide an environment to help users retain control over their personal data in the IoT ecosystem, in line with the GDPR requirements. Following a user-centric approach, the framework aims to satisfy the main GDPR requirements according to which data controllers will, among others, be able to request data subjects' consents and inform them in a transparent and unambiguous manner about (a) personal data to be managed and the sources of origin, (b) the purposes, time periods and legal basis of the processing, (c) the entity(ies) that will process it, and (d) recipients or categories of data recipients.

Similarly, data subjects, in line with the GDPR requirements [10], will (a) be informed about requests for processing their personal data, (b) be able to create privacy preferences, define specific data processing rules and give their consent, (c) have the opportunity to exercise their rights in terms of access, correction, deletion, restriction, and object to the processing, and (d) be aware of the security and quality of the licenses/consents they have given.

Moreover, ADvoCATE utilizes blockchain technology to protect the integrity and versioning of users' consents while an intelligence component analyses policy data to detect conflicts in a data subject's policy and provides recommendations to data subjects to further protect them from unwittingly exposing their personal data. This paper extends the work published in [19] and presents the details of our prototype implementation.

The remainder of this paper is organized as follows. Section 2 describes the related work. Section 3 specifies the proposed framework and its components. Section 4 presents a preliminary implementation details, while Sect. 5 concludes this paper and presents suggestions for future work.

[1] The regulation defines additional lawful bases for personal data processing that do not require users' consents, such as for the protection of data subjects' vital interests. These are out of the scope of ADvoCATE as they do not require user interaction.

2 Related Work

The need to give users the ability to control their personal data generated by IoT devices in their personal environment is widely recognised [20]. The European Research Cluster on the Internet of Things (IERC) also points this need with an extra emphasis on the GDPR [12]. However, user's privacy protection in the IoT is not an easy task [26]. One of the ways to address the privacy challenges is to find appropriate ways to apply policy-based access control. This has been recognised as an important research opportunity by IERC and other researchers in the field [21,22].

The framework proposed in [3], allows users to define their privacy preferences for the IoT devices with which they interact. Communications are performed via a central blockchain-connected gateway, which ensures that the transmitted data is in accordance with the user's preferences. Blockchain technology is employed to protect and manage the privacy preferences that each user of the system has set, ensuring that no sensitive data has been gained without their consent.

The use of Blockchain gateways is also suggested in [4], where the setup is customised for use with IoT scenarios. In particular, the same account can be used for connecting to different Blockchain-enabled gateways rather than having to register to each gateway, which is a very practical approach. These gateways effectively play the role of mediators, handling the various requests/responses to/from the devices accordingly.

Ongoing research efforts regarding user-centric security and privacy in IoT, such as the UPRISE-IoT project [14], consider users' behaviour and context to elevate protection in a privacy-preserving manner. Apart from enabling the user to fine-tune the level of privacy it also makes them aware about what information is being protected as well as the value of the aforementioned information. Good practices to be taken into account for obtaining user's consent for IoT applications in the healthcare sector are also proposed in [17].

The work presented in [6] involves the use of a semi-autonomous context-aware agent, which takes decisions on behalf of the user. The agent takes into account context, behaviour 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.

The EnCoRe project [9], 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 centered on employee data on an organisational 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 of privacy protection in the IoT, particularly with regards to the management of consents, as required by the GDPR, and tries to fill a considerable gap in this area. It permits users to manage

their consents and formulate policies for the distribution of their personal data, taking into account the corresponding recommendations provided by the platform. Likewise, it provides data controllers with a useful tool to facilitate their compliance with the GDPR.

3 Proposed Architecture

The ADvoCATE approach concerns a series of sensors in the user's environment that gather data related to the data subject. Such environments could be a patient health monitoring system, activity monitoring sensors or even a smart home. The usage of a portable device, such as a smartphone, provides data subjects with a user-friendly environment to interact and manage their consents and their personal data disposal policy. Furthermore, it provides a way for data controllers to communicate with data subjects and acquire the necessary consents. Figure 1 presents our proposed architecture and it is focused, for simplicity reasons, on health ecosystems and smart cities. In this architecture, ADvoCATE is visualised as a cloud service platform, that consists of the functional components described in the following sections, while their interaction during the creation of a new consent is presented in Fig. 2.

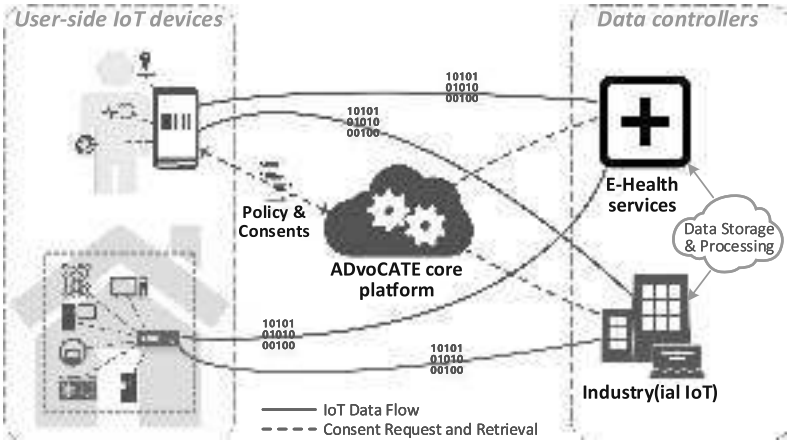

Fig. 1. ADvoCATE infrastructure.

3.1 Consent Management Component

The *consent management* component is responsible for managing users' personal data disposal policies and their respective consents, including generation, updates and withdrawals. These generic, domain-specific, or context-based privacy policies consists of a set of rules that correspond to data subjects' consents

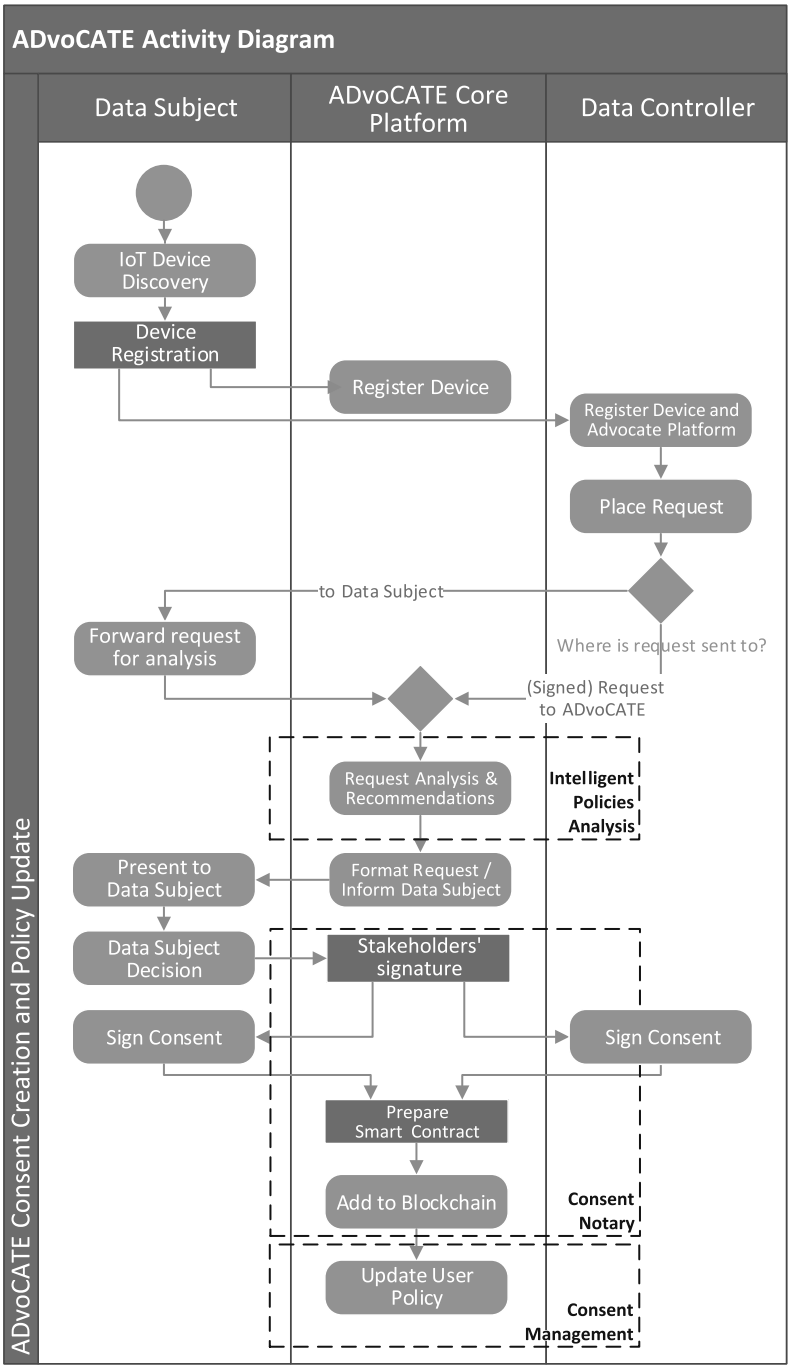

Fig. 2. Interaction of ADvoCATE components during creation of new consents.

and can be formulated as a result of requests submitted by data controllers for access to certain IoT data and for fixed processing purposes and periods, in accordance with the GDPR requirements.

One of the main challenges in establishing such a mechanism that is used across multiple sectors in the IoT ecosystem is to secure the semantic interoperability of the information exchanged among data subjects and controllers. The procedure to place requests, grant permissions and formulate policies requires that it is based on common rules for defining personal data sets and the use thereof, fine-grained privacy preferences, and access privileges. The grounds of this mechanism are data privacy ontologies, which ensure that data controller access requests are displayed to data subjects in a unified and clear manner. ADvoCATE adopted the ontology defined in [1], which models data protection requirements to facilitate data controllers in achieving the desired GDPR compliance.

In ADvoCATE, ontologies also facilitate intelligence policies analysis, as described in Sect. 3.3, and the specification of enforceable privacy policies. This suggests that policy description is based on clearly defined policy languages, such as the eXtensible Access Control Markup Language (XACML), to help the decision-making process. Using policies that conform to a widely adopted policy language standard, such as XACML, offers many advantages that have been also demonstrated by EnCoRe project [9] which has adopted XACML for enforcing policy based access control.

However, adopting a single ontology from ADvoCATE does not preclude the use of competitive or even similar ontologies by participating data controllers. In this case, ontology-matching mechanisms should be developed to reduce semantic gaps among different overlapping representations of the same data privacy-related information [18]. Such mechanisms include those based on machine learning which provide reliable and accurate matching results [8] and those based on a semi-supervised learning approach [27].

3.2 Consent Notary Component

To ensure the integrity, non-repudiation and validity of data subjects' consents and data controllers' commitments, ADvoCATE core platform adopted digital signatures and the usage of blockchain technology. Blockchain technology was firstly introduced to secure transactions in Bitcoin cryptocurrency [15] and nowadays has a wide range of applications to IoT [5], smart contracts and digital content distribution [25], and even to the biomedical domain [13]. The component that acts as mediator between the *consent management* component and a blockchain infrastructure is the *consent notary* component. It ensures that the created consents (and the respective policies) are up-to-date, they protect user's privacy and are protected against unauthorized or malicious attempts to repudiate or modify them.

The concept of smart contracts introduced by Ethereum [2] is our main focus in the ADvoCATE. A smart contract defines the rules and penalties around an

agreement, like a conventional one, and also automatically imposes these obligations. In Bitcoin [15] and Ethereum [2], all the transactions with the blockchain are publicly available and verifiable, yet there is no direct connection to the identities of the participating entities. In ADvoCATE, the consents are also digitally signed by the contracting parties to provide non-repudiation. Moreover, in order to ensure their anonymity, only the consents' hashed version are deployed to a blockchain infrastructure.

Figure 3 presents the workflow of the *consent notary* component which works as follows. As a first step, the *consent notary* component receives as entry the agreed consent from the *consent management* component. This consent could be a new one, an update of an existing one which modifies the respective policies among the parties, or a withdrawal notice. Afterwards, both the data subject and the data controller are requested to independently sign the data subject's consent. These signatures can be later used in a dispute, if necessary. Subsequently, the hash (e.g. SHA-256 or Keccak-256 hash function utilised by Ethereum [2]) of both digital signatures is submitted in the blockchain infrastructure using a *smart contract*.

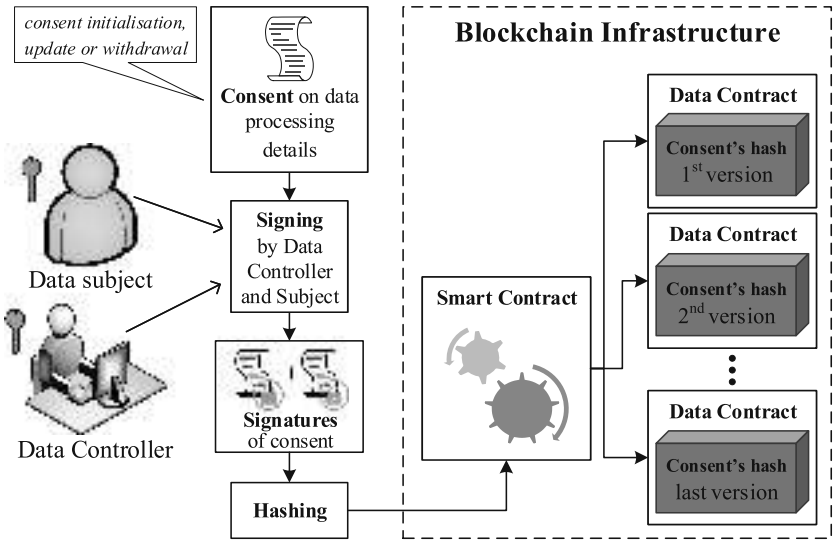

Fig. 3. The workflow of the consent notary component.

The *smart contract* between a data controller and a data subject represents a specific consent (initial, updated or withdrawal) for a particular IoT device, and is deployed in the blockchain that holds the initial consent. Thus, the *smart contract* is responsible for managing each new update of the initial consent or even its final withdrawal while a different version of the consent is represented as a *data contract*. This structure of the smart contract allows verifying whether

a specific consent is the last version of it. Apart from the consents' integrity, the usage of a blockchain infrastructure guarantees the versioning and the withdrawal of consents. Finally, the current version of the signed consent with the corresponding signatures is returned by the *consent notary* component to the *consent management* component, together with the address of the *smart contract* on the blockchain.

At any later time, the data subject and the data controller (or any other authorised third-party) can verify the validity of the consent: (i) by validating the digital signatures on the consent, and (ii) by retrieving the relevant data contract (i.e., the latest version) from the blockchain infrastructure through the smart contract and comparing the retrieved hash with a new hash of the consent digital signatures. The utilisation of a blockchain infrastructure is important for our platform to secure the given consents and validation of all versions thereof, in a public verifiable and distributed 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 is only responsible for managing the hashes of them. 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 and only the contracting parties know data subjects' identity without any leaks from the blockchain infrastructure.

3.3 Intelligence Component

The *intelligence* component is an innovative hybrid computational intelligence framework that combines an Intelligent Policies Analysis Mechanism (IPAM) to distinguish contradictory or conflicting rules/policies of a user's consents and an Intelligent Recommendation Mechanism (IReMe) to endorse in real-time adaptive intelligent policies or rules for the users' privacy strategies.

Intelligent Policies Analysis Mechanism. The Intelligent Policies Analysis Mechanism (IPAM) utilizes intelligent adaptive technologies to identify contradictory or conflicting rules and policies related to the disposal of private information and ensure that these cannot be used for user profiling. These rules or policies concern application-side information, such as the option "Forget me" (in accordance with GDPR), notifications to third-parties for deletion, exporting data, re-requesting or updating consent, encrypting data during transfer, implementing pseudonymisation, options about the available checkboxes in the consents, putting fields in the registration/profile form that are not needed, etc. This information does not concern the disclosure of data for the purpose of assessing personal aspects about a natural person, their habits, location, personal interests and other personal information, and do not compose a centralised entity that threatens users' privacy.

To achieve this, we use Fuzzy Cognitive Maps (FCM). FCM is a method used to achieve and represent the underlying knowledge, it supports causal knowledge

in reasoning process and belongs to the neuro-fuzzy systems. The latter aim to solve decision-making problems and to model/simulate sophisticated environments. Learning algorithms have been proposed for training and updating FCMs weights based primarily on ideas derived from recurrent artificial neural networks and fuzzy logic. Additionally, the learning algorithms are used to decrease the human intervention by suggesting automated FCM candidates, activating only the most relevant concepts at any time of execution, or even making models more transparent and dynamic [7]. The IPAM supervises the overall privacy of users by generating adaptive and automated rules or capabilities. In order to achieve this control, the proposed intelligence mechanism is responsible for monitoring any changes to the user's privacy statement that disturb the overall privacy based on a mapping of the agreements.

Intelligent Recommendation Mechanism. The Intelligent Recommendation Mechanism (IReMe) is a machine learning framework used for recommending personalised rules in real-time. It provides adapted, real-time and personalised information to protect users' privacy by applying an advanced machine learning method called Cognitive Filtering (CF) [24]. It makes automated estimates and predictions by gathering specific non-private information from the user. The CF approach recommends rules based on an evaluation or comparison between the contents of the items and the user's consents. The content of each item is characterised as a set of terms or descriptors. The user's consents are depicted by the same terms and created by examining the content of the items that have been already inspected by the user.

In the IReMe, we use a hybrid process that includes neighborhood-based CF and content-based filtering, which is a vigorous model-based method that expands and improves the superiority of recommendations [23]. The purpose of this mechanism is to achieve more personalised intelligent policy rules and real-time recommendations for the users' privacy strategies to avoid any privacy leakages. Furthermore, this mechanism is more flexible in the sense that it works better when the user's space is large, it scales well with unrelated items, it is easy to implement and does not involve sophisticated tuning parameters.

4 Reference Implementation

A reference implementation for the device registration and the consent management component, based on cutting edge technologies such as Node.js[2] and MongoDB[3] and the ontology defined in [1], can be found in https://github.com/AnthonyK95/adplatform.

The user-friendly interface allows registered users to add new devices and manage them together with the corresponding consents. Moreover, the platform supports the presentation of vendors' requests, policies analysis and the collection of consents to create or update a smart contract. When this sequence is

[2] https://nodejs.org.
[3] https://www.mongodb.org.

finished, the platform creates a new smart contract or update an existing one that is already deployed in the blockchain.

New personal devices can be registered by providing the device name, serial number and type of device. The platform stores the provided information to the database using the pre-built schema shown below, and the registered device is assigned by the platform a unique ID.

```
# Advocate Device:
  "_id":"5b02939aee297917f42c052",
  "owner":"5af3a64f2848d418c425e80f",
  "deviceID":741,
  "vendorID":"IoT Electronics",
  "deviceType":"Lamp",
  "__v":0
```

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, such as processing purposes and recipients, 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 specific type. The json-formatted request contains the following information.

```
{
  "PersonalData":"Uptime data collected periodically",
  "Retention":"We are going to collect data
        until August 5 2019",
  "Purpose":"Identify potential bugs",
  "EURecipient":"We are going to share the
        data with Wayne Enterprise,",
  "NonEURecipient":"We are not going to share
        your data with Non-Eu Recipients",
  "AutomatedProcessing": false,
  "Profiling": false,
  "ManualProcessing": false
}
```

The request is displayed on the user's device as shown in Fig. 4, while the user's response initiates the creation of an instance of a contract which will keep all the requested data and the user's consent in a database entry shown below.

```
{
    "_id":"5b1ff382af6c5810d00a6512",
    "PersonalData":{"Uptime data collected periodically"},
    "Purpose":{"Identify potential bugs"},
    "Response":{"Agreed to Data: Uptime data will be
                collected periodically Purpose: First Purpose"},
    "Controller":"5afd5c52a6399d1f641ca922",
    "deviceID":"5b1ff382af6c5810d00a6512",
    "deviceType":"humidity sensor",
    "Status":"Confirmed",
    "Retention":"Data collected until August 5 2019",
    "EURecipient":"We are going to share your data with Wayne
                  Enterprise",
    "NonEURecipient":"We are not going to share your data with
                     Non-Eu Recipients",
```

```
    "Company_Signature":"a243b69f8df1bec4ecfccd512405...",
    "Client_Signature":"9ed7776be1c79395504af0c8e57e...",
    "ID_Transaction":"a243b69f8df1bec4ec...",
    "AutomatedProcessing":true,
    "Profiling":false,
    "ManualProcessing":false,
    "__v":0
}
```

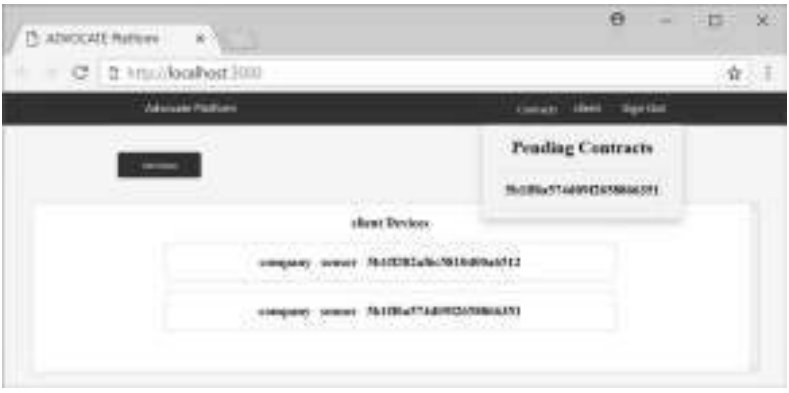

Fig. 4. Pending requests on user's device.

The source code of the smart contract that is shown in Contract 1 is written in Solidity language[4], and represents what is deployed to the Ethereum blockchain infrastructure per device. This contract manages all user's consents for a specific device and can be updated or even withdrawn over time. More specifically, the platform 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 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 time. The cost analysis of this contract at the time of our experiments on 19 September 2018 (1 Ether = 179.78€) using average price of 'gas' 14 Gwei (1 Gwei = 1 M Nanoether) is: deployment cost - 1.03€, initial consent to a data controller - 0.22€ and updating or withdrawing consent - 0.18€.

[4] https://solidity.readthedocs.io.

Contract 1. Smart contract of a consent per device of user.

```
pragma solidity ^0.4.23;
contract ConsentPerUserDevice{
  mapping (bytes32=>ConsentVersion) controller;
  //the address of the ADvoCATE platform
  address private advocate = 0x583031d1113ad414f02576bd6afabfb302140225;
  bytes32 userHash = 0xd35f61ad141d7b92f4c17e609ef394292ca0e9341942c55...;
  bytes32 deviceHash = 0xa018a0957ed590aeb053fa0561ea90453e260eca1846f...;

  struct ConsentVersion{
    bytes32[ ] consentHash;
    mapping (bytes32=>uint256) timeStamp;
  }

  //Function 1: add new consent for a data controller
  function addConsent(bytes32 _ctlhash, bytes32 _csthash) public{
    require(msg.sender == advocate); //only the owner can add new values
    controller[_ctlhash].consentHash.push(_csthash);
    controller[_ctlhash].timeStamp[_csthash]=now;
  }

  //Function 2: return the hash of the last consent for a data controller
  function getLastConsent(bytes32 _ctlhash) view public returns(bytes32){
    if(controller[_ctlhash].consentHash.length==0) return 0;
    else return controller[_ctlhash].consentHash[controller[_ctlhash].consentHash.length-1];
  }

  //Function 3: return the time of consent for a data controller
  function getTime(bytes32 _ctlhash, bytes32 _csthash) view public returns(uint256){
    return controller[_ctlhash].timeStamp[_csthash];
  }

  //Function 4: return all the consents for a data controller
  function getAll(bytes32 _ctlhash) view public returns(bytes32[ ]){
    return controller[_ctlhash].consentHash;
  }
}
```

5 Conclusions and Future Work

In this work, we proposed a framework that covers a major emerging need regarding the privacy of users in the IoT ecosystem. This work in progress sets the foundations for creating trust relationships among data controllers and subjects towards an IoT ecosystem compliant with the GDPR. The goal is to develop a user-centric solution that will allow data subjects to shape and manage the policies of their consents as a response to unambiguous access requests placed by data controllers. Additionally, the proposed approach utilises blockchain technology to support the consents' integrity, non-repudiation and versioning in a publicly verifiable manner. The cost of blockchain usage could be transferred to the data controllers that would gain the benefits of the aggregated knowledge from the management of personal data. Additionally, a private blockchain network maintained by all the data controllers and other data regulators (such as in [16]) could be established to minimize this cost. Finally, an intelligence component analyses incoming requests to identify policy rules conflicts regarding personal data disposal and assists users make the right decisions.

As future work, we intend to explore further the issues surrounding each of the components that make up the proposed framework with an emphasis on the improvement of GDPR-compliant data privacy ontologies and the *intelligence* component. Furthermore, we aim to consider the use of policies, generated by the proposed system, in policy-based access control systems, which will complement a personal data management solution in the IoT ecosystem.

References

1. Bartolini, C., Muthuri, R., Santos, C.: Using ontologies to model data protection requirements in workflows. In: Otake, M., Kurahashi, S., Ota, Y., Satoh, K., Bekki, D. (eds.) New Frontiers in Artificial Intelligence, vol. 10091, pp. 233–248. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-50953-2_17
2. Buterin, V.: A next-generation smart contract and decentralized application platform (n.d.). https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 02 Oct 2018
3. Cha, S.C., Chen, J.F., Su, C., Yeh, K.H.: A blockchain connected gateway for BLE-based devices in the Internet of Things. IEEE Access **PP**(99), 1–1 (2018). https://doi.org/10.1109/ACCESS.2018.2799942
4. Cha, S.C., Tsai, T.Y., Peng, W.C., Huang, T.C., Hsu, T.Y.: Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. In: 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), pp. 1–3, October 2017. https://doi.org/10.1109/GCCE.2017.8229327
5. Conoscenti, M., Vetrò, A., Martin, J.C.D.: Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, November 2016. https://doi.org/10.1109/AICCSA.2016.7945805
6. Copigneaux, B.: Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the Internet of Things. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 411–416, March 2014. https://doi.org/10.1109/WF-IoT.2014.6803201
7. Demertzis, K., Iliadis, L.S., Anezakis, V.D.: An innovative soft computing system for smart energy grids cybersecurity. Adv. Build. Energy Res. **12**(1), 3–24 (2018). https://doi.org/10.1080/17512549.2017.1325401
8. Eckert, K., Meilicke, C., Stuckenschmidt, H.: Improving ontology matching using meta-level learning. In: Aroyo, L., et al. (eds.) ESWC 2009. LNCS, vol. 5554, pp. 158–172. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02121-3_15
9. EnCoRe Project: Ensuring consent and revocation (2010). www.hpl.hp.com/breweb/encoreproject/. Accessed 02 Oct 2018
10. 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 (Apr 2016), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
11. Fortinet Inc.: Fortinet reveals "Internet of Things: connected home" survey results (2014). https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2014/internet-of-things.html. Accessed 02 Oct 2018

12. 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. Accessed 02 Oct 2018
13. Kleinaki, A.S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P.S., Kaldoudi, E.: A blockchain-based notarization service for biomedical knowledge retrieval. Comput. Struct. Biotechnol. J. **16**, 288–297 (2018). https://doi.org/10.1016/j.csbj.2018.08.002
14. Musolesi, M.: UPRISE-IoT: User-centric PRIvacy & Security in IoT (2017). http://gtr.rcuk.ac.uk/projects?ref=EP%2FP016278%2F1. Accessed 02 Oct 2018
15. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf. Accessed 02 Oct 2018
16. Nugent, T., Upton, D., Cimpoesu, M.: Improving data transparency in clinical trials using blockchain smart contracts. F1000Research **5**, 2541 (2016). https://doi.org/10.12688/f1000research.9756.1
17. O'Connor, Y., Rowan, W., Lynch, L., Heavin, C.: Privacy by design: informed consent and internet of things for smart health. Procedia Comput. Sci. **113**, 653–658 (2017). https://doi.org/10.1016/j.procs.2017.08.329
18. Otero-Cerdeira, L., Rodríguez-Martínez, F.J., Gómez-Rodríguez, A.: Ontology matching. Expert Syst. Appl. **42**(2), 949–971 (2015). https://doi.org/10.1016/j.eswa.2014.08.032
19. Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A.: Blockchain-based consents management for personal data processing in the IoT ecosystem. In: 15th International Conference on Security and Cryptography (SECRYPT 2018), part of ICETE, pp. 572–577. SciTePress, Porto (2018). https://doi.org/10.5220/0006911005720577
20. Russell, B., Garlat, C., Lingenfelter, D.: Security guidance for early adopters of the Internet of Things (IoT). White paper, Cloud Security Alliance, April 2015
21. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015). https://doi.org/10.1016/j.comnet.2014.11.008
22. Stankovic, J.A.: Research directions for the Internet of Things. IEEE Internet Things J. **1**(1), 3–9 (2014). https://doi.org/10.1109/JIOT.2014.2312291
23. Shih, Y.-Y., Liu, D.-R.: Hybrid recommendation approaches: collaborative filtering via valuable content information, p. 217b. IEEE (2005). https://doi.org/10.1109/HICSS.2005.302
24. Yang, Z., Wu, B., Zheng, K., Wang, X., Lei, L.: A survey of collaborative filtering-based recommender systems for mobile internet applications. IEEE Access **4**, 3273–3287 (2016). https://doi.org/10.1109/ACCESS.2016.2573314
25. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology?—A systematic review. PLoS ONE **11**(10), e0163477 (2016). https://doi.org/10.1371/journal.pone.0163477
26. Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S.: IoT security: ongoing challenges and research opportunities. In: 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234. IEEE, November 2014. https://doi.org/10.1109/SOCA.2014.58
27. Zhu, X., Ghahramani, Z., Lafferty, J.: Semi-supervised learning using Gaussian fields and harmonic functions. In: IN ICML, pp. 912–919 (2003)