



INTERNATIONAL CONFERENCE INFORMATION AND COMMUNICATION TECHNOLOGIES IN BUSINESS AND EDUCATION



CONFERENCE PROCEEDINGS



Publishing house "Science and economics"
University of Economics - Varna

International Conference
INFORMATION AND COMMUNICATION
TECHNOLOGIES IN
BUSINESS AND EDUCATION

Conference proceedings

**INFORMATION AND COMMUNICATION
TECHNOLOGIES IN
BUSINESS AND EDUCATION**

**Proceedings of the International Conference
dedicated to the
50th anniversary
of the Department of Informatics**

2019

University publishing house “Science and economics”
University of Economics – Varna

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Permission for use must always be obtained from University publishing house “Science and economics”. Please contact izdatel@ue-varna.bg

Published reports have not been edited or adjusted. The authors are solely responsible for the content, originality and errors of their own fault.

With the support of ADASTRA, 411 Marketing Business Services.

© University publishing house “Science and economics”,
University of Economics – Varna, 2019.

ISBN 978-954-21-1004-0

PROGRAMME COMMITTEE

Abdel-Badeeh M. Salem, Egypt

Aijaz A. Shaikh, Finland

Aleksandar Dimov, Bulgaria

Alexander Feldman, USA

Alexander Sergeev, Russia

Antoanela Naaji, Romania

Avram Eskenazi, Bulgaria

Dariusz Mrozek, Poland

Dimitrina Polimirova, Bulgaria

Dmitriy Berg, Russia

Elena Nechita, Romania

Emil Denchev, Bulgaria

Georgi Dimitrov, Bulgaria

Ivan Popchev, Bulgaria

Jeanne Schreurs, Belgium

Julian Vasilev, Bulgaria

Kameliya Stefanova, Bulgaria

Krasimir Shishmanov, Bulgaria

Maciej Czaplewski, Poland

Maciej Pondel, Poland

Maksim Medvedev, Russia

Maria Hristova, Bulgaria

Marian Cristescu, Romania

Marina Medvedeva, Russia

Michael Voskoglou, Greece

Nadezhda Filipova, Bulgaria

Nikola Nikolov, Ireland

Niv Ahituv, Israel

Pavel Petrov, Bulgaria

Rami Malkawi, Jordan

Sara Paiva, Portugal

Silvia Parusheva, Bulgaria

Snezhana Sulova, Bulgaria

Todorka Atanasova, Bulgaria

Valentin Kisimov, Bulgaria
Valery Trofimov, Russia
Veselin Popov, Bulgaria
Violeta Kraeva, Bulgaria
Vladimir Sulov, Bulgaria
Vladimir Zanev, USA
Zdzislaw Polkowski, Poland

ORGANIZING COMMITTEE

Chairman: Prof. Vladimir Sulov, PhD

Members:

Prof. Avram Eskenazi, PhD
Prof. Julian Vasilev, PhD
Assoc. Prof. Todorka Atanasova, PhD
Assoc. Prof. Silvia Parusheva, PhD
Assoc. Prof. Snezhana Sulova, PhD
Assoc. Prof. Pavel Petrov, PhD

Secretary: Tijen Talib

FOREWORD

These proceedings contain the papers of the International Conference “Information and Communication Technologies in Business and Education” which took place at the University of Economics – Varna, Bulgaria, 18 October 2019.

The international scientific conference is dedicated to the **50th anniversary of the Department of Informatics at the University of Economics – Varna**. The conference is also dedicated to the 100th anniversary of the University. The included papers describe recent scientific and practical developments in the field of information and communication technologies, information systems, and their applications in business and education.

The papers in the Proceedings are peer reviewed and are checked for plagiarism.

C O N T E N T S

1. Kamelia Stefanova, Dorina Kabakchieva Challenges and Perspectives of Digital Transformation	13
2. Julian Vasilev, Marian Cristescu Approaches for information sharing from manufacturing logistics with downstream supply chain partners	24
3. Abdel-Badeeh M. Salem Computational Intelligence in Smart Education and Learning	30
4. Marian Niedźwiedziński Proposal of the Multi-aspect Analysis of ICT's Needs in Management	41
5. Krasimir Shishmanov Digital Transformation in Bulgaria	52
6. Tatyana Makarchuk, Valery Trofimov, Svetlana Demchenko Modeling the life cycle of e-learning course using Moodle Cloud LMS	62
7. Vanya Lazarova Exploring the functionality of Bulgaria eGovernment site	72
8. Veselin Popov, Petya Emilova Big data and information security	83
9. Luben Boyanov Approaches for enhancing digitalization and digital transformation in supply chain management	91

10. Monika Tsaneva	
Challenges of GDPR compliance in consumer financing companies	103
11. Todorka Atanasova	
Main factors influencing digitization in construction companies	116
12. Silvia Parusheva	
Digitalization and digital transformation in construction – benefits and challenges	126
13. Snezhana Sulova	
The Usage of Data Lake for Business Intelligence Data Analysis	135
14. Pavel Petrov	
Web security technologies used in banks of Estonia, Latvia and Lithuania	145
15. Tanka Milkova	
ABC analysis of inventory in MS Excel	155
16. Ivan Kuyumdzhev, Radka Nacheva	
Choosing Storage Devices with Consideration of Backup and Restore Performance in MS SQL SERVER	166
17. Yanka Aleksandrova	
Predicting Students Performance in Moodle Platforms Using Machine Learning Algorithms	177
18. Latinka Todoranova, Bonimir Penchev	
M-learning Applications	188
19. Boris Bankov	
The Impact of Social Media on Video Game Communities and the Gaming Industry	198

20. Velina Koleva, Svetoslav Ivanov	
Social media and the recruitment of IT professionals in Bulgarian IT companies	209
21. Deyan Mihaylov	
Modeling and Simulation of Some Functions of Two Independent Random Variables	225
22. Oumar Sy	
Using Association Rules as Semantics for Domain Ontologies	233
23. Ina Stanoeva	
Social media possibilities for improving arts marketing performance	247
24. Iskren Tairov, Vladislav Vasilev	
Perspectives on mobile devices adoption in healthcare sector	257
25. Angelin Lalev	
Deep Neural Networks for Detection of Credit Card Fraud	263
26. Miglena Stoyanova	
Priorities for Digital Transformation in Property Management	275
27. Mihail Radev	
Organizational Variants of IT Department at the University	284
28. Mariya Armyanova	
IoT problems and design patterns which are appropriate to solve them	291
29. Yavor Christov	
Corporate Big Data and Hybrid Integration Platforms	306

30. Ivan Belev	
Making financial data readable using Inline XBRL	314
31. Ivan Belev	
eXtensible Business Reporting Language (XBRL) – a technical overview	322
32. Anna Sobczak	
Entrepreneurship in the education of university students	331
33. Mihaela Markova	
E-commerce in the process of digital transformation: preparedness, requirements and technological tendencies	343
34. Petya Petrova	
Basic Soft Computing Methods In User Profile Modeling	353
35. Petar Dimitrov	
Methods for storing authentication data – a historical review	369
36. Svetoslav Ivanov	
Development stages of starting software company, problems and approaches for software development	382
37. Antonio Hadzhikolev	
The role of the smart city concept in the process of urban transformation	397
38. Oumar Sy	
Ontology-based materialized views for reverse engineering: Toward a set of conceptual guidelines	410

BIG DATA AND INFORMATION SECURITY

Veselin Popov¹, Petya Emilova²

*¹ D. A. Tsenov Academy of Economics, Svishtov, Bulgaria,
v.popov@uni-svishtov.bg*

*² D. A. Tsenov Academy of Economics, Svishtov, Bulgaria,
petiaem@uni-svishtov.bg*

Abstract

Along with the many opportunities that Big Data provides, it brings many threats to society and businesses. Big Data Analytics in security refers to the ability to gather massive amounts of digital information to detect, analyse and visualize insights that enable the prediction and counteraction of cyberattacks. Along with security technologies, organizations are given the opportunity to identify activity schemes that represent network and other types of threats, which is of great practical importance.

The scope of paper is big data, its sources, features, protection, platforms and processing tools, analyses the abilities of big data for cyber security and define some challenges that refer to major Big Data security issues. The methodology of the study involves a research of the literature on the topic.

Keywords: *Big Data, Big Data Analytics, Cyber Security, Information Security.*

INTRODUCTION

Information security issues are among the leading contemporary business problems. Technologies such as Big Data are linked to information security – on the one hand because it needs serious protection and on the other hand because it itself provides new protecting capabilities in terms of analytics and security solutions to protect data and prevent future cyberattacks.

Big Data Analytics (BDA) refers to the strategy of analysing large volumes of data, or big data (TECHNOPEDIA, 2019). It has become an effective tool in many areas of modern information processing, including the area of information security. By providing tools for collecting and analysing large amounts of digital information generated from different sources or logged by different devices, BDA helps detect and define patterns and trends of irregular behaviour, search for methods to track cybercriminals, predict and stop potential cyber-attacks.

This paper focuses on the problems and challenges of protecting Big Data and on Big Data's ability to improve information security.

1. BIG DATA – SOURCES, FEATURES, PROTECTION, PLATFORMS AND PROCESSING TOOLS

In the specialized literature, the term "Big Data" refers to a huge amount of information that is stored, transmitted and processed in computer systems. Today, *the main sources* for generating Big Data are social medias, a huge variety of smart devices, videos, digital images, sensors, and sales transaction records (TECHNOPEDIA, 2019). In addition to their large volume, these data are also complex which is why traditional processing applications cannot handle them.

According to the National Institute of Standards and Technology (NIST, 2015), Big data is data where the volume, required speed for processing, or the manner in which the data is presented limit the possibilities of the data being analysed effectively by traditional relational approaches or the data require significant horizontal scaling to ensure efficient processing. This has created the need for a new generation of software applications and tools.

Big Data differs from traditional databases by four main characteristics related to: the *volume* of data; *velocity* of data generation and transmission; *variety* of data in the form of different types of structured and unstructured data; *complexity* related to the structure, behaviour, and permutation of data sets in the presence of critical factors.

One of the biggest challenges for Big Data platforms is the protection that must be provided at every stage of the platform's lifecycle, using a combination of *traditional* security tools, *new* tools and technologies, as well as *intelligent* security monitoring processes.

The Big Data life cycle includes four stages:

- a) organizing the data,
- b) processing,
- c) data storage,
- d) processing and production.

Organizing data involves the creation and / or access to the data. Big Data is a collection of different types of data that come from different sources. According to sources, Big Data is of three types: human-

generated data - text, photos, video; machine-generated data - computers operating documents, databases, multimedia, GPS, RFID, smart homes; and data generated by objects (various digital devices).

For example, user-generated data includes CRM data, data such as email messages, phones, SMS or social media posts, and more. There are many transaction data and data stored in different databases. There is also a huge volume of data generated from custom software, sensors and sensors. Data transmitted from sources to the platform must be protected.

Data storage. Different tools such as encryption, user authentication, and intrusion protection are used for protection. These security tools must operate in a distributed platform environment with many servers and branch nodes. Security tools must protect log files and analytics tools when they run on the platform.

Many organizations use cloud services to store their data. Cloud technologies also allow companies to use pre-built Big Data solutions or to quickly build or deploy powerful server complexes without the significant cost of acquiring hardware. In addition to the benefits, however, the new technologies pose challenges to security.

The analytical processing (analysis and data outcomes) of different types of data is the essence of Big Data. The results obtained from this processing are directed to applications, reports, dashboards and are goal for attacks. Therefore, the encryption of results, control of access and traffic are crucial.

The classic technologies used to protect Big Data are: encryption, user access control, intrusion detection and countering, physical security. Encryption protects data both during storage and transition. It should be noted that encryption must work with different types of data and with different analytical tools, relational and non-relational databases, special file systems, etc. User access control is a major network-level security tool. The control is important for the Big Data platform, it must be very precise and based on well-defined policies. Intrusion detection and countermeasure systems are also important to the Big Data platform as they contribute to the timely detection of intrusion attempts. Physical security is related to the security of the building premises of the organization's or cloud provider's data centre.

The Big Data Processing Software Market offers hundreds of software tools and integrated platforms. Some of them have a long history

while others have appeared recently. This market is dominated by large enterprise software vendors such as Oracle, IBM, SAS, SAP, Teradata, Microsoft, and more. Their Big data products are typically integrated into complex business management solutions.

Successful products are also available from smaller software companies specializing in Big data such as Tableau, RapidMiner, Pentaho, Alteryx, Alpine and more.

Open source products like Apache Hadoop, MapReduce, GridGain, Storm and others are also available on the market. Some open source software solutions are often included in projects by commercial vendors.

The best software tools for Big Data processing, according to their purpose, functions performed and security level implemented, are (IMPORT.IO, 2018):

- for data storage and management - Hadoop, Cloudera, MongoDB, Talend;
- for data cleaning - OpenRefine, DataCleaner;
- to extract knowledge from data - RapidMiner, IBM SPSS Modeler, Oracle data mining, Teradata, FramedData, Kaggle;
- for data analysis - Qubole, BigML, Statwing;
- for data visualization - Tableau, Silk, CartoDB, Plot.ly, Datawrapper;
- for data integration - Blockspring, Pentaho;
- data languages - R, Python, RegEx, XPath;
- data Collection - Import.io.

2. BIG DATA ANALYTICS FOR CYBER SECURITY

Big data analysis is much more sophisticated than traditional database applications. Big data are large volumes, not aggregated, in different formats and their processing can hardly be performed in the memory of only one computer. Big data processing involves mechanical processes and algorithms. The Big Data analysis methods used are of two main types - responsive and predictive (CHAOVALITWONGSE, W., HUANG, S., 2015).

Reacting analysis aims to provide statistics on current and historical data and information about what happened and why it happened. It includes methods such as statistical modelling, trend reporting, visualization, association, and correlation analysis.

Predictive analysis focuses on the use of known data (training data) that includes input data properties (attributes) and response values (target models) to build a predictive model (solution) to make predictions for invisible data (test data). It uses methods such as vector machines, linear regression / classification, nonlinear regression (generalized linear model), decision tree, Bayes theory, neural networks, and more.

Big Data technologies used in security systems are able to detect threats in advance. For example, they can detect atypical web behaviour, predict an attack, and analyse the sources of an attack.

Big Data creates conditions for the efficient and effective application of some fraud detection techniques. In the specialized literature, they are divided into two main groups: *statistical techniques* and *techniques using artificial intelligence*. Table 1 provides examples of these techniques.

Table 1

Examples of data analytics techniques

Statistical technics
1. Techniques used in pre-processing data to detect, validate, correct errors, fill in missing and inaccurate data. 2. Calculation of various statistical parameters such as averages values, performance indicators, probability distributions, etc. 3. Models and probability distributions of various business activities. 4. Processing user profiles. 5. Time series analysis of time-dependent data. 6. Clustering and classifying to discover possible patterns / schemas and dependencies / associations in the data groups. 7. Combining algorithms to detect anomalies in the behaviour of transactions or users
Artificial intelligence technics
1. Data mining 2. Expert systems. 3. Automatic pattern recognition 4. Machine training techniques 5. Neural networks

Source: (BAJPAI, A., DAYANAND, and ARUSHI, A., 2018)

3. CHALLENGES

Big Data Working Group defines four aspects of Big data security which are: infrastructure security; data privacy; data management, integrity and reactive security (BIG DATA WORKING GROUP, 2013). Each area has many problems. For example, infrastructure security has the following issues:

- Single Layer Security - The companies need to integrate multi-layer defence within the company's defence strategy, which addresses both internal and external security threats.
- Data transfer across multiple devices, which requires additional levels of security and monitoring to ensure that data is not captured on the route from one device to another.
- A rapid development of Big Data technology and its supporting infrastructure (such as cloud services) that must be able to process data from an infinite number of points with speed, security and reliability. Infrastructure should include security measures to keep information in place at all stages of the process.

In addition to enhancing business intelligence, Big Data provides the opportunity to enhance cyber security. This, however, increases the existing problems and challenges that require attention and await solutions.

Major Big Data security issues are related to: Threats to data security; Privacy risks; Big Data credibility needs to be confirmed; Lack of privacy protection security technology for Big Data.

These Big Data security issues require many challenges which need to be tackled, the most important of which are:

- a) Adopting protection as a top priority for Big Data platforms, which will focus the attention of managers and developers in this direction.
- b) Introducing reactive and proactive protection.
- c) The physical protection of devices and servers that contain sensitive information must be managed with particular care and isolated from other devices.
- d) Application security is as important as device security. Data protection solutions are crucial in this regard. These solutions are at the

heart of Big Data platforms, they contribute to the discovery of behaviors and development trends, and on this basis offer business strategies. This importance of Data mining solutions requires that they be protected against both external threats and internal individuals who abuse their privilege to access sensitive information.

e) High level of access control to be provided with encrypted authentication and to determine who can see what data.

f) Use of real-time security tools. These tools generate a wealth of information. The problem here is to ignore the unimportant alerts so that employees are being targeted for real violations.

g) Data storage management. For Big Data, the architecture is typically to store data at multiple levels, depending on their importance to the business and the cost of storing it.

h) Performing a detailed audit that can help determine when missed attacks can occur at this time, what the consequences are, what to change in the current system.

i) Use of distributed systems. For faster analysis, most Big Data platforms actually distribute the huge amount of data processing work across many systems.

CONCLUSION

Along with the many opportunities Big Data provides to consumers, it creates conditions for multiple threats to society, business and individuals. These threats must be countered. At the same time, the BDA has emerged as an effective tool in many areas of modern information processing, including in the field of information security. This report addresses the problems and challenges of protecting Big Data in these two aspects.

REFERENCES

1. ARADAU, C., BLANKE, T. (2015) The (Big) Data-security assemblage: Knowledge and critique. *Big Data & Society*. 1-12, bds.sagepub.com.
2. BAJPAI, A., DAYANAND, and ARUSHI, A. (2018) Big Data Analytics in Cyber Security. *International Journal of Computer Sciences and Engineering*. 6 (7). pp. 731- 734.

3. BIG DATA ANALYTICS TECHNIQUES. Some Effective Techniques of fraud detection analytics. EDUCBA, [Online] Available from: <https://www.educba.com/fraud-detection-analytics/> [Accessed 2/08/2019].
4. CHAOVALITWONGSE, W., HUANG, S. (2015) Computational Optimization and Statistical Methods for Big Data Analytics: Applications in Neuroimaging. [Online] Available from: http://faculty.washington.edu/artchao/INFORMS_Tutorials_2015-Web.pdf [Accessed 12/08/2019].
5. FAN, Y. (2016) Big Data Security and Privacy Protection. *Electronic Technology and Software Engineering* (1): 227
6. IMPORT.IO (2018). All the best big data tools and how to use them. [Online] Available from: <https://www.import.io/post/all-the-best-big-data-tools-and-how-to-use-them/> [Accessed 21/08/2019].
7. NIST. (2015) Big Data Interoperability Framework. NIST [Online] Available from: <https://www.nist.gov/el/cyber-physical-systems/big-data-pwg>. [Accessed 2/08/2019].
8. TECHOPEDIA. Big Data Analytics. [Online] Available from: <https://www.techopedia.com/definition/28659/big-data-analytics>. [Accessed 2/08/2019].
9. ZENG, G. (2015) Big Data and Information security. *International Journal of Computational Engendering Research*. 5(6). pp. 17-21.
10. BIG DATA WORKING GROUP (2013). Expanded top Ten Big Data Security and Privacy Challenges. [Online] Available from: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf. [Accessed 2/08/2019].