Secure Concept for Online Trading of Technology Data in Global Manufacturing Market

Ghaidaa Shaabany, Simon Frisch, Reiner Anderl

Secure Concept for Online Trading of Technology Data in Global Manufacturing Market

Ghaidaa Shaabany*, Simon Frisch, Reiner Anderl

Technical University of Darmstadt, The Department of Computer Integrated Design, Otto-Berndt Strasse 2, Darmstadt 64287, Germany

shaabany@dik.tu-darmstadt.de

Abstract. The high-tech strategy of the German government aims to expand the networking and intelligence capabilities of machines, products and services. Thereby it is essential to apply extensive utilization of information and communication technologies (ICT). The goal of the German term "Industrie 4.0" is to merge the physical world with the virtual world [1]. This interconnected digital world enables various opportunities for creating new business models and increasing companies' revenues at the same time. Online trading of goods increased extensively in the last years, especially online trading of digital goods like music, films and e-books. Various license models and usage control policies are developed for a secure utilization of these goods by customers. Indeed there are still challenges regarding IT security issues that hinder the expansion of digital trading in the industry. This paper demonstrates a new business model for online trading in the automation and manufacturing industry. This model is based on existing resources in companies and hence improves the added-value-chain in companies. Thereby technology data that is required for machine operation in manufacturing processes will be traded. The main concept and workflow of trading processes will be presented. Furthermore various needed license models for usage control of Technology Data (TD) after trading are demonstrated.

Keywords: Industrie 4.0, license models, IT security, online trading, technology data, usage control, DRM

1 Introduction

One of the main goals of the high-tech strategy in Germany is to support small and medium-sized enterprises (SMEs) with the development of innovative services and products and enabling them to lead the future market [2]. Within this scope the fourth generation of industry, known as Industrie 4.0 (I 4.0) in Germany was called into life.

The essential idea of I 4.0 is to apply digitization widely in different perspectives, industries, corporate functions, technologies and various fields of study. A recent survey published in 2016 aimed to find a general understanding of I 4.0 in the global market, which considered six different countries including Germany, US, UK, Japan, South Korea and China. There are five fields of interest which I 4.0 is focusing on, according

adfa, p. 1, 2011.

to that survey. These fields are: increasing networking and digitization in economy (26%), development of smart products, (20%), optimization of production processes (20%), automation (18%) and creation of new business models (16%). [3] In consequence of these changes, new chances and innovative business models are being developed that are mainly based on digital data. However, there are many challenges that SMEs face through implementing I 4.0 use cases that are characterized by intensive networking and digitization especially in the manufacturing sector [4] – primarily challenges regarding IT security issues. New threats and wide attack areas may be figured out by hackers easier. Possible goals of these hackers are manipulation of data and sabotage. Moreover, theft of competitors' know-how and getting financial benefits can be a motivation for hacking. Thus many new security measures regarding sensitive data, know-how and workflow in enterprises should be developed. Many studies and research projects with respect to security issues are carried out currently in the industrial field, especially in the manufacturing sector.

This paper demonstrates a concept of one innovative business model that considers online trading of technology data (TD) that is called technology data market place (TDMP). TD are various sets of data that are needed to calibrate a machine for a manufacturing process in order to ensure a smooth operation of machines under different circumstances e.g. cutting speed and movement and tools features. These sets of data represent the digital goods that will be traded on TDMP. We will use the expression technology data (TD) in this paper to illustrate these machines' functioning parameters. In the first section an introduction of e-commerce concepts and many examples of similar existing market places is given. Then, the concept, the requirements, the scenarios and activities of TDMP during online trading of TD will be illustrated. Moreover different license models for offering TD at TDMP are presented.

2 State of the Art

In this section we have a look on existing online trading concepts before we will present our TDMP concept. E-commerce has seen tremendous growth over the past few decades. It has evolved into several types of online businesses like online marketplaces, online stores, storefronts, virtual communities etc. Online marketplaces are the digital version of the trade fairs of the past, where buyers can discover and do business with sellers and vice versa.

There are several different kinds of e-commerce marketplaces. These are characterized as business-to-business (B2B), business-to-customer (B2C) or customer-to-customer (C2C). Our area of focus is B2B; the marketplaces that involve trading between different companies or businesses, for example between a supplier and distributor. B2B marketplaces are internet-based interorganizational trading platforms that facilitate and foster the exchange of information, products and services, and other business transactions among many buyers and sellers [5]. B2B transaction is a rapidly growing sector within e-commerce. However, despite the increase in the number of B2B transactions, only a few e-marketplaces have successfully attracted a large number of buyers and sellers. There are several factors that are very important in determining the success of

a B2B marketplace. The most important, most researched and most documented factor in this context is trust. Nearly every study about marketplaces in general, mentions the role of trust for success of the marketplace [6], [7] ,[8]. The design of the website and its ease of use has an impact on a user's trust in the marketplace. Furthermore security level of the website play a major role with trust in marketplaces. *Niranjamurthy* provides an overview of e-commerce security issues and threats in [9] that shows the common security threats in online trading. These threats are denial of service (DoS), unauthorized access, theft and fraud. We think, that trust depends mainly on the character of marketplaces and their design that enable an acceptable level of security without affecting the availability of trading processes.

The idea of a platform for trading technology data over the internet is a fairly new concept. There isn't any known work taking a comparable approach in the field of automation and manufacturing. Online marketplaces with certain similarities are, however, established in the fields of consumer electronics and multimedia. Mobile apps for smart phone operating systems such as Android and iOS serve a similar purpose as TD do on machine tools: both are digital goods used to expand the range of functions on a device [10]. Google Play and Apple App Store – digital platforms for trading mobile apps – address issues of maintaining a trustful trade environment. This includes mechanisms to protect the know-how of app providers as well as measures to protect the customers against malicious apps. [11–14] discuss the security mechanisms implemented by the above mentioned platforms and the related operating systems. Microsoft and Amazon run marketplaces comparable to Google's and Apple's platforms for their own mobile o. Further information to mobile app marketplaces in general is provided by [15].

One key element of TDMP's concept is the usage control of purchased and licensed TD. Whereas this as well is a new topic in the automation and manufacturing sector, there are several established solutions dealing with this issue in the area of multimedia. These can be subsumed under the term digital rights management (DRM). One of the main design philosophies of a DRM system is to offer a content with different usage policies. This allows the content to be distributed or downloaded freely. However, it cannot be consumed without a valid li-cense, which has a proper rights object. [16]

For instance, both Amazon and Adobe use DRM technology for their e-book formats [17]. Furthermore DRM solutions are provided by Microsoft (Windows Media Audio), Apple (Fairplay) and others for controlling the use of digital audio content [18].

3 Concept of TDMP

Commonly various sets of data are needed to calibrate a machine for a clean manufacturing process for different conditions. For example under different ambient pressure, temperature or when working up different materials it is necessary to adjust one or many of machine's functioning parameters like cutting speed and movement and tool features. When a machine is purchased from a machine manufacturer, some sets of TD are provided for basic functions and processes. In some cases, the machine might need

to be operated under new conditions for which there are no manufacturer recommendations available. Thus manufacturer have to experiment on the machine in order to derive these new needed parameter. For a company that only uses such a machine to manufacture products, it is mainly concerned with productivity and delivering the orders on time. If manufacturers have to figure out the needed parameters by using their own resources and expertise first, the productivity is diminished because of these extensive effort. It would be much more beneficial for the enterprise to get these parameters from someone else who could be another company making similar products on similar machines. At the same time the other company can improve its added-value-chain by offering the already existing data. To meet such needs of manufacturers we developed the concept of TDMP. The main goal is to design a platform that enables involving those both parties, TD provider and TD customer in an online trading process of requested TD. Moreover it enables a highly interconnected and dynamic industry in the global market and at the same time it improves the added-value-chain in enterprises by generating new business models based on existing resources. [19]

However various threats and risks regarding protection of traded digital goods, namely TD can affect the smooth operation of TDMP. Therefore many requirements should be met in order to operate the TDMP successfully:

- Protecting of manufacturing know-how through encryption of TD as well as secured communication between parties
- Access on TDMP only for authenticated users
- Integrity check of traded TD
- Enabling a usage control policies for TD
- Equipping concerned machines for a controlled handling of TD
- Reliability of TDMP
- Availability of TDMP

This paper focuses on the first five requirements of TDMP concept. The last two points are primary requirements for every marketplace and are adequately discussed in many studies.

3.1 License Models

Digital data has a lot of special characteristics when it comes to ownership, reuse and licensing compared to physical goods. The license file of the presented concept contains the rights object which incorporates the terms and conditions applied for usage of the licensed content. A rights object specifies the permissions for various ways of use of associated content by a consumer or a device. In case the content is encrypted, the license contains the key for decrypting it. Due to license files, the same content can be associated with different usage rights to specify different modes of content consumption. This attempt provides flexibility and ease of management. In our concept, the licensed consists of TD.

Customers can purchase the right to use one or several specific TD sets offered on TDMP. This process is referred to as *purchasing* or *licensing* in this paper. That means that the purchased TD sets can be used under the terms and conditions of license models

only. The terms of use for TD sets are defined via a license file. These terms are enforced by trusted software on the customer's machine while processing the TD set. The tangible license file for a TD set is generated during the purchasing process described in section 3.3. It is individual for every purchasing process. Thus, it includes the following information: TDMP code, purchasing ID, machines ID, customer ID, license features and a time stamp of generating process. The license file is derived from a license model selected by a TD provider when publishing a new offer on TDMP. From one time usage, pay-per-use to fixed price packages or long term subscriptions, TDMP enables a variety of different license models:

- Pay-per-use model: the customer can use a TD set only in a certain amount of manufacturing processes. To enforce this, each use of a TD set is registered on the machine and a counter is increased until the maximum of permitted uses times is reached.
- Time-based model: the customer can use a TD set only within a certain period of time. It can be defined either by a fix date of expiry or by a specific time span since the first use of the TD set. The enforcement of license files based on this model requires a trusted clock on the target machine. Manipulating this clock is prevented by technical means.
- Unlimited use model: the customer is allowed to use the TD set on all licensed machine without further limitations. He is, however, not able to copy or to read the TD set in clear text.

The above-mentioned license models form a basis for other models such as trial licenses which can be understood as special forms of one of the three basic license models.

3.2 Scenarios for trading processes on TDMP

The required scenarios for a clean functionality of TDMP will be demonstrated as follows:

a) Administrating market place. To ensure the smooth running of trading processes on the marketplace, it is necessary to administer the infrastructure of TDMP by a marketplace system. The system ensures that there are no problems with registration of market place users, the data provided is of the correct format and adheres to marketplace policies, as well as security of technology data sets while being stored at the marketplace or when being uploaded or downloaded from the marketplace. Furthermore users' data like needed accounts details and personal data should be managed.

b) Participation at market place. In order to participate on the marketplace either as a buyer or a seller, a user has to be registered with the marketplace according to specific credentials. User business and personal data have to be verified and approved by the administrator of the TDMP.

c) Developing technology data. In order to be able to sell TD at the TDMP, TD providers first have to develop this TD for a specific material on a specific machine. During operating the machine for producing certain products the provider replicates cutting processes many times trying different parameters every time until reaching the desired cutting quality of these products. Then the provider writes a description of TD including operating conditions and quality. This description will then be verified by the system to make sure that it abides by the TDMP policy. Then TD is exported from the machine and has to be signed digitally by the provider to ensure authenticity before being uploaded to the marketplace for starting trading process.

d) Requesting technology data. Once a buyer is an approved, registered member of the technology data marketplace (TDMP), he can then search for the TD that he needs. If needed data is not found, a request for needed TD can be written by the buyer with the required TD properties e.g. machine type and performance, material, use time or duration and desired quality and then the request can be published on TDMP. After that, TD provider can respond to this request and offer TD that is appropriate to this request if it is existing or can be developed by him. After that, the process for purchasing of this data can be initiated, if the offer suits the request conditions.

e) Administration of technology data. TD providers can open their own profiles after a successful log-in on the marketplace (frontend), to get an overview about previous actions they did. TD offers can be administrated for example updates of TD characteristics, prices and handle conditions can be conducted. Moreover existing TD offers can be deleted and, at the same time, new offers can be uploaded and activated by providers.

f) Processing of technology data. The purchased TD that are already saved on TDMP's server are available to be used by an authorized operator. Thus TD can be downloaded to be processed on the machine only if the license is still valid. Thus by every use of TD the license should be checked for its validity and then synchronized with the TDMP. This machine should be capable of using TD according to the provided license.

3.3 Workflow of Trading Process on TDMP

In the following section the workflow of trading processes on TDMP will be presented. These processes are demonstrated by means of two activity diagrams that present the offering as well as the purchasing processes.

TD Offering.

Similar to traditional marketplaces, TDMP acts as a mediating platform where prospective buyers and different providers of goods make contact. Because TDMP doesn't

act as a creator and a vendor of its own TD, TDMP provides a simple workflow that enables every verified participant to offer TD sets securely on the marketplace.

Figure 2 provides an overview over the activities of this workflow. It starts with the actual generation of TD. In the majority of cases, this activity is conducted on a standard machine tool by manually elaborating machine parameters. The newly generated TD set then needs to be exported.

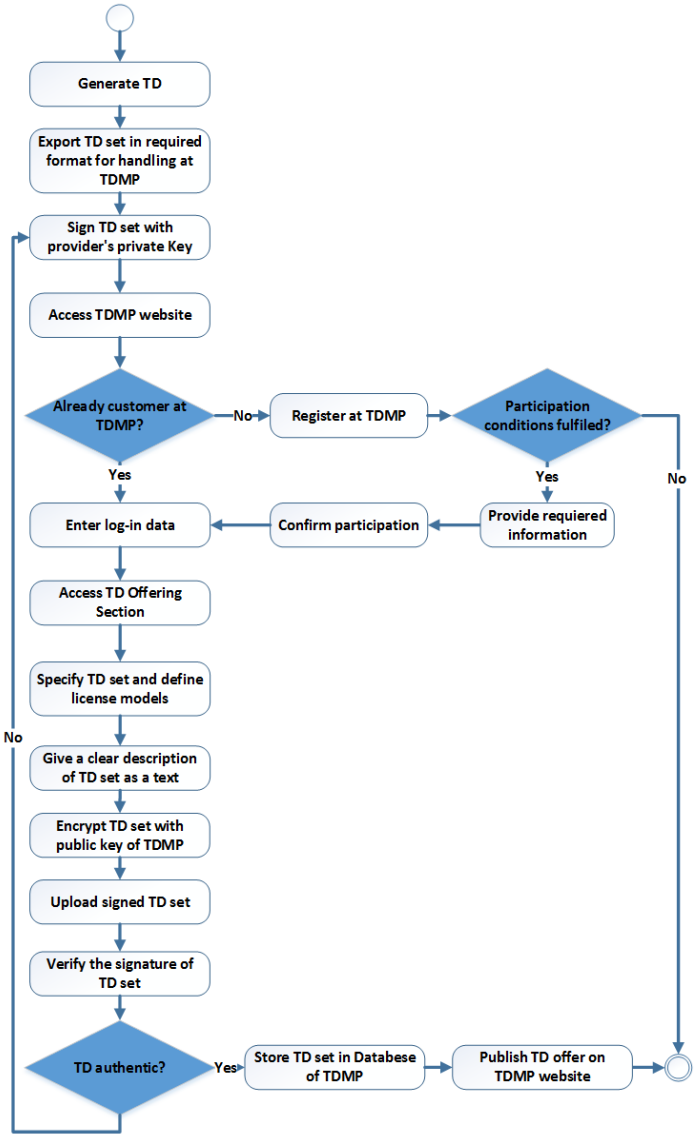

Fig. 1. Technology Data Offering

In order to meet the security objectives integrity and non-repudiation, the provider has to sign the exported TD set with his private key subsequently. The following activities are directly processed on TDMP's website. After having accessed the website, the TD provider has to be authenticated by entering his log-in data. In case he is not already registered, a registration process is initiated instead. During this process several steps are necessary in order to create a valid profile. The most important step is to verify the identity of the new TDMP participant and his business contact data. Also, it's checked if the registrant meets all defined participation conditions. By that, it's made sure that only trustful participants will be able to offer technology data sets on TDMP. The verification of the registrant's identity and stated information can be conducted via a call, a mail, postal letters and submission of official identification documents. Having passed the verification process, the registrant sets his log-in information and provides his public key for later authentication checks. Then he is able to log-in regularly on the TDMP website. After having logged-in, the provider is able to access the TD offering section of TDMP's website. On the offering section a new offer for generated TD set can be created. By doing so, he has to give a description of the TD set as a text, to define machine types and materials that are compatible with the offered TD set and to defines the desired license models for later purchasing processes. As presented in section 3.1, license models specify in which manner the TD set is allowed to be used on a customer's machine. In a final step, the provider uploads the signed TD set to TDMP. It is necessary to check the uploaded TD set integrity by verifying the digital signature with the provider's public key before storing these data in a database on the server and eventually publishing the offer on TDMP's website.

TD Purchasing

When receiving an order for producing a specific product with particular characteristics for example material, quality, etc. machine's operator has two possibilities, to develop the needed TD or to search and buy them from TDMP. Figure 3 shows the activities that should be done by a purchasing process that starts with the action "*access TDMP Website"*. Before beginning trading process on TDMP, a customer should be authenticated by system. This step is important to manage customers' identities and related actions on marketplace. With action "*Enter log-in data"* the customer should enter his username and password to log-in into his own profile. As mentioned by offering TD, new participants should register on TDMP. That is important to ensure the reliability and enables a clean workflow of trading process on TDMP. As soon as this action is done successfully, the customer's participation is confirmed and further actions like purchasing or providing on marketplace can begin. A customer starts the purchasing process with searching for required TD on the marketplace using some search criteria as material type, machine model/serial number, needed quality, etc. After finding the suitable TD, it is also important to specify a license model according to the use case of order and budget requirements. For example, if the buyer only needs to use this data for one week, it might not be suitable or economic to buy a data set that has a one year license model available. Then, the purchased TD is encrypted with the key that is generated from license information for the machine, which uses TD set.

Once a suitable TD set and an acceptable license model is selected, the customer will be asked about the capability of the machine that will process this TD and if it is equipped for this process. The machine should ensure a secure and clean handling of TD and at the same time it should enable to use TD only according to selected license models. This includes being able to verify the availability of using TD by checking the license information and synchronizing them with TDMP server.

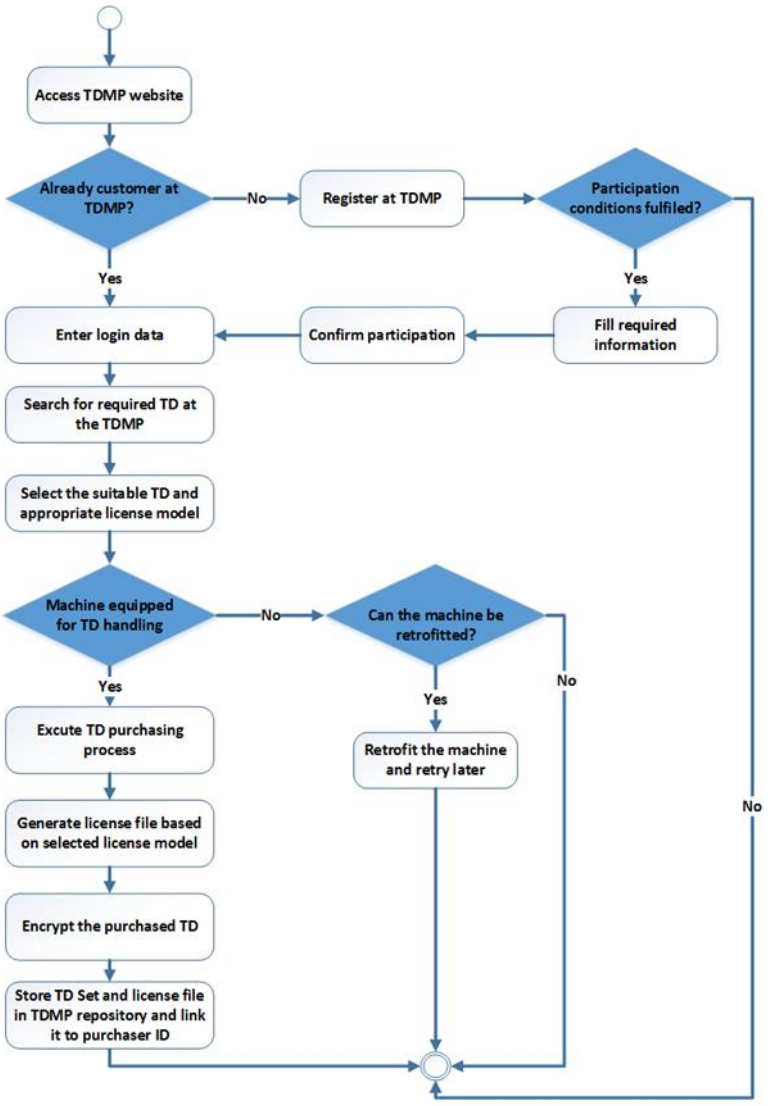

Fig. 2. Technology Data Purchasing

It is also necessary that the machine can use the acquired data set in accordance with the license associated with it. The machine must support the licensing system and be able to properly interpret the usage rights specified in the license file. Meaning that the machine must be able to read, understand and abide by the terms provided by the license file. Otherwise the customer should retrofit the machine to be able to handle TD and try again later. If the machine is not able to be retrofitted, a trading process should be ended.

Once all these conditions are met, the TD set can be purchased and then a license file based on the selected license model is generated by the system. After that, the selected TD set and the generated license file are stored in TD repository with a link to the purchaser's identity. This TD set will be stored on server and is available for use until a buyer accesses the website to download data for operating the machine according to the terms of the license model. Once the license validity period is over, the key that can decrypt the TD set expires and the machine can no longer use this data. As an alternative, the buyer has the option to extend or to buy another license model if the TD is still needed.

4 Conclusion

A new concept for online trading of TD on a technology data marketplace in the sector of automation und manufacturing is presented in this paper. This concept illustrates that existing data are the digital goods of the future. This industry enables to raise enterprises' revenues by facilitating innovative business models that handle with existing resources, namely needed TD for machine operation. However, suitable security means that protect this data overall trading processes are required. Furthermore it is essential to develop appropriate license models that manage usage policies of executing these data. Otherwise it will be ineffective to develop and operate this marketplace. In order to establish TDMP the workflow of offering and purchasing processes are then demonstrated. We focused on these two main scenarios to analyze the requirements that are needed and specified essential protection means.

Acknowledgements. This work has been funded by the German Federal Ministry of Education and Research (BMBF) in the project IUNO – National reference project on IT-Security in Industrie 4.0 (project number 16KIS0328).

References

1. W. MacDougall and M. & C. Germany Trade & Invest, "Industrie 4.0 Smart Manufacturing for the future," Germany Trade and Invest, Gesellschaft für Außenwirtschaft und Standortmarketing mbH, 2014.
2. Federal Ministry of Education and Research (BMBF), "The new High-Tech Strategy Innovations for Germany," Berlin, Aug. 2014.

3. H. Kagermann, W. Wahlster, and J. Helbig, *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0: Deutschlands Zukunft als Produktionsstandort sichern: Abschlussbericht des Arbeitskreises Industrie 4.0*. 2013.
4. T. Ludwig *et al.*, "Arbeiten im Mittelstand 4.0 – KMU im Spannungsfeld des digitalen Wandels," *HMD Prax. Wirtsch.*, vol. 53, no. 1, pp. 71–86, 2016.
5. W. Thitimajshima, V. Esichaikul, and D. Krairit, "Developing a Conceptual Framework to Evaluate Public B2B E-Marketplaces," in *PACIS 2015 Proceedings*.
6. S.-H. Chien, Y.-H. Chen, and C.-Y. Hsu, "Exploring the impact of trust and relational embeddedness in e-marketplaces: An empirical study in Taiwan," *Ind. Mark. Manag.*, vol. 41, no. 3, pp. 460–468, Apr. 2012.
7. S. A. K. Beige and F. Abdi, "On the critical success factors for B2B e-marketplace," *Decis. Sci. Lett.*, vol. 4, no. 1, pp. 77–86, 2015.
8. B. A. Kumar, "Cogniton Based Trust Model for B2B E-Market," presented at the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2015.
9. M. Niranjanamurthy and D. Chahar, "The study of E-Commerce Security Issues and Solutions," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 7, Jul. 2013.
10. comScore, "The U.S. Mobile App Report." 2014.
11. Google, "Android for Work Security White Paper." 2015.
12. Google, "Google for Work Security and Compliance Whitepaper." 10-Nov-2016.
13. D. A. Dai Zovi, "Apple iOS 4 security evaluation," *Black Hat USA*, vol. 24, p. 37, 2011.
14. A. Egners, B. Marschollek, and U. Meyer, "Hackers in your pocket: a survey of smartphone security across platforms," *RWTH Aachen Tech Rep AIB-2012-07*, 2012.
15. A. Holzer and J. Ondrus, "Mobile application market: A developer's perspective," *Telemat. Inform.*, vol. 28, no. 1, pp. 22–31, 2011.
16. W. Rosenblatt, S. Mooney, and W. Trippe, *Digital rights management: business and technology*. John Wiley & Sons, Inc., 2001.
17. M. M. Azad, A. H. S. Ahmed, and A. Alam, "Digital rights management," *Int. J. Comput. Sci. Netw. Secur.*, vol. 10, no. 11, pp. 24–33, 2010.
18. R. Hammersland and J. Strømstad, "Digital Rights Management," 2008.
19. G. Shaabany, M. Grimm, and R. Anderl, "Secure Information Model for Data Marketplaces enabling Global Distributed Manufacturing," *Proc. 26th CIRP Des. Conf.*, Jun. 2016.