Sharing Is Caring

Design and Demonstration of a Data Privacy Tool for Interorganizational Transfer of Data

Hussain, Abid; Lasrado, Lester Allan ; Mukkamala, Raghava Rao; Tanveer, Usman

Document Version
Final published version

Published in:
CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020

DOI:
10.1016/j.procs.2021.01.182

Publication date:
2021

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 181 (2021) 394–402

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

Sharing Is Caring – Design and Demonstration of a Data Privacy Tool for Interorganizational Transfer of Data

Abid Hussain[a,b], Lester Allan Lasrado[b,*], Raghava Rao Mukkamala[a,b], Usman Tanveer[a]

[a]*Centre for Business Data Analytics, Dept. of Digitalization, Copenhagen Business School, Denmark*
[b]*Department of Technology, Kristiania University College, Norway*

Abstract

This paper presents a Data Privacy Tool (IDPT) that is designed to provide a holistic and secure data management in organizations for handling, securing, sharing and re-sharing of data. The current version of IDPT allows the data controller in the organizations to configure data encryptions based on privacy obligations in a given context. This paper presents an inter-organizational use case scenario and subsequent demonstration of IDPT highlighting its user-friendly interface, security features (e.g. 2-way authentication, deletion of data after processing) and transparency of handling data.

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

Keywords: Data Privacy, Data Stewardship, Design Security, Data Transfer

* Corresponding author.
E-mail address: lesterallan.lasrado@kristiania.no

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020
10.1016/j.procs.2021.01.182

1. Introduction

The world has become increasingly digitized, thus generating large volumes of personal data. This user-generated content and personal data are extremely valuable as it contains people's opinions, expressions and judgements and therefore it is extremely important for both research and commercial applications. It is an established idea that properly sharing personal and organizational data will benefit all related stakeholders including users, researchers, organizations and the whole society [33, 35]. However, recent scandals (e.g. Cambridge Analytica) of organizations misusing people's personal information has raised some very serious concerns about the technical, commercial, political and ethical aspects of personal data collection and analysis by platform owners, researchers and other third parties [35, 11].

These privacy concerns regarding data sharing are impacting decisions not only in organizations (e.g. IT operations, cloud adoption, open data initiatives), but also in academia i.e. researchers and students alike. This is especially true in Europe, and particularly in the Nordics wherein there is strict implementation of laws concerning the use, storage and handling of personally identifiable information [27, 14]. One example is the European Union's new GDPR [12], which came into effect in May 2018. According to Faber, Michelet et al. [11], while GDPR is designed to protect the end-users and/or data subjects, the regulation is also seen as a burden by the organizations, researchers and students who work with data. In line with GDPR, other governmental agencies in Europe have also prescribed guidelines and requirements on how research data containing personal information must be handled, hosted and stored for research projects at universities. Recent studies have emphasized on the need of building new tools and frameworks that support data sharing as well as deal with the cumbersome issue of data privacy [5, 3, 32]. In order to minimize data privacy breaches, research community has recently increased its efforts within this domain of enquiry, as a result it can be observed from the literature that such tools and frameworks are being reported [4, 34, 18, 24]. In the pursue of meeting strict guidelines for data privacy requirements, there has been a dearth of automated tools available to researchers and students to secure their data. Therefore, in this paper, we report on the design, development and features provided by a methodologically grounded IT artefact (i.e. Instant Data Privacy Tool "IDPT") that addresses one of the issues associated with securing and sharing data. As discussed in the paper, IDPT focusses on transforming data according to the level of privacy required in any given regulatory system. Our main research question is: How different kinds of techniques and algorithms can be used in a user-friendly manner to secure personal data in such a way to enable sharing of data?

The remainder of the paper is organized as follows. First, we present design science research methodology employed. Second, we present a data-sharing scenario arguing for the need of such an artefact. Through the analysis of this scenario, we present terminologies and requirements. Third, we discuss the system design (IDPT) and demonstrate its current version. Finally, we discuss future work.

2. Design Science Research (DSR) Methodology

IDPT has been developed in a systematic and iterative way, following the design science methodology for developing artefacts [16, 20]. We followed the DSR approach as we were answering a "how to" type of a question. According to Hevner, March et al. [16]), DSR "must produce a viable artefact in the form of a construct, a model, a method, or an instantiation". The final product here is an instantiation in the form of web-based software for facilitating secured data transfer between two entities (i.e. individuals and/or organizations). While there are many frameworks and guidelines proposed on how to conduct DSR, we are following the iterative DSR approach proposed by Peffers, Tuunanen et al. [20] and recommendations by Gregor and Hevner [13].

- The first step was to identify the problem situation; this was done by talking to relevant stakeholders (i.e. researchers, students and practitioners). Requirements for the proposed artefact were gathered in this stage. The scenario presented in the next section will provide an anecdote.
- The second step was to design and develop an artefact (IDPT) to address the problems; web-based tool presented in this paper was developed in this stage. This was done using agile software development and Scrum framework [31, 9].
- Next steps are to demonstrate the artefact in practice, in the process evaluating its applicability and communicating the results (future work).

3. Scenario and Terminologies

3.1. Real life Scenario

Siv is a product manager at a large logistics organization |in the Nordics, who is currently collaborating on a research project with a Norwegian university. She plans to extract and share customer data from her organizations' Facebook page with the researchers at the university. The goal of the short project is to identify people (customers) who associate actively and emotionally with the organization via Facebook. The researchers plan to conduct some interviews with a subset of these customers too. After completing the study, both the university and organization have requested Siv to store the raw data for verification with them. The researchers have also asked Siv to store the data for replication studies in the future. However, Siv has read the guidelines prescribed by the Norwegian Centre for Research Data (NSD)[†] and has concerns over sharing the raw data. The following are some constraints she faces:

- While the IT team at her company suggested Siv to anonymize and aggregate the data, the researchers at the organization fear that anonymization might result in loss of information.
- Neither the university nor her organization has clear guidelines on transfer, storage or handling of data for an inter-organizational operation.
- If Siv wants to facilitate "re-sharing" in the future beyond the current research team without compromising the personal data regulation prescribed by NSD and GDPR, then how could she ensure that?
- Finally, could the logistics company or the university track "re-sharing" of the same data in the future i.e. when someone accesses the data, could the university keep track the event and inform Siv and her organization.

While the scenario above is an anecdote of a real-life situation showcasing a university-organization partnership, similar challenges[‡] are encountered by social scientists, industry managers and government officials. Therefore, in the interest of generalization, we will define some terminologies related to the topic.

3.2. Terminologies

Figure 1 shows a typical data sharing and processing procedure in accordance with GDPR. Firstly, the collection and processing of personal data are allowed only when the "data subject" has given their consent[§]. Moreover, the consent is limited for a specific purpose of data processing and the data subject must be informed explicitly. The "data controller" is an entity responsible for the collection, storage and handling of data and must ensure "anonymity[**]" of personal data before passing it on to a third party for "data processing". The "data controller" cannot define a too generic data processing purpose and cannot change the purpose of use arbitrarily [7, 14].

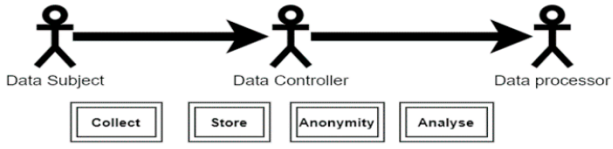

Fig. 1. Personal data handling process [14].

[†] https://nsd.no/nsd/english/index.html

[‡] Siv's scenario presented is just an example. Another scenario: While APIs are the most favourable method for data sharing between organizations, batch data files transfer is still part of everyday data sharing procedures between organizations. E.g.: A company transferring its transactional and sales data to a marketing agency once a week to conduct cold calling campaigns.

[§] Some exceptions are allowed, but GDPR defines the boundaries clearly.

[**] Anonymity here refers to the privacy of the data subject. It refers to policies, practices and techniques employed so that direct or indirect re-identification of a data subject is not possible [11]. Multiple data anonymization and Encryption techniques employed in practice [7, 22].

Data Subject: is an individual(s) whose personal information is collected. Data subjects should give consent and delegate their data sharing rights to the data controller [7]. For the scope of this paper, any information collected about the data subject (be it directly or indirectly from third parties) are subject to privacy obligations.

Data Controller: are entities that collect, store and host the data about the data subject. They are responsible to define and enforce the data sharing policy in accordance with the prescribed regulatory or legislative constraints of their country and/or region [14].

Data Processor: are entities who are granted access to data subject's data resource [7]. The kind of data they access (i.e. anonymized, encrypted or otherwise) is governed by data sharing policy defined by the data controller. The processor could be someone within the organization or an outside third party.

Privacy Obligations: is a policy document that "captures any restriction the data subject wants to put on the data consumer related to reasons for accessing their data, or restrictions on what use that is made of the data. Responsibility for providing data at required granularity (i.e. level of encryption) lies with the data controller" [7].

Sharing and Re-sharing Conditions: are conditions governing the situation wherein a data controller or processor shares the data internally or with a third party. Moreover, it also governs the delegation of "sharing rights" to a third party[††] so that the data can be shared further [33, 7]. In this paper, we propose that the data controller only shares the anonymized or encrypted version under the re-sharing agreement.

Applying the proposed terminologies to our scenario, we argue that Siv is both the data controller and data processor in the meantime, until the current project is completed. Once that is done, all stakeholders (Siv, university and her organization) could take the role of the data controller. Siv would have to clearly define the "privacy obligations" with provisions wherein the data subject has an option to withdraw consent at any point in time. Under the privacy obligation, the responsibility of allocating the appropriate level of sensitivity is collectively allotted by the three main stakeholders. An example of the sensitivity level[‡‡] proposed by Siv is shown in figure 2. While personal information like the name is given a very high level of sensitivity, the number of times the post is shared is allocated the lowest level.

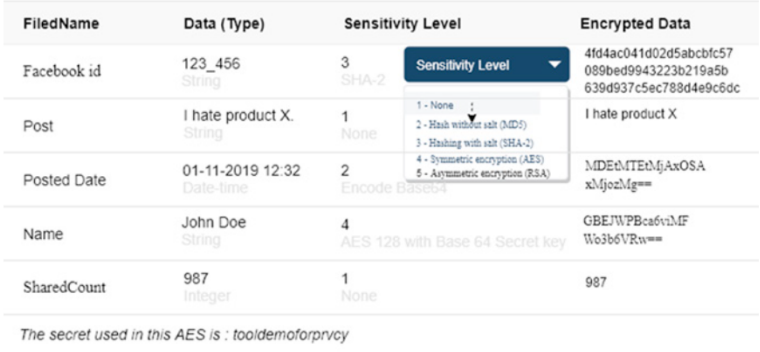

Fig. 2. Personal data and level of sensitivity.

Based on analysis of the scenario (Siv's case), we next present design and demonstration of IDPT; a tool designed to facilitate this secure data transfer between different stakeholders.

[††] When the data is collected from Facebook, the consent for use, storage and re-sharing must be in accordance with Facebooks data privacy policy. The same holds for other platforms as well.

[‡‡] For our research purposes, we operationally define sensitivity level as the level of encryption that a variable is allotted. Higher the privacy requirements, larger the level of sensitivity (i.e. stricter the encryption). This definition will evolve over time as the tool develops further.

4. IDPT: Design and Demonstration

The overarching goal of this paper is to provide a holistic and secure data management tool to the data controller (i.e. secure data, sharing and re-sharing). This can be achieved by designing a system that satisfies the following design guidelines:

- Data Controller centric system: Empowering the controller to a large degree.
- Security: Data processed in an encrypted form and secure interaction with all the stakeholders.
- GDPR-compliant: Delete data immediately when consent is withdrawn by a data subject.
- Transparency: All stakeholders should know the status of the data at any time.
- User-friendly interface: We found our audience would be non-technical, hence the tool must be easy to use.

In the current version of IDPT have incorporated about 60% of the design guidelines. The tool needs further development (as discussed in future work) wherein all the requirements and guidelines would be incorporated. IDPT[§§] (Version 1) is designed as a web-based tool and provides 5 levels of sensitivity as shown in table 1.

Table 1. Proposed layer of sensitivity level – Scale 1 to 5

Level of Sensitivity	No sensitivity (1)	Low sensitive (2)	Sensitive (3)	Highly sensitive (4)	Critical (5)
Algorithm	None	Encode Base64	Hashing with salt (SHA-2)	Symmetric encryption (AES)	Asymmetric encryption (RSA)
Examples	Product name, Asset Value	Gender, Date of Birth	Name, Place of Birth, Parents, Children	Social Security Number	Health Records Details

**Due to page limitations, the encryption algorithms employed are presented briefly in section 4.1.*

Currently, while the design facilitates secure data transfer between the stakeholders, the responsibility of storage and transmission is solely on the data controller. One of the main reasons for representing the encrypting algorithms as the level of sensitivity is to hide the technical details and complexity of algorithms from the users of IDPT, as they are mostly non-technical (i.e. managers, analysts, administrators, student workers, etc.). This design consideration follows the design guideline of making IDPT user-friendly and easy to use by the non-technical users as well. Secondly, this makes scaling or addition of new encrypting techniques easier. For example, SHA-2 is currently considered very good for achieving a reliable hashed output. This is proposed to be on sensitivity level 3 in our framework. However, there may be updates in the domain of data privacy that enables application of even better algorithm for data hashing. In that case another algorithm would be required to achieve sensitivity level 3. Therefore, we have implemented a dynamic framework and policy obligations that could be periodically reviewed to update this mapping of the sensitivity level.

4.1. Data Privacy/Encryption Algorithms Employed in IDPT

The following are the data privacy methods that were employed in IDPT tool to secure the personal data.

Encoding: To store data on computer systems or to transfer data over any medium between two machines, data must be encoded in a standard way. Encoding is a data transformation technique that transforms data between different encoding systems. Base64 encoding scheme is used to encode binary data that needs to be transferred over or stored in a medium and the result of this encoding will be textual data, containing a particular set of 64 characters. Base 64 encoding can be used to transfer binary data in textual form. Here the goal is not to keep data secret, but rather to transform data into another format, such that the original data is unreadable without decoding [17]. With respect to IDPT, Encoding serves the purpose of securing data from naked eye. For example, a user has to decode the data to access the actual contents.

[§§] One can access the tool here: http://151.177.35.200/software/idpt/. IDPT is designed to cater datasets that have structured data formats.

Hashing is a one-way computation that generates a unique digital footprint for any given amount of data. A hash function maps data of any arbitrary size to fixed-size value, normally called as hash-digest [29]. As it produces a unique hash value for a given data, the hash-digest can be stored to check the integrity of the data. Another important property of hashing is the hiding property. It is practically impossible to retrieve the original data from a given a hash-digest, therefore, it is secure to share the hash-value of the original data rather than the original data itself (person names etc.), if the purpose is to hide the sensitive information in sharing. There have been many algorithms that can be used for Hashing [21], however SHA family of algorithms has been accepted as standard for hashing by NIST [23, 29].

SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the National Security Agency (NSA) of United States. SHA-256 generate a 256-bit (32 byte) text representation of the original text. A secured key known as Salt can be used to generate quite unique and secure computed text. Cryptography is a science of secret writing; wherein plain text is transformed into ciphertext that human can't understand without computationally processing it [26, 8]. Data Encryption Standard (DES) was one the first encryption standard published by National Institute of Standards and Technology [30, 22, 15]. There are two widely accepted ways that encryption is utilized a) Symmetric key encryption b) Asymmetric key encryption. IDPT utilizes hashing to achieve anonymity and is ideal for sharing sensitive data safely for research purposes as the actual personal data is not retrievable.

Symmetric key encryption utilized algorithm that relies on same key for encryption and decryption. The person who is providing data and the one consuming data share the same secured key [28, 15]. Advanced Encryption Standard (AES) is one of the most used algorithms for symmetric encryption. The current accepted standard for AES [22] was developed based their algorithm on Daemen and Rijmen [10] and replaced DES according to NIST recommendation in 2001. AES supports different key sizes for encryption and different key sizes versions are referred as AES-128, AES-192 and AES-256 [10, 28].

Asymmetric encryption algorithm relies on a set of public and private key where public key is used to encrypt the data and private key is used to decrypt the data at the receiver end [28]. RSA is an asymmetric encryption algorithm that is one of the most utilized encryption methods. The method was first introduced by Rivest, Shamir et al. [25] back in 1977; RSA and AES have been tested over time and are considered the safest methods to achieve reliable secure transfer of data between two parties [6, 2]. IDPT suggests usage of Symmetric and Asymmetric encryption methods at the highest sensitivity, levels 4 and level 5. Such encryption methods are used in cases where actual data needs to be preserved and restored at the receiver end however making data safe while being shared on even unsecured data transfer channels.

4.2. Demonstration of IDPT: How does it work?4

To demonstrate the application of IDPT using Siv's case, we assume that Siv has completed all her analysis and is now in the process of sharing the data with other stakeholders using IDPT. Her interaction with the system will follow the steps as illustrated in figure 3; which clearly illustrates the sequence of how IDPT can be employed the data controller to secure and share the data.

Firstly, Siv will have to define the data privacy obligations and store the raw data in a secure location. Using the web interface (Figure 4 in Appendix A) she can upload the file with raw data (e.g. CSV file) which has a delimiter separated (e.g. semicolon). Once the file is uploaded, IDPT will read all the columns and Siv is presented with the list of variables and an option to set the level of sensitivity required for each variable. Siv allocates level 4 to name, level 3 to Facebook_id and level 2 to posted date as shown in figure 2. IDPT will ask Siv to enter a passcode depending on the level of sensitivity chosen.

The interface then allows them to submit this selected configuration and an email address for the given dataset. The engine running on the webserver will read the configuration and apply the relevant transformation function. Once data conversion is complete, the data processor (her supervisor) will get an email to download the encrypted data.
This email will contain the WorkflowId, which is a unique id. Siv holds the passcode, which is available directly from the web interface. In the current version of IDPT, we expect Siv to send the passcode via phone or SMS to the researchers. Using the download option, the researchers can get a compressed folder which contains a file with encrypted data (figure 2) and metadata encoded with the privacy key settings. Again, in the current version, we advise that the researchers save the encrypted and metadata file in separate locations.

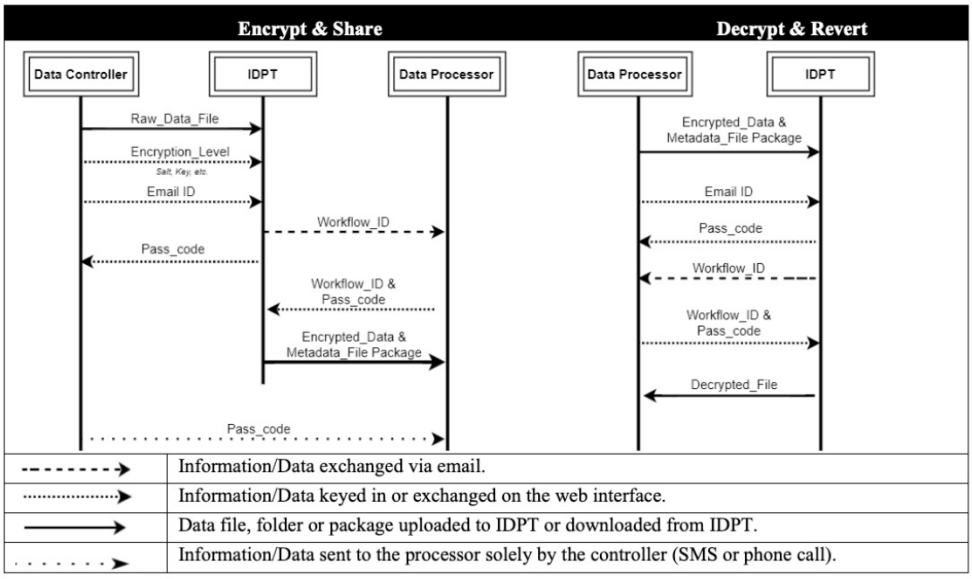

Fig. 3. Sequence to secure and share data.

Using the decrypt and revert feature of IDPT, the researchers can retrieve the original data as well. In our scenario, Siv wants to secure some data (e.g. Facebook_id) permanently and employs sensitivity level 3 (i.e. one-way hashing SHA-2). This ensures that Facebook_id is shared only in its encrypted form in the future. Through this short demonstration, we have showcased a practical application IDPT is a real-life setting. We have also uploaded a demonstration video*** to show its basic features.

5. Conclusion and Future Work

The demonstration of IDPT presented in this paper highlighted the user-friendly interface of IDPT, security features (e.g. 2-way authentication, deletion of data after processing) and transparency of handling data. However, this version of IDPT has a lot of limitations and needs further development to satisfy the holistic goals of creating a secure data management tool. First limitation is lack of secure data storage features in the current version. Second is our expectation from data controllers and data processors to self-regulate with regards to (1) securing the files provided to them, (2) tracking and tracing their re-sharing history. This is a big limitation with regards to ensuring guaranteed transparency and security.

Third, IDPT currently is limited to data transfer only between two entities. Extending this to multi-actors would improve its applicability and usefulness. Therefore, as part of future work, we would first explore the foundations of blockchain, smart contract technologies to develop a system to secure personal data [19, 35, 11]. We believe that by introducing blockchain, we can establish secure storage, high-level trust and security, which are all limitations of IDPT.

We could also hand over full control to the data controllers, while tracking the re-sharing history in a transparent manner. Secondly, we would work of incorporating revoking consents feature in our system design. Third, we will test the current version of the tool with more participants and improve continuously. Finally, we will include data anonymization techniques [27] in future versions of IDPT, thus providing the data controllers with more options. One of such options is zero-knowledge proofs [1], which allow people to share proofs to the original data, rather than sharing the data itself.

*** Video: https://www.dropbox.com/sh/os9c2dsmhc4cegx/AACv67ceXLfdVSqBcZu_ARVja?dl=0

Appendix A. IDPT Web Interface and Process Flow

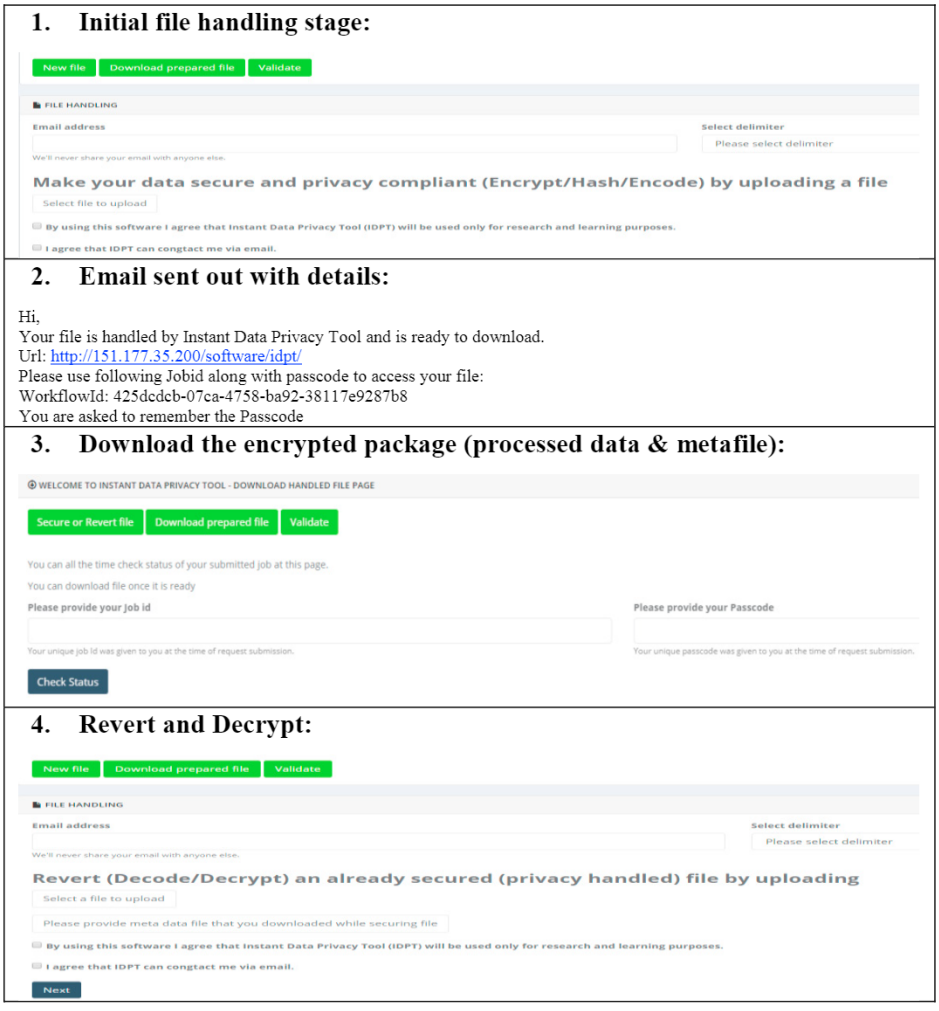

Fig. 4. Instant Data Privacy Tool web interface.

References

[1] Agrawal, S., C. Ganesh and P. Mohassel (2018) "Non-interactive zero-knowledge proofs for composite statements." *Annual International Cryptology Conference*, Springer.

[2] Al Hasib, A. and A. A. M. M. Haque (2008) "A comparative study of the performance and security issues of AES and RSA cryptography." *2008 Third International Conference on Convergence and Hybrid Information Technology*, IEEE.

[3] Alpers, S., S. Betz, A. Fritsch, A. Oberweis, G. Schiefer and M. Wagner (2018) "Citizen empowerment by a technical approach for privacy enforcement." *CLOSER 2018 - Proceedings of the 8th International Conference on Cloud Computing and Services Science*.

[4] Amo, D., D. Fonseca, M. Alier, F. J. García-Peñalvo, M. J. Casañ and M. Alsina (2019) "Personal Data Broker: A Solution to Assure Data Privacy in EdTech," in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). **11590 LNCS:** 3-14.

[5] Bettini, C. and D. Riboni (2015) "Privacy protection in pervasive systems: State of the art and technical challenges." *Pervasive and Mobile Computing* **17**(PB): 159-174.

[6] Boneh, D. (1999) "Twenty years of attacks on the RSA cryptosystem." *Notices of the AMS* **46**(2): 203-213.
[7] Chowdhury, M. J. M., A. Colman, J. Han and M. A. Kabir (2018) "A policy framework for subject-driven data sharing." *Proceedings of the 51st Hawaii International Conference on System Sciences*.
[8] Coron, J.-S. (2006) "What is cryptography?" *IEEE security & privacy* **4**(1): 70-73.
[9] Curcio, K., T. Navarro, A. Malucelli and S. Reinehr (2018) "Requirements engineering: A systematic mapping study in agile software development." *Journal of Systems and Software* **139**: 32-50.
[10] Daemen, J. and V. Rijmen (1998) "The block cipher Rijndael." *International Conference on Smart Card Research and Advanced Applications*, Springer.
[11] Faber, B., G. C. Michelet, N. Weidmann, R. R. Mukkamala and R. Vatrapu (2019) "BPDIMS: A blockchain-based personal data and identity management system." *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
[12] GDPR (2016) "Regulation (EU) 2016/679 of the European Parliament and of the Council." *REGULATION (EU)* **679**: 2016.
[13] Gregor, S. and A. R. Hevner (2013) "Positioning and presenting design science research for maximum impact." *MIS Quarterly* **37**(2).
[14] Gruschka, N., V. Mavroeidis, K. Vishi and M. Jensen (2018) "Privacy issues and data protection in big data: a case study analysis under GDPR." *2018 IEEE International Conference on Big Data (Big Data)*, IEEE.
[15] Gupta, A. and N. K. Walia (2014) "Cryptography algorithms: A review."
[16] Hevner, A. R., S. T. March, J. Park and S. Ram (2004) "Design science in information systems research." *MIS Quarterly* **28**(1): 75-105.
[17] Josefsson, S. (2006) "The base16, base32, and base64 data encodings," RFC 4648, October.
[18] Makhdoom, I., I. Zhou, M. Abolhasan, J. Lipman and W. Ni (2020) "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." *Computers and Security* **88**.
[19] Mukkamala, R. R., R. Vatrapu, P. K. Ray, G. Sengupta and S. Halder (2018) "Blockchain for Social Business: Principles and Applications." *IEEE Engineering Management Review* **46**(4): 94-99.
[20] Peffers, K., T. Tuunanen, M. A. Rothenberger and S. Chatterjee (2007) "A design science research methodology for information systems research." *Journal of Management Information Systems* **24**(3): 45-77.
[21] Preneel, B. (1994) "Cryptographic hash functions." *European Transactions on Telecommunications* **5**(4): 431-448.
[22] PUB, F. (1999) "Data Encryption Standard (DES)." *National Institute of Standards and Technology, FIPS PUB*: 46-43.
[23] PUB, F. (2012) "Secure hash standard (shs)." *National Institute of Standards and Technology, FIPS PUB* **180**(4).
[24] Razak, S. A., N. H. M. Nazari and A. Al-Dhaqm (2020) "Data Anonymization Using Pseudonym System to Preserve Data Privacy." *Ieee Access* **8**: 43256-43264.
[25] Rivest, R. L., A. Shamir and L. Adleman (1978) "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* **21**(2): 120-126.
[26] Robling Denning, D. E. (1982) Cryptography and data security, Addison-Wesley Longman Publishing Co., Inc.
[27] Sedayao, J. (2012) "Enhancing cloud security using data anonymization." *Intel IT White Paper, Intel Coporation*.
[28] Singh, G. (2013) "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." *International Journal of Computer Applications* **67**(19).
[29] Sobti, R. and G. Geetha (2012) "Cryptographic hash functions: a review." *International Journal of Computer Science Issues (IJCSI)* **9**(2): 461.
[30] Standard, S. H. (1995) "FIPS Pub 180-1." *National Institute of Standards and Technology* **17**: 15.
[31] Sutherland, J. and K. Schwaber (2017) "The scrum guide. The definitive guide to scrum: The rules of the game." https://www.scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-US.pdf#zoom=100. Retrieved 26-02-2020.
[32] Vitale, F., W. Odom and J. McGrenere (2019) "Keeping and discarding personal data: Exploring a design space." *DIS 2019 - Proceedings of the 2019 ACM Designing Interactive Systems Conference*.
[33] Wang, X. and M. Komarov (2017) "Survey on Personal Data Protection During Big Data Time Depending on the Context." *Thirty eighth International Conference on Information Systems, Seoul 2017*.
[34] Zaghloul, E., T. Li and J. Ren (2019) "Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts." *2019 International Conference on Computing, Networking and Communications, ICNC 2019*.
[35] Zheng, X., R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere (2018) "Blockchain-based personal health data sharing system using cloud storage." *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, IEEE.