Trust-Based Data Controller for Personal Information Management

Upul Jayasinghe
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
u.u.jayasinghe@2015.ljmu.ac.uk

Gyu Myoung Lee
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
g.m.lee@ljmu.ac.uk

Aine MacDermott
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
a.m.macdermott@ljmu.ac.uk

***Abstract*—In today's data-driven digital economy, user-related information works as oil to fuel the state of art applications and services. Consumers, who use these services, provide personal information to service providers, intentionally or unintentionally and often without considering their trustworthiness. However, this personal information often reveals one's identity and may lead users to face unexpected outcomes, ranging from uninvited advertisements to identity theft. To regulate such issues, the new General Data Protection Regulation (GDPR) act was introduced by the European Union in May 2018. As defined by the act, the data controller plays an important role in determining the purposes, conditions and the means of processing data without compromising the user identities for malicious intentions. Therefore, in this paper, we propose a trust-based data controller in which an intermediate authority named trust manager recommends preferable actions towards the data controller on preserving the privacy of the users in accordance with the GDPR act.**

Keywords—GDPR, PII, Data Controllers, Data Processors, Privacy, Trust management.

I. Introduction

With the exponential growth of connected devices and heterogeneous applications, Service Providers (SP) tend to store digital traces of their customers to either improve their quality of services or to improve the turn over by selling them to third parties. Often, this happens without a user's consent and without a proper declaration of how data is going to be processed in the due course. This has raised many concerns over the privacy of the users and hence a new data protection act called General Data Protection Regulation (GDPR) was introduced by the European Union (EU) in May 2018 to control the unnecessary usage of data, empowering users' right on their data [1].

According to the regulation, information related to an identified or identifiable natural person is known as "*Data Subject*" (DS) and any information related to data subject is known as Personally Identifiable Information (PII) [1]. For example, information associated with a name, social identification number, online identifiers based on physical, economic, cultural, ethnicity, religions, gender, etc, and also any other information that can be used to identify a person directly or indirectly can be categorized as PII. Further, the regulation explains a hierarchical model that governs the PII. It appoints a "*Data Controller*" (DC) who accesses the PII from DS and performs the regulation of data adhering to the user's consent and rights. In addition, DC delegates the actual processing of data towards possible third-party processors called "*Data Processors*" (DP). It is important to recognize that both controlling and processing was carried out by SPs until the GDPR act was introduced. However, the act challenges the outdated order and most of the controlling part related to PII is taken out from SPs and established as a separate entity called DC. SPs are only left with processing segments in relation to the service they provide. Therefore, it is rational to consider SPs essentially represent the role of DP when it comes to the real-world explanation of the regulation.

Even though the DC plays an important role in preserving privacy and accountability of information shared by DSs, in current solutions DC lack the ability to evaluate subjective risks and malicious intentions when it comes to preserving user rights in an autonomous manner. To mitigate such issues in an autonomous version of a DC, this paper proposes a trust-based DC. The trust component of the DC is mainly responsible to evaluate trust in between DSs and DPs considering GDPR principles and requirements for PII. In computer science, trust is considered as a computational value depicted by a relationship between a trustor and a trustee, described in a specific context, measured by Trust Metrics (TM), and evaluated by a mechanism [2]. After the trust is evaluated by the trust manager, DC can take necessary actions based on the results from the trust manager to preserve the privacy of DSs while adhering to GDPR act. For example, let's consider a situation where SPs are utilizing user's data going beyond intended purposes violating the GDPR act. In such situations, the trust manager can assess the trustworthiness of such objects and possible consequences in advance and inform the DC to take necessary actions in the process of selecting appropriate DPs.

However, there is no such trust management platform based on the requirements defined in the GDPR on preserving privacy and integrity of PII. As such, the motivation of this research is to address these substantial gaps and present a platform that can support establishing trustworthy data governance. Moreover, We adapt Reputation, Experience, and Knowledge (REK) based trust evaluation model to implement such mechanisms as defined in our previous work on trust [3], [4] and [5]. In this context, DS is considered as the trustor and the DP is considered as the trustee. Moreover, individual's rights defined by the GDPR act are mainly used as Trust Attributes (TA) to compute the trust among trustor and trustee.

The major contributions of this paper are to (i) define a framework for DC based on the definitions by the GDPR act, (ii) outline a trust model to evaluate user rights compliance, and (iii) present a platform that manages trust evaluation and decision-making process in relevance to safeguarding PII. Incorporating these solutions, the remainder of the paper is organized as follows. In Section II, we describe the related work behind this research. Section III explains the motivation and the philosophy behind the trust based GDPR compliance. Section IV presents the proposed framework for DC based on the concepts of autonomous systems. Section V and VI discuss the trust model that evaluates the individuals' right compliance and the trust management platform which controls each process involved in the PII trust evaluation process respectively. Finally, Section VII concludes the paper and outlines our future research.

II. Related Work

The policy-based mechanisms are usually used in the context of distributed network systems as a solution for access control and authorization [6], [7]. The goal is simply to judge whether a user is trustful or not based on a set of credentials and predefined rules, before granting rights to access network resources. An important issue when exchanging and generating credentials is unintentional information disclosure, which can result in a loss of security and privacy. The question raised is to what extent an object trusts other objects to see its own credential information in exchange for earning their credentials. There are many research works dealing with this trade-off between gaining trust and sacrificing privacy such as in [8], [9]. They analyzed the loss of privacy once any credentials are revealed to other objects.

Authors in [10] describe several design patterns that can support the decision making process for the designers of privacy protection systems. On the other hand, privacy by design concept addresses the privacy issues in a bottom-up approach [11], [12]. That is, privacy requirements must be addressed from the system drafting stage to until the final implementation which is also one of the concerns of GDPR act [1]. Moreover, privacy is often achieved by anonymization, and cryptography to prevent malicious users from learning its content [13]. Therefore, a security mechanism cannot always guarantee privacy as they are more focused on preventing unauthorized access. However, trust modeling and management systems show promising results with respect to preserving privacy as it evaluates the subjective consequences of every action taken place between each object. In this regard, authors in [2-5], [14] describes several trust evaluation mechanisms based on numerical and AI techniques for both objects and data targeting internet of things environment which indeed inspired us to carry out this research.

III. Trust-Based GDPR Compliance

A. The GDPR

The GDPR [1] is an EU regulation that came into force on the 25th of May 2018 and replaced the former 95/46/EC Data Protection Directive [15]. The regulation applies to any individual or company who uses data from or to the EU region. Therefore, businesses outside the EU also must adhere to this regulation if they need to deploy their services inside the region. As the EU represents one of the largest sectors of online users, regulation affects almost all users around the world, making it one of the most influential data management acts, presented in recent history.

The act basically identifies three main stakeholders in the process of data management: DS, DC, and DP as shown in Fig. 1. DS can be any person or online identity whose PII is being collected, stored or processed. PII typically relates to information such as social security number, date of birth, etc. and also behavioral data captured by third-party cookies, such as geo-location traces. DC plays an important role in determining purposes and means of processing personal data and managing the coordination between DP and DS. Finally, DP processes the data on behalf of the DC and DS and often can be recognized as SPs. Therefore, DC usually resides in between DS and DP in data management architectures as in Fig. 1.

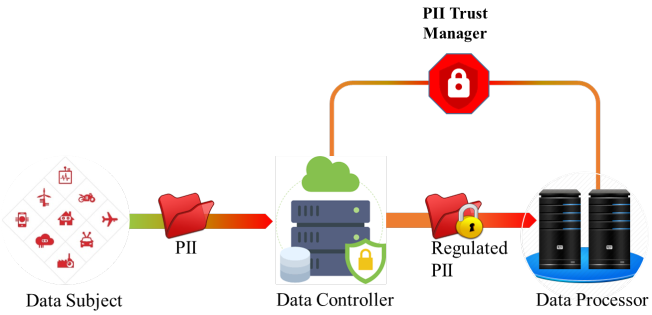

Fig. 1. High level architecture of the Trust based GDPR compliance.

While companies must allocate significant resources on achieving the requirements defined by the GDPR, it provides a greater advantage for users in terms of ensuring greater control, transparency, and accountability over their personal data and its usage. In fact, the act demand six principles [1]: lawfulness, fairness and transparency; purpose and storage limitation; data minimization; accuracy; integrity and confidentiality; and accountability, to ensure a secure and privacy-preserving environment.

The first principle, "*lawfulness, fairness, and transparency*" addresses the issues related to lawfulness, which essentially checks that the DS has given his consent to process the data by DP or DC adhering to common legal obligations; fairness, which ensures the processing of data to match with DS intentions on receiving or providing a particular service; and transparency describes processing data in an honest, open and clear way while keeping DS in the loop at any time of the lifecycle. The second principle, "*purpose and storage limitation*" address the issue of using data for unrelated or unauthorized purposes. Further, this is related to the next principle, "*data minimization*", which in turns prevents extracting and storing redundant data which is not required to achieve the originally expected goal by the DS. "*Accuracy*" essentially identifies the need for keeping up to date information whenever necessary and delete or rectify inaccurate data without any delay before altering the genuine intentions. The principle "*Integrity and confidentiality*" ensures that appropriate security measures are in place to protect the personal data from being compromised, either deliberately or accidentally. The "*accountability*" principle elaborates the responsibility that DSs, DPs, and DCs must take whenever PII is used and how to comply with the before mentioned principles.

B. Trust Management

In the absence of proper safety mechanisms, data can be compromised at various points and interfaces. Moreover, objects in large-scale networks like in the Internet of Things (IoT) possibly lack the knowledge to evaluate services' reliably as both untrustworthy and trustworthy objects can interact with each other at the absence of trusted intermediary which govern each transaction. To fill this gap, we propose an intermediary authority named the Trust Manager to evaluate each interaction in a trustworthy manner as shown in Fig. 1.

For example, consider a scenario where DC must investigate prospective DPs to process PII sent by DS. As the DC is a somewhat localized object to every business model, it might not have enough knowledge and expertise to process such request in an autonomous manner. However, as the trust manager (Fig. 1) is equipped with state of art techniques to judge such situations, it can act as a broker between DC and prospective DPs to determine a suitable DP after evaluating several trustworthiness factors, including individuals' rights as we explained in Section V. Typically, a trust evaluation service takes inputs from several actors as in Fig. 1 and outputs recommendations that have been interesting. Such evaluation of the trustworthiness supports decision-making for both DCs and DSs. As the aim of any legitimate service to provide trustable services with minimum human intervention, the trust concept has enormous potential to securely process and handle data of any SP or customer. For cross-border applications, it can serve as an intermediate broker to handle such negotiations for a particular interaction without any ambiguity or human intervention.

IV. GDPR Compliant Framework for Data Controllers

The ultimate objective of the proposed DC is that it should organize itself under the constraints and guidance of external and internal knowledge to autonomically manage all stakeholders while meeting the goals of GDPR. Hence to achieve mandatory functional requirements demanded by the act, we propose a GDPR compliant framework for the DC based on the MAPE-K feedback loop concept [16]. The main reason for our selection is to enable self-managing capability in DC based on the current and future conditions. The framework mainly consists of five modules: Monitor, Analyse, Plan, Execute and Knowledge Base (KB) as shown in Fig. 2. In addition, KB is supported by two more modules Governance; and Trust and Security.

A. Monitor

Data discovery focuses on collecting data from DCs, DPs and other repositories, to provide an accurate picture of the personal data. The data can include PII and consents demanded by the DSs. Once the data is received, it can be modeled and mapped to find links between individual data points. Artificial intelligence (AI) techniques like data mining and natural language processing (NLP) are promising tools to discover such personal information in the data is being transmitted [17]. It is important to utilize these tools effectively to support advanced data management techniques like metadata indexing and full-text indexing to enable fast and accurate identification and tagging of data [18]. Additionally, the monitor module is responsible to manage the DSs consents in terms of identification, amendment, enforcement, and termination with respect to the lawful basis for processing data.

B. Analyze

Once a structured data set is obtained, the analyze module is responsible for investigating how data is being accessed and used by DPs by using machine learning (ML) and AI techniques. Further, it must analyze to what extent DPs adhere to the GDPR act and consents proposed by the DS. If there are any mismatches between expected results and actual outcomes, a risk assessment must be performed to identify possible vulnerabilities. Moreover, accountability must be also checked against each record of risk to implement possible enforcements in the later stage of the life cycle.

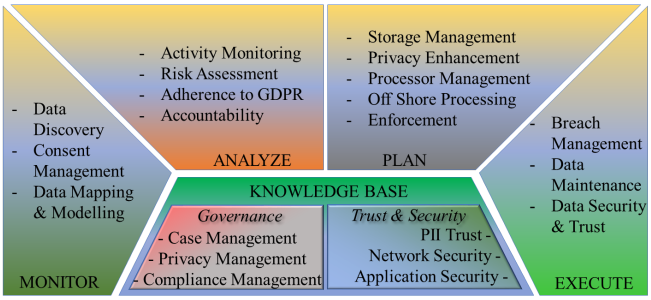

Fig. 2. A Generic framework of the data controller for PII managment.

C. Plan

Upon receiving analytics from the previous module, the planning module generates appropriate plans to improve the quality of services of the ongoing PII management processes and tackle any issues raised with the support from the KB. For example, the privacy enhancement component of the planning module might suggest more appropriate privacy-preserving solutions to uncompleted transactions base on the report from the Trust and Security module inside the KB. Similarly, the data processor management function can seek for new plans to impose a restriction on current processors if their behavior is deviating from the expected and delegate future service requests towards different DP. On the other hand, storage management ensures stored data is managed and deleted in accordance with the agreed regulation rules. The offshore processing component analyses the feasibility of transferring data outside the EU area if there is such a requirement. Finally, the enforcement component takes necessary actions to protect the PII from identified risks in the analysis stage. The enforcement process can vary from an issuing a warning, ensuring additional security measures, revoking the DP from further processing to activating the possible legal process to penalize malicious behaviors.

D. Execute

The Execute module implements the measures suggested by the former module to improve trust and security, manage possible breaches, and maintenance of data according to the GDPR act. For example, security and trust can be further improved using strong encryption and pseudonymization techniques. In addition, the proposed trust platform can be utilized to discover more reliable processors to process data by analyzing the trust relationship between DS and the DPs. Moreover, the trust platform can investigate any breaches and inform all relevant stakeholders including DS about the nature of the breach, impacted objects, and necessary precautions to take in order to avoid such situations in the future.

E. Knowledge Base

Typically, KB contains information shared by all four modules described above, in addition to historical logs, metrics, and rules. However, we introduced two more modules to support the requirements imposed by the GDPR act and their role in the framework is discussed below.

1) *Governance*

The case management component outlines a set of rules that the DC must adhere to when responding to service requests, complaints, emergencies and possible data breaches. The rules can be a combination of values insisted by GDPR and by the DC itself. Similarly, privacy and compliance management components hold information related impact assessments, plans and historical records generated by other major modules in regard to privacy protection and GDPR compliance.

2) *Trust and Security*

The module aids implementing strong security and trust establishment procedures to enhance the level of compliance with the act. The network security component provides robust network and cyber security solutions, while application security component ensures applications who store, process, and manage PII do not compromise the requirements of the data protection act.

In addition to traditional security mechanisms, we propose trust-based data and privacy protection scheme as well as decision-making system to support DC in managing DPs and DSs in accordance with GDPR. The trust model that is described in Section V assesses the relationship between DS and DP by taking individual's rights into account.

V. User Rights Compliance Evaluation

In this section, we propose a user rights compliance evaluation scheme based on trust concepts in addition to standard security techniques like pseudonymization and encryption as suggested by the GDPR. In fact, we identify that trust and security are two different concepts even though many literature work assumed otherwise [2], [4]. The purpose of security is to avoid unauthorized users from obtaining PII of DS in the context of GDPR. However, security mechanisms cannot fully protect privacy disclosure, as an inexperienced or less careful user might share PII without knowing its consequences.

On the other hand, trust mechanisms are implemented in such a way that it can monitor the behavior of every stakeholder in a subjective manner. This approach can help detect any malicious intentions beforehand and prevent it from happening, rather than waiting to fix it at the last minute. To implement such a model that can trace the behaviour of stakeholders, we adopt the threefold REK model based on three factors; (i) Knowledge: trustor's (DS) general understanding about the trustee (DC or DP); (ii) Experience: trustor's previous experience with the trustee; and (iii) Reputation: public opinion on the trustee [3]. According to this model, the first step of the trust modeling is to estimate relevant TMs depending on the application. Therefore, in the context of PII protection, we consider eight metrics; i.e. the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision making which are actually imposed by GDPR to preserve the user rights in data governance. Based on these two concepts, we propose a hierarchical trust evaluation model as shown in Fig. 3.

The knowledge TMs represents all the first party information provided by the trustee to evaluate its trustworthiness. To obtain such information, genuine DPs must register their own information with DC before service provisioning towards DS. We suggest using a publish-subscribe architecture as defined in [4] for this purpose. Once, DP is subscribed, knowledge TM can extract useful information relevant to trust evaluation such as DPs own policies and requirements on data processing, the purpose of requesting such data, and any other information that can be used to evaluate user rights compliance. Having learned enough evidence about trustees through the knowledge TM, DC can ask a trustor to initiate collaborations with selected trustees (DPs) based on the perception that the trustor has already obtained. However, each individual experience is different from others in terms of trustor's perception. For instance, the experience might be feedback from the trustor after each transaction, a value indicating whether a service transaction successfully operates in terms of privacy protection, etc. Hence, it is critical to keep a record of each individual experience to be used in future interactions as an additional awareness compared to knowledge TM.

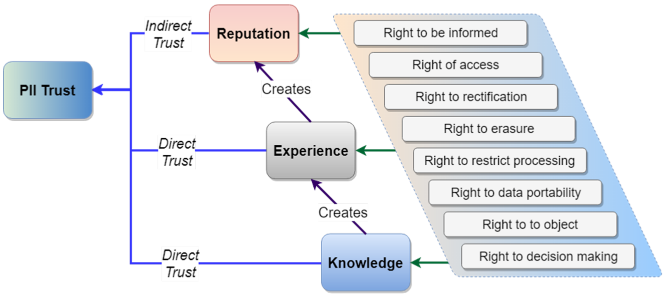

Fig. 3. Hierarchical model based on PII Trust to evaluate the user rights compliance.

Then, by accumulating these experiences over time in relation to the corresponding contexts, tasks and times, the trustor can build up additional intelligence compared to the knowledge and experience TM. For instance, external DPs, DCs, and DSs can share their experience on using the trustee, upon a request by the trustor, which we identify as a reputation or the global opinion of the trustee. That is, the experience TM is a personal observation considering only interactions from a trustor to a trustee, whereas the reputation TM reflects the global opinion of the trustee. According to the above definitions, the formation of trust according to the three TMs is shown in Fig. 4 for the objects who have newly joined the system.

To elaborate the complete scenario, let's take into consideration the *"right to be informed"* metric that collects information related to trustee's behavior towards honoring trustee's privacy data when sharing with third parties. If the model detects any violation where PII is shared without user consent, a penalty is recorded against this specific trustee and the level of trustworthiness will be adjusted accordingly. Such a record can be used by DC to inform the user about the consequences they might face if they use this particular stakeholder. The information collection process in relation to this specific breach can be based on trustors own knowledge, experience or opinion from previous users.

Similarly, the behavior of stakeholders must be traced using other TMs as in Fig. 3. In this regard, the metric *"right of access"* observes an individuals' right to obtain a copy of their personal data as well as other supplementary information held by DPs and DCs. *"Right to rectification"* TM observes the privilege given to DS to change their data

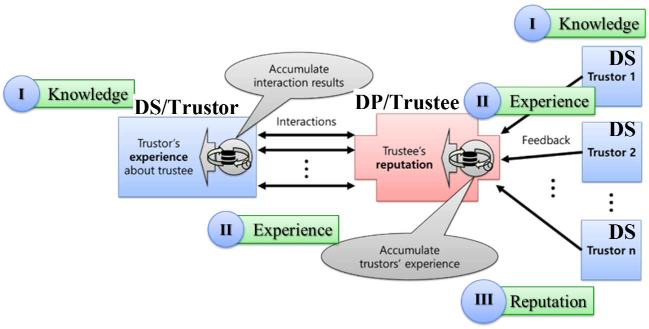

Fig. 4. Direct and Indirect Trust Formation.

whenever necessary and *"right to erasure"* check that DSs have been given the right to delete their data if necessary. Moreover, the *"right to restrict processing"* metric compares user consents over processing and DPs behavior over processing of restricted data. Any match indicates a breach of conduct by DPs and hence the level of trust of entities will be graded accordingly. In relation to this, *"right to object"* TM observes DPs obedience over DSs objection to process any PII owned by this particular DS. On the other hand, *"right to data portability"* check whether DS has given the control over moving their PII, for example from one DP/DC to another. SPs collect various type of PII to form a profile of users using AI techniques like ML. However, once the *"right to decision making"* TM is in place, it can monitor whether DPs listen to DSs' preference on profiling. Based on the number of breaches, the trust model can be used to estimate a trust level of this particular DP.

However, information related to these eight metrics are not readily available and hence attributes, which define these TMs, must be obtained. There are numerous methods available to estimate these TAs ranging from numerical methods, probabilistic methods, and belief theory to data analytics methods such as association rule learning, classification tree analysis, genetic algorithms, ML, sentiment analysis, and social network analysis [2]. In simple terms, the mathematical approach to find the trust level between trustor *i* and trustee *j* can be represented as below.

$$K_{ij}= \alpha_1 K_1+ \alpha_2 K_2+\cdots+ \alpha_n K_n \qquad (1)$$

$$E_{ij}= \beta_1 E_1+ \beta_2 E_2+\cdots+ \beta_n E_n \qquad (2)$$

$$R_{ij}= \gamma_1 R_1+ \gamma_2 R_2+\cdots+ \gamma_n R_n \qquad (3)$$

$$Trust^{PII}_{ij}= \theta_1 K_{ij} + \theta_2 E_{ij} + \theta_n R_{ij} \qquad (4)$$

where α,β,γ, and θ, are weighting factors that normalize each metric in between 0 and 1. K_x, E_x and R_x represent the TAs of Knowledge, Experience, and Reputation, respectively.

Note that equations (1), (2), and (3) denote an iterative process. To determine one TM, it might be necessary to examine several levels deep in the hierarchy, until a sufficient number of attributes are assessed to represent the relevant TM. Therefore, the dimensions of the matrix TA_x can vary depending on the criticalness of the situation.

VI. PII Trust Manager

To facilitate the trust evaluation model discussed in Section V, we propose a trust management platform that coordinates mainly with DC as shown in Fig. 5. For example, the DS who wishes to request a service or amend his PII or consent will first contact DC as shown in step 1 of Fig. 5. Upon receipt of this request, DC must take an appropriate action either to select prospective DP relevant to a particular service or to alter the permission given to DP who is already in the contract. To support this decision-making process, DC might contact PII Trust Manager to evaluate the behavior of DP in regard to GDPR compliance and serviceability.

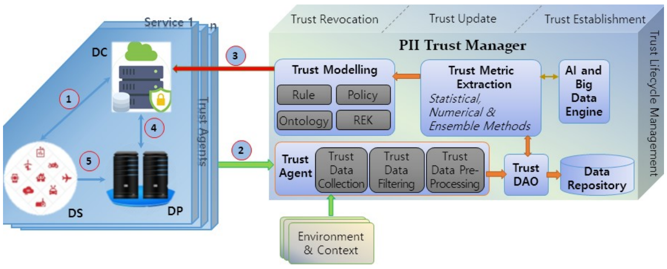

Fig. 5. PII trust management platform.

To support DC in such situations, the platform is equipped with several important modules. Trust Agent (TAG), Trust Data Access Object (DAO), Data Repository (DR), TM Extractor (TME), AI Engine (AIE), Trust Modelling Algorithm (TMA), and Trust Lifecycle Management module (TLM). These modules will perform one or more tasks at a time to achieve the objectives given by the DC. The first step of the trust provisioning process is to collect appropriate data from all the sources (e.g. step 2 in Fig. 5), where applicable, including DC, DP, and DS objects. Generally, TAG works similarly to the client-server application, in which objects and the central platform change their role depending on the direction of data flow. The data could be either information obtained directly from relevant parties, experience or opinions of objects as reputation or feedbacks from/to other objects, applications or services. Once the TAG, inside the platform acquired the data, it will be stored in the local repository, close to the platform to be used by other modules in the platform. Additionally, it stores information from the TME and external trust data sources.

After that, all the information acquired so far is analyzed inside TME with the support from an external AI engine. Depending on the availability of data and attributes, techniques like numerical, statistical, ML or ensemble approaches are utilized to calculate the metrics. Then the final trust level based on the calculated metrics from previous steps is generated inside TMA based on the appropriate model for each application. For example, if the REK model is used, a trust value based on the knowledge, reputation and experience are generated. The TMA should essentially work together with the TME to find the best possible metrics for each model in which some models will combine the metrics according to pre-defined rules or policies, while others will generate these rules and policies dynamically to suit the situation in the best possible way. Finally, estimated trust information is transmitted towards DC (e.g. step 3 in Fig. 5) for appropriate decision-making processes. Once, the information is received by DC, it can take necessary actions to process the data of DS in accordance with GDPR act (as shown in step 4 and 5 of Fig. 5).

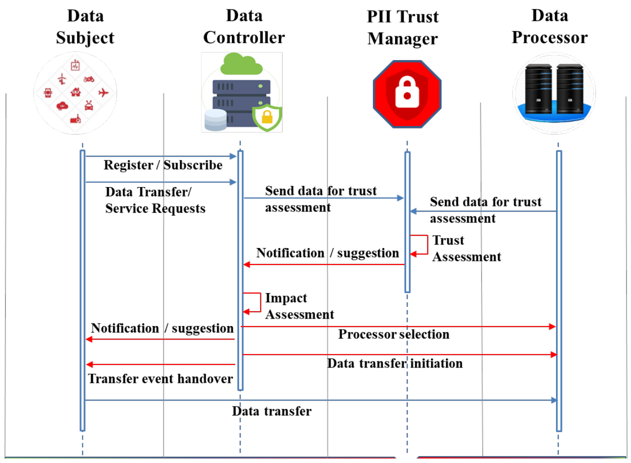

Fig. 6. Interactions among DS, DC, DP and the proposed platform.

To further elaborate the importance of the trust manager proposed in the decision-making process for GDPR compliance, a scaled down sequence of interactions between stakeholders defined by GDPR and Trust manager is shown in Fig. 6. The DS in need of a particular service must first register at DC and then send the data relevant for the service request. The registration process helps DC to identify DS's preferences and consents on regulating his own data. Upon reception of data, DC inquires the trust manager to provide a recommendation on prospective candidates for PII processing and a report on the behavior of currently associated DPs with DS if that is the case. Then Trust Manager will utilize its own AI base algorithms to evaluate the relationship between the DS and DP as well as the behavior of the DPs in relation to user rights compliance as discussed in Section V. The final result is then informed to DC for further processing like impact assessment in regard to privacy protection. If the DC is satisfied with the current status, then it delegates the further processing to carefully the chosen DP while monitoring the process continuously.

VII. Conclusion

This paper proposes several novel concepts to implement a fully automated data controller in order to preserve PII adhering to the GDPR act. First, we present a framework for DC based on the concepts of autonomous systems, utilizing the well-known MAPE-K model which essentially removes the need for human involvement in processing sensitive data. Such an approach is quite beneficial in managing humongous business models while adhering to GDPR laws. Next, we present a trust-based support system for DC in the decision-making process. The proposed PII trust management module basically provide the required intelligence towards DC to take fair and lawful decisions when it comes to personal data management. Unlike, traditional AI engines, the proposed platform assesses every transaction considering preferences, consents, and requirements of DSs, DCs, and DPs. As the underline model that evaluates the transactions, is based on the metrics which define individual rights, the proposed model already complies with GDPR.

For future work, we plan to investigate the scalability of the proposed framework and the trust manager based on the concepts of blockchain approaches like Hyperledger based solutions [19]. Further, it is beneficial to study and improve potential protocols like Platform for Privacy Preferences Project (P3P), to enhance the controllability of PII and reduce the technical complexity in real-world implementation [20].

Acknowledgment

This work was supported by the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT). [2018-0-00261, GDPR Compliant Personally Identifiable Information Management Technology for IoT Environment].

References

[1] European Union, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union,* vol. L119, pp. 1-88, 2016.
[2] U. Jayasinghe, G. M. Lee, T. W. Um, and Q. Shi, "Machine Learning based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing*, pp. 1-1, 2018.
[3] U. Jayasinghe, H. W. Lee, and G. M. Lee, "A Computational Model to Evaluate Honesty in Social Internet of Things," in *32nd ACM SIGAPP Symposium On Applied Computing*, Marrakesh, Morocco., 2017.
[4] U. Jayasinghe, A. Otebolaku, T.-W. Um, and G. M. Lee, "Data centric trust evaluation and prediction framework for IOT," in *ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, Nanjing, China, 2017, pp. 1-7.
[5] U. Jayasinghe, N. B. Truong, G. M. Lee, and T.-W. Um, "RpR: A Trust Computation Model for Social Internet of Things," in *2016 Intl IEEE Conference on Smart World Congress*, Toulouse, France, 2016.
[6] P. Bonatti, and P. Samarati., "Regulating service access and information release on the web," in *Proceedings of the 7th ACM conference on Computer and communications security*, Athens, Greece, 2000, pp. 134-143.
[7] R. Gavriloaie, W. Nejdl, D. Olmedilla, K. E. Seamons, and M.Winslett, "No Registration Needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web," in *1st European Semantic Web Symposium (ESWS)*, Berlin, Heidelberg., 2004, pp. 342-356.
[8] T. Yu, and M. Winslett, "Policy migration for sensitive credentials in trust negotiation," in *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society*, New York, USA, 2003, pp. 9-20.
[9] T. Yu, M. Winslett, and K. E. Seamons, "Interoperable Strategies in Automated Trust Negotiation," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, New York, USA, 2001, pp. 146–155.
[10] M. Hafiz, "A collection of privacy design patterns," in *Proceedings of the 2006 conference on Pattern languages of programs*, Portland, Oregon, USA, 2006, pp. 1-13.
[11] S. Spiekermann, "The challenges of privacy by design," *Commun. ACM,* vol. 55, no. 7, pp. 38-40, 2012.
[12] J.-H. Hoepman, "Privacy Design Strategies," Berlin, Heidelberg, 2014, pp. 446-459.
[13] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy Preservation in Big Data from the Communication Perspective—A Survey," *IEEE Communications Surveys & Tutorials*, 2018.
[14] G. M. Lee, U. Jayasinghe, N. B. Truong, and C.-h. Cho, "Features, Challenges and Technical Issues," in *The Second Bright ICT Annual Workshop on Bright ICT 2016*, Dublin, Ireland, 2016.
[15] European Union. "EU GDPR Information Portal, " 2018; [Online] Available: https://www.eugdpr.org/eugdpr.org-1.html.
[16] IBM Corporation, "An architectural blueprint for autonomic computing.," 2005.
[17] E. Rahm, and P. A. Bernstein, "A survey of approaches to automatic schema matching," *The VLDB Journal,* vol. 10, no. 4, pp. 334-350, December 01, 2001.
[18] A. Gani, A. Siddiqa, S. Shamshirband, and F. Hanum, "A survey on indexing techniques for big data: taxonomy and performance evaluation," *Knowledge and Information Systems,* vol. 46, no. 2, pp. 241-284, February 01, 2016.
[19] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017, pp. 3-7.
[20] W3C. "Platform for Privacy Preferences (P3P) Project, " 2007; [Online] Available: https://www.w3.org/P3P/.