IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 13, 2020, accepted June 24, 2020, date of publication June 29, 2020, date of current version July 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005509

GDPR Compliance Verification in Internet of Things

MASOUD BARATI[1], OMER RANA[1], (Member, IEEE), IOAN PETRI[2], (Member, IEEE), AND GEORGE THEODORAKOPOULOS[1]

[1]School of Computer Science and Informatics, Cardiff University, Cardiff CF24 3AA, U.K.
[2]School of Engineering, Cardiff University, Cardiff CF10 3AT, U.K.

Corresponding author: Masoud Barati (baratim@cardiff.ac.uk)

This work was supported by EPSRC under grant EP/R033439/1, Project title: ''PACE: Privacy-aware Cloud Ecosystems.'' The work of Omer Rana was supported by extend appreciation to the Deanship of Scientific Research at Princess Nourah bint Abdualrahman University for supporting his work through the visiting scholar program.

ABSTRACT Data privacy in Internet of Things (IoT) applications remains a major concern of regulation bodies. The introduction of the European General Data Protection Regulation (GDPR) enables users to control how their data is accessed and processed, requiring consent from users before any data manipulation is carried out on their (personal) data by smart devices or cloud-hosted services. Blockchains provide the benefits of a distributed and immutable ledger recording digital transactions across a global network of peer nodes. Blockchain support for tracking of operations carried out by an IoT-based system provides greater confidence to a user that the IoT device is not infringing user privacy (as the Blockchain can be audited to verify which operation was carried out, by which actor). A formal model (following the privacy-by-design approach) is proposed for supporting GDPR compliance checking for smart devices. The privacy requirements of such applications are related to GDPR obligations of device (and software systems) operators (such as user consent, data protection, right to forget etc). Three smart contracts are proposed as a practical solution to support automated verification of operations carried out by devices on user data, in accordance with GDPR rules. We evaluate the performance and scalability costs of our approach using a Blockchain test network.

INDEX TERMS Blockchain-based auditing, business processes, general data protection regulation, Internet of Things, user privacy.

I. INTRODUCTION

The rapid growth in the usage of Internet of Things (IoT) devices has led to the emergence of various IoT-based applications in domains such as energy consumption and utility monitoring, smart buildings, transportation, healthcare and assisted living environments [1]. Smart devices can collect many types of data about a user or their environment, such as location, acceleration/ speed of movement, nearby sound intensity – in addition to other information through specialist apps hosted on the smart device (e.g. healthcare information or context information for customizing or optimizing service provision to a user). The collected data is (often) transmitted to unknown third parties without the awareness of users. For example, some IoT customers may set their wearable devices in broadcast mode and when they are within discoverable range, any other smart object can access their personal data by sending unsafe requests. Understanding how data protection can be supported by the IoT-based application is becoming a significant concern. Moreover, data usage (including storage duration and analysis) can become important for sensitive data items, where personal data requires a higher level of privacy and security. However, what is considered to be *sensitive* is often subjective – but may include political/religious views of the user, user addresses, banking and health information etc. In order to address this, the General Data Protection Regulation (GDPR) has recently been extended to also include IoT environments, to give users the right to control their data and restrict how such data is shared and processed [2], [3]. Some IoT applications also make use of Blockchain-based techniques to incorporate user privacy and security in the development of their applications [4], [5].

GDPR introduces a number of rules to support a user in managing access to their own data. The basic elements of GDPR are: a data subject, a data controller or joint controller, and a data processor. The data subject has an identifier

The associate editor coordinating the review of this manuscript and approving it for publication was Hong-Ning Dai.

(e.g. name and location), and the data controller is a person or organization specifying operations/ processing activities on personal data. The data joint controller is introduced where there are two or more data controllers that jointly determine the purpose of data processing. The data processor is responsible for analysing user data on behalf of a data controller or joint controller [6]–[8]. GDPR associates responsibility of any violation in data processing to data controllers or joint controllers, but also gives a shared responsibility to data processors when data subject has no control on the data processing steps. The GDPR legislation proposes a number of obligations (i.e. informed consent, data protection etc) that must be followed by data processing actors with the roles of data controllers or processors [3]. The importance of verifying such GDPR obligations in IoT environment was widely discussed in [9], [10]. Furthermore, the necessity of accountability for data protection in IoT based on GDPR legislation was discussed in [11].

Blockchain is a public ledger that involves a distributed database and a set of connected nodes called miners [12]. It introduces ''smart contracts'' that can be deployed and checked by everyone connected to a Blockchain network. The contracts transform business rules to programmatic code that can be automatically executed on a Blockchain. However, this conversion has limitations, as mapping rules that encode legislation is often subject to interpretation and an exact mapping is difficult. To overcome this limitation, we only consider GDPR rules that relate to specific types of operations that can be carried out on user data – e.g. read, write, and transfer. In this way, for instance, any operation that involves reading user data will trigger GDPR compliance checking, i.e. seeking consent from the user of the IoT device when a service requests this data. We acknowledge that a more general consideration of GDPR compliance checking is a challenge – and outside the scope of this work.

Both Blockchain and smart contracts have been deployed in IoT devices to enhance transparency, trust and data privacy analysis as reviewed in [13]–[15]. A privacy-preserving approach combining Blockchain, edge computing and IoT was proposed in [16]. The use of a Blockchain in this approach improves the privacy of data aggregated by IoT devices from unauthorized third parties including miners.

Although the aforementioned approaches utilise either GDPR legislation or Blockchains indendepently, none of them proposed a combined approach to automatically verify GDPR rules on data processing units. Existing approaches also lack a formal representation for verifying GDPR compliance for IoT devices at design time before accessing or manipulating user data. An assisted living scenario is used to show how the integration of GDPR and Blockchain can appear as sub business processes for a number of IoT devices that are part of this scenario. The key contributions of this work are summarized below:

- a formal representation of business process models to support verification of IoT devices based on GDPR rules;
- specification of business processes to support data analysis from IoT devices (in the context of the proposed scenario), and a formal description of the associated privacy policies;
- verifying whether business processes (and their privacy policies) are compliant with GDPR rules;
- implementing GDPR rule verification through multiple smart contracts using a Blockchain network;
- performance and scalability analysis of smart contracts to assess their execution costs and mining time in the context of the proposed scenario.

This work primarily focuses on data privacy, particularly on improving visibility of how smart devices use personal user data. There is limited focus in this work on other aspects of security (or related threats). Security operations (e.g. user authentication, encryption, etc) are primarily application layer services that are used in the proposed model – however the key focus is on data privacy and relationship to the GDPR legislation (references to particular articles in the legislation are provided to cross reference the mentioned electronically-supported obligations reported in this work). The rest of the paper is structured as follows. Section II reviews related work. Section III describes an assisted living smart building scenario, the IoT devices involved, and the business processes for processing data from devices within the building. Section IV provides a formal representation for verifying GDPR compliance of business process models in accordance with multiple obligations identified in the GDPR legislation. Section V describes the design and implementation of GDPR rule verification through a Blockchain and smart contracts. Section VI provides experimental results and Section VII concludes the paper and identifies directions for future work.

II. LITERATURE REVIEW

Internet of Things research has made use of both Blockchain and GDPR to enhance user privacy. Blockchain-based techniques were used for improving user privacy, and a variety of concerns were identified in [17]. The approach implemented five privacy preservation methods: encryption, anonymization, private contract, mixing, and differential privacy in IoT ecosystems using Blockchains. In [18], the authors investigate how Blockchain infrastructure can assist in securing deployment of updates for IoT objects. The technique enables accountability of smart objects, supporting the audit trail of changes that have been made to objects. An IoT-based smart city architecture was designed in [19]. The architecture made use of Blockchain to preserve the authenticity, availability, integrity, non-repudiation and privacy issues associated with objects used in a smart city environment. A Blockchain-based IoT forensics framework was presented in [20] which maintains an interaction log generated by these IoT devices

in a transparent way. In [21], a Blockchain-based trust framework was proposed whereby multiple smart contracts were defined to enable IoT platforms to utilise pre-defined interaction rules. A Blockchain-based method that facilitates secure management of healthcare data in IoT environment was introduced in [22]. Private key, public key and smart contracts were used to improve user privacy and provide an access control mechanism for digital medical records. In [23], the authors presented a privacy-preserving Blockchain-based publish/subscribe model to protect data privacy and interests of IoT subscribers. The model enabled publishers to fully control any data access.

In [24], the authors proposed a framework for supporting GDPR-compliant processing of user data generated using IoT devices. The framework enabled data controllers to inform users about the status of their personal data in a transparent way. An IoT databox model was proposed in [25] that provides accountability for IoT devices. The model realized GDPR requirements focusing on how to promote trust and user privacy. In [26], a GDPR controller for IoT was proposed that enabled data owners to have full control on how their personal data was used. Such control comprised of tracking data flow between IoT devices and other systems, and informing owners about accesses made to IoT devices for user data. In [27], the authors presented an efficient method to obtain user consent during collection of personal data from IoT devices. The method was GDPR compliant in terms of protection of personal data as well. A series of security requirements and challenges imposed by e-health IoT were analyzed in [28]. The authors designed an architecture for supporting a GDPR-compliant mechanism for providing secure e-health services to elderly individuals.

Although these contributions took advantages of either GDPR or Blockchain technologies, there is limited evidence of how these approaches can be used in a combined way. The ability to track GDPR compliance in an automated manner is also missing from existing efforts – as many existing efforts require manual data analysis to be carried out to perform compliance verification. Generating an audit trail of interactions that take place on IoT devices, specifically focusing on the use of GDPR rules, was presented [2] through which several GDPR rules were translated as opcodes in smart contracts to automatically protect IoT user data. In [3], a Blockchain-based architecture together with business processes were designed to show how the integration of GDPR and Blockchain can appear as design patterns for IoT devices to enhance user privacy. However, these solutions do not formally examine the verification of GDPR rules on IoT devices at design time prior to the use of any personal data usage.

III. ASSISTED LIVING SMART BUILDING SCENARIO

Assisted living smart buildings are IoT-based systems where building management data (e.g. energy usage) and user data through wearable and *user-proximity* devices are combined. Such environments can have several data operations (using sensors, actuators, and devices) that are carried out on a user's personal data that require GDPR compliance. Such systems involve embedded monitoring and control equipment with the potential to observe users and their medical status through bracelet sensing devices and smart monitoring objects that can record heart rate, blood pressure, physical movement and indoor location [30]. User data is then analysed either locally or in a Cloud system, and based on the results third parties can be informed to intervene for preventing potential incidents for the monitored user(s) [31]. In such systems, building and user data are integrated within a Building Management Control System (BMCS) and a range of electronic actuators to achieve balance of building resource consumption (e.g. energy for Heating, Ventilation and Air Conditioning (HVAC)) and comfort, and to determine the medical/ physical status of users. Figure 1 illustrates the business processes of a heart monitor, a motion detection smart device, a blood pressure monitor, and a BMCS used in a smart building.

Heart monitor—measures and displays the heart rate of a user and stores it locally. If the rate is abnormal, the measured data is sent to the BMCS for emergency actions.

Blood pressure monitor—measures the blood pressure of user and keeps such measured data in its local storage. In case of an abnormal condition, the data is transmitted to BMCS and user is notified through a warning alarm.

Motion detection device—monitors a certain zone, senses physical movements and transfers the location of monitored user to BMCS. It alerts users If they enter a restricted area/ zone within a building.

Building management control system—interprets the messages or data received by aforementioned devices. In case of a critical health condition, it calls an emergency service. Otherwise a normal situation is displayed. It profiles or analyses the status or behavior of users based on their medical information or physical movements during a period of time – referred to as *profiled data*. Moreover, such data is stored locally, and a copy is sent to cloud storage to be accessible by authorized physicians or other support agencies. BMCS also manages access to connected devices to control their function, and receives user data from these devices as required.

Using Business Process Modelling Notation (BPMN) in Fig. 1, four pools are used to illustrate different business processes that can be carried out (manually or in an automated manner). Activities with dark envelopes denote sending messages; and those marked with service icons in boxes are automatically undertaken or processed by the system. The green circle with dark envelope shows a receiving message, and the box with a plus mark denotes a sub-process. The solid arrows between activities denote their sequence in a design pattern. Each activity may use or produce data recorded in databases, demonstrated by dashed arrows. Finally, the parallel executions and conditions are represented by rhombus notations with plus and cross marks, respectively.

The monitoring service and IoT devices used within the assisted living scenario are managed by a system administrator. From a GDPR perspective, the building administrator

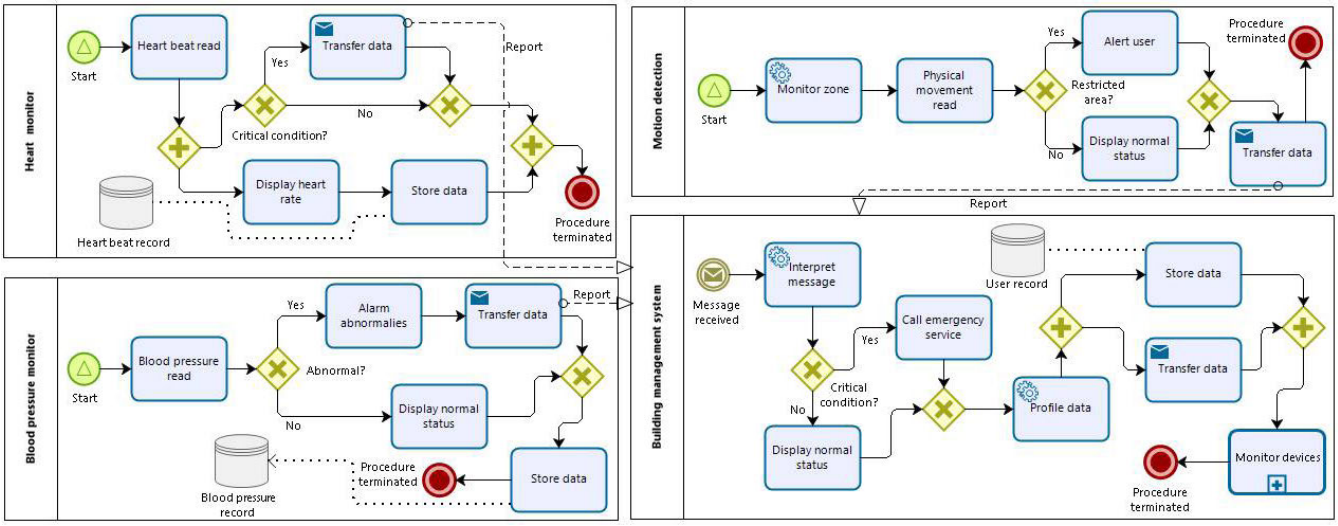


FIGURE 1. Business processes of an assisted living smart building.

should determine the purposes of data processing and have the role of data controller. The devices shown in Fig. 1 generate or transfer medical information and user location, which are generally considered as personal data. The secure protection of the former is an obligation in GDPR, since such information is categorized as sensitive data. For instance, a BMCS device installed in a building can analyze or store such information and also give permission to other third parties (e.g. a remote BMCS or cloud provider) to access this information. However, if the information is not encrypted, operations on user data are not compliant with GDPR and the data controller of the building is responsible.

IV. A GDPR COMPLIANT PROCESS COLLECTION MODEL

As the GDPR regulation focuses on data processing on personal user data, it requires system developers to show such purpose in a more transparent way to a user. This can be achieved by implementing a collection of design patterns covering all activities undertaken on personal data during the life cycle of a service. Business processes can explicitly show the purpose of data processing carried out by actors such as IoT devices [32]. A business process contains a number of activities and relationships, identifying the types of personal data being generated/ collected and where it is processed. For instance, the blood pressure and heart rate information collected by building management system is used for monitoring the health condition of the user. We can therefore associate a process with a purpose (e.g. heart monitor process/purpose or motion detection process/purpose). Using such a business process, a user is now aware of how their data is being processed, and the particular device involved in undertaking this processing.

In some cases, personal data may be generated or collected from one process and be used in another. For example, the location information collected and stored in the motion detection process is used by the BMCS process. In fact, two business processes interact with each other by exchanging personal data between them. However, GDPR requires data controller to receive consent of a user before the migration of their data between business processes. To ease the analysis of such GDPR regulations based on business process models, the collections of business processes in a system can formally be defined as follows (Appendix provides a list of notation used in these definitions).

Definition 1: A business process collection $\mathcal{P}_S$ designed for a system S is a tuple $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$, where Act is a set of actors each of which handles a number of processes; P is a set of processes; $\mathcal{A} = \mathcal{A}_{op} \cup \mathcal{A}_{\overline{op}}$ is a set of activities such that $\mathcal{A}_{op}$ and $\mathcal{A}_{\overline{op}}$ are the sets of processing and non-processing activities on personal data, respectively. The set D contains any data classes, including both relevant and irrelevant data to user; $\mathcal{D}_h \subseteq Act \times \mathcal{A}_{op} \times D \times P$ is a data handling relation set such that each relation determines what data is handled by which process and processing activities executed by an actor.

Processing activities in the definition refer to those that directly use or process personal data. They cover a wide range of operations executed on user data. The operations involve the "collection, reading, recording, organisation, structuring, storage, adaptation or alteration, retrieval, use, consultation, profiling, transfer, dissemination, combination, alignment, restriction, and erasure of personal data" (Art. 4(2) of GDPR). For instance, the BMCS process involves a user profile activity (classified as data processing) dealing with user data for the purpose of medical analysis. Identifying processing activities enables checking their compliance with GDPR, since there are legal obligations associated with each activity. Take for example the prohibition of profiling activities for underage users (Art. 22 of GDPR) or the prohibition of storing data longer than its processing time (Art. 17 of

GDPR). According to GDPR regulations, it is the responsibility of data controller to specify all processing activities executed on personal data and to define a clear purpose for each activity in advance. Section IV-A presents how *purposes of data processing* can be explicitly defined to notify data subjects (users) about the privacy policies associated with a business process.

Example 1: Assuming that $\texttt{act}_1$, $\texttt{act}_2$, $\texttt{act}_3$, and $\texttt{act}_4$ are smart objects (actors) handling *heart monitor*, *blood pressure monitor*, *motion detection*, and *building management control* processes, respectively. The process collection model for the scenario in Section III using Def. 1 is as follows:

$$
\begin{aligned}
Act &= \{\texttt{act}_1, \texttt{act}_2, \texttt{act}_3, \texttt{act}_4\}\\
P &= \{\texttt{Heart monitor, Blood pressure monitor,}\\
&\qquad \texttt{Motion detection, BMCS}\}\\
\mathcal{A}_{op} &= \{\texttt{Read, Transfer, Profile, Store}\}\\
\mathcal{A}_{\overline{op}} &= \{\texttt{Display status, Emergency call, Alarm, Monitor}\}\\
D &= \{\texttt{Blood pressure(BP), Heart beat rate}\\
&\qquad \texttt{(HB),User location (UL), Profiled data (PD)}\}\\
\mathcal{D}_h &= \{\cdots;\langle \texttt{act}_4, \texttt{Read, \{BP, HB, UL\}, Building management control}\rangle;\\
&\qquad \langle \texttt{act}_4, \texttt{Profile, \{BP, HB, UL\}, Building management control}\rangle;\\
&\qquad \langle \texttt{act}_4, \texttt{Store, PD, Building management control}\rangle;\\
&\qquad \langle \texttt{act}_4, \texttt{Transfer, PD, Cloud analysis}\rangle;\cdots\}
\end{aligned}
$$

We represented the set $\mathcal{D}_h$ only for the building management control (BMCS) process for simplification. A similar representation can be used for the other processes. The "`Read`" activity refers to the "`Interpret message`" in Fig. 1, which is classified as a processing activity. The "`Cloud analysis`" is the name of an external business process receiving the profiled data of a user – initiated by the BMCS process. Given the set of non-processing activities, the "`Alarm`" implicitly refers to "`Alarm abnormalities`" and "`Alert user`" activities in Fig. 1. Finally, both "`Monitor zone`" and "`Monitor devices`" activities are denoted by "`Monitor`".

After specifying a process collection model (Def. 1), the following steps are used for auditing GDPR-compliance [32]:

1) Implementation should conform to process collection. Only the processes specified in the process collection model should only be implemented.
2) Process collection should include a privacy policy, i.e. a process should only collect or use data based on a privacy policy.
3) Process collection should conform to GDPR regulation. As an example, processes should receive user consent before any access to personal data.
4) The privacy policy should conform to GDPR regulation. For instance, a privacy policy cannot say that personal data is to be used for unknown purposes.

A. GDPR-COMPLIANT PRIVACY POLICY

To comply with GDPR regulation, a privacy policy must explicitly state the purpose for collecting personal data. For instance, in the scenario presented in Section III, a GDPR-based privacy policy can be expressed as "BMCS device profiles user data for building management control". The following definition can be used to specify a privacy policy:

Definition 2: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h\rangle$ be a process collection and $\mathcal{D}_h \subseteq Act \times \mathcal{A}_{op} \times D \times P$ be a data handling relation set. A privacy policy on $\mathcal{D}_h$ denoted by $Pr(\mathcal{D}_h)$ is a set of statements: "act_i `executes` α `on` d `for` p" for each $\langle act_i, \alpha, d, p\rangle \in \mathcal{D}_h$, where $act_i \in Act$, $\alpha \in \mathcal{A}_{op}$, $d \in D$, and $p \in P$.

This definition states that a privacy policy can include a number of statements, each of which must clearly define the purpose of data processing. Informally, each statement clarifies what processing activity is carried out, by which actor, on what data classes, and for what purpose.

If an actor processes personal data without identifying a specific purpose, it is classified as a *violator* in accordance with Recital 50 of GDPR. Given Def. 2, if there is a handling relation $\gamma = \langle act_i, \alpha, d, p\rangle \in \mathcal{D}_h$ such that $pr(\gamma) = \emptyset$, where $pr(\gamma) \in Pr(\mathcal{D}_h)$, there is a breach based on GDPR.

Example 2: Let act_1 be an actor handling heart monitor process. Given Def. 2 and allowing meaning preserving natural language transformations, the typical privacy policies of heart monitor process will be:

"act_1 `executes` *read* `on` *heart beat rate* (*HB*) `for` *heart monitor*",
"act_1 `executes` *store* `on` *HB* `for` *heart monitor*",
"act_1 `executes` *transfer* `on` *HB* `for` *building management control*".

Since the heart beat rate is transferred to the BMCS device, the purpose or process of the last privacy policy is *building management control*.

B. VERIFICATION OF GDPR RULES ON PROCESS COLLECTION MODEL

This section presents a formal verification for GDPR compliance of four typical obligations, including user consent, data minimisation, data protection, and data transfer. Such GDPR obligations are verified with the aid of formal definitions proposed for processes collection model and privacy policy.

1) DATA SUBJECT CONSENT

Users (data subjects) should give their consent for any activity executed by actors on their personal data (Recital (32), (43) of GDPR). When data analysis purpose and privacy policy of process collection is formally proposed (as in Def. 2), the vote (i.e. a positive or negative consent) of a data subject to a privacy policy can also be formally defined by the following function.

Definition 3: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$, $\mathcal{D}_h \subseteq Act \times \mathcal{A}_{op} \times D \times P$, and $Pr(\mathcal{D}_h)$ be the process collection in system S, a handling relation set, and a set of privacy policies over $\mathcal{D}_h$, respectively. The vote of data subject j to $Pr(\mathcal{D}_h)$ denoted by Γ_j is a boolean function:

$$\Gamma_j : Pr(\mathcal{D}_h) \mapsto \{\top, \bot\}.$$

Let $\gamma = \langle act_i, \alpha, d, p \rangle \in \mathcal{D}_h$ be an instance of the handling relation set. A consent has been given to $pr(\gamma) \in Pr(\mathcal{D}_h)$ by data subject j if $\Gamma_j(pr(\gamma)) = \top$.[1]

We can verify the process collection of a system in terms of Recital (32), (43) of GDPR—legislated for data subject consent—as follows.

Definition 4: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$ be a process collection of S and $\mathcal{D}'_h \subseteq \mathcal{D}_h$ be a processed data relation set such that each relation determines what data was used by which processes and what processing activities were executed on this data by actors. With the assumptions identified in Def. 3, the data controller violates GDPR requirements on obtaining consent if there is an actor $act_i \in Act$ such that

$$\exists\ \gamma = \langle act_i, \alpha, d, p \rangle \in \mathcal{D}'_h\ s.t.\ \Gamma_j(pr(\gamma)) = \bot,\ or$$
$$\exists\ \gamma = \langle act_i, \alpha, d, p \rangle \in \mathcal{D}'_h\ and\ pr(\gamma) = \emptyset.$$

Informally, this states that any data usage that has been confirmed by a data controller must have an explicit privacy policy, and require consent from a data subject; otherwise the controller has committed a breach according to GDPR regulations.

The processed data relation set $\mathcal{D}'_h$ is not constructed at design time. It can be formed after the online execution of a process. For instance, to use such a set in practice, we propose a smart contract – called *submission* – which makes use of the $\mathcal{D}'_h$ relationship via a Blockchain network. This is realised during the run time data processing of an actor (see Section V-A2).

2) DATA MINIMISATION

GDPR enforces data controllers to limit (minimise) the collection of personal data to only those data items which are necessary for processing. In other words, data received from a data subject must only be the items required for carrying out processing (Art. 5(1)(c) of GDPR). Definition 2 led to the generation of the *purposes statements* for business processes. The following definition identifies data classes used by actors for a collection of business processes:

Definition 5: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$ be business processes within a system S. The used data set is denoted by D_u, where:

$$D_u = \{d \in D \mid \langle act_i, \alpha, d, p \rangle \in \mathcal{D}_h\}.$$

It states that $d \in D_u$ is used if at least one process handles or utilizes it in accordance with $\mathcal{D}_h$. Given this definition, the compliance of a process collection model with the rule—legislated for data minimisation—can be verified.

[1] $pr(\gamma) \in Pr(\mathcal{D}_h)$ is a privacy policy exposed for γ.

Definition 6: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$ be business processes in system S, $\mathcal{D}_h \subseteq Act \times \mathcal{A}_{op} \times D \times P$ be the set of data handling relation set, and $D_u \subseteq D$ be a set of used data. Moreover, assuming that $D_r \subseteq D$ is the set of personal data received from data subject and injected to all business processes in $\mathcal{P}_S$. The process collection model $\mathcal{P}_S$ is GDPR compliant with respect to data minimisation rule if: $D_r \subseteq D_u$.

This indicates that activities within business processes should not receive or collect data which is not used for processing. We can have $D_r \subset D_u$ for cases where personal data is generated and used by business processes without consent by data subject.

3) DATA PROTECTION

According to Art. 32(1)(a) of GDPR, data controllers and processors should implement technical measures such as encryption to ensure the protection of personal data prior to or during its processing activities such as read, storage, profiling or transfer.

Definition 7: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$ be business processes in system S and $\mathcal{A}_{op} \subseteq \mathcal{A}$ be the set of processing activities. The encryption status of personal data handling by actor $act \in Act$ is a Boolean function:

$$\mathcal{E}_{act} : D \times \mathcal{A}_{op} \times P \mapsto \{\top, \bot\}.$$

Let $\langle act, \alpha, d, p \rangle \in \mathcal{D}_h$ be a handling relation. Given the relation, actor act encrypted $d \in D$ for activity α in process p if: $\mathcal{E}_{act}(d, \alpha, p) = \top$.

We can generalize this definition to check whether a process collection model is compliant with the data protection rule in GDPR (Art. 32(1)(a)).

Definition 8: Let $\mathcal{P}_S = \langle Act, P, \mathcal{A}, D, \mathcal{D}_h \rangle$ be business processes in system S, $act \in Act$ be an actor, and $\alpha \in \mathcal{A}_{op}$ be a processing activity executed on personal data d. The process model $\mathcal{P}_S$ satisfies the GDPR rule for data protection if:

$$\nexists\ \langle act, \alpha, d, p \rangle \in \mathcal{D}_h\ such\ that\ \mathcal{E}_{act}(d, \alpha, p) = \bot.$$

This indicates that for every processing activity on personal data within a business process, the encryption of data is required. Notably, one time encryption is adequate for the same processing activity executed on the same data in a business process.

4) DATA TRANSFER

GDPR is primarily applicable for data controllers and processors located in Europe. Data subjects have a risk of losing the protection of their personal data when it is transferred outside Europe. GDPR therefore restricts data transfers to non-European jurisdictions, unless the protection of personal data is ensured through appropriate safeguards such as pseudonymisation and encryption (Art. 44 of GDPR). If data receiver does not guarantee the protection of data, GDPR prohibits a data sender from transferring this data for processing.

Definition 8 enables verification of actors in accordance with data protection rule in GDPR. This verification can also

be used to check that data transfer will satisfy the rules in Art. 44 of GDPR under which the encryption/ protection of personal data must be ensured. This assumes that the location of the actor can be identified, and the data senders and receivers of personal data are recognizable in the business process. A controller sending the personal data is classified as a violator if its data receiver is outside Europe and the verification of Def. 8 is not satisfied within the process p handled by data receiver (act).

Example 3: Consider that in Fig. 1 the data processing actor of heart, blood pressure, and motion detection monitors are situated in a European country. These actors send their measured or sensed data without notifying a user about a remote BMCS (act_4) server located outside Europe. Given GDPR requirements, the satisfaction of the following is an obligation before transfer of data by actors can take place.

$$\mathcal{E}_{act_4}(\{\texttt{HB,BP,UL}\}, \texttt{Read}, \texttt{Building management control}) = \top \wedge$$

$$\mathcal{E}_{act_4}(\{\texttt{HB,BP,UL}\}, \texttt{Profile}, \texttt{Building management control}) = \top \wedge$$

$$\mathcal{E}_{act_4}(\texttt{Profiled data}, \texttt{Store}, \texttt{Building management control}) = \top \wedge$$

$$\mathcal{E}_{act_4}(\texttt{Profiled data}, \texttt{Transfer}, \texttt{Cloud analysis}) = \top.$$

The notations HB, BP, and UL refer to heart rate, blood pressure and user location, respectively. The process *cloud analysis* is an external business process interacting with the remote BMCS. Such verification checks on encryption of any relevant data to a user that should be provided by act_4 during the life cycle of the building management control process.[2]

V. GDPR COMPLIANCE VERIFICATION VIA SMART CONTRACTS

After an electronic encoding of GDPR obligations, the automatic verification of such obligations within an IoT environment is a main challenge. Furthermore, the implementation of a privacy policy based on operations that have been agreed by a data controller, in an easy to interpret manner for users, remains another challenge. In order to address this, we make use of a Blockchain network, to support the accountability of operations carried out on smart objects in a secure, transparent and automatic way [2]. Moreover, the verification of the aforementioned GDPR obligations over IoT devices along with the privacy policies associated with the use of these devices, can be implemented using smart contracts [33] – executed over a Blockchain virtual machine. An architecture that connects participants within IoT environment to a Blockchain network, and implements three GDPR-supported smart contracts for undertaking such verification is presented in this section.

A. A BLOCKCHAIN-BASED MODEL

IoT devices can be heterogeneous in nature (using a variety of different hardware configurations and firmware) and support a number of different data formats. Many IoT devices – called lightweight nodes – simply collect or transmit data [34]. In contrast, some IoT devices – called full nodes – have computational resources that enable processing of collected data (e.g. single-board computers and smart phones). Some IoT-based systems presently make use of container virtualization for increasing the level of trust in services. Lightweight containers can be hosted directly on the IoT device, and can execute operations on device hardware. Containers therefore decouple hardware resources from the supported software environment. Their use has increased significantly in data centers, and also recently in IoT gateways (often referred to as ''edge computing'' systems) to monitor devices [35]. An adaptive and modular IoT gateway – called AGILE – was presented in [36]. The gateway hosts multi-containers and micro-service based framework to provide device management, data storage and access control. The use of trustable containers in cloud and IoT-based ecosystems has led to tracking of processing activities executed by services/ devices on personal data. Such containers record the operations carried out on data using a monitoring tool so that the log generated by the tool cannot be altered [37]. Another similar approach is the development of ''intelligent hubs'', essentially gateway nodes that can interface with a number of IoT devices available within a home or a factory environment [29]. The approaches proposed in [37]–[39] introduce a number of approaches for realizing such a trustable container. The container can be connected to a Blockchain virtual machine (e.g. Ethereum) to store the activities of full nodes on user data in a Blockchain. Storing such information can provide a basis for the verification of smart devices. Lightweight nodes have computation and storage limitations. Hence they should be served by the full nodes to be monitored by a container and can be indirectly registered in the Blockchain network. For instance, the BMCS device depicted in Fig. 1 can involve a number of sensors – classified as lightweight nodes. Such sensors should be accessed or controlled via a user-friendly platform installed on the BMCS to be observed by a trusted container (e.g. a trustable version of AGILE container) hosted on a gateway.

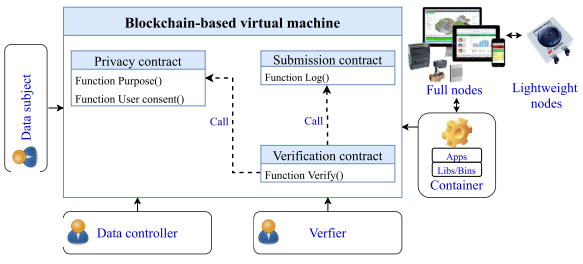


FIGURE 2. Supporting user privacy using Blockchains.

A conceptual architecture for connecting participants within an IoT ecosystem to a Blockchain network is illustrated in Fig 2. The architecture provides a reactive mechanism for the accountability of data controller and the activities carried out by smart devices on user data. Such a mechanism

[2]The responsibility of checking GDPR compliance of data delivery to *cloud analysis* is subsequently delegated to the data controller.

allows devices to freely collect and process personal data and verifies them at the end. It does not implement any enforcement smart contract, which may impact (negatively) on the performance of devices.

All parties in our model, namely data subject (IoT user), verifier, data controller and devices have a unique identity called the Blockchain wallet ID (e.g. Ethereum [43] account) to be registered in the Blockchain. After registration, any of these parties can access and use smart contracts implemented to protect user data based on GDPR rules. The data controller manages an IoT-based system and requires personal user data for analysis (e.g. the health data for a user over a particular time frame) and determines the purpose of data processing. Verifier is a third party interacting with the Blockchain virtual machine to support the verification of a data controller. The devices whose processing activities do not comply with GDPR requirements can also be detected by the verifier. The (trusted) container, which has also a Blockchain account, locally stores the user data generated by smart devices or received from an end user, and records any usage or access to such data in the Blockchain. The conceptual architecture identifies three smart contracts: privacy, submission, and verification contracts. Descriptions of these are provided below.

1) PRIVACY CONTRACT

This contract identifies the purpose of data processing and a user vote (i.e. whether a user has given consent) for such purpose. The former is identified by the data controller and the latter by a data subject. The implementation of this smart contract conforms to Definitions 2 and 3 presented for privacy policy and user consent, respectively. As seen in Fig. 2, the contract contains two functions: `purposes` and `user consent`. The former gets actor address (e.g. Ethereum account), the activity of an actor on user data, the personal data classes that will be processed using the activity, and the name of the process. Such inputs, which are associated with the privacy policy expressed by Def. 2, are directly recorded by data controller in a Blockchain – to be accessible by a data subject. Providing data subject with such information meets Art. 5 and Art. 30(1)(b) of GDPR enforcing data controllers to explicitly define their purpose of data processing. The `user consent` function receives a user vote based on information already stored through *purposes* function in the Blockchain and logs whether consent has been obtained ($\top$) or not ($\bot$).

2) SUBMISSION CONTRACT

The contract is deployed by a container to store device's address, process name, executed activity (on user data), the personal data that has been processed by the activity, and the encryption status ($\mathcal{E}_{act}$) of the activity in a Blockchain.[3] The contract has a `log` function to submit such information to the Blockchain. The logged information can be used to verify operations carried out by a smart device in accordance with GDPR rules presented in Section IV-B. It is worth noting that both processed data relation set $\mathcal{D}'_h$ and used data set D_u can be formed in practice through this contract, as their related information are stored in the Blockchain.

[3]Recording such information through the contract complies with Def. 7 and also data transfer rules.

3) VERIFICATION CONTRACT

This contract is deployed by the verifier to check GDPR compliance of devices (actors) and data controller in accordance with the rules expressed in Sections IV-A and IV-B. The contract makes use of both privacy and submission contracts to access data stored by them in the Blockchain. The `verify` function in this smart contract checks:

- whether an actor conforms to the purpose of data processing identified previously – according to Sect. IV-A.
- whether operations carried out by an actor on personal data has received user consent – according to Def. 4.
- whether an actor only collected data needed for processing (or if additional data was collected that was not directly required) – according to Def. 6.
- whether the encryption of processing activities on user data was supported or not? – according Def. 8.

Any violation is detected through the aforementioned verification and the data controller committing a breach of GDPR rules is reported as violator.

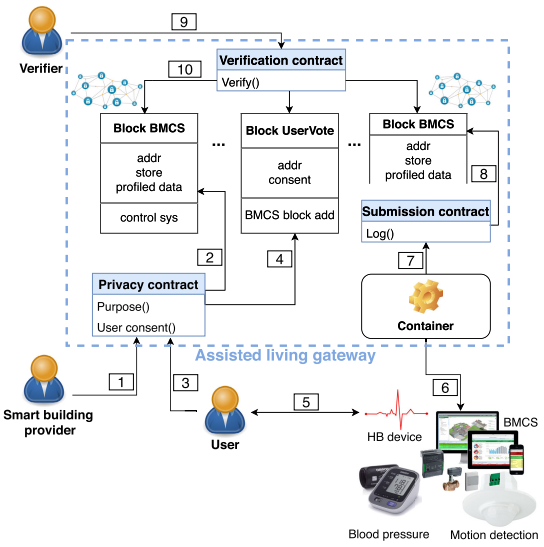


FIGURE 3. Interactions within an assisted living smart building.

B. ADAPTING SMART BUILDING WITH BLOCKCHAIN-BASED MODEL

Participants in the assisted living scenario utilise a Blockchain as illustrated in Fig. 3, which includes a gateway for connecting and monitoring devices within a smart building. The gateway hosts a trusted container to track operations carried out by these devices on user data and also provides access to a Blockchain virtual machine (e.g. Ethereum) in order to use and deploy our proposed smart contracts. The administrator of such a gateway is a data controller in the

GDPR context. Before a user is given access to such smart devices, the provider should register devices and their privacy policies in a Blockchain (step 1). To achieve this, the provider deploys the *privacy* contract and activates *purpose* function to store a device address (e.g. motion detection address), its processing activity (e.g. transfer), required/ generated data (e.g. user location) and purpose (e.g. building management control) in the Blockchain (step 2). A user can then connect to the gateway and query the registered devices (step 3). Such a query is, however, subject to being given access to the deployment address of the *privacy* contract that has been shared by the provider. Using such an address, a user can activate the *user consent* function to see the list of devices and retrieve their privacy policies from the Blockchain and give consent (step 4). Once the user has been connected to a smart device through the gateway (step 5), the container starts tracking activities (e.g. read, store and transfer) executed by the device on user data (step 6). Meanwhile, it automatically deploys the submission contract (step 7) and runs the *log* function to send data items that are part of the *processed data relation* set $\mathcal{D}'_h$ (e.g. BMCS address (act), transfer (α), profiled data (d), cloud analysis (p)) along with the encryption status of the processing activity ($\mathcal{E}_{act}$) into the Blockchain (step 8). Finally, to check for GDPR compliance of data controller and devices, the verifier can connect to the gateway and deploy the verification contract at any time (step 9). It executes the *verify* function to retrieve the Blockchain records and detect any GDPR violation (step 10).

C. TRUST AND SCALABILITY

Our Blockchain-based approach can make use of the authentication technique proposed in [40] to enhance the trust of IoT users and smart nodes. The technique uses Blockchain to build virtual secure zones in IoT environments, where nodes can trust each other. A zone (e.g. an assisted living smart building) involves a collection of smart devices interacting with each other to provide services to users. A provider of the zone operates as the manager of a zone and can play the role of a *leader* for registering identities (i.e. Blockchain wallet IDs) of other nodes – called *followers* of the zone. Hence if any node in a zone requests access to user data or queries the processing purpose of another node, it must already be registered by the leader. Moreover, each zone is equipped with a verifier to check data stored in the Blockchain network containing transactions of leader and followers on user data. The verifier can use this transaction log to identify GDPR violations.

In order to improve the overall scalability of our Blockchain-based approach, we can utilise a number of multi-Blockchain frameworks such as Cosmos [41] and Polkadot [42]. Cosmos is a network for supporting distributed ledgers, including an independent network of parallel Blockchains – each of which keeps the transactions carried out by a leader and followers on personal data in a specific zone. The interaction between the networks is realized through an inter-Blockchain communication protocol provided by the Cosmos framework. Such a protocol enables the transfer of personal data and the communications of smart nodes in different zones. Polkadot supplies the connection and communication of various Blockchain networks through its key components, namely *parachain* and *relay-chain*. Parachains can use a Blockchain for storing the transactions of smart nodes in different zones. A Relay-chain ensures coordination between the different Parachains.

For integration of our approach in the Polkadot framework, the leaders of zones can also play the role of *collators* who confirm transactions created from registered valid nodes prior to sending them to *validators*, leading to the confirmation (“sealing”) of new blocks.

VI. EXPERIMENTAL RESULTS

An initial prototype of our Blockchain-based approach has been implemented using the Ropsten [44] test network. Our proposed smart contracts were implemented on Ethereum using Solidity [45]. Ropsten is a public test network that supports a number of miners and has a gas limit of 4712388 for contract deployment. Gas is a metric used to measure the computational complexity of executing transactions [46]. Our proposed smart contracts were developed to minimise gas consumption for each function or transaction. They were tested using Remix – an online development environment for Solidity running deployed contracts. The smart contracts *Privacy*, *Submission*, and *Verification* were deployed in the Ropsten test network. The amount of gas consumed for deploying the contracts were 1088628 for *Privacy*, 598293 for *Submission*, and 951865 for *Verification*.

We consider the change in gas required by increasing the number of actors (devices) and the average time taken for the mining process. When a GDPR rule violation is detected, we evaluate the relationship between user payment and violation detection rate under different number of processing activities in an assisted living smart building. This is undertaken to investigate the budget a user should allocate to execute the verifier smart contract. In some instances (depending on the number of processing actors and operations involved), a user may not have the budget to carry out such verification.

A. NUMBER OF ACTORS VS. GAS CONSUMPTION

This experiment involved changing the number of actors to measure the amount of gas used for the execution of all functions or transactions in the privacy, submission, and verification contracts. We assume that the number of actors (BMCS devices) in the assisted living smart building varies from 2 to 10, each of which runs four different processing activities (i.e. read, store, profiling and transfer) on the personal data of a monitored user.[4] Moreover, the personal data items involve blood pressure, heart beat rate, user location, and user ID. In the experiment, for each activity, the number of processed personal data was randomly selected

[4]The reason of choosing BMCS device for the experiment was that it covers all the aforementioned operations and deals with the designated personal data items.

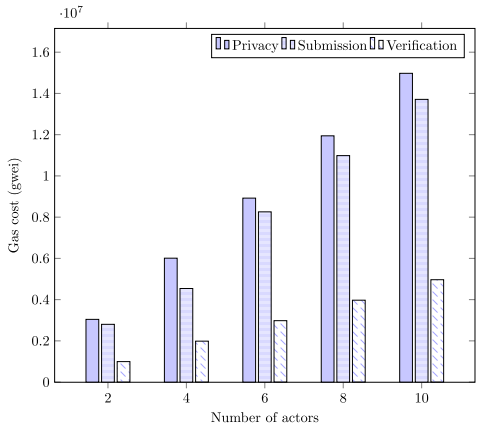


FIGURE 4. Number of actors vs. gas cost (gwei).

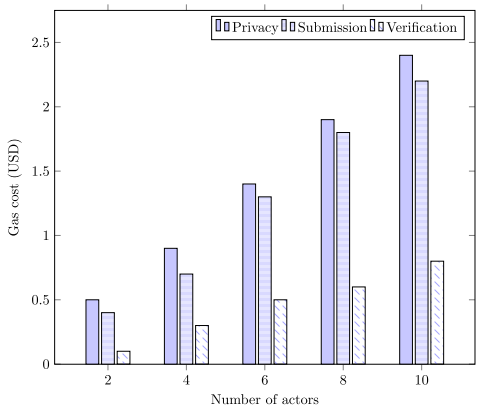


FIGURE 5. Number of actors vs. gas cost ($).

between 1–4. The gas price for running transactions was 5 *gwei* and our proposed smart contracts were executed 10 times to calculate their average gas consumption. Figures 4 and 5 shows the results of the experiment. The gas cost for executing transactions in both *gwei* and USD units were obtained.[5] The gas price unit is *gwei*, equivalent to 1×10^{-9} ether[6] and the gas cost is calculated as: *used gas* × *gas price*. By increasing the number of actors, the transaction costs rise gradually. In our implemented smart contracts, the privacy contract has the highest complexity, and therefore the greatest cost to execute.

B. EVALUATION OF MINING TIME

Two different experiments are undertaken here: (i) the relationship between contract deployment and mining time under different gas prices; (ii) the relationship between the number of actors (BMCS devices here) and the mining time taking for their verification. We used Ropsten test network to obtain the results of both experiments, since it provides a measurement of the time taken from activation to mining of a transaction. In the former experiment, we evaluated the average mining time for deploying *privacy*, *submission*, and

[5]https://ethgasstation.info/

[6]Ether is a cryptocurrency in Ethereum that allows smart contracts to be executed.

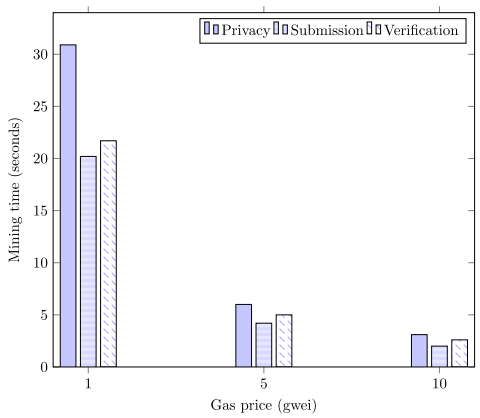


FIGURE 6. The relationship between contract deployment and mining time.

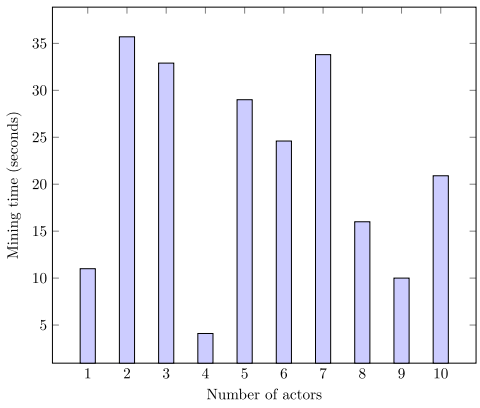


FIGURE 7. The relationship between the number of actors and mining time.

verification smart contracts with various gas prices: 1, 5, and 10 *gwei*. The contracts were deployed ten times to get the average time. Figure 6 shows the results of this experiment – when the gas price increases, the mining time decreases sharply. Given a fixed gas price, we observe a direct relation between gas consumption (for contract deployment) and mining time. Notably, this result can only be visible when there is a big difference between the gas consumption of two contracts. For instance, since the amount of gas consumed for deploying submission contract was less than the other smart contracts, its mining process took the shortest time.

In the latter experiment, the number of BMCS devices (actors) varies from one to ten and each executes a processing activity (e.g. read, store etc) on the personal data of a monitored user in the smart building. Moreover, the number of personal data items (i.e. user location, blood pressure, heart beat rate, and user ID) being requested is varied randomly from two to four. Our proposed smart contracts were executed ten times to calculate the average mining time of *verify* function, belonging to the verification contract. The gas price was 1 *gwei* in the experiment. Figure 7 represents the time taking in seconds for the verify function to be successfully mined since its activation time. The results show that the

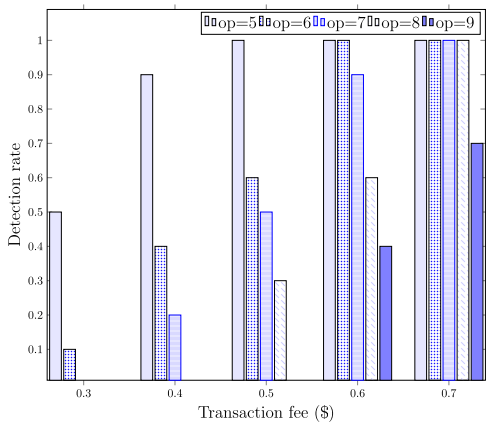


FIGURE 8. Relationship between cost and violation detection rate.

time depends on the interest of miners for mining the verify function and does not depend on the number of actors or the function parameters. Given a fixed gas price and when there is limited difference between gas consumption of transactions, it is found that miners can usually take an arbitrary time for the mining process.

C. VERIFICATION COST VS. VIOLATION DETECTION

This experiment involves changing the number of processing activities, and measuring the cost of carrying out compliance verification. We consider one actor (a single BMCS device) and the number of processing activities (*ops*) executed by the device on monitored user data varies between 5–9. The number of personal data items required for each activity (i.e. read, store etc) is randomly selected between 1–4. Moreover, we assume that during each execution, a GDPR violation (as outlined in Sect. IV-B) occurs. We used Ropsten for executing the contract transactions and the rate of gas price was 10 *gwei*. Figure 8 shows the results of this experiment. The x-axis shows the fee paid by a monitored user for verifying operations performed by an actor through the verification contract. The y-axis indicates the number of successful detected violations. Given a specific number of processing activities and a cost paid for verifying the operations of an actor, the *verify* function was activated ten times – indicating the overall detection rate. The results show that when the number of processing activities is five and a user pays \$0.5 for verification, the verify function is successfully activated even if the processing activities deal with four personal data items. As seen from the figure, there is a direct relationship between the fee paid by the user and the number of violations detected. Moreover, for a given price, as the number of processing activities increases, the violation detection rate decreases. For example, GDPR-compliance cannot be detected when the number of processing activities is nine and our budget is \$0.4. This approach can therefore be used to determine the budget to allocate to support compliance checking.

VII. CONCLUSION

We describe how GDPR obligations, including user consent, data protection, data minimization, and data transfer can be verified for processing units. Although primarily intended for IoT devices, such verification can also be applied to other service-based systems such as Cloud and Fog computing. This paper extends formal models of GDPR compliance verification proposed in [32] and [3], focusing specifically on business processes. To carry out GDPR verification in IoT environments, a Blockchain-based method with three smart contracts is proposed. The smart contracts were deployed in the Ropsten test network and our evaluation shows the influence on verification cost as the number of smart objects increases. For a given *gas* price (used to characterise execution of opcodes within a smart contract), we identify how the mining time for executing transactions is arbitrary and independent of the growth in the number of smart objects.

Our future work focuses on the implementation of our Blockchain-based technique using an IoT testbed with a heterogeneous group of smart devices, to evaluate its scalability. Furthermore, we will examine other GDPR obligations that can be programmatically verified and propose their formalism. The realization of the designed abstract model through available Internet of Blockchains such as Polkadot or Cosmos remains another challenge for future investigation.

TABLE 1. Glossary.

Notation	Description
$\mathcal{P}_S$	A business process collection
Act	A set of actors
P	A set of processes or purposes
$\mathcal{A}$	A set of activities
$\mathcal{A}_{op}$	A set of processing activities
$\mathcal{A}_{\overline{op}}$	A set of non-processing activities
D	A set of data
$\mathcal{D}_h$	A data handling relation set
$\mathcal{D}'_h$	A processed data relation set
$Pr(\mathcal{D}_h)$	A privacy policy set on $\mathcal{D}_h$
Γ_j	Vote function activated by data subject j
D_u	A set of used personal data
D_r	A set of received personal data
$\mathcal{E}_{act}$	Encryption status function activated by actor act

APPENDIX
GLOSSARY OF USED NOTATIONS

Table 1 provides the brief descriptions of all notations or symbols used in Section IV.

ACKNOWLEDGMENT

The work reported in this article was funded by EPSRC under grant EP/R033439/1, Project title: "PACE: Privacy-aware Cloud Ecosystems." Omer Rana would also like to extend appreciation to the Deanship of Scientific Research at Princess Nourah bint Abdualrahman University for supporting his work through the visiting scholar program.

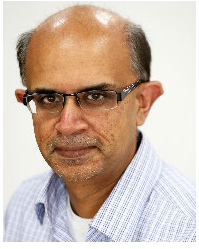
REFERENCES

[1] S. Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, Jun. 2018.

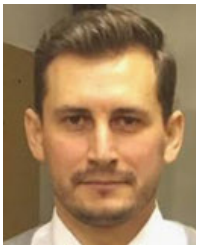
[2] M. Barati, I. Petri, and O. F. Rana, "Developing GDPR compliant user data policies for Internet of Things," in *Proc. 12th IEEE/ACM Int. Conf. Utility Cloud Comput.*, Dec. 2019, pp. 133–141.

[3] M. Barati and O. Rana, "Enhancing user privacy in IoT: Integration of GDPR and blockchain," in *Blockchain Trustworthy Systems* (Communications in Computer and Information Science), vol. 1156, Z. Zheng, H. N. Dai, M. Tang, and X. Chen, eds. Singapore: Springer, 2020, pp. 322–335.
[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[5] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.
[6] E. Mougiakou and M. Virvou, "Based on GDPR privacy in UML: Case of e-learning program," in *Proc. 8th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, Aug. 2017, pp. 1–8.
[7] B. Russo, L. Valle, G. Bonzagni, D. Locatello, M. Pancaldi, and D. Tosi, "Cloud computing and the new EU general data protection regulation," *IEEE Cloud Comput.*, vol. 5, no. 6, pp. 58–68, Nov. 2018.
[8] M. Barati, O. Rana, G. Theodorakopoulos, and P. Burnap, "Privacy-aware cloud ecosystems and GDPR compliance," in *Proc. 7th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2019, pp. 117–124.
[9] H. A. Abdulghani, N. A. Nijdam, A. Collen, and D. Konstantas, "A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective," *Symmetry*, vol. 11, no. 6, p. 774, Jun. 2019.
[10] S. Imtiaz, R. Sadre, and V. Vlassov, "On the case of privacy in the IoT ecosystem: A survey," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 1015–1024.
[11] L. Urquhart, T. Lodge, and A. Crabtree, "Demonstrably doing accountability in the Internet of Things," *Int. J. Law Inf. Technol.*, vol. 27, no. 1, pp. 1–27, Mar. 2019.
[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
[13] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the Internet of Things: A survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–34, Jan. 2020.
[14] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[15] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.
[16] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4156–4165, Jun. 2020, doi: 10.1109/TII.2019.2948094.
[17] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.
[18] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2017, pp. 50–58.
[19] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, and S. B. Mandal, "IoT based secure smart city architecture using blockchain," in *Proc. 2nd Int. Conf. Data Sci. Bus. Analytics (ICDSBA)*, Sep. 2018, pp. 215–220.
[20] D.-P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A blockchain-based IoT forensics framework with identity privacy," in *Proc. TENCON IEEE Region Conf.*, Oct. 2018, pp. 2372–2377.
[21] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: A blockchain-based trust framework for collaborative Internet-of-Things," in *Proc. 24th ACM Symp. Access Control Models Technol.*, May 2019, pp. 83–92.
[22] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.
[23] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IOT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, 2019.
[24] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain-based consents management for personal data processing in the IoT ecosystem," in *Proc. 15th Int. Joint Conf. e-Bus. Telecommun.*, 2018, pp. 572–577.
[25] A. Crabtree, T. Lodge, J. Colley, C. Greenhalgh, K. Glover, H. Haddadi, Y. Amar, R. Mortier, Q. Li, J. Moore, L. Wang, P. Yadav, J. Zhao, A. Brown, L. Urquhart, and D. McAuley, "Building accountability into the Internet of Things: The IoT databox model," *J. Reliable Intell. Environments*, vol. 4, no. 1, pp. 39–55, Apr. 2018.
[26] M. Rhahla, T. Abdellatif, R. Attia, and W. Berrayana, "A GDPR controller for IoT systems: Application to e-Health," in *Proc. IEEE 28th Int. Conf. Enabling Technol., Infrastruct. Collaborative Enterprises (WETICE)*, Jun. 2019, pp. 170–173.
[27] G. Y. Lee, K. J. Cha, and H. J. Kim, "Designing the GDPR compliant consent procedure for personal information collection in the IoT environment," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2019, pp. 79–81.
[28] M. Koutli, N. Theologou, A. Tryferidis, D. Tzovaras, A. Kagkini, D. Zandes, K. Karkaletsis, K. Kaggelides, J. A. Miralles, V. Oravec, and S. Vanya, "Secure IoT e-health applications using VICINITY framework and GDPR guidelines," in *Proc. 15th Int. Conf. Distrib. Comp. Sensor Syst.*, Santorini Island, Greece, May 2019, pp. 263–270.
[29] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, and P. Burnap, "EclipseIoT: A secure and adaptive hub for the Internet of Things," *Comput. Secur.*, vol. 78, pp. 477–490, Sep. 2018.
[30] H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN- and IOT-based smart homes and their extension to smart buildings," *Sensors*, vol. 15, no. 5, pp. 10350–10379, May 2015.
[31] Y. Dong, Y. Wen, H. Hu, C. Miao, and C. Leung, "Design tradeoffs for cloud-based ambient assisted living systems," in *Proc. 2nd Int. Conf. Crowd Sci. Eng. ICCSE*, 2017, pp. 144–151.
[32] D. Basin, S. Debois, and T. Hildebrandt, "On purpose and by necessity: Compliance under the GDPR," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2018, pp. 20–37.
[33] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.
[34] H. Qiu, M. Qiu, G. Memmi, Z. Ming, and M. Liu, "A dynamic scalable blockchain based communication architecture for IoT," in *Proc. Int. Conf. Smart Blockchain*, Tokyo, Japan, Dec. 2018, pp. 159–166.
[35] R. Morabito, "Virtualization on Internet of Things edge devices with container technologies: A performance evaluation," *IEEE Access*, vol. 5, pp. 8835–8850, 2017.
[36] K. Dolui and C. Kiraly, "Towards multi-container deployment on IoT gateways," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[37] T. Al Said, O. F. Rana, and P. Burnap, "VMInformant: An instrumented virtual machine to support trustworthy cloud computing," *Int. J. High Perform. Comput. Netw.*, vol. 8, no. 3, pp. 222–234, 2015.
[38] N. E. Ioini and C. Pahl, "Trustworthy orchestration of container based edge computing using permissioned blockchain," in *Proc. 5th Int. Conf. Internet Things, Syst., Manage. Secur.*, Oct. 2018, pp. 147–154.
[39] E. Casalicchio and S. Iannucci, "The state-of-the-art in container technologies: Application, orchestration and security," *Concurrency Comput., Pract. Exper.*, p. e5668, Jan. 2020, doi: 10.1002/cpe.5668.
[40] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.
[41] *Cosmos Network: Internet of Blockchains*. Accessed: Jun. 10, 2020. [Online]. Available: https://cosmos.network/
[42] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," White Paper, 2017. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf
[43] *Ethereum*. Accessed: Jun. 10, 2020. [Online]. Available: https://www.ethereum.org/
[44] *Ropsten Testnet Pow Chain*. Accessed: Jun. 10, 2020. [Online]. Available: https://github.com/ethereum/ropsten
[45] *Solidity*. Accessed: Jun. 10, 2020. [Online]. Available: https://solidity.readthedocs.io/en/v0.5.3
[46] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

MASOUD BARATI received the Ph.D. degree in computer science from Sherbrooke University, Canada, in 2018. He is currently a Research Associate with the School of Computer Science and Informatics, Cardiff University. His research interests include distributed systems, blockchain, formal methods, and cybersecurity.



OMER RANA (Member, IEEE) received the Ph.D. degree in neural computing and parallel architectures from the Imperial College, University of London. He is currently a Professor of performance engineering with the School of Computer Science and Informatics, Cardiff University, and a member of Cardiff University's Data Innovation Institute. His research interests include distributed systems, blockchain, and scalable data analysis.



IOAN PETRI (Member, IEEE) received the Ph.D. degree in cybernetics and statistics and specialises on artificial intelligence, energy optimisation, cloud and edge computing, and data analytics with an application for the built and natural environment. He is currently a Lecturer with the School of Engineering, Cardiff University. He has published over 60 peer-reviewed articles in high impact journals and conferences in the field of applied distributed systems and energy management. He has served on the program committees of more than 25 international conferences and workshops. He is an inventor and the ICT Leader of the CUSP platform.

GEORGE THEODORAKOPOULOS received the Diploma degree from the National Technical University of Athens, Greece, in 2002, and the M.S. and Ph.D. degrees from the University of Maryland, USA, in 2004 and 2007, respectively, all in electrical and computer engineering. He is currently a Senior Lecturer with the School of Computer Science and Informatics, Cardiff University. His research interests include data privacy and security.