Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 00 (2016) 000–000

www.elsevier.com/locate/procedia

Product-Service Systems across Life Cycle

The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance

Jaime Campos[a], Pankaj Sharma[b], Erkki Jantunen[c], David Baglee[d], Luca Fumagalli[e]

[a] *Department of Informatics, Linnaeus University, SE-35195 Växjö, Sweden*

[b] *Mechanical Engineering Department, IIT Delhi, New Delhi, India*

[c] *VTT Technical Research Centre of Finland, P.O.Box 1000, FI-02044 VTT, Finland*

[d] *Department of Computing, Engineering and Technology, University of Sunderland, UK*

[e] *Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Italy*

*Corresponding author . Jaime Campos. Tel.: +46-(0) 470-708829 *E-mail address:*jaime.campos@lnu.se

Abstract

The main objective of the paper is to highlight the important aspects of the data management in condition monitoring and maintenance, especially when the emergent technologies, such as the cloud computing and big data, are to be considered in the maintenance department. In addition, one of the main data management elements highlighted in the current work are the cybersecurity issues which might be one of the biggest obstacles hindering the development of cloud based big data for condition-based maintenance (CBM) purposes. Further, the benefits and current risks of storing a company's data in the cloud are highlighted. The authors discuss as well different data needs in various processes in the area of asset management. In addition, the challenges and issues to be addressed for the optimal use of the company data at the cloud together with the big data approach are addressed. This is seen as an important part in an effort to achieve sustainable information and communication technologies for the industry.

Peer-review under responsibility of the scientific committee of the 8th Product-Service Systems across Life Cycle.

Keywords: Big data; cloud computing; maintenance engineering; asset management

1. Introduction

Internet came in civilian use at the beginning of the 1990's and its use has increased manifolds after that. Its popularity has led to various new technology developments such as the e-maintenance, the Internet of Things (IoT), Industry 4.0, etc., which are all based on the broad implementation of ICTs, especially web technologies having the objective to support different processes of a company. The new Industry 4.0 initiative aims to connect these new ICTs to create smarter factories resulting in a revitalized manufacturing sector, promising to be the next industrial revolution for manufacturing [1]. Consequently, for its successful use it is important to understand the characteristics of the new emergent technologies to be able to use them properly in a company. In the cloud computing the entire network - based computing over Internet is seen as a service. It has evolved from the comprehensive dissemination of data and information virtualization from client server and service oriented architectures, automatic to utility computing [2]. The security aspects are rather important when the cloud computing is used since the security strategies that have been developed since the 1980's are not applicable to the cloud computing. The prime reason for this increased importance of

Peer-review under responsibility of the scientific committee of the 8th Product-Service Systems across Life Cycle.

security is that the servers' part of the Cloud is not in the same domain, i.e. the data owner and Cloud computing servers are normally in two different domains. Consequently, numerous efforts have been made considering this matter and evolving system models and security strategies are being debated and tried, explicit for the system with the features of cloud computing. These efforts omit, for example, cryptographic methods and data decryption keys [3, 4]. Many private users as well as organizations hesitate over the adaptation of cloud computing and its services because of the risks related to the security and privacy of these services [5]. Kumar et al. [6] believes that security and privacy are the two major factors that hinder the growth of real time business related cloud computing for business purposes. It is, therefore, important for the academia and industry to develop new ways, services and technologies to provide a secure way for their storage and communication when using the cloud computing services. In addition, with the ICTs developments a new concept and approach named big data has emerged in academia and industry and most definitions highlight its increasing technological ability to capture, aggregate, and process an ever larger volume, velocity and variety of data, i.e. the 3 Vs. The main objective of data mining is to turn a large collection of data into knowledge and find hidden patterns [7]. In connection with the above mentioned the management of the stored data for later use in different processes and for different purposes is crucial to handle in a proper manner to avoid the security aspects mentioned above. It becomes, therefore, important to understand the obstacles that might impede the successful development and use of the cloud based big data for purposes of condition based maintenance (CBM) in asset management. In section 2, the current paper discusses different aspects of the big data, followed by the cloud computing and its architecture in section 3. Section 4 emphasizes the cloud computing security issues. Section 5 highlights important aspects to consider with respect to big data and the cloud computing approach in maintenance, especially when CBM is applied and finally the conclusions are presented.

2. Big data

Big data is essentially a similar analytical technique, but it differs from these earlier attempts like KDD (Knowledge Discovery in Databases), Data Mining and other numerous analytical techniques in terms of the Volume, Velocity, Variety, Veracity and other characteristics of the data. *The volume* of the data collection from the machines has increased. There are greater numbers of sensors placed on equipment that is being monitored. An increased ease of data collection and transfer by the operator with the help of hand held computers has also resulted in higher volume of data being created. Higher volume of data also means that there is a higher risk of data theft. Larger volume of data stored centrally has an amplified technical impact (entirety of data in jeopardy rather than a subset of data) and other privacy related issues [8]. *The velocity* refers to not only the speed of data being received, but also the speed at which data is being processed and analyzed. Data is being created, stored, processed and analyzed in real or near real time. What complicates the issue even further is that this data can arrive and require processing at different speeds. Data arrival at peak hours poses an opportunity to the malicious seeker to steal it. It is during such periods that organizations may lack internal capacity and tools to manage and protect information. A related point is that the attractiveness as a crime target is high during such periods [9]. While for some applications, the arrival and processing of data can be performed in batch, other analytics applications require continuous and real-time analyses, sometimes requiring immediate action upon processing of incoming data streams [10]. Less critical machines can resort to batch processing of data, whereas more critical ones like those deployed in nuclear and military applications may have to undergo real time processing of data for possible diagnosis/prognosis. This characteristic the data is referred to as variability in some literature [9]. *The variety* has to do with the large amount of historical data available regarding condition monitoring of machines. In addition, a variety of sensors capture different types of data from the machines. Some of this data is more structured; other that is picked up from the users is more unstructured. Most organizations lack capability to manage unstructured data, which arguably contains more sensitive information [9]. A large variety of information would make it more difficult to detect security breaches, react appropriately and respond to attacks (freepatentsonline.com, 2013). Data from various sources has different formats thereby making it difficult for the analysts to integrate this data. There is a need to have standard formats like Machinery Information Management Open System Alliance (MIMOSA) databases. *The veracity* is described as the trustworthiness of data. There may be instances of incorrect feeding of data by the operator or wrong inferring from the user's response. The problem assumes greater significance because of the sheer volume of data and hence difficulty in finding out the mistakes in the analysis. In addition, other characteristics can be defined in terms of exhaustive (capture entire population), fine grained resolution; uniquely indexical in identification; relational and flexible with extensionality and scalability [11].

3. The cloud computing and its architecture

The associated problem in dealing with this deluge of data was that it required higher computing resources and processing power to analyze this data to arrive at decisions. This invited higher spending in acquiring this computing power for the enterprises, which makes it economically unviable. This led to the development of cloud computing where the resources like networks, applications and servers can be hired for use. Organizations now have higher computing power available to them without having to establish and maintain such cost prohibitive infrastructure in their own premises. Industries are moving towards the Cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied [12]. The National Institute of Standards and Technology (NIST) channels its efforts into the standardization of the cloud computing, its definition, cloud

computing reference architecture, which are generally accepted in the community (www.nist.gov). The NIST proposes cloud computing reference architecture, which is a general high-level conceptual model. The focus of the architecture is on the services it provides. The NIST cloud computing reference architecture is a tool that provides an understanding of different cloud services with the support of the cloud computing conceptual model. According to the architecture, there are five main actors, i.e. cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier. The cloud consumer is an important actor, since the cloud computing services are created ultimately to support him, i.e. the individual actor or organization. The activities and usage scenarios might differ among cloud consumers depending on the services demanded (www.nist.gov). The clouds can be categorized as Infrastructure as a Service (Iaas), Platform as a Service (PaaS) and Software as a Service (SaaS). The important aspects of cloud computing, in connection with the resource management of IaaS, such as scalability, customization and reusability as well as the performance metrics, namely delay, bandwidth reliability and security, are discussed in comprehensive survey paper of Manvi and Shyam [13]. In cloud computing everything is seen as a service, i.e. Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) [14]. Some authors such as Armbrust et al. [15] refer to cloud computing as both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), for instance, Software as a Service (SaaS), enables the access to some software applications through the internet, and at the same time one can avoid the “binding” to software and hardware management [16].

4. Cloud computing security

The cloud security services can be ranged from authentication, authorization, auditing, accountability, etc. Such authors as Krutz and Vines [17] provide a comprehensive and detailed overview of different aspects of cloud security, which consist of the above mentioned among others. The cloud computing has the same security issues as traditional ICT architectures, as mentioned earlier, however, with the cloud other aspects arise such as confidentiality, integrity and availability [17]. The confidentiality has to do with the prevention of deliberated or unintended unapproved admission of data or information contents. The loss of confidentiality of a company or private data might occur by mismanagement or abuse of network rights. Confidentiality can normally be achieved through network security protocols, network authentication services and data encryption services, which is the focus of the current paper. The integrity involves the assurance that the e-mail/s or any other communicated messages sent are received as well as the information on a web site that is the same intended to be published. In addition, it involves the assurance that the communicated messages are not changed deliberately or otherwise. Integrity losses might occur, for instance, by a deliberate attack to change data or information on a web site. Moreover, it can be unintentionally changed by a person working with the company data. The technologies normally used to avoid integrity failure are firewall services, communication security management and intrusion detection services. Finally, availability involves the reliability and stability in the provided networks and their systems. It guarantees that the network and its systems are accessible when they are required and by so allows approved users to have admission to these (network and systems). Furthermore, it provides the guarantee that the security for the network and systems are working as expected. Normally within the availability concept there are also aspects such as guarantee and quality of service, the performance and resource requirements as well as up time of the server and its systems. Availability of the network and its systems is generally ensured by, for instance, backups, satisfactory/working login procedure into the system, reliable security and network security methods. As mentioned earlier, organizations hesitate over the adaptation of cloud computing and its services, because of the risks related to the security and privacy of these services [5]. The cloud security Alliance group (CSA) highlight the data security aspects for cloud computing, which got increased notice during the 2008 within the information security community. The cloud security aspects, especially for the cloud computing, are gone through by the Cloud Security Alliance group (CSA), (cloudsecurityalliance.org). The CSA is led by industry practitioners, corporations, and associations and additional important stakeholders. In addition, the CSA is a not-for-profit organization aiming to promote the utilization of best practices within the cloud computing as well as offer education on the implementation and use of cloud computing. The National Institute of Standards and Technology (NIST) is also contributing to the domain of cloud security with the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information (www.nist.gov). The emphasis area of the NIST when it comes to the cloud computing security ranges from technology such as portability, interoperability and security requirement, standards and guidance. In conclusion, cryptography is the most common technique to protect data within the cloud [18]. However, there is still work to be done in this area, since different cryptography approaches are not optimal as the need varies among different users. For instance, the secured data at the moment cannot be processed if needed, since it needs to be transferred to its owner to be able to process it because it needs to be decrypted to be able to make, for instance, any business logic or analytics. Anyway, what is important is to give different users the possibility to choose the security they want to provide for data, i.e. user-oriented control over data stored and managed through the services that the cloud offers [19].

5. Asset management when prospective ICTs are used in maintenance

The management of big data has to do with the practice of merging huge volume of data from different sources and analyzing it with the use of advanced algorithms for decision

support, i.e. one of the main objectives is to take complete benefit of the stored data, especially with the support of analytics software. The data for purposes of CBM can be understood through different layers of the communication and presentation ISO 13374-1 standard. The ISO 13374-1 consists of 6 layers. The first is the data acquisition layer, the second is the data manipulation layer, the third is state detection, the fourth is the health assessment, the fifth is the prognostic assessment and the last one is the advisory generation. However, for more comprehensive decision making, i.e. reaching the level of efficient Condition Based Maintenance (CBM), it is important that other aspects are considered together with the ISO 13374-1 standard such as costs, maintenance tasks, maintenance history, operations & work, etc. It is in the layers 3-5 of the ISO 13374-1 standard where different statistical and data mining technologies can be employed for different purposes. As mentioned above, for more comprehensive decision making, there is a need to use other data together with data included in the ISO 13374-1 standard. The reason is because one of the main objectives of big data is to find hidden patterns that data can disclose resulting in optimization of different processes, which can only be understood through analytics. Within the field of maintenance of assets, big data has become a new specialization for monitoring, maintaining, and optimizing assets for better quality and performance. Kurtz et al. [20] state that big data helps to solve complex technical and operational issues in maintenance including a lack of visibility into asset health, unexpected costs for unscheduled maintenance, unexpected failure and a lack of analytical insights and tools for maintenance optimization. Therefore, potential benefits of big data technologies in the field of maintenance will require predictive algorithms using heterogeneous data sources, scalable data structures, real-time communications and visualizations techniques. These technologies and methodologies applied to such a challenging industry relevant sector will provide the expected system component degradation prediction modelling, maintenance cost prediction modelling, and asset condition monitoring. This should lead to boosting the efficiency and maintenance cost reduction. Big data is a multi-stage process, including data acquisition, information extraction, data modelling and analysis and, decision making. Big data can also be used to influence the next generation of products by identifying the issues that cause unnecessary and unplanned downtime. An analysis of the data could provide an insight into known and unknown issues and by feeding the results back into the design process the aim is to improve the manufacturing process and product quality based upon accurate data. When it comes to the cloud computing, the originator of the data does not have it stored within the physical boundary of its enterprise. Worse still, the originator does not even know where his data is stored. The issue attains more significance when we start dealing with sensitive military equipment or nuclear equipment data. Leakage of the information related to health of this equipment to a malicious hacker can have catastrophic results. Therefore, the security of data is a crucial factor when the cloud is used. However, there are some pitfalls with the cloud if data has to be analyzed in the cloud and still remain secure. It means that in case that data needs to be analyzed in encrypted form, it loses in speed since it is not possible to read the results of encrypted data due to the fact that it needs first to be decrypted. Homomorphic Encryption is a special kind of encryption that allows operating on cipher texts without decrypting them; in fact, without even knowing the decryption key [21]. This methodology can avoid losing speed when operating on the data that has been encrypted. In addition, it provides secure data in the Cloud, since no one is able to understand the encrypted data. Nevertheless, there is no fully homomorphic encryption developed and implemented yet. However, there are some efforts done in that direction, for instance, a PhD thesis of Stanford University, which proposes a fully homomorphic encryption scheme that could solve the former mentioned problem [22]. Furthermore, the data being gathered from the machines that are being monitored is becoming huge in amount and is required to be dealt with through faster processors that are located in the Cloud. This eventually will result in better analysis; hence improved diagnosis and prognosis. But before doing that, there is a need to holistically assess the strengths and weaknesses of these newer concepts of big data and cloud computing. The inherent concern of not having data stored within the premises of the owner needs to be addressed with better techniques of securing data at-rest and in-transit. Other serious issues of data lineage and data provenance must also be adequately taken care of. There are a number of problems that data in the cloud has to encounter. Malicious data seekers are always finding newer methods to steal data whereas the clouds service providers are working to neutralize this threat through techniques like encryption, fragmentation, etc. Companies that do not have confidential data to worry about could use the benefits of the Cloud for better asset management. However, others that require protection of their data will have to make an informed decision to use the Cloud by doing a risk-benefit analysis of putting the confidential machine data in the Cloud. More research has to be focused on this facet of asset management using the cloud computing services. The research must also be carried out to identify security risks specific to e-maintenance domain. In addition to addressing the problems related to security of the data on the cloud, the research must be focused on the developing interoperability of the asset management systems that are being used by various service providers. This will ensure that the data from a number of assets can be used collectively by the asset management system to arrive at a more accurate diagnosis and/or prognosis. Therefore, interoperability will increase the chances of data being used additively. Muller et al. [23] aptly describe e-maintenance as “maintenance mutation” which has evolved from “Normal Maintenance” and takes into account innovative maintenance orientations related to lifecycle approach (i.e. maintenance-oriented lifecycle management), new services (i.e. prognosis), new capacities (i.e. pro-activity, velocity), new organizations (i.e. intelligent system), and new technologies (i.e. wireless communications). It is described as ‘‘scientifically and technologically’’ another thing that is a mosaic, a patchwork of models, technologies and, standards. Big data and cloud computing add yet another patch to this complex mosaic. Researchers and practitioners of e-

maintenance need to evolve the discipline of e-maintenance to keep it relevant to the current and future requirements of the end-user. In addition, according to some researchers the future will be in the hands of companies that offer cloud computing and provide different services within the area of big data, i.e. big data analytics [10]. It is, therefore, crucial that researchers and industry make an effort to understand how big data in conjunction with the cloud computing can work as an innovator in the domain of interest resulting in increased organizational performance for the companies adopting the concept. The elements a cloud based big data system should contain for the domain of interest are, for instance, a data collection module comprising of sensors and maintenance agents in the field where heterogeneous data in large volume, velocity and variety gets collected as big data. The analysis of this big data is done using the resources in the cloud. Users interact with this chain of information flow through queries and answers. However, the entire chain is geographically spread over large distance and spans over the physical as well as the virtual world, making it extremely vulnerable to the malicious hackers. Therefore, the data on the different modules should be protected through various security measures applicable to each of the phases of the chain to counter possible security issues. The sensors and agents have to be guarded physically against possible thefts. In addition, once the data is collected and is passed to the data storage, it has to be guarded. This data in-transit needs to be sent and received via Secure Socket Layer (SSL) over TCP/IP where the data packets are encrypted with a secret key or through Virtual Private Network [24]. During this time, data integrity must be maintained in the cloud to ensure that the transactions use the data that is correct (genuine data), complete (whole data) and fresh (most recent data) [25]. Further, once the data reaches its storage site, both physical and virtual security is necessary. The virtual security is ensured through various forms of encryption and fragmentation [25, 26, 27, 28]. The communication of the data with the cloud resources and the users has to be secured from the malicious seekers. This can be done by using virtual firewalls [29], DNS Security protocols [30] and homomorphic encryption [21]. End to end encryption and self-encryption should also sometimes be used. The queries are to be guarded against breach of access and pattern confidentiality by using various means. Active counter measures like honeypots should also be used to avoid data theft [31].

Conclusions

The cloud computing provides several advantages for any company that implements it due to a vast variety of services that it offers. However, the security constraints are still an issue, since data needs to be secured during all its life cycle. For instance, currently data cannot be encrypted in the cloud during all its phases because in certain occasions it needs to be decrypted as is the case when some kind of analytics needs to be performed on the data. There are some efforts made to solve this kind of issues but none of these are fully functional yet. However, when the fully homomorphic encryption becomes a reality then even analytics can be performed on the cloud with encrypted data. Further, a number of competitive pressures have forced organizations to examine systems, strategies, tools and techniques to increase asset efficiency and effectiveness. Managements are now aware that for decades manufacturing and maintenance data have been collected yet rarely utilised due to the large amounts of data and the uncertainty of what to analyse and how to decipher data to make sure it is supporting new approaches to manufacturing and maintenance. This paper has provided the main factors to understand this complex context both for academic researchers and for industrial maintenance practitioners that often don’t have the perfect understanding of ICTs issues and still focus more on daily activity. Nevertheless the proper future development of e-maintenance within the industry 4.0 environment cannot be a simple evolution of present available solution, but it needs experts to focus on the identification of the right path to follow in order to exploit the right capability of available ICTs, like the one discussed, i.e. cloud based big data for CBM purposes. Without posing the right basis now, the industry risks to not being able to exploit future technological solutions because they might be not compliant with requirements pertaining to dimension different from pure performances (i.e. security). Naturally, much of the research today is focused on making the adaption of new technologies easy and finding solutions that can guarantee the necessary security, availability and reliability level of these systems among two actors: asset manager and CBM solution providers. Nevertheless, the future of asset management ecosystems for what concerns CBM should consider different tasks in connection to the MIMOSA which could be carried out by different actors remotely, by providing their services in the Cloud, exploiting the possibility to create a competitive environment (i.e. ecosystem) where the best services are provided to analyse the data at the best capability. Researchers should thus particularly pay attention to this research stream not only from the technological point of view, but considering the security aspects that will surely be stressed by the evolution of the ecosystems, considering on the approaches that will boost the development of CBM solutions. In conclusion, the use of big data and cloud computing has been thoroughly discussed in the paper. In addition, the elements that should be included into a cloud based big data system has been highlighted. Nevertheless, these technologies provide huge economical potential but in the case of cloud computing at the same time it has a high technological risk, indeed. There is no prior experience of building of such large and integrated systems which could be very vulnerable. However, it is clear that in the long run the competition in the markets will force companies to adapt the new technology due to the great influence it has.

References

[1] Lee,J., Bagheri, B., Kao, H.A., Lapira, E. Industry 4.0 and Manufacturing Transformation, Manufacturing Leadership Journal, 2000; 02; 1-8.

[2] Geelan, J. Twenty-One Experts Define Cloud Computing, Cloud Expo: Article, cloud computing journal, published. 2009.

[3] Tysowski, P. and Hasan, M.A. Towards secure communication for highly scalable mobile applications in cloud computing systems, Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR. 2011; 33; 1-33.

[4] Yu, S., Wang, C., Ren, K and Lou, W. Achieving secure, scalable and fine-grained data access control in cloud computing," in IEEE INFOCOM'10. 2010.

[5] Khan AN, Mat Kiah ML, Khan SU, Madani SA. Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 2013; 29; 5; 1278–1299.

[6] Kumar, N.S., Lakshmi, G.V.R., Balamurugan, B. Enhanced Attribute Based Encryption for Cloud Computing. Procedia Computer Science, 2015; 46; 689– 696. doi:10.1016/j.procs.2015.02.127

[7] Han, J., Kamber, M and Pei, J. Data Mining: Concepts and Techniques, Third Edition, The Morgan Kaufmann Series in Data Management Systems. 2011.

[8] ISACA. Generating value from big data analytics,White Paper. 2014. Retrieved from (http://www.isaca.org).

[9] Kshetri, N. Big data's impact on privacy, security and consumer welfare, Telecommunications Policy.
2014; 38; 1134–1145.

[10] Assuncao MD, Calheiros RN, Bianchi S, Netto MAS, Buyya R. Big Data computing and Clouds: trends and future directions. Special Issue on Scalable Systems for Big Data Management and Analytics. Journal of Parallel and Distributed Computing. 2015; 79–80:3–15

[11] Kitchin, R. Big Data and Human Geography: Opportunities, Challenges and Risks, Dialogues in Human Geography. 2013; 3; 3; 262-267.

[12] Padhy, R.P., Patra, M.R. and Satapathy, S.C. Cloud Computing: Security Issues and Research Challenges, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS): 2009; 1; 2; 136-146.

[13] Manvi SS, Shyam GK. Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. Journal of Network and Computer Applications. 2014;41:424–440. doi: 10.1016/j.jnca.2013.10.004.

[14] Xu, X. From cloud computing to cloud manufacturing, Robotics and Computer-Integrated Manufacturing. 2012; 28; 75–86.

[15] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. and Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report. No. UCB/EECS-2009- 28, EECS

[16] Sultan, N. Cloud computing for education: A new dawn?, International Journal of Information Management. 2011; 30; 109–116.

[17] Krutz RL, Vines RD. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 1 edition. Wiley, Indianapolis, IN. 2010.

[18] Kant, C and Sharma, Y. Enhanced Security Architecture for Cloud Data Security, International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3; 5; 570 – 575.

[19] Michael, J.B. Empowering Users through Secure On-Demand Data Provisioning, Computer. 2013; 46; 6; 84–85.

[20] Kurtz, J., Hoy, P., McHargue, L and Ward, J. Improving Operational and Financial Results through Predictive Maintenance, Smarter Analytics Leadership Summit, New York, USA. 2013.

[21] Micciancio, D. A First Glimpse of Cryptography's Holy Grail, Communications of the ACM. 2010; 53; 3; 96.

[22] Gentry. C. A fully homomorphic encryption scheme, PhD thesis, Stanford University. 2009.

[23] Muller, A., Marquez, A.C. and Iung, B. On the concept of e-maintenance: Review and current research, Reliability Engineering and System Safety. 2008; 93; 1165–1187.

[24] Hsieh, J.C., Li,A.H. and Yang, C.C., (2013), Mobile, Cloud, and Big Data Computing: Contributions, Challenges, and New Directions in Telecardiology, International Journal of Environmental Research and Public Health, 2013; 10; 6131-6153.

[25] Di Vimercati, S.D.C., Foresti, S. and Samarati, P. Managing and Accessing Data in the Cloud: Privacy Risks and Approaches, In Proceedings of the 7th International Conference on Risks and Security of Internet and Systems Cork, Ireland. 2012.

[26] Samarati, P. Data Security and Privacy in the Cloud, Proceedings of the 10th International Conference on Information Security Practice and Experience, 2014; 8434; 28-41.

[27] Müller, T., Latzo, T. and Freiling, F.C.Self- Encrypting Disks pose Self-Decrypting Risks: How to break Hardware-based Full Disk Encryption, Technical report for the German talk "(Un)Sicherheit Hardware-basierter Festplattenverschlüsselung" given at the 29th Chaos Communication Congress. 2012.

[28] Bhadauria, R. and Sanyal, S. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques, International Journal of Computer Applications. 2012; 47; 18; 47-66.

[29] Jansen, W. and Grance, T. Guidelines on Security and Privacy in Public Cloud Computing, Report by National Institute of Standards and Technology, US Department of Commerce. 2011.

[30] Ateniese, G. and Mangard, S., (2001), A new approach to DNS security (DNSSEC), In Proceedings of the 8th ACM Conference on Computer and Communications Security, 2001; 86-95.

[31] Zhang, F., Zhou, S., Qin Z. And Liu, J., (2003), Honeypot : A supplemented active defense system for network security, In proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 231-235.