Implementation of the GDPR Compliant Data Handling for Smart Home Solution

Sandra Bugarin, Sandra Ivanović, Marija Antić

***Abstract*—The amount of personal data collected and shared in the Internet of Things (IoT) is causing increasing concerns regarding the user privacy in IoT. The recently introduced General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information and aims to strengthen user rights. In order to comply with the GDPR requirements, the existing smart home system is extended with the cloud service, responsible for user consent management and appropriate data handling. The architecture of the solution, as well as the results of functional and performance testing are presented in this paper.**

***Index Terms*— GDPR; smart home automation; IoT**

I. Introduction

The users surfing the web are under a risk of privacy violation, as the websites are collecting data about them and may be sharing it with third party services. Recently, the General Data Protection Regulation (GDPR) has entered into force, with the aim to protect the user privacy, and allow them better control over the collected data and the scenarios it is used in [1]. According to GDPR, the services are required to inform the users about the types of data collected and the purpose of this action, so the users can choose to engage only with websites and services that do not violate their privacy, or opt out of the use of their information for particular purposes.

While the data collected by the websites usually serves only marketing purposes, and is not necessary for the normal operation of the website, the problem of GDPR compliance in Internet of Things (IoT) solutions is of a more complex nature [2]. Namely, IoT systems typically connect multiple devices owned by a single user, and allow them to perform a certain function together. Therefore, the exchange of data is in the essence of IoT. On the other hand, there exists a tendency in the IoT solutions to collect more data than actually needed for the normal system operation, as it may become useful in the future scenarios [3], [4]. This data should be carefully stored and protected, as well as anonymized [5], and the users should be provided with the mechanisms to inspect or delete the collected data at any time [6]. Also, it is necessary to be transparent about the ways data is processed, to inform the users timely when the privacy policies change, and to allow them to opt out of the service if they do not agree to the changes.

Studies have been conducted that show that the user attitude towards data collection depends on multiple factors, such as the environment the data is related to (home, office, traffic), types of data collected (video, photo, sensory data, voice), who has access to it (government, businesses), as well as the purpose of data collection (safety, convenience, marketing) [7]. Smart home users are willing to allow data collection as long as it is used only within the system, for the purpose of connectivity and convenience [8], but seem not aware of the possible privacy issues associated with machine learning and potentially sensitive information that can be revealed by data analytics [9]. This information should be communicated through the privacy policy and terms of use, in a manner that is transparent and clear to the user, and explains why certain types of data are needed for the normal operation of the system [10].

In this paper, we extend the existing smart home solution with the cloud service responsible for GDPR-compliant data handling. This service allows administrators to handle privacy policy updates, and the users to request the export or deletion of personal data, as well as the deletion of the user account. First, we introduce the smart home solution architecture in Section II. Then, in Section III the operation of the GDPR service is explained, while the results of functional and performance testing are presented in Section IV and Section V.

II. SMART HOME SYSTEM ARCHITECTURE

The smart home solution we extend is comprised of a gateway, client applications (Android, iOS and web) and cloud services.

The gateway is a key component in the smart home because it acts as a bridge between clients and smart devices in the smart home system. Gateway's main purpose is to pull together all compatible devices into a universal platform. This allows applying control scenarios to all of them while being agnostic of the actual communication interface – ZigBee, ZWave, and IP nodes are seamlessly integrated into one unified device/node network. On top of this core functionality gateway implements network API's for client applications, mechanism to define and execute rules, advanced control over the home zones, firmware upgrade, backup/restore, etc.

Sandra Bugarin is with OBLO Living, Narodnog fronta 21a, Novi Sad, Serbia (e-mail: sandra.bugarin@ obloliving.com).

Sandra Ivanović is with the Faculty of Technical Sciences, University of Novi Sad, Serbia (e-mail: sandra.ivanovic@rt-rk.uns.ac.rs).

Marija Antić is with the Faculty of Technical Sciences, University of Novi Sad, Serbia (e-mail: marija.antic@rt-rk.uns.ac.rs).

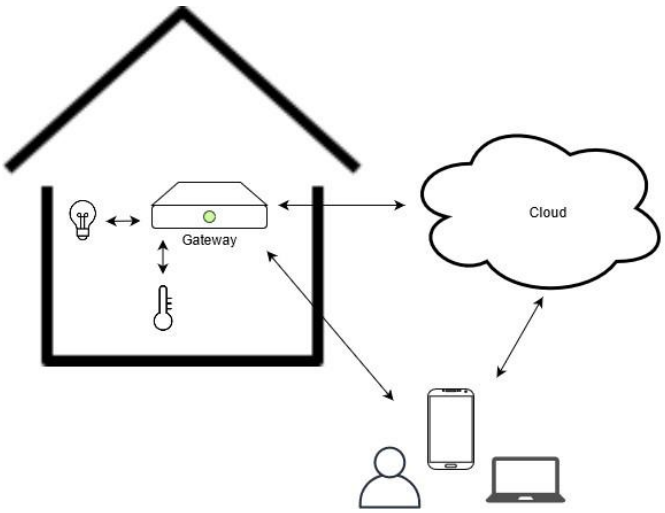

Fig. 1. Smart home system architecture.

Client applications provide the user interface for system provisioning, configuration and management. They enable users to access their home gateway in local network or remotely over the cloud. On the other hand, the cloud is responsible for user and gateway identity management, mirroring the smart home gateway configuration and data, allowing remote access for the client applications, historical data collection and analytics.

For certain functionalities of the system to be enabled, the user needs to provide the address of the household, i.e. their geolocation [11]. Also, phone number and email are needed for the purpose of smart notifications. Additionally, the system collects and stores the state changes of all devices, in order to provide the users with the possibility to inspect the way certain device types have been used in the previous period [12]. Also, the information about the local IoT network is stored for diagnostics purposes. All of these entries represent the data that should be treated according to GDPR.

III. GDPR-Compliant Data Handling

To comply with the GDPR requirements, the microservice is created within the smart home solution cloud, which enhances the system with the following functionalities:

- Update of Privacy Policy and Terms of Service
- Export of Personal Data,
- Deletion of User Account

In this section, the details about the service implementation will be presented. All of the cloud services are highly available, and GDPR service is no exception. The simplified architecture is presented in Fig. 2. Multiple instances of the service implemented in Node.JS are running on the environment. They share the long-term MongoDB data storage, as well as the temporary Redis storage. Also, the shared cloud storage disk is available to all services that need to store large files, not suitable for MongoDB database. To control the load and orchestrate tasks within the environment, RabbitMQ is used.

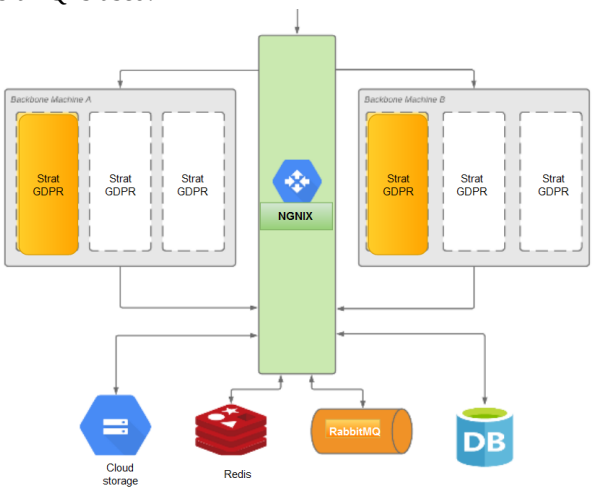

Fig.2. Highly available GDPR service.

A. Update of Privacy Policy and Terms of Service

The Privacy Policy should help users to understand what information is collected, for which purpose, and how users can update, export, and delete their information. Information about privacy policy and terms of service is the part of registration process, so all new users have to read it, and agree in order to register their smart home account.

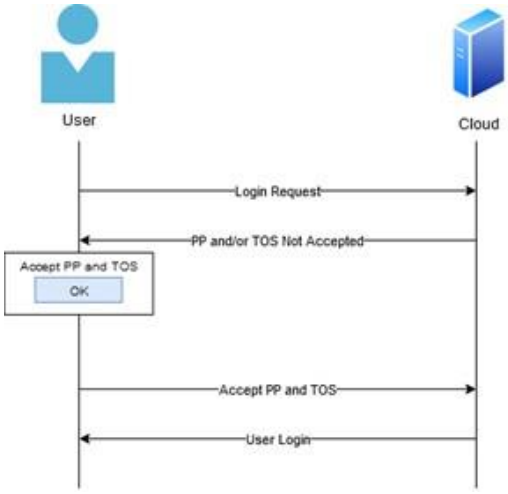

Fig. 3. Privacy policy acceptance upon login.

The existing users that have not read the new privacy policy well be prompted to read it and agree to it after logging onto web or mobile applications, as presented in Fig. 3. Until they agree to new privacy policy, users will not be able to use the applications. Gateways connected to user's account will be deactivated and prevented from sending any new sensory information to the smart home cloud.

Users can reactivate their account and gateways if they accept new privacy policy on login, or if they click on the link to new privacy policy that has been emailed to them.

B. Personal Data Export

As already said, personal data consists of user's personal profile information, such as name, email, phone contact, geolocation and address of the household. It also includes the state history of the end devices in the system, gateway backups and local IoT network history logs, which are stored for the purpose of diagnostics. Therefore, the exported data contains three groups of JSON files. The first group contains the data from the user's profile, the second one represents the snapshot of the gateway's current state, while the third one represents the usage history of all devices that have been connected to user's gateway(s).

The data export service will run on demand, under control of administrator. It performs the following tasks:

- Database crawl for personal data,
- Compression of this data to a ZIP archive, which is temporarily stored in the cloud, until the user downloads it,
- Deletion of outdated personal data

The collection and deletion of all data for an individual user can be started by the administrator, upon a request from the user (Fig. 4). Administrators can start or stop data export task that have not been completed, and delete completed export tasks and data file associated with them if they are older than 15 days. Also, they can monitor the progress of currently running data collection tasks. Administrators are not able to view the contents of the exported data files or to remove data export tasks that still haven't completed.

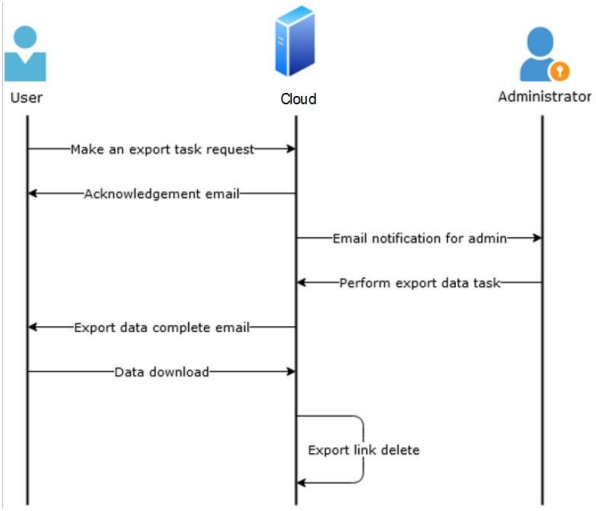

Fig. 4. Export data flow

When the user makes a personal data export request, they will be notified via email that their request has been acknowledged. A similar notification will be sent to the administrator, with the link that allow to monitor that export task. When the export task has been completed, another notification will be sent, this time with a HTML link to data export file. Download link will be available for the next 15 days. After this period, the export task and the associated export data file will be removed.

By default, only single process per backbone instance is allowed to execute data collection and compression tasks. Reason for this is intense I/O and CPU utilization (for DB crawl and data compression, respectively). Every process will be given a certain amount of time to complete it (e.g. 5 minutes) by placing the key-value pair in redis with the same expiration time. Given that database and redis are the only shared state between backbone instances, they can be used for tracking of task progression: if one of the instances that is running collection task crashes or restarts, time for task completion will expire and this task will fail.

C. User Account Deletion

At any time, a user can request to delete their account. Administrators are obliged to fulfil this request, by performing the account deletion operation via the administrative portal – Fig. 5. During this process, all of the gateways assigned to the user will be un-assigned from the user account, and all personal data from the cloud will be deleted.

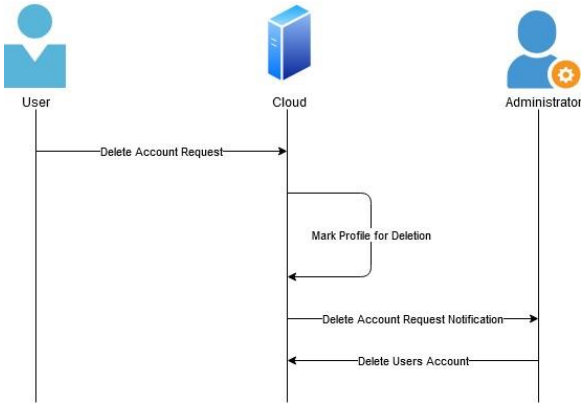

Fig. 5. Account deletion flow

However, the device usage data will be kept for analytics purposes. This data is in anonymized state, which means that it does not contain any information that can be traced to the original user.

IV. Functional Verification

A. Privacy Policy Acceptance and Modification

During the process of account creation, the user is asked to agree to the terms of service and the privacy policy.

The administrator can upload the new privacy policy and terms of service documents using the web portal for system administration – Fig. 6.

Fig. 6. Privacy policy and terms of service update.

Fig. 7. Modal dialog prompting the user to accept new privacy policy.

On next login attempt, every user will be prompted to accept new privacy policy and terms of service via modal dialog – Fig. 7. Until they accept, they will not be able to use the applications.

B. Data Export

On the user profile, a button is implemented which allows them to request the export of personal data. This button is disabled if another request is already processed. This tab also contains a link to personal data when collection task is finished – Fig. 8. Implications are, that a new data export request can be made after 15 days (guaranteed duration of the valid export link) plus the time needed to perform the data export request.

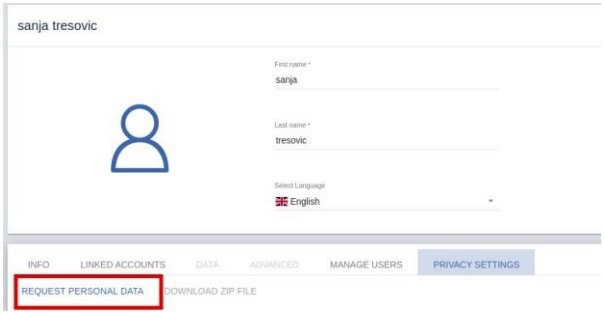

Fig. 8. User requesting personal data export.

From the administrator side, the status of the pending, current and past data export tasks can be monitored, as in Fig. 9.

Fig. 9. Administrative panel for export task monitoring.

V. Performance Testing

We have tested the implemented solution to asses the average time needed to prepare the export ZIP file with user data, depending on the data size. Typically, the size of the exported data is 5-10 MB, although for the setups with many devices it can increase up to 30 MB. The time needed for data export is presented in Fig. 10. It can be observed that the data export can be performed in less than 10 s for typical setups, while for the larger setups the time needed increases to the order of minutes. However, since the user will be informed by the notification when this process is finished, the performance of the solution is acceptable for the practical purposes.

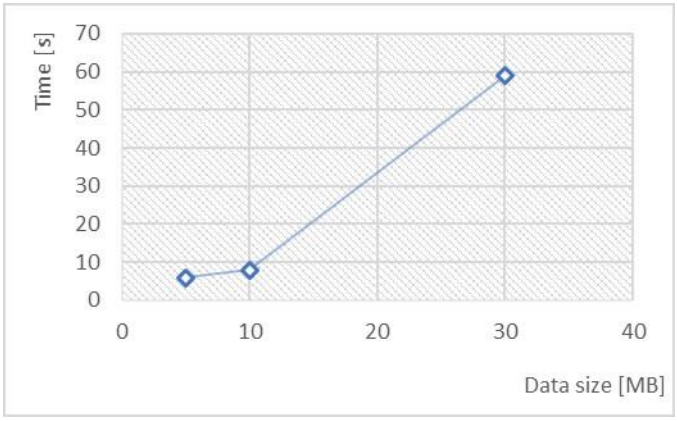

Fig. 10. Time needed to export data depending on the total size of the data file.

VI. Conclusion

In this paper, one implementation of the GDPR-compliant data handling in smart home solution has been presented. The cloud service was created, that handles the relevant aspects of data handling and user consent management, such as the update of terms of use and privacy policy, data export and account deletion. The implemented functionality has been verified, and it has been shown that the times needed for data export are acceptable. In the future work, this solution will be extended to allow users the finer granulation over the types of data collected and services enabled. For example, the users may want to opt out of the advanced functionalities, based on data analytics and machine learning, while still wishing to allow the exchange of data needed for the basic system operation.

Acknowledgment

This research has been supported by the Ministry of Education, Science and Technological Development through the project no. 451-03-68/2020-14/200156: “Innovative scientific and artistic research from the FTS activity domain”.

References

[1] A. Tsohou, E. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, B. Gallego-Nicasio Crespo, “Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform,” *Information and Computer Security*, vol. 28, no. 4, pp. 531-553, Oct. 2020

[2] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, A. V. Vasilakos, “The Quest for Privacy in the Internet of Things,” *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36-45, Mar. 2016

[3] S. Wachter, “The GDPR and the Internet of Things: a three-step transparency model,” *Law, Innovation and Technology*, vol. 10, no. 2, pp. 266-294, Sept. 2018

[4] S. Watcher, “Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR,” *Computer Law & Security Review*, vol. 34, no. 3, pp. 436-449, June 2018

[5] C. Perera, R. Ranjan, L. Wang, S. Khan and A. Zomaya, “Big Data Privacy in the Internet of Things Era,” *IT Professional*, vol. 17, no. 3, pp. 32-39, May 2015

[6] A. D. Kounoudes, G. M. Kapitsaki, “A mapping of IoT user-centric privacy preserving approaches to the GDPR,” *Internet of Things*, vol. 11, no. 100179, Sept. 2020

[7] H. Lee, A. Kobsa, “Understanding user privacy in Internet of Things environments,” *Proc. of World Forum on Internet of Things (WF-IoT)*, Dec. 2016

[8] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, ChungHorng Lung, “Smart Home: Integrating Internet of Things with Web Services and Cloud Computing,” *International Conference on Cloud Computing Technology and Science*, Dec. 2013

[9] S. Zheng, N. Apthorpe, M. Chetty, N. Feamster. “User Perceptions of Smart Home IoT Privacy”, *Proc. of the ACM on Human-Computer Interactiion.* vol. 2, no. CSCW, pp. 1-20, Nov. 2018

[10] K. Renaud,L. A. Shepherd, “How to make privacy policies both GDPRcompliant and usable,” *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Nov. 2018

[11] M. Matić, M. Tucić, M. Antić, R. Pavlović, “Using online third party geolocation services to improve smart home user experience,” Serbian Journal of Electrical Engineering vol. 17, no. 1, pp. 83-94, Feb. 2020

[12] S. Ivanović, M. Antić, I. Papp, N. Jović, “Data Acquisition, Collection and Storage in Smart Home Solutions,” *Proc. of 6th International Conference on Electrical, Electronic and Computing Engineering (IcETRAN)*, May 2019