Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 50 (2016) 360 – 365

www.elsevier.com/locate/procedia

26th CIRP Design Conference

# Secure Information Model for Data Marketplaces enabling Global Distributed Manufacturing

Ghaidaa Shaabany*, Marco Grimm, Reiner Anderl

*Technische Universität Darmstadt, The Departemnet of computer integrated Design, Otto-Berndt Strasse 2, Darmstadt 64287, Germany*

* Corresponding author. Tel.: +49 6151 16-21848; fax: +49 6151 16-21793. *E-mail address:* shaabany@dik.tu-darmstadt.de

**Abstract**

The German term “Industrie 4.0” is distinguished by expanding networking and intelligence of machines, products and services. In this context new business models are developed, many of them is based mainly on digital design and production data. In this paper, a new concept for a technology data marketplace (TDMP) is presented, which allows trading manufacturing process data. Digital data distribution involves various risks by hackers’ attacks, theft or manipulation of data. So, the use of effective security methods and mechanisms is the key to the success of this TDMP. At the same time authority, authenticity, privacy and availability of these machine data are highly required for secure use and confidential identities. The scientific challenge is to develop a secure concept of technology data exchange between market members. Furthermore providing machines with required data automatically from the marketplace is desired. This distribution of data introduces a basic concept to exchange and protect production information. In addition it discusses developing new business models based on existing resources, which create a new value stream in the industry.


Peer-review under responsibility of the organizing committee of the 26th CIRP Design Conference

*Keywords:* Industrie 4.0; business models, networking; digital design data; production data; security methods, data market place

## 1. Introduction

German industry is the heart of economy in Germany. Worldwide German companies have top positions in several market branches. A recent report from the Federal Ministry of Economics and energy in Germany asked essential questions, which discusses the capabilities and chances of German enterprises in the digital age and its consequences at German industry and also at economy. What are the challenges and chances German industry is facing by digital innovation? How can German companies stay competitive in the world market?

This study illustrates that digitalization opens new successful approaches and leads to developing new enterprise directions. Indeed German industry companies should exchange their traditional strategies with an innovative management vision concerning digital transformation worldwide. Moreover revolutionary business models as well as innovative value-added-chain processes regarding new ICT (information and communication technology) are the key to enhance their existence in the world economy. The study advises German enterprises to analysis digital potentials in production, products and added-value-processes. As a result of realizing these potentials, the new business models will be defined and determined to the digital age of the global industry. Without concerning these recommendations German companies will lose their essential economical role [1].

In order to remain competitive in the global digital competition and tackle the new market challenges, the High-Tech strategy of the German government facilitated the new future ways of connected industry with the term “Industrie 4.0”. Industrie 4.0 is characterized by the next evolution to past industrialization phases (steam machine, assembly line mass production, digitalization with logic controls). Its fundamental idea is to merge the physical with virtual world by extensive use of information and communication technologies. The main goal is improving the added-value-chain over all phases of the product’s lifecycle. Main Condition of administrating this industrial revolution is digitizing, connectivity and interconnection between products, machines and operators overall product lifecycle processes. As a result, the high flexibility, agile adaptation in manufacturing processes will be


Peer-review under responsibility of the organizing committee of the 26th CIRP Design Conference
doi:10.1016/j.procir.2016.05.003

enabled as well as the individuality in development and production [2].

Many German companies recognized this fact and started changing their strategies, thus they are tending to digitalization according to a survey published in 2014, the results are shown in Figure 1. Current results illustrate that 27% of German companies have already implemented a high level of digitizing in their products. 35% of all companies are still working with low and medium digital levels. In five years the digitalization process are forecasted to be strongly increased. About 50% in high level digitalization alone, over the entire product portfolio, according to the company's expectations [3].

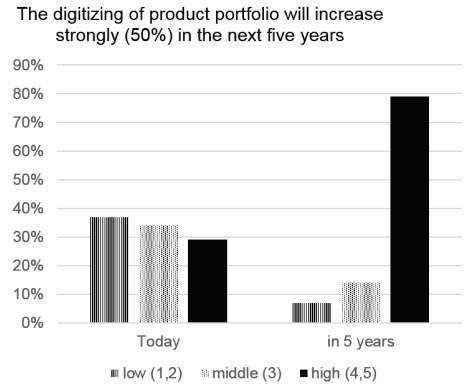


Fig. 1. Digitizing trend in Germany [PwC AG 2014].

In this paper the essential concepts for development an industrial marketplace trading digital technology data will be illustrated. Cloud computing technology, e-commerce concept and its types will be explained. Implementation of such services has hindrances due to protection, hence common security issues and solution approaches are presented. These issues are required over all phases in e-commerce business transactions for safe online trading [4]. To bring the explained technologies together to new business opportunities, a new concept for digital marketing of data under value usage and protection aspects will be introduced.

## 2. Cloud computing

Cloud computing conception was used for the first time by University of Texas in 1997. In this domain VMware was founded in 1998. It provides cloud and virtualization software and services [5]. According to its features and provided services, cloud computing can be defined as a framework, which provides on demand configurable computing resources through internet, such as networks, servers, storage, applications, and services. These services are available everywhere and can be accessed from different devices [6].

Cloud computing technology provides three different types of services, which serve resources on demand by the user. These services are Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) and involve different business models.

1. Software as a Service (SaaS): in this model software applications will be provided over the internet to the client.

2. Infrastructure as a Service (IaaS): it uses the cloud infrastructure (software/hardware) as a service on demand enabling users to provision their applications and platforms via virtual machines as well as it provides storage capabilities.

3. Platform as a Service (PaaS): it enables users to run or to develop applications at a provided platform layer resources such as operating system [5, 6].

Cloud computing technology offers effective, flexible and low cost services that give enterprise high chance to increase their revenues. Indeed, these services are the fundament of development new business models in the digital age.

## 3. E-commerce

E-commerce is defined according to Kalakota and Whinston as following, *"E-commerce is a dynamic set of technologies, applications and business process that links enterprises, consumers and communities through electronic transactions and electronic exchange of goods, services and information"* [7]. E-commerce is carrying on business over computer systems and networks e.g. online (internet) and bulletin board system (BBS). The growth of e-commerce is related to the growth of the financial transaction techniques, and their security techniques. Because most e-commerce activities are online, it is called (Internet commerce, or I-commerce). E-commerce is divided into four types of business models [7]:

1. B2B-business to business: this is done between companies e.g. manufacturers selling to distributers like *Covisint* for automotive industry
2. B2C-business to consumers: companies selling to the general public, e.g. *Amazon*
3. C2B- consumers to business: individuals sell products or services to companies e.g. *Mobshop*
4. C2C- consumers to consumers: consumers selling products or services directly on internet to each other e.g. public sales platforms like *eBay*.

Online marketplaces enable trading goods and services online. First, people register on the web site of this marketplace and then start trading products. *eBay* was the first marketplace enabling an auction service, which was established in 1995 in USA [9]. Nowadays there are several electronic marketplaces with different business models in the World Wide Web.

## 4. Protection means

In order to implement technical and organizational means for efficient protection of industrial assets, attack vectors and vulnerabilities must be analyzed. Fig. 2 shows a layer-based representation of industrial connected systems as used in Industrie 4.0 scenarios. Exemplary attack vectors are depicted by stars. The system boundary is represented by a dashed box containing networking, software, electronic and physical elements. Outside the system, other machines and humans are entities with which interactions are performed via network connectivity or human machine interfaces (HMI).

Common weak spots in this system representation are as follows:

1. Knowledge theft, social engineering, phishing;
2. Protocol analysis, DDoS, network intrusion;

3. man-in-the-middle, recording unencrypted data streams;
4. sidechannel attacks;
5. tampering with active components;
6. signal recording with logic analyzers;
7. disassembling and reverse engineering;
8. decompiling, memory editing and malcode injection;
9. malware applications.

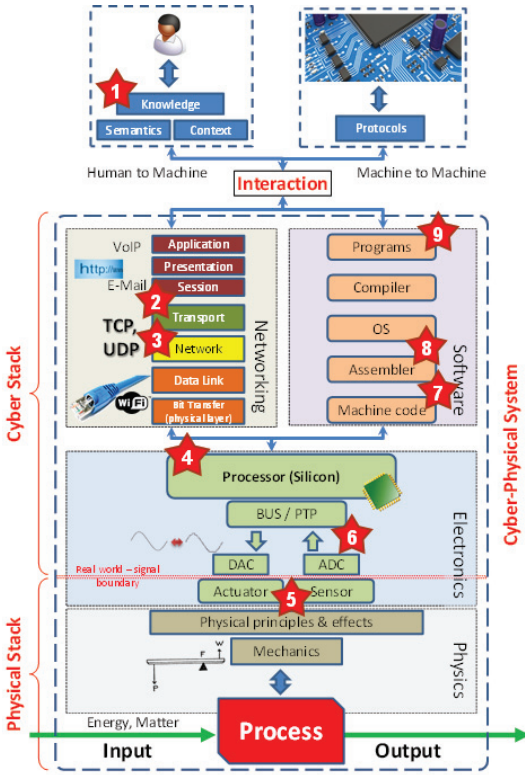


Fig. 2. Attack vectors in cyber-physical systems [8]

This list of attack vectors is not exhaustive; depending on system infrastructure and use case, there are different and may be more weak spots.

There are a variety of available technical (T) and organizational (O) protection means which are well-established in other areas than industrial systems. They can be applied to industrial systems in order to reduce vulnerabilities without decreasing system functionality or performance. Some of these protection means are listed below and categorized in technical (T) and organizational (O) protection recommendations:

1. Staff training regarding IT security and knowledge management, non-disclosure-agreements and corporate security guidelines (O).
2. Firewalls with packet inspection techniques, network intrusion detection systems (T).
3. Encryption of all internal and external data streams, tunneling via virtual private network (VPN) of external traffic through untrusted
4. Hardware protection techniques such as masking and obfuscation, certified by the Common Criteria (CC) for Information Technology Security Evaluation (ISO/IEC 15408-1) (T).
5. Integrity and plausibility checks for active components derived from fuzz testing evaluation (T).
6. Obfuscation and shielding of signal lines and bus systems (T).
7. Resource encryption and software protection by runtime integrity checks (T).
8. Sandboxed or virtualized execution of software code (T).
9. Anti-malware and anti-virus software (T).

## 5. Developing a new concept of trading manufacturing data

In general, machine manufacturers provide their customers with a set of common technology data (TD) for general manufacturing processes. Technology data is a set of manufacturing process parameters such as cutting and movement speeds, energy, tool dimensions etc. With the use of this data (e.g. for laser cutting process, which is the manufacturing technology considered in this paper) a manufacturing process can be executed reliably. The use of correct technology data which is suitable for the given materials to be processed is the most decisive factor for high quality results and best accuracy. According to the machine operator's order, such as when extraordinary materials have to be machined for the product end user, suitable TD for the manufacturing process is required. In this case operators have to experimentally derive this required TD. They need to use their own know-how and resources to develop the new relevant TD set. This development process requires time and effort as well as monetary resources due to material use. Particularly for operators specialized on productivity for the actual manufacturing job, this research effort pictures annoyances reducing productivity and benefit. Hence, viable and requested alternative for operators is to buy the needed TD from a 3rd party, commonly the machines' manufacturer or supplier. Here, new high potential business models arise, which target on improvement of productivity on the operator side and added value for knowledge owners, since the required digital TD can be employed as a valuable digital asset.

We will illustrate a new way of digital trading with these assets by utilizing the advantageous effects of industrial digitalization in the sense of Industrie 4.0. As a central platform for commercializing the of digital manufacturing technology data, a technology data market place (TDMP) is proposed.

The main idea of TDMP is based on an online marketplace concept, where goods (digital assets) are traded online [9]. Thus a new business model based on existing resources, namely existing TD is developed. The system, use cases and activities as well as stakeholder are defined in the following sections. First, a use case diagram figures the system, its boundary, its main components and interactions between users. It is important to show and understand the system goal as well as its use. Second, all involved Stakeholders are identified.

Here all partners interested to participate on the TDMP and to trade digital manufacturing data are considered.

The realization of TDMP and leveraging its associated values by all involved parties strongly depend on effective techniques for information security and knowledge protection as well as capturing used data by customers. This will be implemented later by using some of the known technical (T) and organizational (O) protection recommendations, which are mentioned before

### *5.1. Use Case Diagram*

This section explains the concept of the TDMP in a use case diagram, as shown in figure 3. The marketplace function is based on three main member roles, which enable a digital manufacturing data trade. The first role is called technology data provider (TDP). TDP develops the technology data (TD) set and provides it for sale at the TDMP. The TDP can be a manufacturing company itself sharing its develop data sets but also a third party material research institution, material supplier or organization specialized to enrich materials with specific data sets. These TD can be developed by TDPs either during operating their machine or particularly researching new manufacturing materials and their suitable process parameters. However these TD can be used to operate the same machine to do same manufacturing processes all over the world regardless of operators.

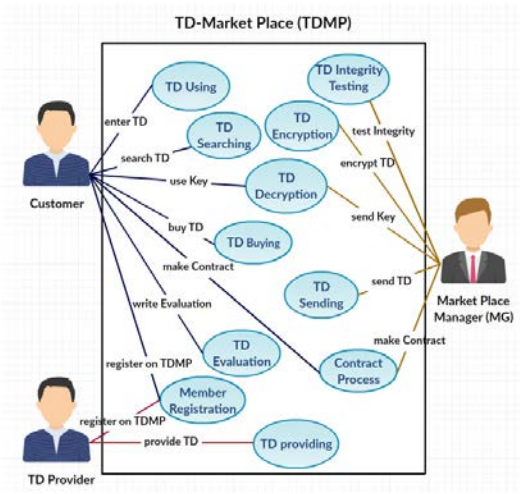


Fig. 3. Use case Diagram for TDMP

Digital trade of TD increases the operator revenues by sharing self-developed TD as digital goods in the market place. In this case the operator will have the role as a TDP, providing proven TD sets at TDMP. This use case is captured by the item “TD providing” in figure 3. This providing action has to be done in two steps. First TDP writes a description about self-developed TD according to the TDMP policy. That includes its usage conditions like material type, machine type/serial number, product quality and/or some other special properties. After that, the description with TD-set can be uploaded to the TDMP. Before providing TD, TDP must register at the market place and make his own profile. This identity is necessary for a trustworthy identity management at the market place as well as the implication that each partner has a certain role with particular authorization at TDMP. The use case “Member registration” illustrates this activity. All participants. i.e. as TDP or as a customer have to register at TDMP before they can trade digital data.

The second main member at TDMP is the market manager (MG). Mainly MG ensures the integrity of provided TD as well as the needed security requirements for trading. That is shown in the two use cases “TD Integrity Testing” and “TD Encryption”. Several license models enabling different business models should be provided at TDMP. These models based on one or more criteria, namely date, use times, machine identity or user identity. In order to enforce usage licenses, the data should be secured with cryptographic keys and digital policies for one of these models. After selling a TD set, this key is sent to the customer machine when usage is requested. For encryption, it is proposed to use a hybrid encryption scheme. The TD plaintexts $m_i$ are encrypted with random symmetric keys (content keys $k_i$), e.g. with the Advanced Encryption Standard (AES).

$$c_i = Enc(m_i, k_i)$$

These content keys are then encrypted with the public key $pk$ of the TDMP’s asymmetric keypair, e.g. using RSA (Rivest Shamir Adleman) public key cryptosystem.

$$k_{i,enc} = Enc(k_i, pk)$$

The result is that the encrypted content keys $k_{i,enc}$ can only be decrypted by the TDMP. The ciphertexts of the TD (TD-set) $c_i$ are then stored with the usage policy $u$ in a readable form, e.g. XML file. Finally, to protect the policy and TD against manipulation, they are signed with the public key cryptosystem. This signature can be checked with the public key of the TDMP later in order to prove the integrity of the TD.

$$v = Sign([h(u), c_i], sk)$$

MG makes the contracts by accepting the TD of TDP. On the other hand MG makes contracts with customer by selling TD.

The third main partner at TDMP is customer. Action is started by searching needed TD set after registration at TDMP. The search can be done by different criteria, for example machine type/serial number, material type and/or operator Identity Number, when it is given. . Just the above mentioned given description from TDP of the TD-set will be shown as searching results, which suits the search criteria. Thus manufacturing know-how of the data provider will be protected against manipulation and theft as an encrypted TD-set. These encrypted TD-sets are stored at the TDMP server and are delivered to the customer, after a contract with MG was made.

The purchase and contracting processes begin after customer finds the desired TD set according to the relevant description. In this process, involved partners are customer and MG. After the purchase is made, the encrypted TD set is delivered to the customer. When the customer receives the

purchased TD set, it can be used on the machine by decrypting the protected data for use in the process. The usage conditions for the data set and access permission is defined with the usage policy specified by the contracting system of MG. The relevant information is generated in the e-commerce system and written to the TD set. The control over the data is bound to the cryptographic keys, hence MG provides access to the encapsulated data in the case that the requested access is permitted by the license. MG keeps royalty over the protected data at all times, either inside the market place or after it was sent out to customers by controlling it with the cryptographic keys. The data stored on the market place can be decrypted for migration to other systems under the condition that MG permits this action by providing the required cryptographic keys. With this, the stored TD is protected for the TDMP-Customer relationship while exchange with other systems is still possible.

However, this leads to the necessity that the keystore has to be protected adequately. This is done by use of special hardware, such as hardware security modules (HSM). For the proposed concept it has to be assumed that the data security strength provided by the cryptosystem is not degraded by the storage of the keys at the TDMP. To build trust between market place members, an evaluation system for data quality is necessary. This evaluation consists of general opinion and remarks about the product and trading process quality. The main purpose of this use case is to help other partners by their future trading. Additionally it helps MG for price management.

### *5.2. Stakeholder*

This section discusses all potential partners at TDMP, which are interested in digital trading of TD. Most of them have a role either as customer (consumer) or as provider of TD. These roles are distinguished in authorities, goals, interests and benefits from participating at TDMP. Each stakeholder will be defined and characterized in several categories.

MG is responsible for managing the digital trade of TD, as mentioned before. That means MG receives TD from a provider and then tests their structural integrity, quality and value. That means MG receives TD from a provider and then tests their structural integrity, quality and value. MG tests the integrity of the relevant description of these TD as well. Additionally, the integrity of the relevant description of these TD is tested. MG encrypts TD according to the specified conditions from TDP. Then the encrypted TD is saved on the server with their associated key. On the other hand MG is responsible for selling and sending processes. Additionally, MG ensures the privacy of personal and bank account data of TDP and customers, too.

End product manufacturers can take the role as main customers and as main providers at TDMP. They fulfill customer orders on their machines using relevant TD. Depending on the job, for them it is more effective to buy these TD instead of investing time and resources by developing them on their own. The machine operators have exactly the same role at the market place. One difference between these two partners is that the machine operator works with the machine directly - TD is typed in at the machine and good functionality is ensured. That means the machine operator is an employee by end product manufacturer, which owns the machine. Both of these parties can be as mentioned before, a customer by TDMP. This depends on the enterprise policy.

The machine manufacturers produce and sell machines. Usually they have enough experience and resources to develop high quality TD. Thus they will be one of the more important providers at TDMP. At the same time, they can use TDMP as an information resource to recognize the market trend. This helps to identify future business models.

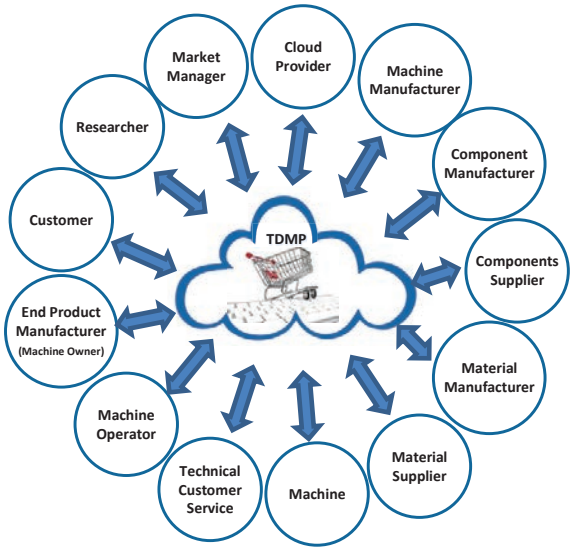


Fig. 4. Stakeholder at TDMP

Component manufacturers and suppliers can use the same strategy, so they are interested in participating at TDMP. Material manufacturers and suppliers have also the same goal. New business models will be created. For example they purchase TD from TDMP, suitable to their material and provide both of them together to their customers.

Academic or industrial research institutes are interested in exchanging innovative TD. So TDMP enables experience exchange and improves research work. The cloud provider operates the necessary infrastructure for this market place. In the digital age the machine is considered as an active member at TDMP. Industrie 4.0 defines machines as smart objects. Smart machines are able to request needed TD from the TDMP and can provide TD in return. Anyone that does not belong to any mentioned category above can be a customer at TDMP.

### *5.3. Security concepts*

For all data exchange processes regarding the trading asset TD, the application of suitable data protection means is required. Protection means applied in the concept can be distinguished by their protection goals. In particular, the concept pursues three main protection goals:

1. *Data confidentiality*, i.e. the transmitted and used TD cannot be read or copied by unauthorized users (machines or people) at any time.

2. *Data integrity*, i.e. data being transmitted must be protected against manipulation by third parties. This is achieved by verifying that the received TD set is genuine and unaltered.
3. *Authentication*, i.e. a specified resource can only be accessed and worked with by authorized users.

While the first protection goal puts its primary focus on knowledge protection for the traded data, the second goal assures that the data cannot be changed in order to manipulate or damage the operator's machine that executes the manufacturing process with the altered TD set.

As described in section 4, the system infrastructure can be described by connected systems, which are exchanging information between each other via the Internet. To achieve confidentiality, cryptographic systems (e.g. AES, Advanced Encryption Standard) are used. After purchase of a TD set, the specified data is encrypted with a random symmetric content key by the TDMP system and delivered to the using enterprise or machine. With this, man in the middle attacks, protocol analysis or wiretapping during data exchange is prevented since the transferred data cannot be decrypted without the content key issued by the TDMP. However, an attacker could change and corrupt the encrypted data to make it useless. To avoid this, the second protection goal is fulfilled by the usage of a qualified digital signature of the data. For that, the data set is hashed with a cryptographic hash function (e.g. SHA, Secure Hash Algorithm) and the hash value is encrypted with the secret key of the issuing TDMP by using an asymmetric cryptosystem (e.g. RSA, Rivest-Shamir-Adleman cryptosystem). With this, the digital signature of the issuing TDMP for the data is finished and can be later verified for integrity when received by using the public key of the TDMP.

Finally, authentication and usage control is provided by means of secure identification of user and machine to the TDMP so it only provides the executing entity with the cryptographic key if it is authorized to use the data. By using hardware measures to store cryptographic key material, e.g. in Trusted Platform Modules (TPM) or Smartcards, a secure root of trust (hardware trust anchor) is provided to securely identify the requesting unit and prove integrity of the system software for the machine, e.g. with secure boot technique. Timestamps and machine identification can be used to control access not only per count of requests but also have a limited time of permitted usage applied to the data.

Combined, these means can be implemented to the system environment by using a comprehensive rights management as used for enterprise data exchange (ERM, Enterprise Rights Management) with granular permission policies as well as connecting it to the hardware security means and cryptographic providers of the TDMP cloud service.

## 6. Future work

As future work, the system elements with its boundaries, data in- and outputs as well as interactions are defined. On that basis, a generic model for manufacturing industrial data exchange regarding security and privacy issues will be developed. Moreover, a prototypical implementation of the marketplace architecture and its technical infrastructure connected to a laser manufacturing system will be made.

## 7. Conclusion

This paper demonstrates a new concept for technology data marketplace, which is targeted to support the requirements of cloud enabled industry solutions in future enterprises. Firstly, the general features of cloud computing technology and e-commerce are discussed. The key security technologies for realizing this form of electronic trading are presented. Initial approaches for a technology data marketplace is introduced and detailed in a use case diagram. Furthermore, the potential stakeholders participating in this system are defined. This paper illustrates how these innovative technologies and systems significantly enhance the capability of digital technology data trading in the context of industry and enterprise environments. It is expected that this cloud enabled industry solution strongly increases enterprise revenues based on already existing digital resources, namely technology data for manufacturing processes. Protection of the digital asset over the lifecycle is a key factor; therefore initial concepts on how to fulfill protection requirements in context of digital technology data trading were presented.

## 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] BMWi. Industrie 4.0 und Digitale Wirtschaft. Berlin, 2015
[2]. Anderl R. Industrie 4.0 – Technological Approaches, Use Cases, and Implementation. at - Automatisierungstechnik 2015;63:10. doi:10.1515
[3]. PwC AG. Industrie 4.0 - Chancen und Herausforderungen der vierten industriellen Revolution. October 2014.
[4] Sheshadri Chatterjee. Security and Privacy Issues in E-Commerce: A Proposed Guidelines to Mitigate the Risk: 12 - 13 June 2015, B.M.S. College of Engineering, Bangalore, India. Piscataway, NJ: IEEE; 2015.
[5] Shekanayaki K, Chakure A, Jain A. A Survey of Journey of Cloud and Its Future. 2015. p. 60–64.
[6] Mishra D. Cloud Computing: The Era of Virtual World Opportunities and Risks involved. International Journal of Computer Science Engineering (IJCSE), Jaipur, India, 2012.
[7] Neeraj kumar A. E-Commerce: An Evolution. International Journal of Enhanced Research in Management & Computer Applications. International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471 Vol. 3 Issue 4, April-2014, p: 1-3, April 2014
[8] M. Grimm, R. Anderl, and Y. Wang, editor. Conceptual Approach for Multi-Disciplinary Cyber Physical Systems Design and Engineering. in Proceedings of the 10th International Symposium on Tools and Methods of Competitive Engineering (TMCE), Budapest, Hungary, 2014, p. 61-72.
[9] Dominik A, Wojciechowski J. Analysis of the Structure of Online Marketplace Graph. In: Kłopotek MA, Wierzchoń ST, Trojanowski K, editors. Intelligent Information Processing and Web Mining. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 243–25.