Trust Mechanism for Enforcing Compliance to Secondary Data Use Contracts

Zeinab Noorian, Johnson Iyilade, Mohsen Mohkami, Julita Vassileva

Department of Computer Science, University of Saskatchewan, 110 Science Place S7N5C9 Saskatoon, Canada
zen951@mail.usask.ca

***Abstract*—In many research and business domains, there are efforts to develop systems that aggregate user data gathered by various data sources. This approach involves secondary sharing of user data and potentially benefits the user in terms of improved personalization and better experience. However, concerns regarding privacy arise when sharing user data with unknown third parties. These concerns can be alleviated at two stages: i) ensuring selective control of the applications to share user data with, and ii) monitoring and penalizing errant data consumers who violate the terms of their contractual agreement and potentially abuse user data. This paper addresses the second stage of data use contract enforcement.**

We propose a trust management mechanism for monitoring data consumers' compliance to the contractual agreements for which data was shared with them. The trust mechanism is based on user complaints about suspected privacy violations and is able to identify the data consumers who are responsible. The framework penalizes the data consumer found guilty of violating its data use agreement by decreasing its trust value. This makes the data consumer less likely to be selected to receive user data, and limits its participation in the user data marketplace, forcing it to pay a higher price for purchase of user data.

Keywords: trust, reputation, data use contract, compliance monitoring, privacy policy enforcement, secondary data use

I. Introduction

Recent advances in mobile, social and ubiquitous computing have made available online an enormous amount of data about users from various sources and in various contexts. Most of these data are contributed voluntarily by users; others are obtained by the system from observation of user activities, or inferred through advanced analysis of volunteered or observed data. At the same time, the required technologies and tools to store, connect, aggregate, and analyze massive amount of data gathered from many sources have matured.

Inspired by these developments, there is a growing interest in many sectors towards developing systems that utilize the massive amount of disparate user information available in various sources and databases on the Web. Researchers in the user modeling and personalization community are developing new approaches of user modeling (so-called, decentralized [1] or cross-system user modeling [10]) which focus on the problem of aggregating user data gathered across many data sources online. Also, the recent advances in big data technologies allow for pooling together a high volume of heterogeneous user data from many sources and performing analytics on the aggregated data for knowledge discovery.

The presumption of all these systems is that user data collected by an application (i.e. data provider) for its own predefined (primary) purpose of use can be beneficially shared, reused, and combined by another application (i.e. data consumer) for new (secondary) purposes that might not be known at the initial point of data collection.

Generally, there are various benefits in allowing secondary sharing of user data. For example, in user modeling and personalization, it will enrich the user model as more information is available about the user and in greater depth. This will in turn lead to better personalized services and improved quality of experience for the user [5]. Also, the opportunity to reuse and recombine user data in big data analytics is currently driving innovation, with opportunities for cost saving and operational effectiveness in many sectors including national security, health care, home automation, fraud detection, and urban planning [3].

However, allowing secondary sharing and use of data poses privacy risks to the user since her data may be used for unwanted purposes such as surveillance or discrimination for employment or insurance, impersonation, and others. Therefore, in view of the growing interests in secondary sharing of user data and the need to protect the user from harm, we envisaged the emergence of marketplace infrastructures [6] to support secondary sharing and reuse of user data among applications and services on the Internet based on a privacy policy agreement between the trading parties that stipulates what data is shared or traded, with whom and for what purpose.

In such an open environment, two main challenges need to be addressed to adequately protect the users privacy: i) how to control with which Data Consumer (DC) the user data is shared with, and (ii) how to monitor and penalize DCs who violate the terms of their contractual agreement and possibly abuse the user data for unethical purposes.

This paper is focused on the second challenge of data use policy enforcement. The paper formulates a trust mechanism for monitoring and enforcing DCs compliance with the contractual agreements made for utilizing user data. The mechanism accepts as input user complaints that might be related to violations of contracts involving their data. By proactively requesting and accumulating evidence, the mechanism can pinpoint the DC(s) responsible for the violation. The mechanism penalizes the violating DC by decreasing its trust value. DCs with low trust values are either excluded or disadvantaged in

the exchange of user data by being constrained with respect to the purposes for which they can negotiate to purchase user data, the types of user data that can be shared with them, the duration for which they can keep the data, and the price they need to pay. This creates an incentive for DCs to respect the contracts for user data utilization and thus facilitates appropriate secondary use of data, and ultimately, user privacy.

II. Marketplace for sharing user data

As more and more independent applications, services, and devices collect and store data about the user and are subsequently required to connect and collaborate with other applications to re-share the data for secondary purposes, finding a privacy-aware framework for sharing and controlling usage of user data for secondary purposes has been a growing concern [4]. In this regard, we envisioned the emergence of a new data exchange infrastructure that could be conceptualized as a secondary user data marketplace. The marketplace will allow for trustworthy and transparent trading and exchange of user data among applications.

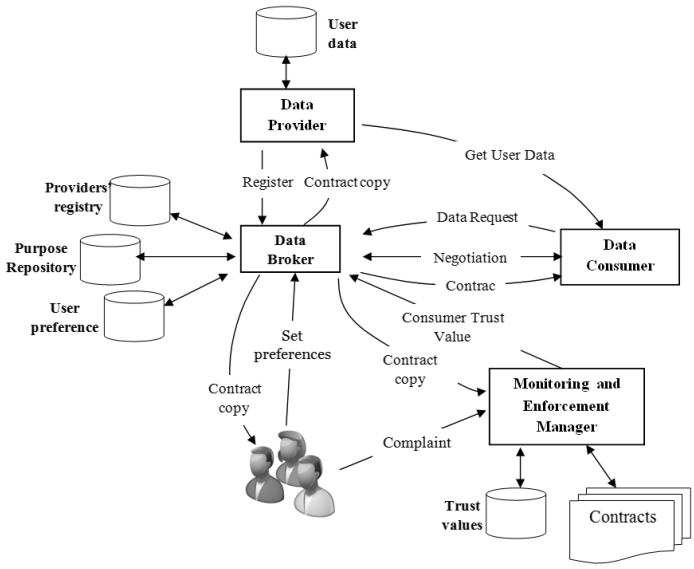

Fig. 1. Main players in secondary user data market and their interactions

This section describes briefly the marketplace framework, proposed in our previous work [8] to which the TR mechanism, the main contribution of this paper, is applied. As shown in Figure 1, the main players in the marketplace are:

- *user* - the person who agrees to the secondary sharing and use of her data for explicitly stated purposes respecting her privacy preferences.
- *data providers* (**DP**s) - entities which collect data about the user, store it and are willing to share the data on the market for secondary use;
- *data consumers* (**DC**s) - entities which request and purchase user data for secondary use;
- *data broker* (**DB**) - a middleware infrastructure responsible for: (i) selecting among the many possible DCs who are requesting user data those that are trustworthy, (ii) semantic matching of the requested user data by the DCs and the data offered for sharing by the DPs; (iii) facilitating negotiation of the privacy policy with the DCs considering the users preferences and the *purpose* (context) of use of the data; and (iv) creating a *contract* for sharing the users data between the user, DP and DC.
- *Police* - a monitoring and enforcement manager, tasked with ensuring that data consumers comply with the policy agreements for which data was shared with them. The police maintains a database of trust values for DCs. It accepts user complaints for possible data use violations; verifies them and use a trust mechanism to find the violating DCs. The Police then punishes violators by recalculating their trusworthiness value.
  The core functionality of the Police is based on the TR mechanism (described in Section III).

Generally, addressing privacy concerns of secondary data sharing and usage involves two main challenges [6]: (i) data sharing discrimination challenge, which control with whom (i.e. data consumer) the user data is re-shared and for what purpose; (ii) privacy policy enforcement challenge, which ensures that a data consumer complies with the contractual obligation for which the data was shared and does not use the data for unauthorized purposes- after user data has been re-shared.
We addressed the challenge (i) in our earlier work [8] through the formulation of a flexible privacy policy framework called Purpose-to-Use (P2U). P2U is designed to support secondary user information sharing among applications so that a DP can offer and negotiate user data sharing with other applications (data consumers) according to an explicit user-editable and negotiable privacy policy. The policy guides the formulation of a (secondary) data use contract which represents the agreement between the parties for sharing user data for specific purpose. Copies of the contract are stored by the user whose data is being shared, the DP releasing the data, and the Police who handle user complaints about violations of the contract by the consumer. Data sharing discrimination, therefore, occurs at the point of interaction between applications by using the privacy policy to control who has access to user data and for what purpose.

However, ensuring that data consumers comply with their contractual obligations on data use, after the data has been released, is still an open challenge [6]. This challenge is non-trivial, considering that in a secondary context, the major harms to the user come from the use of her data for the wrong purposes such as surveillance or discrimination for jobs, loan or insurance. Therefore, an appropriate mechanism is needed, within the market framework, to enforce compliance by DCs to the secondary data use privacy policy agreement. The rest of this paper focuses on mechanisms for addressing this challenge.

III. Trust Mechanism for Detecting Malicious Data Consumers

We describe our trust mechanisms for data use policy contract enforcement in this section. As stated earlier in Section II, the *contract* represents the data use agreement among the entities interacting in the marketplace for specific *purpose* P. Copies of the contract are sent to: 1) the user whose data is being shared, 2) the data provider (DP) releasing the data, and 3) the *Police* - the policy enforcement entity that handles user complaints about violations of the contract.

The contract ct_i stipulates what data is to be shared ($Data$), for how long (Ret), a timestamp of the time the contract was created ($ContTime_{ct_i}$), the number of user records in the contract ($UserNum_{ct_i}$), the users identities ($UsersId$), and the importance of a contract (Imp_{ct_i}).

More formally, a contract ct_i contains the following attributes:

$$ct_i = \langle P; DC; Data; Ret; ContTime_{ct_i}; UserNum_{ct_i}; UsersId; Imp_{ct_i} \rangle$$

Note that, the attribute (Imp_{ct_i}) is a function of: 1) the privacy risk level associated with a particular contract and is assigned to each contract based on a purpose P, 2) the sensitivity of $Data$, 3) Ret, and 4) $UserNum_{ct_i}$. The privacy risk level of the contract and the sensitivity of the data are based on an estimate by a human privacy expert.

Consider a scenario in which a user perceives a suspicious behavior (e.g. receiving particular spam e-mail). The user files a complaint to the Police reporting possible violation of data use via an online form. The Police stores this information in the Complaint Storage (CompST). The user complaint explicitly includes information on the context (including the purpose of use and possible data compromized) in which the user thinks her data has been violated. For example, if a particular user A receives spam emails related to diabetes medicine, the user reports P="email marketing" (which she will choose from a menu of all available purposes of correct or improper user of data) and "health-related data" as the *context* of the complaint with the Police. The Police stores the identity of the users who have complained along with the time $CompTime$ when the complaint was submitted.

A. Measuring the Violation Degree of DCs' Contracts

Since various DCs may have purchased similar data for the same purpose, this makes the task of discovering the culprit non-trivial. The Police will require an effective means of accurately discovering the malicious DCs based on the existing evidence (i.e. user complaints). The basic process is presented in Figure 2

As a first step, the Police classifies the received complaints based on their context[1]. As one context may indicate different number of contracts, the Police further extracts the contracts

[1]In this paper we consider the pre-defined contexts like those in the example above. Dealing with the possible semantic relations between different contexts is out of the scope of this paper.

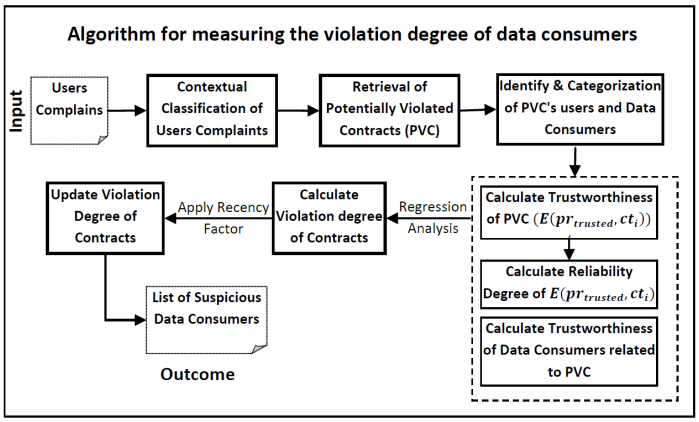

Fig. 2. Process design of the proposed algorithm

involving the complaining user whose purposes are the same as the context of the complaints. In the example above, the Police will retrieve all contracts ct_1, ct_2, ct_3 and ct_4 whose purpose is "email marketing" and which involve "health-related data".

The Police counts the number of users who have complained about a particular context - $UserNumComp_{ct_i}$, and assigns this number to the contracts involving this context, with which these users have been associated with. For example, if 120 users who filed complaint are related to contract ct_1, while 210, 32, and 50 users who file complaints are related to contracts ct_2, ct_3 and ct_4 respectively, the Police counts $UserNumComp_{ct_1} = 120$, $UserNumComp_{ct_2} = 210$, $UserNumComp_{ct_3} = 32$ and $UserNumComp_{ct_4} = 50$ for the contracts ct_1, ct_2, ct_3 and ct_4, correspondingly.

Given this information, the Police measures the probability of trustworthiness of a contract ct_i, as follows:

$$E(pr_{trusted}, ct_i) = \frac{r+1}{r+s+2} \quad (1)$$

Where r indicates the number of users in ct_i who did not complain; and s indicates the number of users who complained regarding ct_i, which are defined as follows:

$$r = UserNum_{ct_i} - UserNumComp_{ct_i}$$

$$s = UserNumComp_{ct_i}$$

Clearly, $0 \leq E(pr_{trusted}, ct_i) \leq 1$ and as it approaches 0 or 1, it indicates unanimity in the body of evidence (here, users complaints). Large values of r or s provide more certainty about the trustworthiness of contracts. In contrast, $E(pr_{trusted}, ct_i) \approx 0.5$ (i.e., $r \approx s$) signifies maximal conflict in received evidence, resulting in increased uncertainty in determining the trustworthiness of the contracts (i.e. only half of the users involved in ct_i complained about its possible violation).

Thereafter, to identify culprits more confidently, the Police calculates the reliability degree of $E(pr_{trusted}, ct_i)$ [18] as follows:

$$Reliability(r,s)_{ct_i} = \frac{1}{2}\int_0^1 \mid \frac{x^r(1-x)^s}{\int_0^1 x^r(1-x)^s\ dx} - 1 \mid\ dx \tag{2}$$

Where x represents $E(pr_{trusted}, ct_i)$.

Theoretical analysis [13] demonstrates that for a fixed ratio of r and s the reliability degree increases as the number of evidence (i.e. r and/or s) increases. On the contrary, given a fixed number of evidence, as the extent of conflict increases, the reliability of the contract decreases proportionately. That is, the reliability of the contract is at its minimum value when $E(pr_{trusted}, ct_i) = 0.5$ - the case where $UserNumComp_{ct_i} = UserNum_{ct_i}/2$.

In the next step, the Police calculates the trustworthiness of data consumers associated with possibly violated contracts. For example, the Police measures the trustworthiness of data consumers dc_1, dc_2, dc_3 and dc_4 related to ct_1, ct_2, ct_3 and ct_4, respectively. The trustworthiness of a data consumer dc_j is the weighted aggregation of the trustworthiness of all their associated contracts, formalized as,

$$trust_{(dc_j)} = \frac{\sum_{k=1}^{n} Imp_{ct_k} * E(pr_{trusted}, ct_k)}{\sum_{k=1}^{n} Imp_{ct_k}} \tag{3}$$

where Imp_{ct_k} represents the importance of a contract ct_k. Given the set of independent continuous variables: $\{E(pr_{trusted}, ct_i), Reliability(r,s)_{ct_i}, trust_{(dc)}\}$, the violation degree of the contract ct_i is modeled using linear regression [16] as follows:

$$\begin{aligned} Violation_{(ct_i)} = \theta_0 &+ \theta_1 E(pr_{trusted}, ct_i) \\ &+ \theta_2 Reliability(r,s)_{ct_i} \\ &+ \theta_3 trust_{(dc)} \end{aligned} \tag{4}$$

The goal of the regression model is to estimate the coefficients $\theta = \{\theta_0, \theta_1, \theta_2, \theta_3\}$ in Equation 4 to derive the value of $Violation_{(ct_i)}$.

As the final step, as it is more probable that a malicious DC who violates the contract agreement has acted recently (i.e., close to the time of the complaint), the Police updates the degree of violation to reflect the recency of the contract in its evaluation:

$$Violation'_{(ct_i)} = RF_{(ct_i)} * Violation_{(ct_i)} \tag{5}$$

where

$$RF_{(ct_i)} = e^{\frac{(ContTime_{(ct_i)} - CompTime)}{10\eta}} \tag{6}$$

represents a recency factor of the contract ct_i.
According to Equation 6, as the difference between the complaint time ($CompTime$) and the contract time ($ContTime_{(ct_i)}$) increases, the likelihood that the respective contract (i.e. ct_i) has been violating the contract decreases. It is noteworthy to mention that $ContTime_{(ct_i)}$ are prior to $CompTime$ so that $ContTime_{(ct_i)} - CompTime < 0$.

The η parameter, which resides between $\langle 0, 1\rangle$ defines the deterioration rate that enables the Police to adaptively determine the importance of the recency of the contracts. For instance, setting up η to a smaller value enables the Police to consider recent contracts in a greater risk of violation. On the contrary, as the η value grows the deterioration rate gets smaller, resulting in the augmentation of the susceptibility of violation of the older contracts.

B. Ranking and Classification of the Data Consumers

After the process of measuring the violation degree of contracts, the Police sorts them based on degree of violation and further classifies them in two categories namely, *trustworthy* and *suspicious*. That is, the Police considers a dishonesty threshold $T1$ and classifies contracts whose violation degrees are below $T1$ as trustworthy and the ones whose violation degree are above $T1$ as suspicious.

Next, in order to correctly detect *malicious* DCs, the Police adopts a *two-dimensional ranking procedure* to further sort DCs corresponding to the contracts in the suspicious list.

In the first dimension, the Police ranks the contracts based on their violation degree determined by Equation 5. The processed list will be called $List_{dimension1}$.

In the second dimension, Police sorts DCs based on the number of suspicious contracts they are related to. That is, since a data consumer might be associated with more than one contract, if a subset of the DC's contracts exists in the suspicious list, the probability that the DC is malevolent increases. Thus, the Police ranks data consumers who are related to multiple suspicious contracts. The ranked list is called $List_{dimension2}$.

Then the Police selects the first K suspicious contracts existing in $List_{dimension1}$ in addition to all DCs existing in $List_{dimension2}$, and adopts the *proactive solicit trust measure* (**PSTM)** to detect the malicious data consumers. The key idea of PSTM is that the Police solicits evidence from users whose data was shared in the contract but who have not filed any complaints so far. This may result in new user complaints that could be related to this contract. If the number of unsatisfied (complaining) users (i.e. $UserNumComp_{ct_i}$) increases, the Police re-calculates the violation degree of data consumers considering the acquired additional evidence using the mechanism proposed in Section III-A.
The Police further differentiates the current value of the violation degree with the old value and if it is found to be significantly greater (i.e.,$Violation'_{(ct_i)} - Violation''_{(ct_i)} > \epsilon$), the suspicious DCs are recognized as malicious.

Otherwise, if malicious DCs are neither detected amongst the K number of suspicious $List_{dimension1}$ nor in the $List_{dimension2}$, the Police recursively selects K from the remaining DCs in $List_{dimension1}$ (yet to be interrogated) and repeats the process.

C. Updating the Trustworthiness of Malicious Data Consumers

After discovering the malicious DCs, the Police updates their trustworthiness values. The key idea is that the Police discounts the trustworthiness of malicious DCs based on the

severity of the damage they cause to the users. That is, the more important the violated contract is, the more the trustworthiness of the involved DC will decrease.

Considering $E(pr_{untrusted}, ct_i) = \frac{s+1}{r+s+2}$, as the expected value of the probability of untrustworthiness of a contract ct_i, the updated trustworthiness of malicious data consumer dc can be formalized as follows:

$$trust'_{(dc)} = trust_{(dc)} - \sum_{i=1}^{n} Imp_{(ct_i)} * E(pr_{untrusted}, ct_i) \quad (7)$$

Where n is the number of contracts that has been violated by a data consumer dc, and $Imp_{(ct_i)}$ is the importance of the contract ct_i. Note that we can alternately calculate $E(pr_{untrusted}, ct_i) = 1 - E(pr_{trusted}, ct_i)$ as well. It is noteworthy to mention that, $trust'_{(dc)} < 0$ would be considered as $trust'_{(dc)} = 0$.

IV. Experiments

We conduct a set of experiments to illustrate efficacy of the proposed trust mechanism in a secondary data use market. Specifically, we evaluate the effectiveness of our approach in detecting malicious data consumers who significantly violated their contracts and abused users data. The e-marketplace environment used for experiments is populated with data consumers and users and operate up to time $t = 290$. We initialize the marketplace with 2000 users and 80 data consumers who agreed on 110 data sharing contracts. We assume that within a time interval [180, 240], users share 1500 complaints in which the Police classifies them to three classes of contexts: 1) email marketing based on user *health-related data*, 2) email marketing based on *user search queries data*, 3) mobile ads based on *location data*, each of which contains 280, 820, 400 complaints, respectively. The experimental results present the outcomes within a time window [180, 240][2].

The Police have recorded the observation of *previous complaints* in time period [0,180] issued by users in this marketplace. Table I presents the basic properties of the previous complaints records: the context of complaints $context$, the number of complaints $CompNum$ and the time of the complaint $CompTime$. For example, when $CompNum = 100$, the Police stored *hundred* users complaints regarding the violation of their contracts with the context of "email marketing based on users travel interests" and records different variables of the associated contracts such as trustworthiness of the contracts, $E(pr_{trusted}, ct_i)$, their corresponding reliability, $Reliability(r, s)_{ct_i}$, the trustworthiness of associated data consumers, $trust_{(dc)}$, and the violation degree of contracts, $Violation'_{(ct)}$.

The Police retrieves contracts with the purpose of "email marketing based on user health-related data" from the contract repository at time point $t = 240$. Table II presents the list of contracts with their corresponding data consumers along with other attributes such as the importance of the contract Imp_{ct}, the number of users involved in the contract $UserNum$, the identities of users $UserId$ which are captured in $Record_{(ct_i, C_j)}$ (denoting the record of the identities of all the users who have sold their data to the consumer C_j via the contract ct_i).

[2]Due to space limitations, we only analyse the complaints with the first context of those listed above.

Dataset	context	CompNum	CompTime
Set1	email marketing with travel interest data	430	100
Set2	Mobile add with location data	640	120
Set3	email marketing with user search queries data	720	180

TABLE I
THE PROPERTIES OF PREVIOUS RECORDS OF USERS' COMPLAINTS

Evaluating the information shown in Table II, the Police differentiates between users who complain about a certain contract and who did otherwise and determine r and s, respectively. She then measures the expected value of trustworthiness of contracts $E(pr_{trusted}, ct_i)$ along with their reliability value $Reliability(r, s)_{ct_i}$, and the trustworthiness of the associated data consumers $trust_{(dc)}$. The outcomes are presented in Table III.

Given the independent variables presented in Table III, the Police employs the standard regression methods: linear regression and regression tree- the tree-based regression model is induced with the M5 algorithm [17]-, implemented in the data mining suite Weka [19], to predict the violation degree of the contracts, $Violation_{(ct)}$.

The predicted value of the violation degree of different contracts, $Violation_{(ct_i)}$, using 10-fold cross validation is presented [3] in Table IV. The Police further adjusts the degree of violation of contracts based on the recency of their contract time. Given a chosen value $\eta = 0.8$, the third column of Table IV presents the updated value for the violation degree $Violation'_{(ct)}$.

We use root mean squared error (RMSE) and mean absolute error (MAE) to evaluate quality of prediction of the violation degree obtained from different regression models as follows:

$$RMSE = \sqrt{\sum_{i=1}^{m} (\widehat{vd_{ct_i}} - vd_{ct_i})^2} \quad (8)$$

where m is the number of training examples and $\widehat{vd_{ct_i}}$ and vd_{ct_i} are the predicted and observed values of the dependent variable for the $i-th$ training example, respectively.

Table V presents three different performance measures calculated by Weka. The results signify high positive relationship between the independent variables such as trustworthiness of DCs and the dependent variable $Violation_{(ct)}$. Moreover, the low values of MAE and RMSE indicate a high accuracy of the regression tree-based model in predicting the violation degree.

[3]We run the experiments using two regression methods: linear regression and regression tree-based model. We observe that the latter model yields higher accuracy than the linear regression model thus we only report the predicted value derived from the regression tree based model.

Contract Name	DC Name	UserNum	ContTime	UsersId	$Imp_{(ct)}$
ct_1	C_1	719	177	$Record_{(ct_1,C_1)}$	0.75
ct_5	C_2	553	175	$Record_{(ct_5,C_2)}$	0.43
ct_4	C_1	407	178	$Record_{(ct_4,C_1)}$	0.67
ct_{12}	C_{13}	760	179	$Record_{(ct_12,C_{13})}$	0.34
ct_{23}	C_1	1228	177	$Record_{(ct_{10},C_1)}$	0.23
ct_{67}	C_{43}	481	176	$Record_{(ct_{23},C_{43})}$	0.86
ct_{13}	C_{13}	602	177	$Record_{(ct_8,C_{13})}$	0.33
ct_{142}	C_{24}	550	174	$Record_{(ct_{67},C_{24})}$	0.79
ct_{24}	C_{24}	116	176	$Record_{(ct_{13},C_{24})}$	0.50
ct_{33}	C_1	72	178	$Record_{(ct_{33},C_1)}$	0.19
ct_8	C_3	17	179	$Record_{(ct_{142},C_3)}$	0.94
ct_{15}	C_{19}	80	177	$Record_{(ct_{15},C_{19})}$	0.67
ct_9	C_{32}	778	179	$Record_{(ct_9,C_{32})}$	0.43
ct_{123}	C_{13}	764	175	$Record_{(ct_{123},C_{13})}$	0.72
ct_{53}	C_{43}	104	178	$Record_{(ct_{53},C_{43})}$	0.84

TABLE II
THE CONTRACTS WITH CONTEXT "EMAIL MARKETING BASED ON USER HEALTH-RELATED DATA"

Contract Name	r	s	$E(pr_{trusted}, ct_i)$	$Reliability(r,s)_{ct_i}$	$trust_{(dc)}$
ct_1	300	419	0.41	0.89	0.56
ct_5	211	342	0.38	0.88	0.71
ct_4	259	148	0.63	0.86	0.56
ct_{12}	598	162	0.78	0.91	0.67
ct_{23}	293	642	0.31	0.91	0.56
ct_{67}	0	481	0.002	0.98	0.25
ct_{13}	301	301	0.5	0.88	0.67
ct_{142}	100	450	0.18	0.90	0.49
ct_{24}	111	5	0.94	0.89	0.49
ct_{33}	32	40	0.44	0.72	0.56
ct_8	9	8	0.52	0.53	0.91
ct_{15}	42	38	0.52	0.73	0.85
ct_9	135	643	0.17	0.91	0.33
ct_{123}	534	230	0.69	0.90	0.67
ct_{53}	25	79	0.24	0.79	0.25

TABLE III
THE VARIABLES FOR CALCULATION OF THE VIOLATION DEGREE

Contract Name	$Violation_{(ct_i)}$	$Violation'_{(ct_i)}$
ct_1	0.96	0.66
ct_5	0.66	0.35
ct_4	0.20	0.16
ct_{12}	0.18	0.16
ct_{23}	0.82	0.56
ct_{67}	0.92	0.56
ct_{13}	0.26	0.18
ct_{142}	0.83	0.39
ct_{24}	0.18	0.11
ct_{33}	0.89	0.69
ct_8	0.24	0.21
ct_{15}	0.25	0.17
ct_9	0.93	0.82
ct_{123}	0.18	0.10
ct_{53}	0.92	0.72

TABLE IV
THE PREDICTED VIOLATION DEGREE EVALUATED BY M5 ALGORITHM

Considering a dishonesty threshold $T1 = 0.5$, the Police classifies the contracts whose violation degree is below 0.5 as trustworthy and those with violation degrees above 0.5 as suspicious. The list of suspicious contracts are presented as follows:

$$L_{sus} = \{ct_1, ct_{23}, ct_{67}, ct_{33}, ct_9, ct_{53}\}$$

Having L_{sus}, the Police adopts the proposed two-dimensional ranking procedure and creates:

$$List_{dimension1} = \{ct_9, ct_{53}, ct_{33}, ct_1, ct_{23}, ct_{67}\}$$

a list of contracts sorted in decreasing order with respect to their violation degree, and

$$List_{dimension2} = \{C_1, C_{43}\}$$

Performance Measure	Value
Correlated Coefficient	0.93
Mean Absolute Error (**MAE**)	0.08
Root Mean Squared Error (**RMSE**)	0.11

TABLE V
THE PERFORMANCE OF REGRESSION TREE-BASED MODEL

a list of data consumers sorted in decreasing order with respect to the number of violating contracts they are involved with.

Setting up $K = 1$, the Police selects the first member of $List_{dimension1}$ as well as all the members in $List_{dimension2}$ to re-evaluate their violation degrees more precisely. Thus, the Police adopts PSTM (explained in subsection III-B) to acquire more evidence (users complaints) from the users whose data has been traded by the first member of $List_{dimension1}$, and all member of $List_{dimension2}$.

Table VI presents the updated value of violation degree of the contracts that the Police acquires more complaints from users[4].

Contract Name	E	R	T	$Violation'_{(ct_i)}$	$trust'_{(dc)}$
ct_9	**0.08**	**0.93**	**0.33**	**0.97**	**0**
ct_{53}	0.28	0.81	0.25	0.74	N/A
ct_{23}	**0.20**	**0.95**	**0.56**	**0.78**	**0.37**
ct_{67}	0.002	0.98	0.25	0.56	N/A
ct_{33}	0.44	0.72	0.56	0.69	N/A

TABLE VI
THE UPDATED VALUE OF VIOLATION DEGREE OF CONTRACTS WITH NEW SET OF USERS COMPLAINTS USING PSTM

Given $\epsilon = 0.1$, results presented in VI indicate that the contracts ct_9 and ct_{23} have been detected violated. The Police classifies the associated DCs: C_{32} and C_1 as malicious and further updates their trustworthiness, $trust'_{(dc)}$, adaptively (using Equation 7).

The Police further considers a data consumer C_{32} *untrustworthy* and will ban it from the marketplace. The data consumer C_1 will not be banned, but will be penalized. It could be limited to participate in contracts with lower importance, i.e. buy only data related to "safe" purposes, involving less sensitive user data, keep it for shorter time, or pay a higher price.

The experimental results show that the proposed trust-mechanism can identify and penalize DCs that violate their contracts for using shared user data by reducing their trust level, so that they can be either excluded or disadvantaged in their dealings on the user data sharing marketplace.

V. Related Work

Various approaches have been proposed in the past for addressing the challenge of enforcing compliance to data use contracts. Existing solutions include the use of encryption mechanisms and digital right management techniques such as digital water-marking [12]. However, these solutions are inadequate in the sense that they simply focus on ensuring data integrity by preventing data modifications and re-sharing by recipients without authorization.

Encryption mechanisms ensure that only authorized parties have access to user data, but once the data is decrypted, the recipient can still carry out illegal operations. Mont et al. [15] proposes a sticky policy technique to attach obligations about personal data usage to the data by means of an encryption scheme at the point of collection. An authorized data consumer will then get the decryption key from a trusted third party. The limitation of this technique is that there is no guarantee that data consumers cannot further disclose the decrypted data and there are no mechanisms for penalizing errant behavior. In response to this, Sundareswaran et al. [3] focuses on providing data provenance. Data access policy and a log file are bundled with the data when shared. Whatever the data consumer does with the data is logged and periodically sent to the cloud. However, the framework provides no means of penalizing data consumers when misuse of user data is detected.

Just like in digital products such as music and books, digital right management techniques, such as digital watermarking, are used to detect unauthorized copies and modifications to user data. [7] suggested the use of digital watermarks as a means of indicating ownership of user profile data shared on social network thereby preventing illegal copy of the data. According to [12], many users consider digital right management techniques too restricting to data sharing and use as they impose constraints on how many copies of the data can be made and often require a special hardware or software to access the data. Detection of unauthorized user data stored or used by applications to personalize their functionality or content is especially hard, since the data would be processed and acted upon, rather than presented or played in a public site, as is the case with digital images and music. Therefore, the violations can be recognized only by the undesirable effects they may cause on users.

Trust and reputation (TR) mechanisms present a compelling approach to detect violators based on feedback from others. Although TR mechanisms have been successfully applied in managing interactions and mitigating misbehaviors in open networks in e-commerce, peer-to-peer networks, and mobile ad-hoc networks [14], [9], they have not been used for enforcing compliance by data consumers to their data use contract. We propose a TR mechanism specifically tailored to detect contract violations of privacy in a provider-user-consumer marketplace for sharing user data. Our proposed TR mechanisms can be used to detect violating data consumers (DCs) after interactions have taken place, based on incoming evidence of bad behaviour or poor quality of service (complaints). In the market for secondary data sharing, users might share the same data with various DCs. To find out which DC might have violated their contracts of data use, the Police collects users complaints regarding privacy violations, for example, suddenly receiving a lot of spam. It maps these complaints to possible purposes of data use and then it finds the contracts made for these purposes that involve the complaining users. Finally, the Police narrows down the list of "suspects", and make decisions under uncertainty.

VI. Conclusion and Future Work

As the commercial interest in secondary sharing and usage of user data increases, there is a growing need for appropriate data sharing infrastructure that addresses two main challenges:

[4] E, R and T are the acronyms for $E(pr_{trusted}, ct_i)$, $Reliability(r, s)_{ct_i}$ and $trust_{(dc)}$ in Table VI.

i) how to control with whom data is shared; and ii) how to identify and punish data consumers who violated their data usage contract.

In this paper, we present a trust mechanism to address the second challenge. The proposed trust mechanism is a contribution to the area of privacy on one end, as it represents an important part of the design of market-based solution to user data sharing framework addressing one the two main privacy-related challenges with secondary data sharing. On the other end, it is a contribution to the area of trust and reputation systems, as it demonstrates the applicability of trust and reputation mechanisms in the area of big data security and privacy. The proposed solution involves a novel step of soliciting proactively feedback from market participants to increase the amount of evidence and decrease the level of uncertainty in identifying violators. Generally, there are only a few existing complaint-based approaches in the trust and reputation literature [2], [11]. The experimental results show the effectiveness of our approach in detecting and penalizing malicious participants who violated their mutually agreed contracts with users. To preserve users' privacy, the proposed mechanism provides users with means to control their data sharing so that they can decide for what purposes, with which of the eligible data consumers to allow their data to be shared, and even to earn some money in exchange for their data.

There are, however, several limitations of the proposed technique. First, the framework relies on the assumption that there is evidence of privacy violation that will trigger user complaint. In a case where the data usage contract violation does not result in any directly observable evidence, then there will be no process triggered to detect and punish the violator. Second, the system assumes that the user complaints are genuine, i.e related to actual data use policy violations. This could be exploited by interested user groups to fake complaints regarding data they know is purchased by a particular data consumer to badmouth it or extort higher price as penalty for having violated their contract. Currently the mechanism does not detect fake complaints and user collusions.

A lot of future work remains to be done to ensure that the framework is functional in practice and responsive to user complaints. We plan to conduct experiments to evaluate the robustness of the proposed trust mechanism against the manipulation of the market participants, specifically the badmouthing attacks and collusions of users. Furthermore, the user interface and protocol for involving users in defining their privacy and data trading preferences, as well as the user interfaces for accepting and classifying complaints will need to be elaborated and evaluated. Another interesting direction for future work is to develop guidelines in consultation with privacy experts to define a method for determining the contract importance based on the risk associated with the purpose and the user data sensitivity.

REFERENCES

[1] Fabian Abel. *Contextualization, user modeling and personalization in the social web: from social tagging via context to cross-system user modeling and personalization.* PhD thesis, University of Hanover, 2011.

[2] Karl Aberer and Zoran Despotovic. Managing trust in a peer-2-peer information system. In *Proceedings of the tenth international conference on Information and knowledge management*, pages 310–317. ACM, 2001.

[3] Mohamed Ahmed, Daniele Quercia, and Stephen Hailes. A statistical matching approach to detect privacy violation for trust-based collaborations. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 598–602. IEEE Computer Society, 2005.

[4] Christina Aperjis and Bernardo A Huberman. A market for unbiased private data: Paying individuals according to their privacy attitudes. *arXiv preprint arXiv:1205.0030*, 2012.

[5] Shlomo Berkovsky. Decentralized mediation of user models for a better personalization. In *Adaptive Hypermedia and Adaptive Web-Based Systems*, pages 404–408. Springer, 2006.

[6] Francesca Carmagnola, Federica Cena, and Cristina Gena. User model interoperability: a survey. *User Model. User-Adapt. Interact.*, 21(3):285–331, 2011.

[7] Dominikus Heckmann. *Ubiquitous User Modeling*. PhD thesis, Saarland University, November 2005.

[8] Johnson Iyilade and Julita Vassileva. A framework for privacy-aware user data trading. In *Proceeding of User Modeling, Adaptation, and Personalization (UMAP)*, pages 310–317. Springer, 2013.

[9] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, 43:618–644, March 2007.

[10] Anne Kayem. On monitoring information flow of outsourced data. In Hein S. Venter, Marijke Coetzee, and Marianne Loock, editors, *ISSA*. ISSA, Pretoria, South Africa, 2010.

[11] Wendy M. Maiden, Ioanna Dionysiou, Deborah A. Frincke, Glenn A. Fink, and David E. Bakken. Dualtrust: A distributed trust model for swarm-based autonomic computing systems. In *DPM/SETOP*, pages 188–202, 2010.

[12] M.C. Mont, S. Pearson, and P. Bramhall. Towards accountable management of identity and privacy: sticky policies and enforceable tracing services. In *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, pages 377–382, Sept 2003.

[13] Zeinab Noorian, Stephen Marsh, and Michael Fleming. Multi-layer cognitive filtering by behavioral modeling. In *The 10th International Conference on Autonomous Agents and Multiagent Systems - Volume 2*, AAMAS '11, pages 871–878. International Foundation for Autonomous Agents and Multiagent Systems, 2011.

[14] Zeinab Noorian and Mihaela Ulieru. The state of the art in trust and reputation systems: a framework for comparison. *J. Theor. Appl. Electron. Commer. Res.*, 5:97–117, August 2010.

[15] Smitha Sundareswaran, Anna Cinzia Squicciarini, and Dan n. Ensuring distributed accountability for data sharing in the cloud. *IEEE Trans. Dependable Sec. Comput.*, 9(4):556–568, 2012.

[16] Ljupčo Todorovski, Peter Ljubič, and Sašo Džeroski. Inducing polynomial equations for regression. In *Machine Learning: ECML 2004*, pages 441–452. Springer, 2004.

[17] Yong Wang and Ian H Witten. Induction of model trees for predicting continuous classes. 1996.

[18] Yonghong Wang and Munindar P. Singh. Formal trust model for multiagent systems. In *IJCAI*, pages 1551–1556, 2007.

[19] Ian H Witten and Eibe Frank. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann, 2005.