VOLUME 9 NUMBER 2 BANJA LUKA, DECEMBER 2019 (49-128) ISSN 2232-9625 (Print) ISSN 2233-0194 (Online) UDC 004

Journal of Information Technology and Applications

(BANJA LUKA)

JITA

Exchange of Information and Knowledge in Research

APEIRON

THE AIM AND SCOPE

The aim and scope of the Journal of Information Technology and Applications (JITA) is:

- to provide international dissemination of contributions in field of Information Technology,
- to promote exchange of information and knowledge in research work and
- to explore the new developments and inventions related to the use of Information Technology towards the structuring of an Information Society.

JITA provides a medium for exchanging research results and achievements accomplished by the scientific community from academia and industry.

By the decision of the Ministry of Education and Culture of the Republic of Srpska, no.: 07.030-053-160-4/10 from 3/3/2010, the journal „Journal of Information Technology and Applications“ Banja Luka is registered in the Registry of public organs under the number 591.
Printed by Markos, Banja Luka in 300 copies two times a year.

Indexed in: LICENSE AGREEMENT, 3.22.12. **EBSCO** Publishing Inc., Current Abstracts

ebscohost.com
citefactor.org/contact
scholar.google.com
doisrpska.nub.rs
crossref.org
road.issn.org
citefactor.org
cosmosimpactfactor.com

Printed on acid-free paper

Annual subscription is 30 EUR
Full-text available free of charge at http://www.jita-au.com

UDC 004

ISSN 2232-9625 (Print)

ISSN 2233-0194 (Online)

JITA

VOLUME 9 NUMBER 2 BANJA LUKA, DECEMBER 2019 (49-128)

Contents

Welcome to the eighteenth edition of the Journal of Information Technology and Applications (JITA), published by Pan-European University APEIRON Banja Luka.

The Journal of Information Technology and Application (JITA) publishes quality, original papers that contribute to the methodology of IT research as well as good examples of practical applications.

JITA journal is a scientific and professional information magazine that aims to promise a forum for engineering, research and academics, the university and industry to showcase their scientific careers and whether it will make them learn and explore.

JITA offers the perfect convenience to share scientific resources, share your own research highlights, and innovate science with the entire scientific world.

Our mission is to promote and establish cooperation and dialogue between academic institutions and research institutes belonging to the field of information technology, which are as follows:

- Promoting the best research output in the academic field.
- Support in the professional training of IT staff.
- Introducing computer scientists with advanced modern technological achievements.
- Announcement of newspapers in the most advanced information technologies.

Gratitude

On behalf of the Editorial Board, we would like to thank the authors for their high quality contributions, and also the reviewers for the effort and time invested into the preparation of this issue of Journal of Information Technology and Applications.

Acknowledgments

I would like to thank many who read and/or commented on earlier versions of this journal including Leonid Avramovič Baranov, Efim Naumovič Rozenberg, Ljubomir Lazić and Dražen Marinković. However, any errors or shortcomings remain my full responsibility.

Conflicts of Interest

The author declares no conflict of interest.

Editors, Gordana Radić, Dušan Starčević
Editor-in-Chief, Zoran Avramović
zoran.z.avramovic@apeiron-uni.eu

Cybersecurity of Railway Command and Control Systems

Alexey Ozerov
JSC NIIAS

Contribution to the state of the art
DOI: **10.7251/JIT19020530** UDC: **725.31:[681.513.6:007.5**

Abstract: With the large-scale migration to computer-based and network technology, the threat of unauthorized remote access to railway command and control systems does not appear to be something extraordinary.But external effects shall be considered alongside with internal factorsof signalling software and hardware such errors and undocumented features. Risk mitigation in terms of cybersecurity of signalling installations can onlybe achieved as a combination of means designed within some holistic approach integrating both safety and IT security aspects.

Keywords: Cybersecurity, functional safety, signalling, undocumented features, wrong-side failure.

Introduction

Railways are generally considered as critical infrastructure. This means that failures and incidents can ultimately cause national-level disruptions.They could also have a dramatic effect on the safety of the public, business performance and reputation.

Year to year, the number, sophistication and diversity of registered cyberattacks are steadily growing. Attackers use a variety of tactics; they have different motivations – from financial benefits to revenge.

In 2016, the UK's railway system was affected by at least four major cyber attacks, while in 2017 the WannaCry virus caused the failure of the PIS/PAS system of a German railway carrier and affected other railways.In 2018aDDoS attack at Danske Statsbaner, the biggest Danish train operator, halted trains operations and blocked passenger services.

What is more important is that cyber attacks can also cause wrong-side failures within the command and control system. And that could mean severe harm to assets, environment and people. Nowadays "malicious cyber activity" is becoming more of a safety concern for digitalized railway command and control systems rather than just a security concern.

The range of potential consequences of cyber security incidents related to railway command and control is wide and includes:

- Loss of system availability
- Degradation of system performance
- Manipulation or loss of data
- Loss of production control
- Environmental disaster
- Risk of death and grave injury
- Damage to company image
- Financial loss [1].

Cybersecurity threats and railway command and control

Until recently, it was generally believed that railway signalling systems,being isolated from external effects, are immune to any cybersecurity threats and attacks. That is no longer the case. Now, the focus is on providing resilience, rather than preserving immunity.

The potential scenarios of cyber attacks against safety critical systems are many. They include unauthorized access to equipment, tampering with hard-

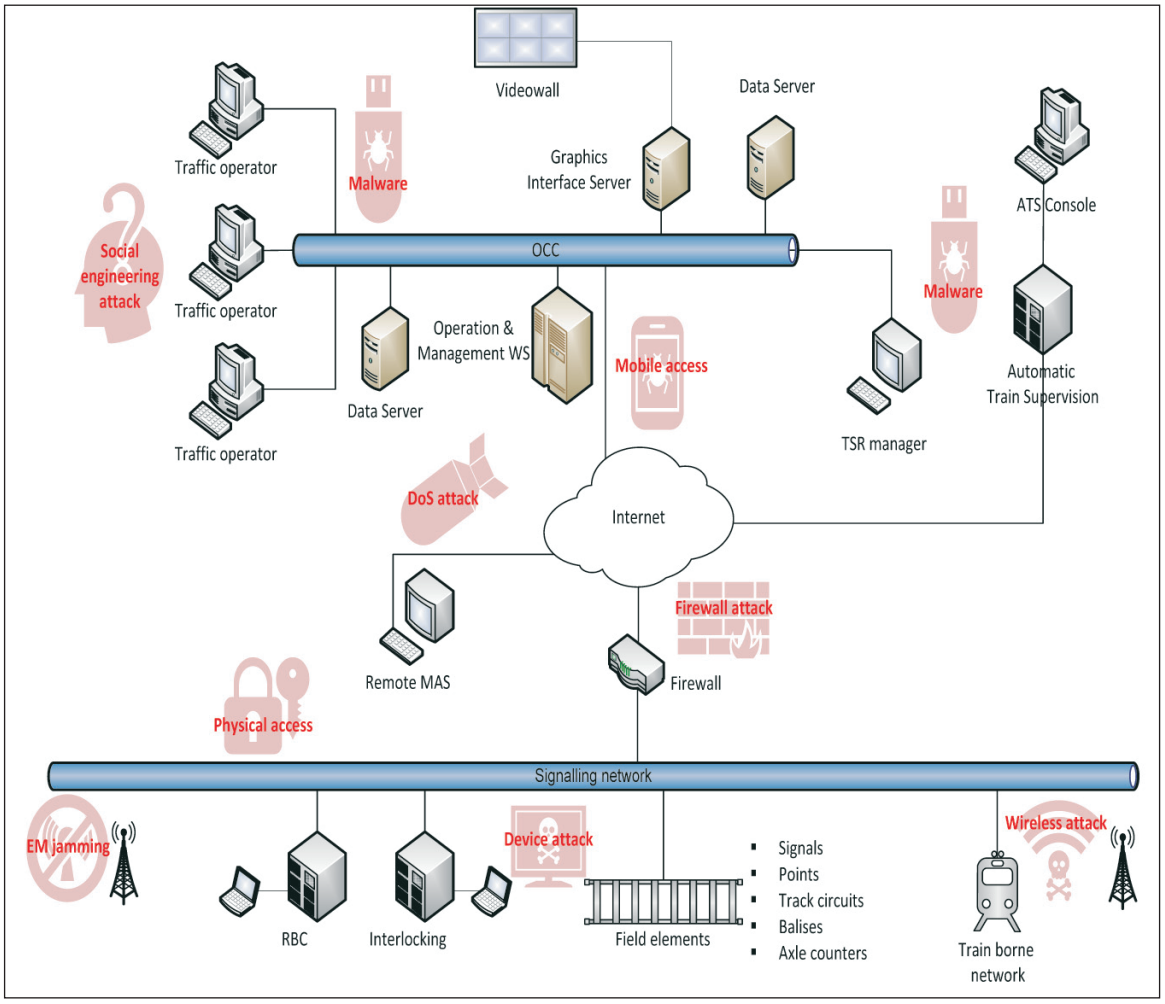


Figure 1. *Railway command and control levels and cyber threats*

ware and software and more. But unlike non-critical IT systems, their aim does not consist in the breach of confidentiality.The motivation can include compromising the system safety and manipulating critical commands and controls in order to cause train collisions, unexpected train stops, power cuts etc. That, for instance, can be achieved by clearing the signal that should not be cleared, releasing the track section that should be blocked, etc.

Even a simple USB flash drive can be used to compromise the functional safety of a critical signalling installation. Social engineering (man in the middle) is a very important factor here. A lot depends on the company's cybersecurity policy and personnel training, monitoring of staff behavior and motivation assessment.

The vulnerability of signalling installations has been shown by various projects and by in-house hackers. The vulnerability of the ERTMS system was demonstrated in the SECRET (Security of Railways against Electromagnetic Attacks) project. The project focused on assessing the risks and consequences of electromagnetic attacks on the rail infrastructure and developing protection solutions. Such critical data channels as GSM-R and balises were identified as the most probable "targets". The possibility of effective suppression of these communication channels with the low-priced «jammers» was experimentally confirmed [2].

The railway system includes a number of layers and interfaces to external systems. Therefore, we must take into account and map all possible threats, techniques and devices that could target each zone and conduit of signalling installations.

From the perspective of safety-critical signalling installations' operators, it is not the issue of confidentiality, integrity and availability of information in general, rather than the issue how to be protected

Vulnerabilities	Source of threat	Examples of threats	
Company data transmission network level			
Software vulnerabilities	Outside intruder	• Execution of a malicious code on a gateway computer • Denial of service	• Remote application launch • «Password attack»
Vulnerabilities of network protocols and communication channels	Outside intruder	• Network scanning • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Information support level			
Software vulnerabilities	Outside intruder	• Execution of a malicious code at workplaces • Denial of service	• Remote application launch • «Password attack»
Vulnerabilities of network protocols and communication channels	Outside intruder	• Network scanning • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Information logic processing level			
Software vulnerabilities	Insider	• Execution of a malicious code on an industrial control computer • Denial of service	• Wrong route setting • Network scanning • Substitution of the entrusted object
Vulnerabilities of network protocols and communication channels	Insider	• Network scanning • Wrong signal setting • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Input/output interface and actuators levels			
Vulnerabilities of network protocols and communication channels	Outside intruder or insider	• Substitution of the entrusted object • Decoy object embedding • Network scanning	• Network traffic analysis • Denial of service

against malicious code in the software and undocumented features of the signalling system, to prevent open access to safety-critical installations, to identify and eradicate vulnerabilities etc.

Below are some examples of software and network vulnerabilities and threats [3].

With all these threats in mind, we need to face the current and emerging challenges of cybersecurity of railway systems and to understand the risks and their possible impact. It means that we have to carefully study all the historical cases of cybersecurity incidents, their consequences and who was be-

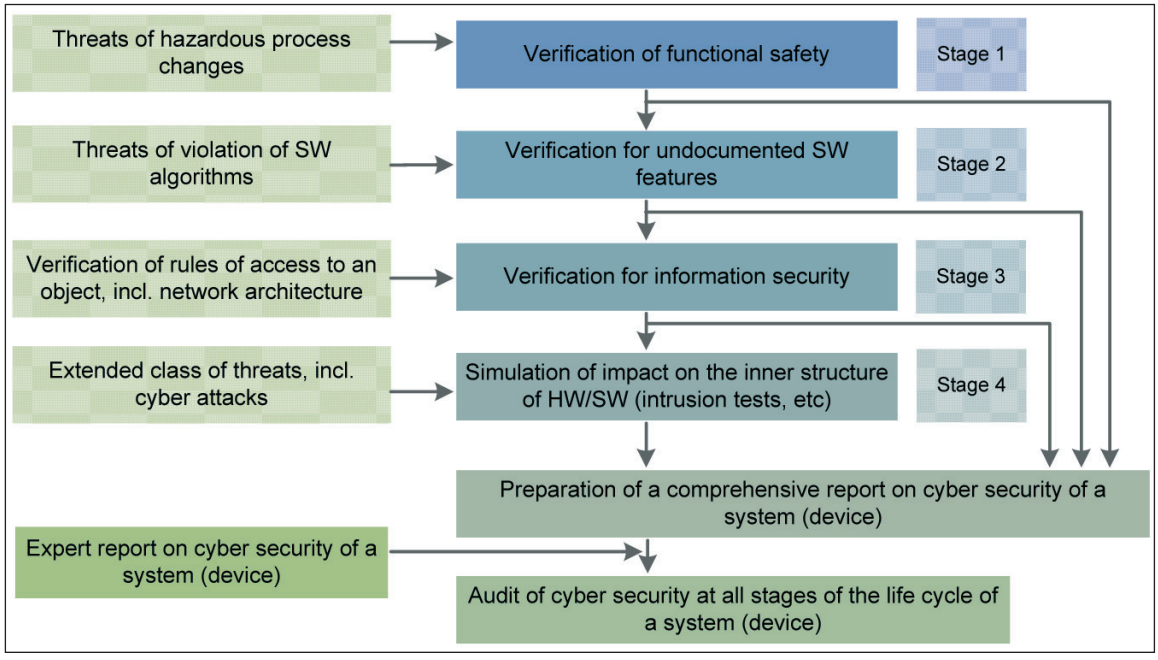


Figure 2. *Railway system assessment and evaluation cycle*

hind and how they deployed them. That must be followed by a thorough risk assessment and an inventory of vulnerabilities and threats, and those have to be updated at every stage of a system's life cycle starting from the design stage. So, it's like a V model with review and revision at each stage.

Assessment and audit of a railway system's software includes detection and identification of undocumented features which are not intended for use by end users, but left available for use by the vendor for software support and development.

The problem, though, is that if hackers discover such undocumented features, they can also remotely access the device and possibly take control of the entire system. This is why all types of undocumented features present potential security and cyber security risks.

- Unintended undocumented features could be the result of developer errors,
- Intentional undocumented features could be deliberately introduced in the software during its development. Intentional undocumented features include design, algorithmic and malicious logics.

SECURITY AND SAFETY OF RAILWAY CRITICAL SYSTEMS

In railway control systems that make use of today's networking technologies, cyber security is the continuation of technical (functional) safety and must be taken into consideration in the system lifecycle the same way as the technical safety. As one of the fundamental principles of the dependability theory postulates, there is no absolute safety. The only option isto take measures to minimize the possible risk, a procedure that leaves the residual risk. And as we know, risk is a combination of the rate (probability) of an event and the gravity of its consequences.

For a railway operator, the basic task consists in defining the justified acceptable level of residual risk subject to the available funds and other means of reducing the risk at the company's disposal. A comprehensive approach to safety management based on the risk assessment allows examining the aspects of technical safety and cyber security as a whole. A widely used tool is the risk matrix that allows classifying the existing risks based on their probability and possible damage (see the Figure below). The risks classified as intolerable must be eliminated at the design stage. For tolerable risks, damage reduction measures are to be developed [4].

System safety and system security are closely related to each other in terms of the availability of authorized functions. The safety and security of a system in general mean that a system does what it is supposed to do and does not do what it is not supposed to do.

However, while the tolerable hazard rate(THR) of functional safety is in fact a mathematical probability, the security level cannot be based on the prob-

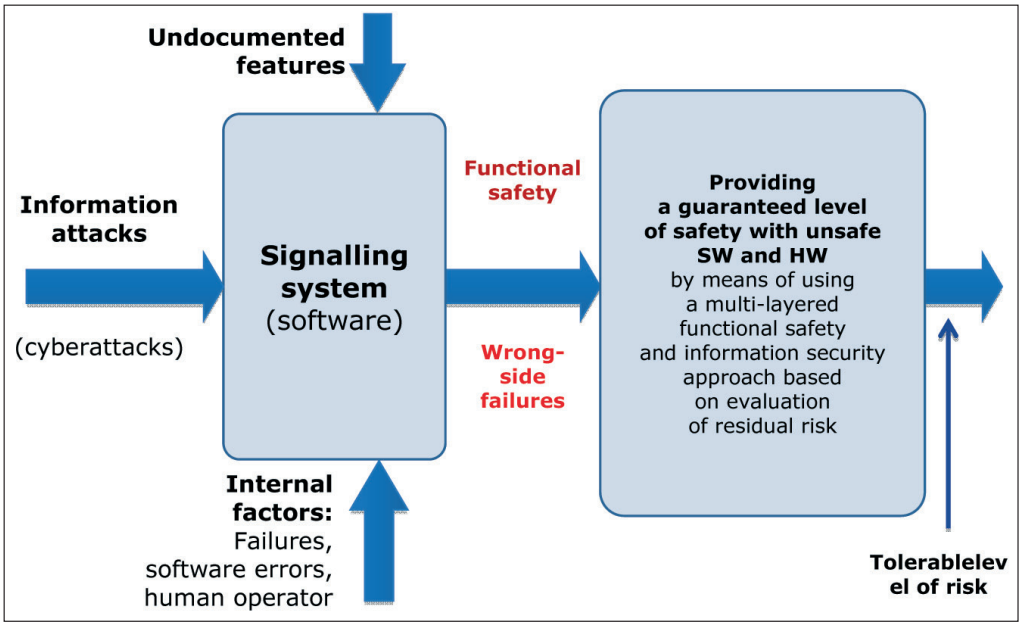
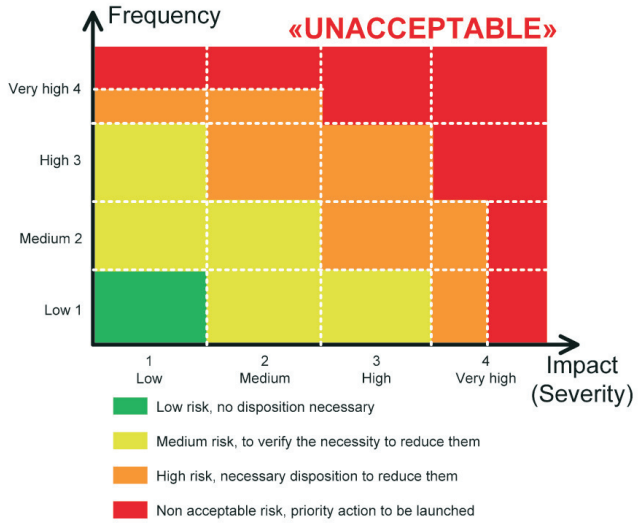


Figure 3. *Software assesment and evaluation*



ability principle since there is an intentional action by an attacker or a group of attackers.

There are still other conflicts between safety and security requirements and approaches. For example, safety requirements may overrule security requirements: security requires complex and unique passwords to login, safety requires short term login to avoid critical loss of time in stressful situation.

The great number of international conferences dedicated to the cyber security of railway systems held over the past few years demonstrates the growing awareness of the existing cyber threats. Railway companies have accumulated some experience in correlating cyber threats with types of technical failures, conducting penetration tests and identifying the vulnerabilities of existing systems. However, these activities are performed in a situation when there is no common international railway cyber security standard and no standardized procedures and methodology.

Cybersecurity as a multi-layered approach

Various research projects aim to cover the existing lack of a common safety/security standard.

For example, the European project CYRail (Cybersecurity in the railway sector) defined a number of recommendations for the development of a structured cybersecurity strategy for the railway industry with some emphasis on the identification of most critical railway services, zones and conduits, and definition of detection and mitigation strategies. As a basis the project uses a series of IEC 62443 standards intended for industrial automated control systems. The standards are considered by many experts as a guideline for building a cyber security management system. The project also uses these standards to develop requirements for a secure-by-design railway system [5].

In IEC 62443 security levels (SLs) are parts of the qualitative approach to addressing security for a zone.

SL0 – no special protection requirements

SL1 – protection against casual or coincidental violation

SL2 – protection against intentional violation using simple means with low resources, generic skill and motivation

SL3 – protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation

SL4 – protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

Research and practice produces a long list of recommended measures to be used as part of a cybersecurity strategy. Among other things, they include regular updating of critical signalling systems software, as well as application of trusted software and hardware.

Naturally, a secure-by-design system could be one of the options. In particular, a cybersecurity system should have a number of independent inbuilt security mechanisms to ensure sufficient protection in case of failure or compromise of any of them.Apart from the inbuilt security mechanisms, of utmost importance is the availability of tools for early attack detection, suspicious activity monitoring within hosts and networks. Though such features can only be regarded as complimentary to the inbuilt mechanisms and security procedures.

The UIC ARGUS (Security & Safety Analysis for Electric and Computerized Signalling Systems) project addressed the safety and security issues of computerized railway signaling systems. The project aimed at identifying vulnerabilities of signaling systems from the perspective of cyber threats and developing counteraction methods. The project also considered human factor management during the life cycle of the system.

The results of UIC ARGUS project as well as the activities of the UIC Cybersecurity Platform laid the

foundation for the development of a comprehensive standardized approach to the issue of safety and security, like UIC Guidelines for Cyber-Security in Railway issued in 2018.

The Guidelines have some particular focus on railway signalling and telecommunication and describe how to evaluate the security needs through ISO 27001 and using best practices applied in others industries, with company's Information Security Management System taken into account. In some way the Guidelines provide recommendations about how to develop a Security Management System for the railway cyber security that should present "a systematic approach aiming at establishing, operating, monitoring, auditing, updating and improving the railway cyber security in order to achieve the organization's objectives". It shall be based on risk management and on the implementation of solutions designed to protect the railway assets.

As to the UIC Guidelines for Cyber-Security in Railway, a multi-layered approach should be used meaning that "for every threat, several protection barriers should exist. These should be established in such a way that, to overcome them, a potential intruder would need professional skills in several unrelated areas".

According to the UIC philosophy, evaluating SL in close relation to SIL as part of the comprehensive, holistic approach to safety-security of signalling installations, infrastructure manager (IM) should apply some well-structured strategy incorporating the following fundamental components:

- Conscious and well-grounded selection of a governing principle (modus operandi) ofthe company in terms of acceptable risk level
- Identification of threats and their consequences (threat scenarios)
- Treatment of threats and their consequences at the system level
- Formalized safety and security requirements (with identification of 4 SIL/SL levels) imposed on suppliers
- Well-substantiated choice of system design and mitigation measures.

Cyber security is intertwined with all the business issues from service availability to safety. Nowadays, all systems rely on their computer and communications systems for all operational purposes including availability and safety. Moreover, they also rely on the integrity of the data itself.

So, cyber security issues should be treated as integral part of the IM's asset management system. Cyber security must be considered in the complete scope of railway exploitation and operations (network security, deployment security, signalling security) and atall stages of development (design, architecture, etc.), assessment and audit. Existing international standards traditionally treat safety and security issues from the point of requirements for railway systems suppliers. However, it is usually infrastructure managing companies who are ultimately in charge of security of railway transportation and the lives of passengers, while outside threats are rapidly growing. IMshave two options – either to just rely on suppliers, or to incorporate in their asset management system some measures and methods how to protect their safety-critical installations against cyber threats using a cycle of assessment and evaluation iterations based on a railway-specific methodology.

Conclusion

Currently there is no common international standard for safety and security. Railway operators have to take care of security of their signalling installations on their own. They develop management systems to identify and eliminate existing vulnerabilities, establish cybersecurity teams and units and elaborate internal regulatory provisions.

In a number of countries, national railway authorities and companies have been gaining experience and best practice in terms of security threat mapping and specifying security requirements as part of tendering procedures. Though one problem is still there – a cybersecurity expert in the railway signalling domain isnot an easy target for a market headhunter.The industry definitely needs a robust cybersecurity strategy that would include training of a new kind of experts equally well-versed in both signalling systems engineering and information technology.

References

[1] UIC Guidelines for Cyber-Security in Railway.June 2018, ISBN: 978-2-7461-2732-6.
[2] http://www.secret-project.eu/ (10 September 2019)
[3] Methods of Assessment of Signalling Systems for Cybersecurity. International Union of Railways (UIC). May 2019, ISBN: 978-2-7461-2819-4.
[4] http://www.secret-project.eu/IMG/pdf/20150128-02-uic-argus.pdf (10 September 2019)
[5] CYRail Recommendations on cybersecurity of rail signalling and telecommunications systems. UIC-ETF, September 2018, ISBN: 978-2-7461-2747-0.

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

Alexey Ozerov is the Head of International Department of JSC NIIAS, Research & design for Information Technology, Signalling and Telecommunications on Railway Transport, subsidiary of Russian Railways. Hehas been working with JSC NIIAS for 14 years in various positions related to research, signalling business unit and international cooperation. He is Deputy Chairman of the Committee for Development of Electrotechnical and Intellectual ATP/ATC Systems of the Russian Association of Railway Manufacturers, JSC NIIAS representative in UIC, member of UIC Rail System and Cybersecurity Platforms, expert of IEC/TC 9.

For citation

Alexey Ozerov, Cybersecurity of Railway Command and Control Systems, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:53-59, (UDC: 725.31:[681.513.6:007.5), (DOI: 10.7251/JIT19020530), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

MISSION CRITICAL ICT

Goran Đukanović, Dragan Popović
djukanovicg@gmail.com, popdragan@yahoo.com

Critical Review
DOI: **10.7251/JIT1902060DJ** UDC: **004.783.5:621.396.61**

Abstract: In this paper, three technologies intended to be implemented in Private Mobile Radio systems are analyzed and compared: TETRA (Terrestrial Trunked Radio), LTE (Long Term Evolution) and DMR (Digital Mobile Radio). Characteristics of these networks are collected and compared in one SWOT table. Based on this analysis, appropriate recommendations are made, which should be taken into account when choosing a specific solution for specific uses in Critical Communications systems.

Keywords: DMR, ICT, TETRA.

INTRODUCTION

Critical mission is a basic function that is extremely important for the functioning of the organization. Depending on the scope of activity of the organization, the use of the term critical mission is changing. Here, we will imply that the critical mission relates to PPDR (Public Protection Disaster Relief) organizations. Mission critical communications imply that PPDRs have technical communications systems in place, that allow for safe and reliable communication during operations. When planning such systems, special attention is paid to the reliability of the system. Statistics show that 85% of radio sessions is exposed to concentrated disturbances [5]. The risks that could lead to communication interruptions during operations must be minimized or, if possible, avoided altogether.

MISSION CRITICAL COMMUNICATIONS

In the relatively recent period, there has been a global technological shift from analogue to digital systems, which, in terms of public safety, is most reflected in the adoption of TETRA standards [2] and the introduction of TETRA systems in operational use in most European countries. Since the introduction of the TETRA system is a costly and time-consuming process, other standards have been specified, primarily intended for business users, such as DMR (Digital Mobile Radio) and dPMR (Digital Private Mobile Radio). As TETRA systems provided quality and secure communication, the development of commercial mobile technology did not meet the needs of public services. However, the need to transmit large amounts of data, primarily video streaming in real time, has led to the adaptation of both TETRA and mobile telephony standards.

The TCCA (TETRA and Critical Communications Association) has embraced a scenario whereby public security services are moving from voice-oriented to data-oriented communications, which covers a much broader aspect. Also, TCCA identified a lack of support for modern applications that produce and transmit large amounts of data, as the biggest limitation of the TETRA system and selected LTE as the technology for broadband mobile networks for mission critical and business critical communications. Future public safety networks must maintain the same level of management, security and high availability as existing public safety networks does, but they must additionally be capable of enabling the use

of advanced applications which are present in commercial networks today [3].

The mobile radio communications system must meet the key requirements in order to be used for mission critical communications: Reliability (High availability of system infrastructure and minimums of service availability when infrastructure is unavailable); Centralization-decentralization of operations (central dispatch point for customer management and possibility of DMO (Direct Mode Operation) - operations without centralized control or without infrastructure); Different types of calls (individual call, group call - for all members of a specific group, general call - for users outside the group); Making a call (minimum time for making a call, PTT (Push To Talk) function, Receive calls immediately); Communication security (User authentication, Air interface encryption); Call priorities (Divide users by priority level, Assigning priority to emergency-alarm calls); Transmission of text data (the ability to send and receive text messages, ability to implement GPS location); Packet data transmission (the ability to transmit and share video signals, ability to work with the business information system) [1], [9].

In the rest of the paper, three technologies intended to be implemented in PMR (Private Mobile Radio) systems are described and compared:

1. TETRA - the most widely accepted technology for PMR in public services,

2. LTE - the latest mobile radio standard, initially intended for mobile operators, but it is supplemented by requirements for PMR use

3. DMR - PMR standard, newer than TETRA standard, intended for less demanding PMR users. DMR is a mission-critical, lower-cost variant most commonly used by regional rather than national services.

TETRA (TERRESTRIAL TRUNKED RADIO)

TETRA is a telecommunication standard for private mobile radio systems, developed by ETSI (European Telecommunications Standards Institute).

TETRA is a system designed for services that require the highest level of communications security and system reliability, whose efficiency and cost-effectiveness are reflected in the ability to share infrastructure between multiple users while maintaining privacy and security. Virtual networks within a single TETRA network enable each organization to use the system independently of others. Implementing the TETRA system for several different services lowers the cost of implementation because all services share the same infrastructure. TETRA is a technology that achieves superior communications security through encryption of voice communication, data transmission, signaling data and user identities. TETRA system [2] is primarily intended for the transmission of voice communications, although it can also be used for data transmission (short text messages and "slow pictures"). Tetra system architecture is shown in Figure 1.

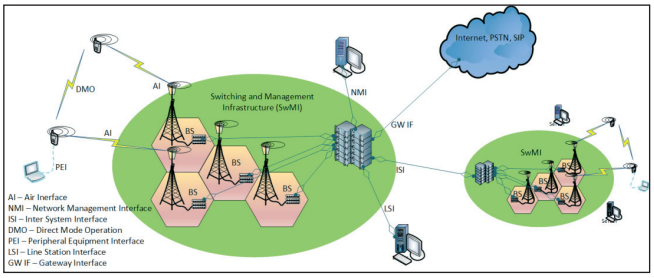


Figure 1. *Tetra system*[1]

For data transmission, the basic data rate per time slot is 7.2 kbps, but if all four slots are used it is possible to achieve a data rate of 28.8 kbps. When a time slot is used for packet data, no voice call can be made through that slot.

TETRA 2 - TEDS (TETRA Enhanced Data Service) standard offers an improvement in data transmission. This increase in speed also requires an increase in the bandwidth used. Thus, at a channel width of 150 kHz, a transmission speed of about 500 kbps is possible in best case.

The basic mode of operation of the system is the tranking mode. Tranking is a term used in telecommunications to refer to a situation where multiple users are sharing the same set of frequencies, rather than each user using only his own frequency. User devices exchange radio messages with the base station. The base station is connected to the switch. The base station authenticates the terminal device and only devices that have been approved in advance can log on to the system. All communication between the user devices is done through SCN (Switching Control Node).

[1] ETR 300-1, May 1997

In case of unavailability of infrastructure, other modes of operation are possible to provide minimum service:

- **mobile repeater mode** - mobile terminal device can play the role of a radio repeater - increase signal coverage. In this case, call establishment is done through SCN,
- **DMO - mode** when communication is performed between two or more terminal devices without the mediation of SCN,
- **Repeater mode** - when the base station does not connect to the SCN, it acts as a classic radio repeater for devices that are logged in and authenticated.

There are two prevalent models of TETRA system implementation: the private network and the establishment of TETRA operators.

LTE (LONG-TERM EVOLUTION)

LTE represents the fourth generation of wireless communication standards, i.e. continued development of GSM / EDGE (second generation) and UMTS / HSPA (third generation) network technologies. The main advantage over previous generations is the mobile broadband capacity, ie. multiple increase in data rate.

GSM technologies are primarily intended for mass commercial telephone services. As such, they were not intended to satisfy the communications requirements of mission critical implementations.

It must be taken into account that in parallel with the development of GSM, TETRA has been developed as a system for critical communications. However, commercial standards are evolving much faster than TETRA, which is primarily intended for PPDR, and as a result, critical communications requirements have been incorporated into commercial standards since 3GPP (The 3rd Generation Partnership Project) issue 12. Current issues of the standard, as specified in the 3GPP Specification Release version matrix[2], supports critical communications requirements [7], [8]: ProSe - Proximity Services (DMO), GSCE - Group System Communication Enablers, IOPS - Isolated E-UTRAN Operation for public safety, MCPTT - Mission Critical Push to Talk.

ProSe - Proximity Services (DMO) service is an upgrade of the LTE standard that should allow communication between two terminal devices directly, i.e. without LTE infrastructure participation or via eNB (E-UTRAN Node B), but without LTE core network participation. This service is the counterpart to the DMO and to the repeater mode of operation of the TETRA terminal and base station. The aim is to provide communication between terminal devices also in areas that are not covered by the LTE radio network for whatever reason or when there is a radio signal with an eNB, but the eNB does not have connection to the network core. This method is primarily used to transmit voice communications.

GSCE - Group System Communication Enablers is a service that supports group calling, the use of dispatch consoles, and streaming audio and video signals to multiple devices using a single downlink data stream.

IOPS - Isolated operations for Public Safety - represents the ability of terminal devices to operate without network infrastructure or over isolated eNBs. This functionality is intended for PPDR organisations.

MCPTT - Mission Critical Pust to Talk service over LTE is an application layer service designed to extend the architecture of the LTE system. It provides PTT functionality over LTE infrastructure and DMO communications. The extension over the TETRA system is reflected in the possibility of duplex communication.

The LTE access network is a base station network - eNB, which has a flat architecture because, unlike earlier generations, it does not have a central intelligent controller [4]. The flat architecture allows to reduce delays in network response, which is positive for applications that require high data rates. LTE elements are highly optimized and very complex with the aim of making the most of the available radio spectrum. Basic LTE network infrastructure is showed in Figure 2.

LTE technology enables an optimum bandwidth of 2 x 20 MHz to achieve a downlink speed of 300 Mbps, or downlink speeds of 75 Mbps are possible for reduced allocation of the 2 x 5 MHz spectrum. These values are much larger than the TEDS and allow for seamless video sharing.

The implementation of the LTE network for public security is observed from three aspects:

1. Technology aspect - LTE standardization organization has adopted a version of the standard that

[2] https://www.3gpp.org/DynaReport/SpecReleaseMatrix.htm

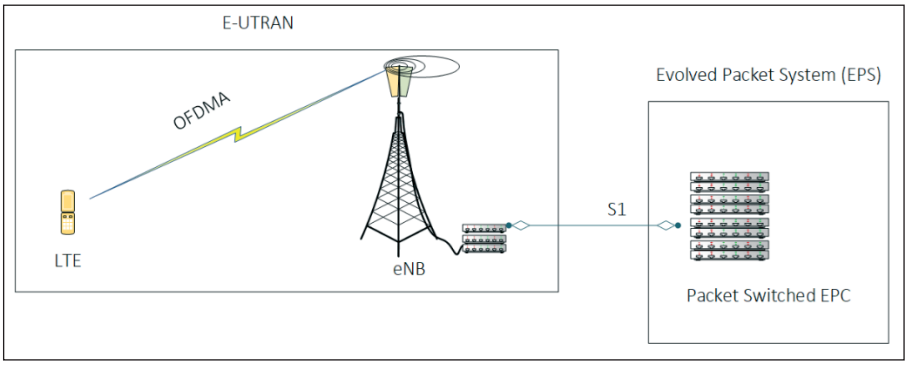


Figure 2. *LTE network Architecture*

is tailored to the requirements of communications of critical situations,

2. The network aspect is reflected through various ways of realizing business models,

3. Radio frequency spectrum - a prerequisite for implementing the system is to regulate the use of the RF spectrum both nationally and globally.

From a network point of view, the system of critical communications can be implemented by utilizing the resources of commercial telecom operators to a greater or lesser extent. It is also possible to build a private LTE network, but in this case the problem of RF spectrum allocation arises. Therefore, there are three models [7]:

1**. Private LTE network** - a special system established for the needs of the public security service. There are also two implementation principles for implementing a private LTE network:

a. The network is owned and operated by the organization that uses it,

b. The network is owned by another organization in charge of resource management, and public safety is the beneficiary.

2. **Commercial LTE Network** - Resources for public security are reserved within commercial networks. There are two models here too:

a. SLA - Service Level Agreement, when a subscription agreement is reached with commercial operators that perform customer management,

b. Virtual Private Operator - when the resources of commercial operators are used to organize own system in which the organization can manage capacity and customers.

3. **Hybrid solutions** - a combination of the previous two, especially in terms of infrastructure use.

DMR (DIGITAL MOBILE RADIO)

DMR is a telecommunications standard for private mobile radio (PMR) systems, developed by ETSI (European Telecommunications Standards Institute)[3]. In relation to TETRA, this is a newer standard and the aim of the introduction was to reduce the complexity of the system as is the case with the TETRA standard. It is intended for use in three Tier: Tier I, Tier II and Tier III. Tier I is intended for unlicensed use, Tier II is intended for licensed use in a conventional network and Tier III is intended for licensed users in Trunk mode.

Data transmission involves the ability to exchange text and control messages, but packet data transmission has a modest capacity that is lower than the capabilities of the TETRA system but is sufficient to transmit telemetry data.

DMRs can also operate in analogue mode and are compatible with existing analog devices. However, not all digital mode functionalities are available when operating in analogue mode.

The DMR Tier II system consists of: repeaters, dispatch stations and terminal equipment, as Figure 3 shows. Device manufacturers on the market offer devices that can be upgraded from a DMR Tier II to a Tier III, with software upgrade, without the need for hardware changes.

Traditionally, repeaters are not connected and it is not possible to communicate between two users who receive signals from different repeaters. However, the advancement of technology has brought novelty to such systems as well. These news are reflected in the connection of the repeater via internet protocol. In this way, it is possible for users to communicate regardless of distance.

[3] ETSI TS 102 361 (1-4)

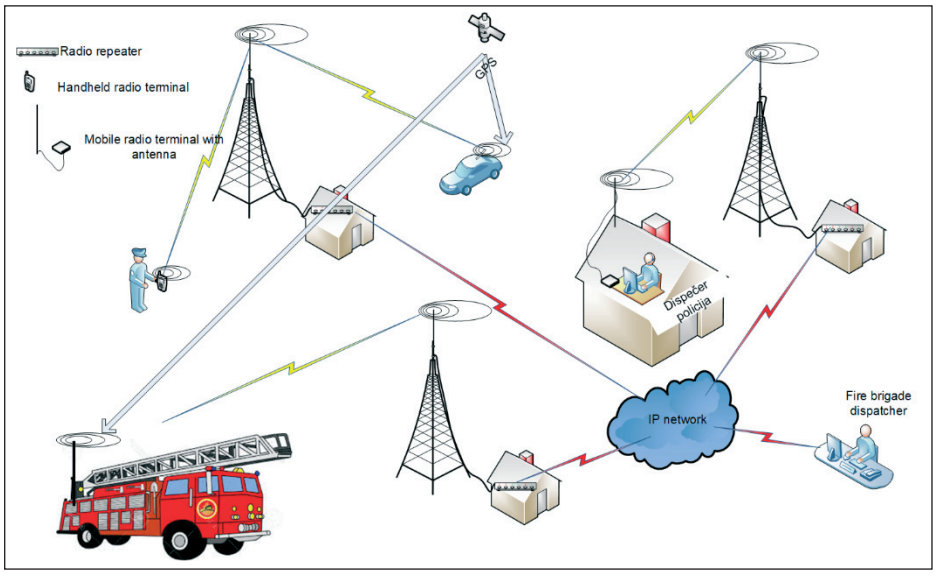


Figure 3. *DMR II system Architecture*

The DMR Tier III system has a trunking architecture. Repeaters have the role of base stations, and with respect to the DMR Tier II, all parts of the system must be connected into a single entity, the control of which uses a central switch. Connecting the system to one unit makes it easier to manage users, i.e. assigning rights to user devices.

COMPARING

TETRA, as the most recognized technology for use in public safety services, has the highest number of implementations in public services worldwide. LTE with TETRA and DMR with TETRA technology are most commonly compared in the professional literature. Direct comparisons of DMR with LTE have not been made, primarily because DMR II is not a trunking technology and therefore has limitations in the requirements for mission critical systems. DMR III systems are just beginning to be implemented and are mostly implemented in organizations that do not have a budget sufficient for the TETRA system.

Tables 3, 4, 5 and 6 present the SWOT analysis of DMR, TETRA and LTE technologies respectively . SWOT analysis is one of the management tools used when making some strategic decisions related to the organization.

Table 3. *SWOT Analysis - Streinghts*

DMR	TETRA	LTE
Open standard	Open standard	Open standard
Supports analog devices	Device and infrastructure compatibility	Very high data rates
Low spectrum requirements	Low spectrum requirements	Suitable for modern applications
VHF Possibility to work in VHF range	Full duplex	Full duplex
Territory coverage by signal	Communication protection	Interoperability with other communication systems
Cost of implementation	Evidence of technology - a large number of implementations	Supported by manufacturers of commercial systems

Table 4. *SWOT Analysis – Weaknesses*

DMR	TETRA	LTE
DMR Tier II is not intended for critical communications	Cost of implementation	Critical communication systems have not yet come to life
Insufficient interoperability of devices from different manufacturers	Territory coverage by signal	Territory coverage by signal
Low data transfer capacity	Low data transfer capacity	

Table 5. *SWOT Analysis – Opportunities*

DMR	TETRA	LTE
Particularly suitable for rural areas	A standard that is still evolving	A standard for developing mobile communications, including mission critical communications
Ease of implementation	Proven high reliability	

Table 6. *SWOT Analysis – Threats*

DMR	TETRA	LTE
A standard designed to fit into the ranges traditionally intended for analog PMR systems, thereby also overcoming the limitations of those data transmission ranges	Implementation complexity	Lack of available frequency spectrum in recommended areas
High availability of the system is still not ensured	The emergence of quality PMR solutions, above all DMR Tier III	

Based on the SWOT analysis, we can conclude that there is no ideal solution. What can be said with certainty is that the future of communications belongs to LTE technology, so when the system is built from the beginning the decisions are most often for LTE technology. Countries that already have a TETRA system in place throughout the territory resort to hybrid solutions, where existing infrastructure is retained prior to voice communications. LTE is used to transmit video signals.

When deciding on a technology choice, we can choose some of the crucial factors to choose from, such as the cost of implementation, the time it takes to bring the system to operational use, and the need to transfer large amounts of data. In this case we will choose:

- DMR system - if the price of the system would be a crucial factor,
- TETRA - if there is an adequate budget, and time to provide the frequency spectrum is short,
- LTE - if the system must support the transmission of lots of data.

Conclusion

TETRA is the most recognized standard for radio communications in public safety organizations. It enables very efficient customer management, but system administrators need to be properly trained. Building a system requires time and considerable material resources, and still, new and expensive system will not be able to transmit video. In this sense, financial and technical justification of implementing TETRA as green field is questionable.

LTE and incoming 5G [6] technologies are the future of radio communications. Implementing a private LTE system is expensive and can be hampered by the regulator's inability to provide adequate frequency bandwidth. Implementation in collaboration with commercial operators carries its security risks, that can be kept under control by an adequate organization of the cooperation. It is the only system that allows the transmission and sharing of video content.

Finally, based on the research and SWOT analisys which is conducted in this paper, we can say that DMR technology is a very convenient solution if closed networks is the main goal, because of the cost, the time of implementation, the training of the administrators, and because it offers same functionalities to users as other digital technologies do. By encrypting the air interface, communication security is also achieved.

References

[1] C. C. B. GROUP (2013), Mission Critical Mobile Broadband: Practical standardisation & roadmap considerations.

[2] ETR 300-1 – ETSI Technical Report (May 1997), Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 1: Overview, technical description and radio aspects.

[3] Forge S, Horvitz R and Blackman C (2016) Is Commercial Cellular Suitable for Mission Critical Broadband? , Study on use of commercial mobile networks and equipment for "mission-critical" high-speed broadband communications in specific sectors, final report to European Commission.

[4] Kaleem Z et al. (2019) UAV-Empowered Disaster-Resilient Edge Architecture for Delay-Sensitive Communication, *IEEE Network*, pp 1-9.

[5] Mikhailovich KL (2018), Use of multiparameter adaptation in communication systems. *Journal of Information Technology and Applications* (JITA).

[6] Parvez I et al. (2018) A survey on low latency towards 5G: RAN, core network and caching solutions, *IEEE Communications Surveys & Tutorials*, Volume 20, Issue 4, pp 3098 – 3130.

[7] Stojkovic M (2016) Public safety networks towards mission critical mobile broadband networks. Master Thesis, NTNU Trondheim.
[8] Study on the relative merits of TETRA, LTE and other broadband technologies for critical communications markets, P3 communications GmbH, 2015.
[9] TCCA (2013) The Strategic Case for Mission Critical Mobile Broadband: A review of the future needs of the users of critical communications.

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

Goran Đukanović earned his PhD at the Faculty of Electrical Engineering in Banja Luka. He has published 35 scientific papers mostly in the ICT research area, as well as one university textbook. His area of scientific research is in ICT, in general with respect to allocation, management and control algorithms in the conditions of limited resources, especially in Wireless Networks and Wireless Sensor Networks, Cyber-Physical Systems and Internet of Things (IoT). He is a member of the IEEE for 15 years, and a member of the editorial board of the scientific journal JITA Apeiron.

Dragan Popović is a Business Development Manager at Roaming Networks Banja Luka, where his fields of interest are: Mission critical communications and video surveillance systems. Dragan has worked in the Republic of Srpska Ministry of the Interior as Head of the Department of Radio Communications and Technical Systems. Also, he has experience as a Project Manager, Network and Security designer and AFIS (Automatic Fingerprint Identification System) consultant. He has attended seminars in Russia, Japan, China and other countries, which are dedicated to ICT in the service of citizen security. He graduated from the Faculty of Electrical Engineering, University of Banja Luka.

For citation

Đukanović G., Popović D., Mission critical ICT, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:60-66, (UDC: 004.783.5:621.396.61), (DOI: 10.7251/JIT1902060DJ), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

DDLM - Quality Standard for Electronic Education Programs in Higher Education of Bosnia and Herzegovina

Siniša Tomić, Dalibor Drljača

Pan-European University APEIRON, Banja Luka, Republic of Srpska, Bosnia and Herzegovina

Contribution to the state of the art

DOI: **10.7251/JIT1902067T** UDC: **004.735.8:621.39(497.6)**

Abstract: The Web-based technological revolution has brought new teaching opportunities and concepts. This expands the range of educational opportunities based on new digital technologies, while certain obstacles and dangers appear that this type of education brings with it at the same time. Electronic education systems should be flexible and it would be ideal if able to meet the specific needs of each student individually. On the other hand, it is extremely important to standardize teaching electronic content, define all vertical and horizontal processes in the electronic education system, and set quality standards that must be respected. Higher education institutions must take an active part in the development and implementation of information technologies in teaching processes. DDLM (Demand-Driven Learning Model) clearly defines the structure of Web-based teaching delivery, so that it essentially defines the quality standard of e-learning programs based on Web technologies. The problem of non-standardization of electronic educational content, poorly defined processes in the system, such as the delivery of electronic content, control activities, personalization or irregular updates, is present everywhere in the world, and so with us. The research conducted in this paper examines the population of students of higher years of study, as well as students of the second and third cycle of study at 5 universities in Bosnia and Herzegovina, in order to get a clear picture of the current state of electronic education in our country. The survey was conducted on 565 students between October 2016 and January 2017. Following the methodology of scientific research, the empirical research was primarily conducted through a survey questionnaire, where primary quantitative data were stored in a database and further analysed, after which we reached the relevant scientific knowledge.

Keywords: Electronic education, DDLM standard, LMS.

Introduction

Educational institutions that provide teaching in an online environment must pay particular attention to the design, implementation and distribution of electronic educational content, which predominantly is now multimedia. Creating quality electronic educational materials is a very serious and difficult task. With the increasing prevalence of teaching in electronic form, institutions providing this type of teaching are inevitably entering the market race for creating high-quality multimedia educational content. On the other hand, many educational institutions are predominantly focused mainly on the delivery of electronic educational content, taking into account only technological parameters or visual criteria, while neglecting educational goals, which is not a correct approach. In doing so, the basic Mayer principles [1] [2] of the organization and rules of visualization of multimedia educational content are ignored and grossly violated. Effective e-learning models must be guided by sound pedagogical principles and be flexible in order to adapt to the needs and goals of students. The

literature recognises different teaching and learning strategies – linear and constructivist; some authors advocate teacher-centred and other processes- and procedures based learning, but each model deserves attention and consideration as the choice for selection of the learning model should depend on the goals of the program and the needs for the trainees (students) [3].

DDLM - Quality Standard for Electronic Education Programs

The following group of American and Canadian authors was particularly concerned with the quality standards and the issue of the implementation of electronic educational programs. Colla MacDonald et al [4] set a quality standard in the design, development and distribution of electronic education programs - DDLM (Demand-Driven Learning Model). DDLM clearly defines the structure of the delivery of WEB-based teaching.

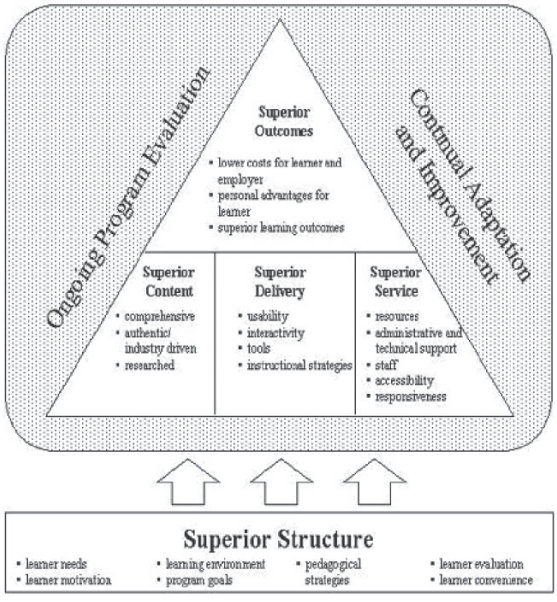


Illustration 1: *DDLM – Quality standard for electronic educational programs [4]*

DDLM looks at the delivery of e-learning programs from multiple angles and at different levels:

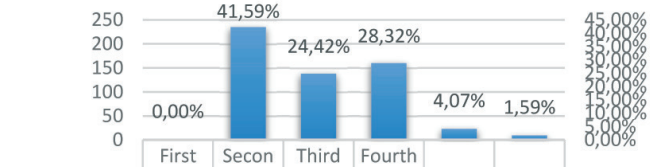
- Structure - Understands the basic needs of online education learners, creates a stimulating environment that affects students' motivation. Other pedagogical strategies are developed and periodic examinations are made of the students through tests, quizzes and the like.
- Content - must be understandable, authentic and based on previously acquired knowledge.
- Distribution - interactivity, ease of use of the distance learning system, tools for navigating the system and manipulation of electronic educational multimedia content should be ensured and encouraged.
- Service - must provide administrative and technical assistance, accessibility to the system with mandatory optimization and must provide a communication channel to provide prompt answers to the queries, which are usually communicated via e-mail reserved for technical support, although support may also be provided by telephone, video link, chat, forum etc.
- Outcomes - online education users expect lower study costs (travel, food, lodging, time, e-textbooks ...), while on the other hand, they expect specialized knowledge and skills equal to delivering classical classroom instruction that will enable them to compete at the labour market.

Delivering this type of teaching and meeting quality at all levels, as described by the DDLM, requires significant financial investment presenting a major obstacle to quality online education, which is especially noticeable in economically underdeveloped countries, including our country. On the other hand, even if the necessary financial investments are provided, there is an equally big and serious problem, which is the lack of skilled people who understand the principles of multimedia and modern e-education and who should be prepared to put enormous effort into creating quality multimedia educational content according to the set quality standards. Communication and interaction between trainees and responsible teachers in such systems are necessary, but unfortunately, it is often insufficient or non-existent. Distance learning systems also raise other issues, such as data protection, copyright protection, privacy policies, the autonomy of the environment and content, server capacity, limits on the data flow through the network, technology choices, licensed software, compliance with online education laws etc. Online education requires constant monitoring

of teaching processes and timely implementation of necessary corrections.

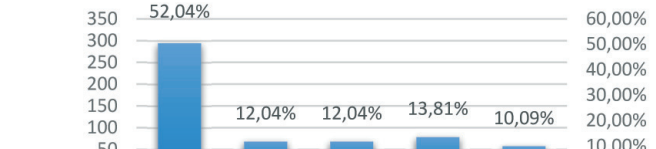
Research

The Survey [5] was created as a web-based application, and Drupal 7 (a content management system) was used as the platform. Most of the collected surveys were realized through a printed form on-site at the premises of the home universities with the presence of a control person, which made the students aware of the importance of the survey and gave an additional dose of seriousness during the filling, as recommended by prof. dr. Goran Milas [6, p. 467]. A total of 565 students were surveyed. The largest number of respondents was at Pan-European University APEIRON, Banja Luka (294 or 52.04%). Following are represented by University / University "Vitez" (78 or 13.81%), BLC - Banja Luka College (68 or 12.04%), International BURCH University (68 or 12.04%) and finally Faculty of Electrical Engineering at University of Banja Luka (57 or 10.09%).



	First year of Bachelor studies	Second year of Bachelor or...	Third year of Bachelor studies	Fourth year of Bachelor studies	Master studies	Doctoral studies
No of students	0	235	138	160	23	9
%	0,00%	41,59%	24,42%	28,32%	4,07%	1,59%

Illustration 2: *Year and type of studies*



	Apeiron	BLC	Burch	Sveučilište Vitez, Travnik	ETF - Banja Luka
No of students	294	68	68	78	57
%	52,04%	12,04%	12,04%	13,81%	10,09%

Illustration 3: *Number of respondents by the educational institution*

The surveyed students were mostly students in the second, third and fourth years of the first cycle academic studies. A particular quality of the research is given by the participation of students of the second and third cycle, ie masters, masters and doctoral studies. The following chart shows student participation by year and type of study.

The survey sought answers to the questions:

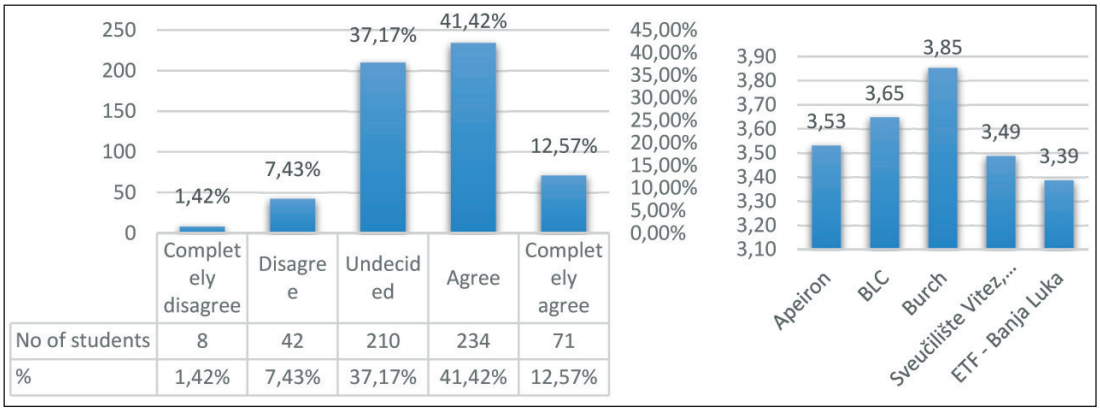
- What is the representation and utilization rate of ICT in higher education in Bosnia and Herzegovina?
- To what extent are educational institutions prepared to use new ICT technologies in teaching?
- What are the effects of the use of multimedia in e-Education in Bosnia and Herzegovina taking into account all the specificities of this educational space?
- How much is e-education represented in higher education in Bosnia and Herzegovina?

The infrastructure, tools, method and concepts of collecting, processing and publishing multimedia content through e-education system were investigated. The readiness of the teaching staff and students to accept and use new educational concepts based on modern ICTs with the indispensable use of multimedia in e-Education is analysed and suggestions are given on how to improve the existing e-education in BiH.

The research fully or partially answered the following questions:

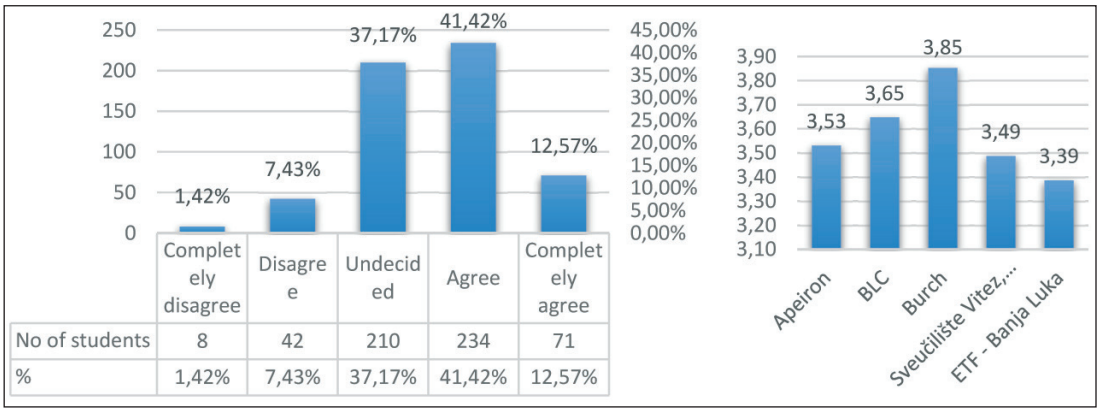
- To what extent are ICTs represented in e-Education in our country?
- What is the willingness of teachers and students to use ICT in e-Education?
- What is the relation of educational institutions to e-education in BiH?
- What are the most commonly used e-Learning models in higher education in BiH and why?
- What technologies and tools are used in the creation of multimedia content and what is the quality of the content?
- To what extent does the existing information and communication infrastructure provide the technical prerequisites for quality e-Learning delivery?
- In what direction will e-Education move in BiH?

This paper does not present all the results and all considerations for the above questions and the



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	8	42	210	234	71
%	1,42%	7,43%	37,17%	41,42%	12,57%

Illustration 4: *Survey claim 1 results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	8	42	210	234	71
%	1,42%	7,43%	37,17%	41,42%	12,57%

Illustration 5: *Survey Claim 2 Results*

results obtained due to its nature and limitations. That is why in the following charts we will be based solely on the quality of teaching via the DLS system of distance learning at the observed institutions.

Survey Claim 1: The distance learning system provides me with quality educational resources, essential for my study.

Average rating 3.56

The marks obtained are even and range from 3.39 to 3.85. The average rating is good, but there is still room for improvement. Learning resources come in a variety of multimedia forms. It is interesting that Pan-European University Apeiron has around 10,000 hours of mounted video material published at all times in its closed Distance Learning system (Learning Cubes 4.0), which are recordings of direct instruction from the classroom and related exercises. The survey shows that students use multimedia educational electronic resources and that they are important.

Survey Claim 2: It is important for me to access educational materials at the moment, regardless of the place and time of access.

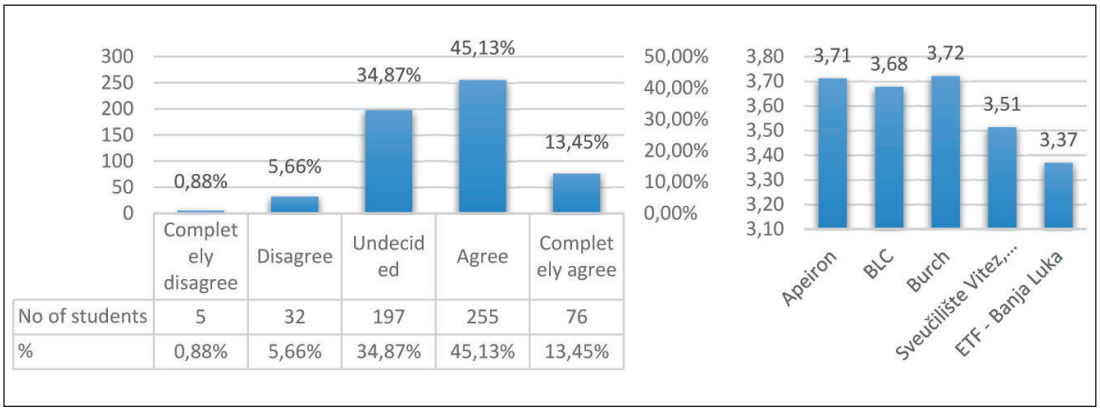
Average rating 4.13

Educational materials in DL systems are most commonly found in a closed environment, for which access requires authentication through unique user data. Instant access is the standard of using DL.

Survey Claim 3: The materials in the DL system are a great complement to the classic classroom teaching.

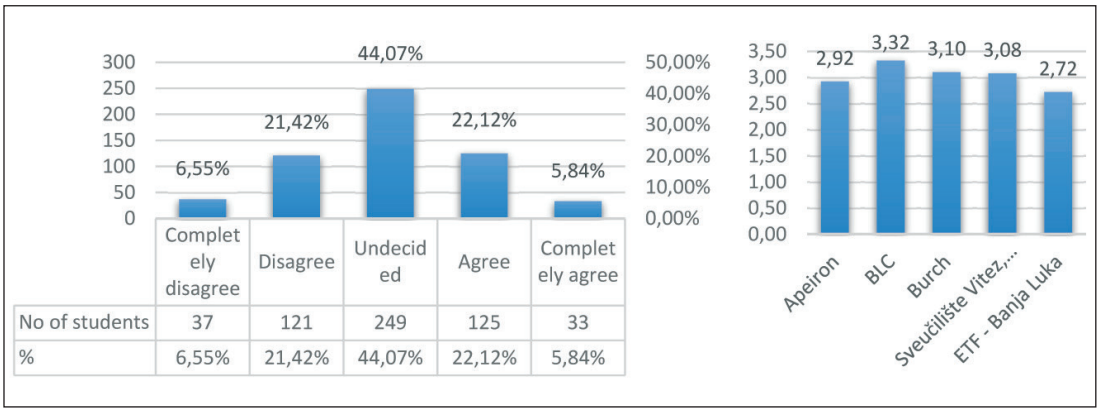
Average rating 3.65

Most respondents felt that the DL systems they access were a great complement to classic classroom teaching. E.g. Pan-European University Apeiron performs Screen Capture of the screen, which is displayed in HD quality combined with accompanying classroom video. This is how the exercises in the Higher Programming Languages-C ++ are per-



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	5	32	197	255	76
%	0,88%	5,66%	34,87%	45,13%	13,45%

Illustration 6: *Survey Claim 3 Results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	37	121	249	125	33
%	6,55%	21,42%	44,07%	22,12%	5,84%

Illustration 7: *Survey Claim 4 Results*

formed in the computer room with video projection, where the students monitor the performance of the tasks (programming tasks) with the lecturer, and then the recorded activities from the lecturer's screen are later thoroughly reviewed and the tasks are taken home (the programming code is perfectly visible). Some teaching activities require dominant classical teaching where the role of multimedia via the DL system is diminished. An example of such an activity is the practical fabrication of a denture in the dental laboratory of the faculty.

Survey Claim 4: The DL system is a more important resource for me to study than classical classroom teaching.

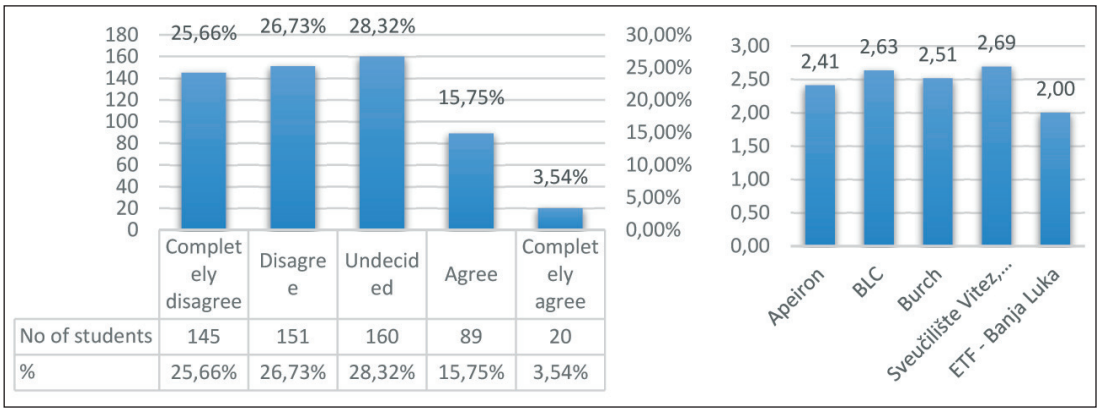
Average rating 2.99

The results of this survey claim prove that in Bosnia and Herzegovina a hybrid model of learning is represented, which is a combination of the best practices of classical educational forms innovated through interactive teaching and online education supported by information and communication technologies. The result (2.99) shows that classical teaching and multimedia learning through the DL system are equally important to students. The graph shows the small differences and models preferred by the observed institutions, so the BLC tends to multimedia learning through the DL system, while the ETF Banja Luka prefers to provide multimedia-assisted teaching in the classroom.

Survey Claim 5: I based my study solely on the DL system, I do not attend the classical teaching.

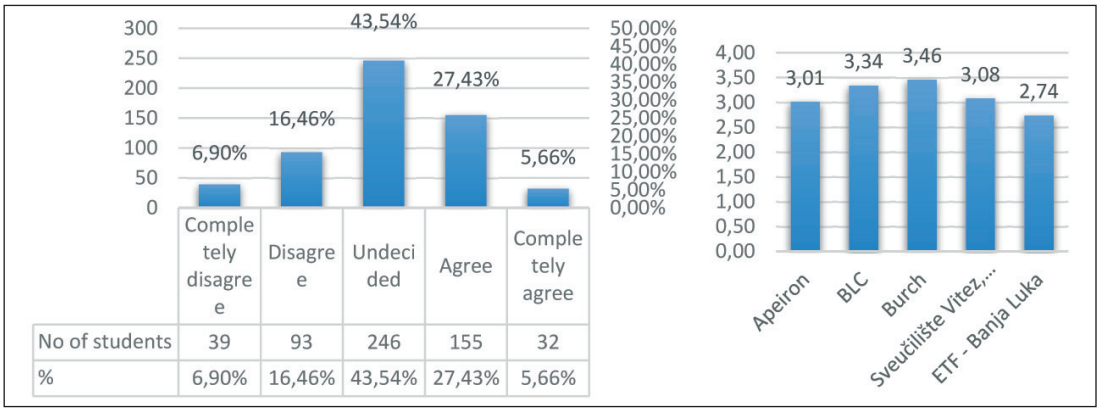
Average rating 2.45

Full-time students are obliged to attend classroom instruction, while extramural (part-time) students do not have this obligation or their attendance is diminished and in this context, the grade of 2.45 should be considered. That's why DL systems for part-time students are of particular importance. A hybrid form of learning can also be recognized in



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	145	151	160	89	20
%	25,66%	26,73%	28,32%	15,75%	3,54%

Illustration 8: *Survey Claim 5 Results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	39	93	246	155	32
%	6,90%	16,46%	43,54%	27,43%	5,66%

Illustration 9: *Survey Claim 6 Results*

this survey question, that is, a combination of classical educational forms combined with e-education.

Survey Claim 6: DL study fits my way of studying.

Average rating 3.08

Just over half of the respondents accept DL teaching as a study method that suits them. This does not mean that the other half does not use DL, as can be seen from the results of the statement made earlier: "The distance learning system provides me with quality educational resources essential for my study (Score 3.56)." Existing DL systems still need to be done more interactive and enrich them with even better quality and more interesting and useful multimedia electronic educational materials for students. Then this average grade can be expected to rise.

Survey Claim 7: The multimedia materials in the DL system are well organized.

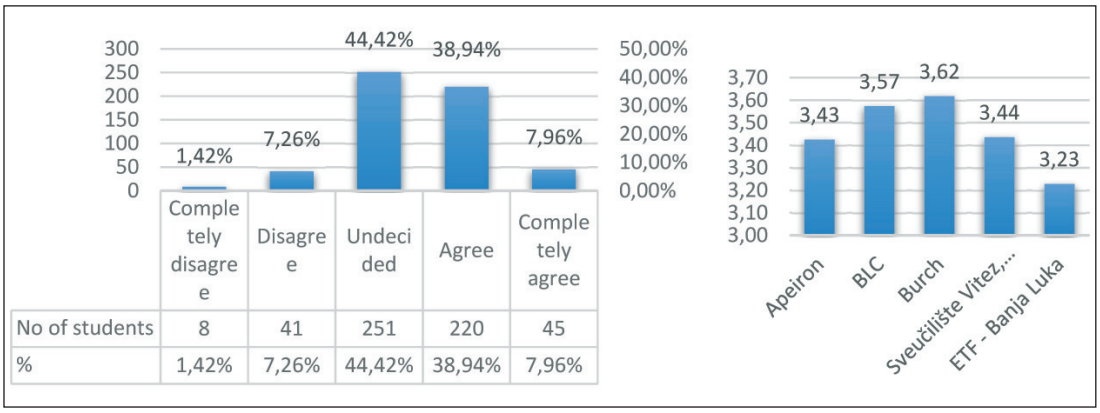
Average rating 3.45

Distance Learning systems are composed of a number of subsystems, such as course creation and guidance systems, testing systems, and up to systems for monitoring progress and student status. DL systems must provide students with access to and delivery of various types of multimedia electronic educational materials in a logical manner. Synchronizing all these systems and providing logical use is a big deal, but that's what students expect from a DL system.

Survey Claim 8: The quality of multimedia in DL is good.

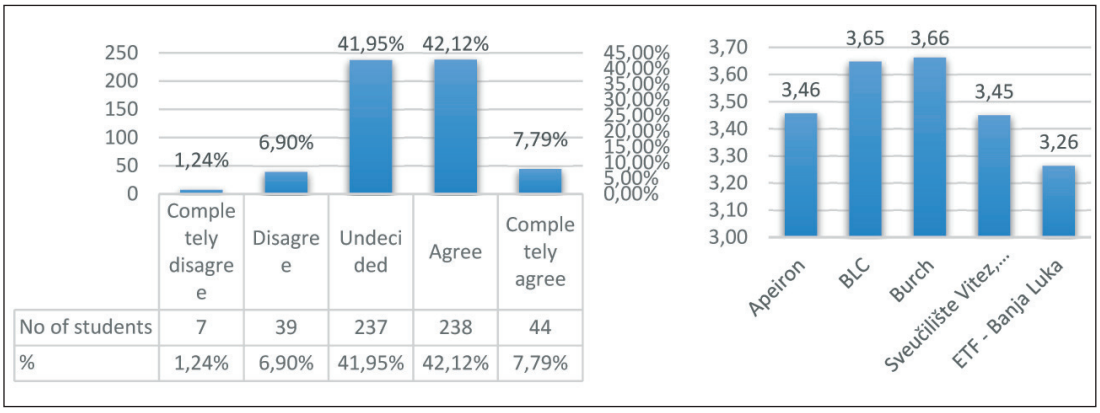
Average rating 3.48

The average score of 3.48 is good, but there is certainly plenty of room for raising the quality of multimedia materials. We can relate the survey claim to one of the previous statements stating: "The distance learning system provides me with quality educational resources that are essential for my study." - (Average grade 3.56).



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	8	41	251	220	45
%	1,42%	7,26%	44,42%	38,94%	7,96%

Illustration 10: *Survey Claim 7 Results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	7	39	237	238	44
%	1,24%	6,90%	41,95%	42,12%	7,79%

Illustration 11: *Survey Claim 8 Results*

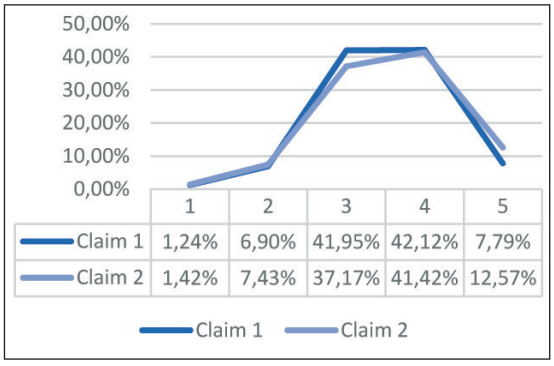


Illustration 12: *Comparative analysis (Quality of multimedia materials in DL systems)*

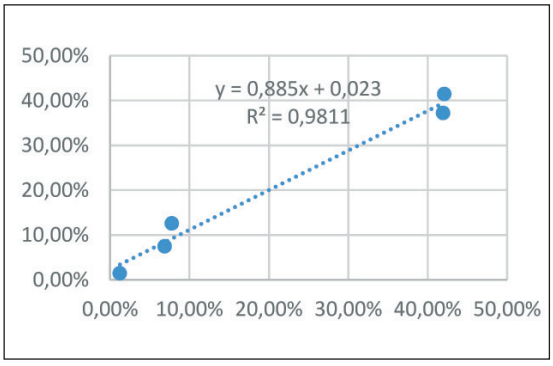


Illustration 13: *Correlation analysis*

Survey Claim 9: Many multimedia materials are missing from the DL system.

Average rating 3.17

The result obtained should not be viewed solely in a negative context. Previous survey statements have positively evaluated the quality of multimedia materials and new multimedia concepts, so a score of 3.17 should be seen as a need for knowledge delivery systems to become even better and that most of the multimedia materials needed can be found by students within the DL. The monitored universities should positively accept the student criticism expressed by the results of this survey statement and work on improvements every day that are of interest to both universities and students

Survey Claim 10: Communication with professors and assistants via DL is good.

Average rating 3.35

Primarily, the role of students in DL systems is

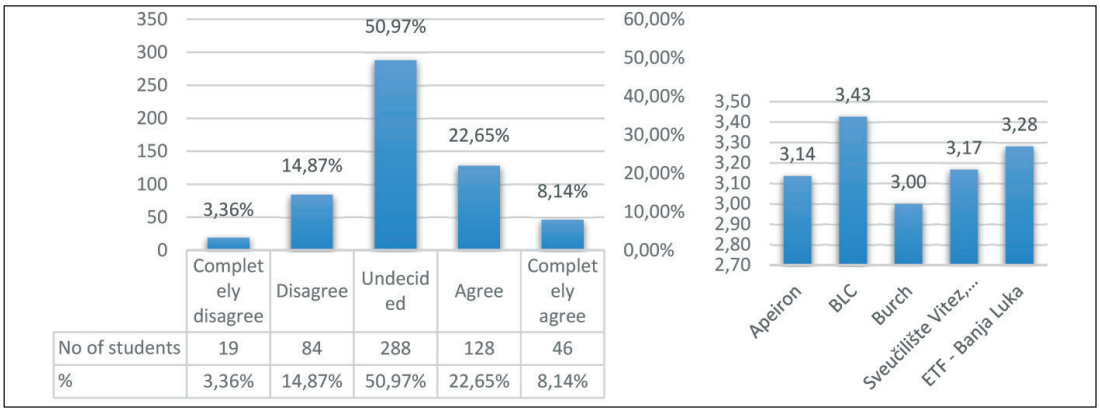


Illustration 14: *Survey Claim 9 Results*

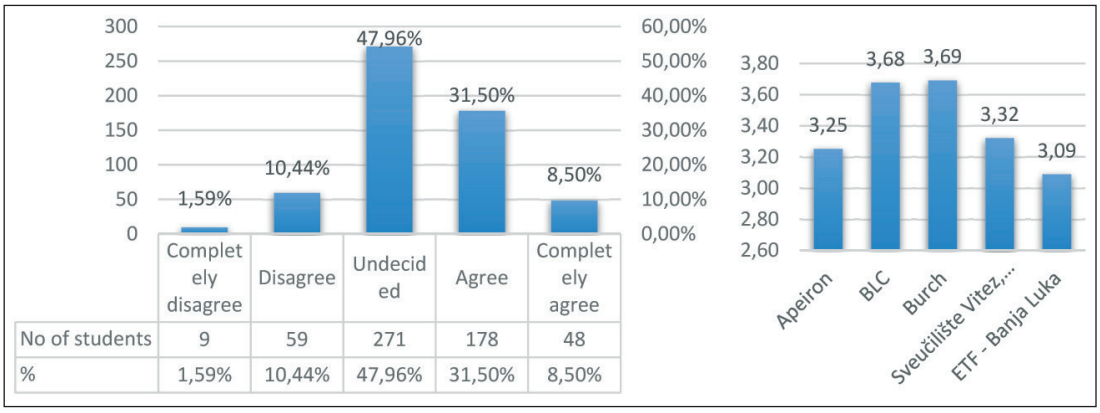


Illustration 15: *Survey Claim 10 Results*

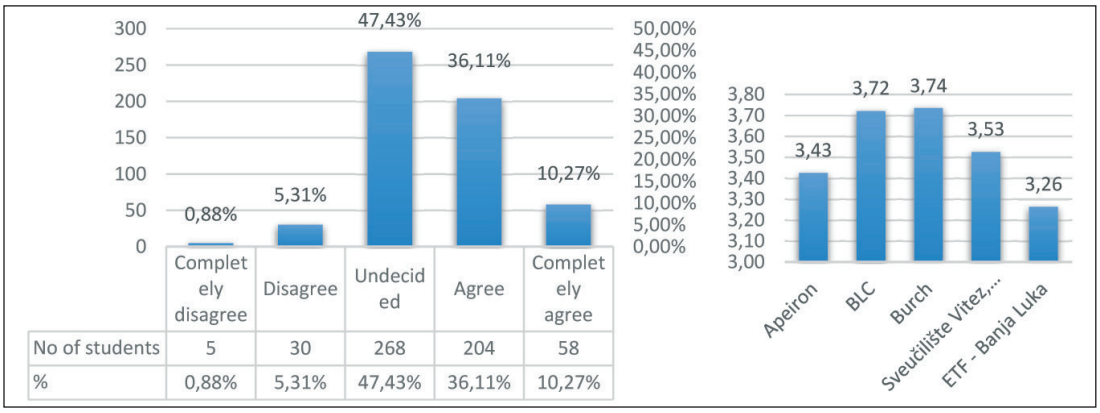
to learn, and this requires planning, motivation and the ability to analyse and apply the content offered. This is where the role of the professor is primary, as the professors in collaboration with the assistants, plan the curriculum, taking into account the needs of students and the specifics of creating multimedia educational materials and multimedia communication that can take place in real-time or be delayed. The systems enable pre-scheduled online communication, exchange of messages and documents, or the joint collaboration of professors, assistants, and students on a single document (all observed institutions have a Microsoft Office 365 suite supported, which supports this), and many other features. It all shows that there are preconditions for quality online communication between professors, assistants and students, and the average rating obtained indicates that there is still work to be done to improve this kind of communication.

Survey Claim 11: Administrator support in the DL system is good.

Average rating 3.50

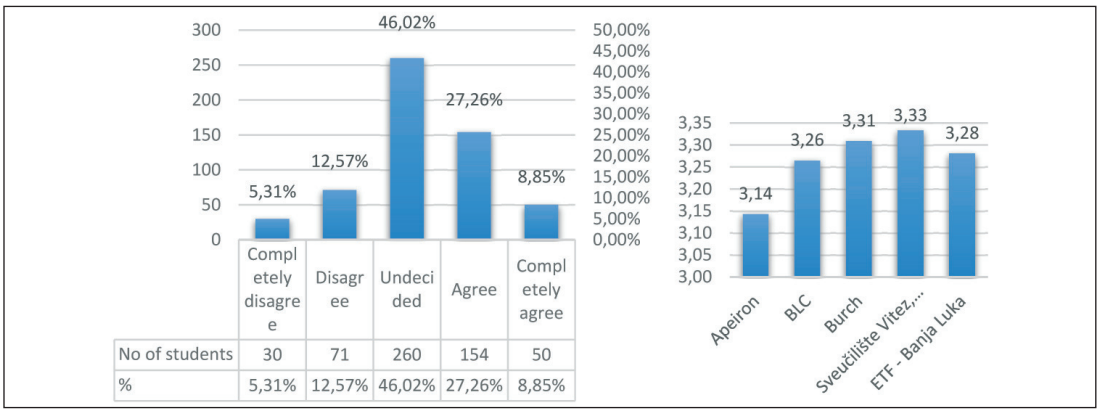
Administrator support for the system can be viewed in two ways:

1. **Professors and Assistants as Administrators** - They are moderators of their respective subjects and as such have frequent communication with the trainees at the course level. They can reorganize a virtual object or detect perceived technical problems that they can sometimes solve on their own or seek the help of an appropriate professional technical person
2. **Administrators (technical persons)** - They only deal with technical matters. They take care of the stability and security of the system, receive complaints and eliminate any technical problems identified. They work on the introduction of new modules and other functionalities including constant communication with the professors and the educational institution that employs them (the introduction of new functionalities usually requires consider-



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	5	30	268	204	58
%	0,88%	5,31%	47,43%	36,11%	10,27%

Illustration 16: *Survey Claim 11 Results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	30	71	260	154	50
%	5,31%	12,57%	46,02%	27,26%	8,85%

Illustration 17: *Survey Claim 12 Results*

able financial investment, which is approved by the University Administration).

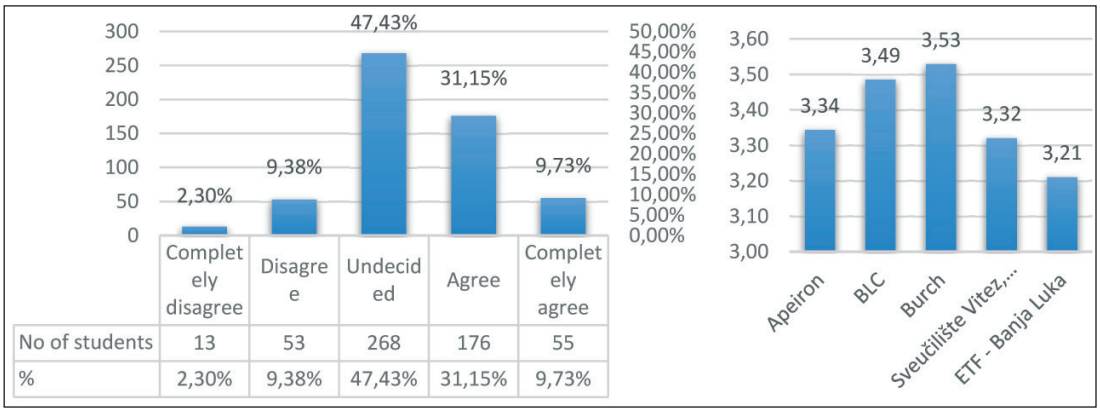
The average score of 3.5 is very good and shows that the DL systems under review have provided administrative support which could be better in the coming years.

Survey Claim 12: DL provides the ability to test knowledge (tests, quizzes, online discussions, etc.).

Average rating 3.22

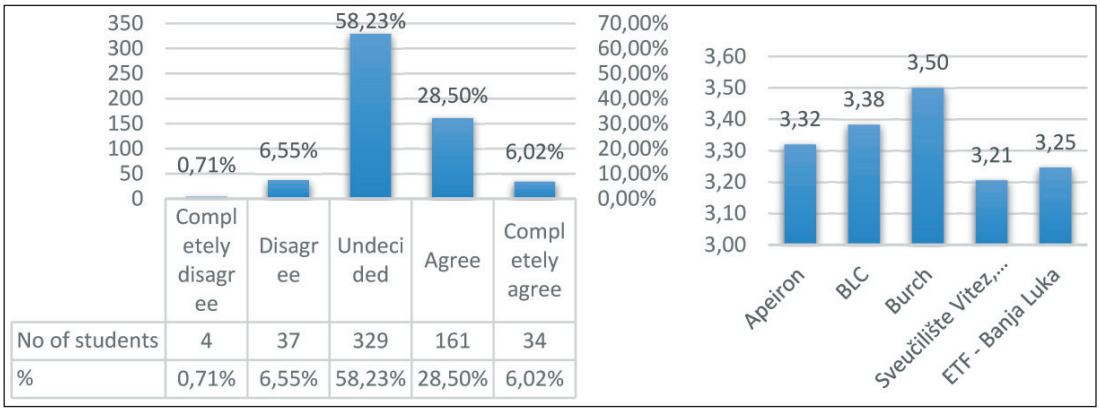
Today, all modern Distance Learning systems have the abilities to test knowledge, create tests, lead discussions, advance students etc. The question is how much these possibilities are used. Technically, there are no problems to provide testing and automatic knowledge testing, where the answers offered are selected or to link related terms offered. The problems arise in case of answers that should be descriptive or thoroughly written. The automatic assessment then falls out of the game, as the systems do not currently have sufficiently developed artificial intelligence that can intelligently analyse and score such answers (this is an ongoing issue). The observed problem is that these simple forms of assessment are not used to the full extent. The reason for this is a non-systematic approach to solving the problem identified, that is - there is no clear position of the University Board that the teaching staff is obliged to create a number of online tests or quizzes that can be easily published within the existing LMSs. The surveyed educational institutions conduct certain online examinations, but there is certainly still plenty of room for this type of testing and verification of the knowledge shown. The right solutions lie in intelligent two-way communication [7] between intelligent tutoring systems and students where the e-learning system contains intelligent methods for analysing and evaluating users' knowledge and skills, as well as controlling e-learning processes, monitoring and optimization.

Survey Claim 13: Studying through the DL system has more advantages than disadvantages.



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	13	53	268	176	55
%	2,30%	9,38%	47,43%	31,15%	9,73%

Illustration 18: *Survey Claim 13 Results*



	Completely disagree	Disagree	Undecided	Agree	Completely agree
No of students	4	37	329	161	34
%	0,71%	6,55%	58,23%	28,50%	6,02%

Illustration 19: *Survey Claim 14 Results*

Average rating 3.37

Students rated this statement positively, with an average score of 3.37. It is felt that the Distance Learning mode of teaching at the observed universities is appropriate for students and is increasingly becoming an indispensable part of their studies.

Survey Claim 14: Multimedia content in the DL system is uniform.

Average rating 3.33

The uniformity of the content and the establishment of certain visual and technical standards that should be adhered to are extremely important. Thus, the Pan-European University Apeiron Banja Luka has set the visual and technical standard for publishing recorded lectures and exercises in video form. This standard describes image size and resolution, fps rate, video layout, meta-tags, video compressor and amount of video compression, audio compressor and amount of audio compression. When creating multimedia materials, the Mayer principles of creating multimedia materials that give them some uniformity and quality standards must be taken into account. The results obtained on this survey claim can be compared with one of the previous statements: "Multimedia materials in the DL system *are well organized.*"

Survey Claim 15: The multimedia content in DL is interesting and of high quality.

Average rating 3.44

Creating interesting and quality multimedia educational materials is a very serious and difficult task. With the increasing prevalence of teaching in electronic form, institutions that provide this type of teaching are inevitably entering a competitive marketplace for creating high-quality multimedia educational content. On the other hand, many educational institutions are predominantly focused on the delivery of electronic educational content, taking into account only technological parameters and visual criteria, neglecting educational goals (ne-

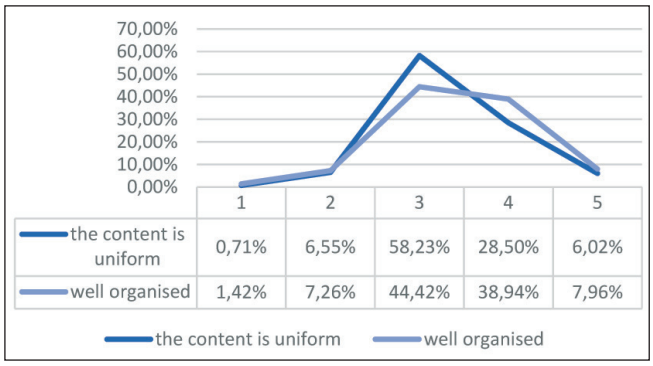


Illustration 20: *Comparative analysis*

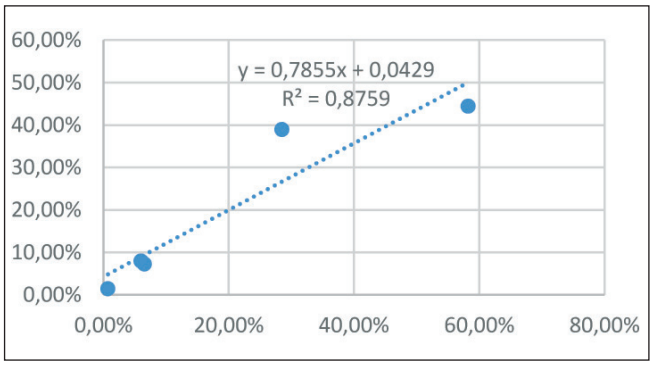


Illustration 21: *Correlation analysis*

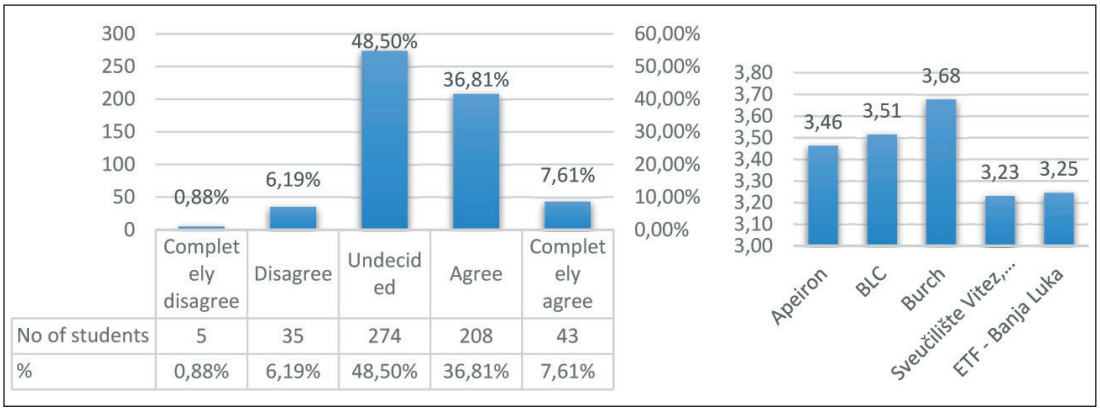


Illustration 22: *Survey Claim 15 Results*

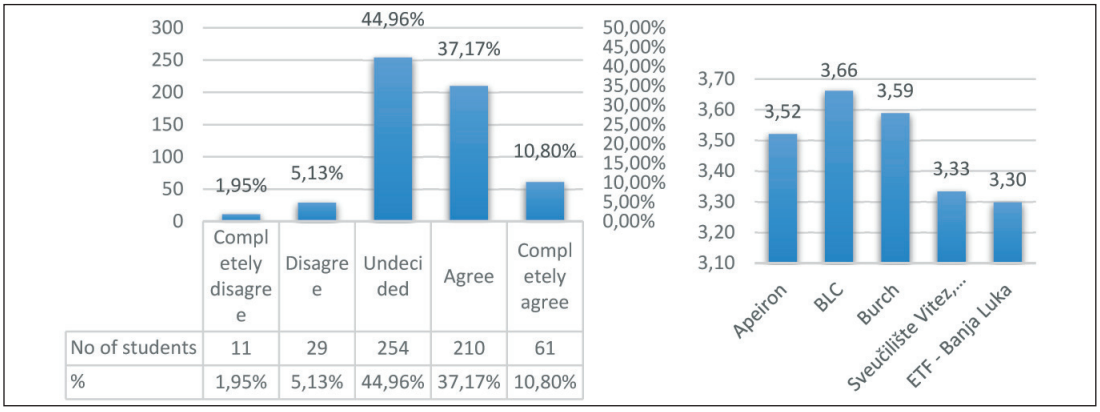


Illustration 23: *Survey Claim 16 Results*

glecting the basic Mayer's principles of organization and rules of visualization of multimedia educational content). The knowledge, experience and skills that students acquire are the most relevant indicators of the quality of e-learning delivery. The resulting average score of 3.44 indicates that the observed educational institutions have made considerable efforts in standardizing the quality of multimedia electronic educational content.

Survey Claim 16: Staying on DL is comfortable, the connection is stable, and educational multimedia content is started and executed smoothly.

Average rating 3.50

Multimedia systems process, store and publish multimedia information. All of these actions require certain prerequisites, the most important of which are stability and data flow over the Internet and to meet hardware and software preconditions, both

from the server and client-side. Only then can we talk about a comfortable use of DL systems. Particular attention must be paid to optimizing multimedia materials to avoid unnecessary memory usage and speed up data flows through the network. Optimization also requires a standardization, which should not be detrimental to the quality of multimedia educational content, while optimized multimedia content, on the other hand, must meet the established audio and visual criteria for their smooth listening or viewing.

Conclusion

The academic community must be able to embrace the development of new IT technologies and outstanding multimedia capabilities in order to provide more dynamic teaching and learning, more efficient use of space, time and financial resources. It is evident that there are no umbrella policies or standards in the delivery of e-learning that higher education institutions adhere to, nor that such a standard shall be obtained in the near future. All observed institutions have implemented their own solutions and policies for publishing and using multimedia educational forms in the form of various open and closed multimedia educational information systems. It has been observed that the delivery of teaching via distance learning systems, both in the Republic of Srpska and in the Federation of BiH, is conditioned primarily by limited financial resources and poor IT infrastructure. Perhaps the biggest problem is the lack of understanding, that is, the lack of vision and initiatives on the part of the University Administrations to set financial frameworks and to find accordingly creative and acceptable solutions for the implementation of DL and in general to provide the necessary material and logistical support conducting e-learning. However, the observed 5 Institutions in this paper are positive examples that investment in eLearning pays off and delivers excellent and measurable results. They have entered the educational market where the technical equipping of the institution and IT support in carrying out educational processes are extremely important factors. The knowledge, experience and skills that students acquire are the most merit factors that set good universities and colleges apart from the bad ones. Many educational institutions in Bosnia and Herzegovina are predominantly focused on delivering electronic educational content, taking into account only technological parameters and visual criteria, while neglecting educational and didactic goals, which is by no means good. With the exception of the 5 educational institutions observed in this paper, in most cases in the remaining higher education institutions, there is an under-utilization of existing personnel and technical capacities, which, with the appropriate organization, can give good results in the implementation of e-education in the current conditions.

E-education in BiH has already crept into all its pores with a tendency to raise the quality of multimedia educational forms and the participation of teaching staff in the active process of creating electronic educational materials and interacting with students through various multimedia systems, based on the WEB. This research undeniably confirms this. In the future, major developments in all fields of e-learning should be expected. First of all, one must keep in mind the rapid development of artificial intelligence that can find application in such systems. Then the individual needs of the students could be fully monitored, adjusted to their predispositions, learning styles and the speed of learning the course material. The development of artificial intelligence and intelligent tutoring systems will allow each student to have their own personal e-Tutor, available 24 hours a day. Certainly, in the future, many interesting IT solutions await us and it will be interesting to observe how all this will affect the execution of teaching processes, both in the world and in our country. We hope that higher education of Bosnia and Herzegovina will fully embrace these new multimedia educational concepts and actively participate in their further development.

Bibliography

[1] Mayer, R. E., (2001), Multimedia Learning", Cambridge: Cambridge University Press
[2] Mayer, R. E., (2009), Multimedia Learning", Cambridge: Cambridge University Press
[3] MacDonald, C. J. et al., Available at: https://elearnmag.acm.org/featured.cfm?aid=609737/, [Last accesseds 23 Novembar 2019]
[4] C. J. MacDonald, C. J. et al., (2001), The Internet and Higher Education, vol. 4
[5] Tomić, S., Efekti i induktivni karakter multimedijalnog koncepta elektronskog obrazovanja u Bosni i Hercegovini, 2017, (Doctoral dissertation, Sveučilište/Univerzitet Vitez, Vitez)
[6] Milas, G., (2009) Istraživačke metode u psihologiji i drugim društvenim znanostima, Zagreb
[7] Potode, A. and Manjare, P., „E-Learning Using Artificial Intelligence," *International Journal of Computer Science and Information Technology Research,* Vol. 3, no. 1, pp. 78-82, 2015.

Submitted: October 15, 2019
Accepted: November 24, 2019

About the authors

Siniša Tomić was born on October 10, 1972 in Doboj, Bosnia and Herzegovina. He is an assistant professor at the Faculty of Information Technologies at Panevropic University APEIRON, Banja Luka. His special interests are in computer multimedia and graphics, 3D animation and special digital visual effects.

Dalibor Drljača is a Ph.D. candidate at the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka and has MA in information technology and MA in technologies for the Development of European Projects. His main research interests are in e-Government, audit of information systems and e-Commerce. He is part-time engaged as a Senior teaching and research assistant at Pan-European University APEIRON Banja Luka and employed at the University Clinical Centre of the Republic of Srpska in Banja Luka.

For citation

Tomić S., Drljača D., DDLM - Quality Standard for Electronic Education Programs in Higher Education of Bosnia and Herzegovina, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:67-79, (UDC: 004.735.8:621.39(497.6), (DOI: 10.7251/JIT1902067T), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

ON POSSIBLE CRYPTOGRAPHIC OPTIMIZATION OF MOBILE HEALTHCARE APPLICATION

Goran Đorđević[1], Milan Marković[2]

[1]AET Europe, IJsselburcht 3, NL-6825 BS Arnhem, The Netherlands, goran.djordjevic@aeteurope.com

[2]Paneuropean University Apeiron, Banja Luka, Republic Srpska, Bosnia and Herzegovina, milan.z.markovic@apeiron-edu.eu

Critical Review

DOI: **10.7251/JIT1902080DJ** UDC: **004.056.55:621.39**

Abstract: The paper deals with a possible SOA based m-healthcare online system with secure mobile communication between patients and medical professionals with medical and insurance organizations. An example of an Android-based secure mobile client application is presented which can be used in the described secure m-healthcare model and it is experimentally evaluated. In the paper, we focus on possible optimization of cryptographic algorithms implemented in the secure Android mobile client application. The presented experimental results justify that security operations related to X.509v3 digital certificate generation and XML/WSS digital signature creation/verification are feasible on some current smart phones and justify the use of the proposed optimization techniques for implemented cryptographic algorithms.

Keywords: Secure Android Mobile Application, SOA, M-Healthcare, Digital Signature, Encryption.

INTRODUCTION

This paper is related to consideration of possible secure m-healthcare model and applying secure Android Web services based mobile client application in it. Overviews of possible secure systems based on similar model, secure JAVA mobile Web service application and SOA-Based central platform are given in [4], [5], [6], and [7] where the model is conceptually and theoretically presented and evaluated in domains of m/e-government and m/e-banking.

In this paper, as an extension of the previous work, a possibility of applying the similar model in domain of m-healthcare systems is considered. Additionally, a possibility of using the secure Android based mobile client application in the proposed m-healthcare model is considered and experimentally evaluated.

First, we consider a possible model of secure SOA-based m-healthcare online systems, i.e. about secure mobile communication between patients and/or medical professionals with the medical and healthcare insurance organizations for different purposes. This model could be considered in both local and cross-border case. The latter means either crossing borders of municipalities/regions in the same country or crossing borders between countries (e.g. some medical organizations in different countries).

As a main goal of this paper, we consider a possible usage of the Android-based secure mobile Web service client application in the proposed secure m-healthcare model. A feasibility of using such Android based secure mobile client application is experimentally evaluated in the paper. An emphasis is given on possible optimization techniques of cryptographic algorithms implemented on the Android platform. In this sense, we give two approaches of possible optimization of RSA private key operations. The proposed optimization techniques are experimentally verified in the paper.

The paper is organized as follows. Security requirements in m-healthcare systems are elaborated in Section 2. The architecture of the proposed m-healthcare model is proposed in Section 3. Information about some related work in literature is given in Section 4, while some features of the secure mobile client applictions are presented in Section 5. Proposed optimization cryptographic techniques are described in the Section 6. Experimental results obtained by the secure Android-based mobile client application is given in Section 7 while conclusions are given in Section 8.

Security Requirements in M-Healthcare systems

This Section deals with the basics of security mechanisms/requirements in m-healthcare systems. Key players in Healthcare systems are: medical organizations (hospitals, clinics, pharmaceutical organizations), insurance organizations, healthcare professionals (doctors, physicians, nurses, pharmacists, etc.), and patients – end users.

Most modern Healthcare systems are information systems based on TCP/IP computer networks and they work fast move toward the electronic business in Healthcare industry – electronic Healthcare (e-Healthcare). In this environment, security mechanisms for e-business must be implemented with necessary adaptation to the Healthcare environments. There are a lot of technical and security issues for these systems that include, between the others: electronic patient record or electronic health record (EHR) must be fully private, central database of patient electronic records must be enabled for use from all players (medical organizations, professionals, insurance, patients), privacy protection of the patient records, secure communications between all players in the system, electronic order entry, enabling mobile Healthcare, HIPAA compliance, etc.

Thus, security mechanisms that are necessary to be implemented in these e-healthcare systems are: strong user authentication procedure, digital signature technology, confidentiality protection of data in the system on the application, transport and network layers, privacy protection of the patient personal data, strong protection of the central healthcare database based on multiple firewall architecture, and PKI systems, which issues X.509 digital certificates for all users of the system (Healthcare professionals and patients) - digital identities (IDs) for the users.

However, with nowadays extreme penetration of mobile communications and usage of smart mobile phones/devices, earlier e-business models and systems move fast towards m-business models and systems. The same holds for e-healthcare systems and thus in this paper we considered, elaborated and experimentally evaluated a possible m-healthcare systems based on Secure Android based Web service mobile client application and SOA based Web service front end m-healthcare system. Some initial considerations of security requirements that need to be applied in the m-Healthcare systems are given in [8].

Possible Secure M-Healthcare model

The proposed secure m-Healthcare model, depicted in Figure 1, consists of:

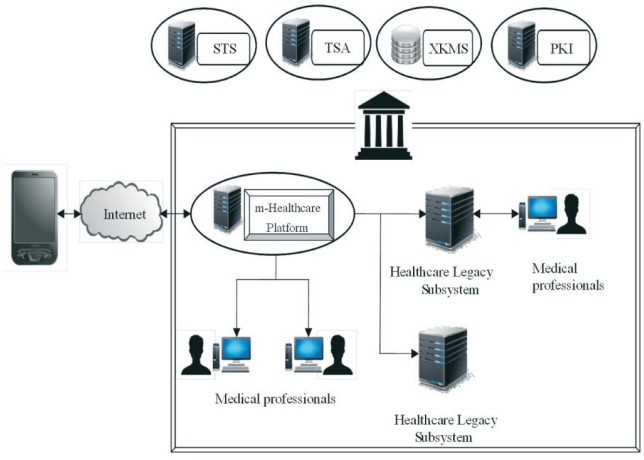


Figure 1: *A proposed secure m-healthcare model*

- **Mobile users** (patients, medical professionals) who send some Web services requests to m-healthcare platform for different purposes (sending some patient data to the central system, asking for some medical advices, checking some information about patients, checking insurance data, etc.). These users use secure Android mobile Web service client application on their mobile devices (mobile phones, smart phones, tablets, etc.) for such purpose.

- **SOA based Web service endpoint implementation** on the Platform's side that implements a complete set of server based security and business features. Well processed requests with all security features positively verified, the Web service platform's application proceeds to other application parts (i.e. legacy subsystems) of the proposed SOA-Based platform of the medical or insurance organizations.
- **External entities** such as: PKI server with XKMS server as a front end, the Authentication server, and TSA (Time Stamping Authority).

Functions of the proposed external entities are following:

- **PKI server** is responsible for issuing PKI X.509v3 electronic certificates for all users/entities in the proposed m-healthcare model (patients, medical professionals, administrators, servers, platforms, etc.). Since some certificate processing functions could be too heavy for mobile users, the PKI services (certificate location/validation) could be exposed by the XKMS server which could register users, as well as locate or validate certificates on behalf of the mobile user. This is of particular interests in all processes that request signature verification on mobile user side.
- **Authentication server (e.g. STS (Security Token Service))** is responsible for strong user authentication based on PKI X.509v3 electronic certificate issued to users and other entities in the proposed model. Possible communication between the authentication server and the user's mobile Web service application could be SOAP-based and secured by using WS-Security features. Possible scenario is that, after the successful user authentication, the STS server issues a SAML token to the user which will be subsequently used for the user authentication/authorization to the Web service of the proposed m-healthcare platform. The SAML token is digitally signed by the STS server and could consist of the user role for the Platform's user authorization. The alternative is that it could be a general-purpose Authentication server which will authenticate users by using any kind of authentication credentials, such as: username/password, OTP, PKI digital certificates, etc. In the latter case, there could be possible Web service based communication between the SOA-based central platform and the authentication server in order to authenticate users.
- **TSA server** is responsible for issuing time stamps for user's requests as well as for platform's responses (signed electronic documents). Time stamping of requests/documents could be requested from users, from the platform or from both entities.

Security operations in electronic business (e-government, e-healthcare, e-banking, e-commerce, e-payment, etc.) and mobile business (m-government, m-healthcare, m-banking, m-commerce, m-payment, etc.) systems are mostly based on two secure actions:

- Strong user authentication
- Transaction authorization

In the proposed model, the strong user authentication is based on the X.509v3 digital certificate as unique identifiers of users. Regarding the transaction authorization, it is based on digital signature of the electronic documents with additional usage of the timestamping. Since both choices represent techniques of the highest cryptographic level which are required in the Healthcare based systems, we believe that this model is the best suited for m-healthcare systems. Besides, in the proposed model, we use the encryption technique (WS-Encryption) in order to preserve confidentiality of information transmitted which represents an additional reason why this model is the best suited for m-healthcare systems.

Related Work

There are no many similar works in the literature. One work worth mentioning is the session based Web application system presented in [3]. Compared to a session based Web/application platform, presented in [3], in this paper we proposed a usage of the SOAP-based request-response technologies which is much better fitted to mobile environment. The model proposed in this paper could have the following advantages compared to the model given in [3]:

- Web service based request-response system is much more efficient system in the mobile environment than the session based Web application system. Especially when some back office processing (Healthcare legacy systems) are needed to respond on the user requests.
- Web service based model provides much more flexibilities and an easier way to implement all security features (e.g. XML security, WS-Security, Time Stamping, XKMS, PKI) compared to the Web based solution.
- Web service based system provides much more flexibilities compared to the session based Web application system in cross-border scenarios when business process includes also some processing of the user request outside of the contacted government organization.

Also, there are some conceptual discussions about security issues in the m-government systems, given in [2]. In this paper, we go further in experimental approving the usage of the secure Android mobile client application in the context of complex m-healthcare model presented in this paper.

Compared to the m-government system based on mobile qualified electronic signature in Austria (http://www.buergerkarte.at/langswitch.php?lang=en), where the mobile phone is used as a strong user authentication tool and where a server based signature is employed (user's private key is on the HSM on server side – generated and used), our proposed model is based on the „fat" client on the mobile user side where all cryptographic mechanisms are implemented in the Android based secure mobile client application. Thus, the system implemented in (http://www.buergerkarte.at/langswitch.php?lang=en) has emphasized on the authentication part of the security operations and for the transaction authorization it is implemented on the server side. In our model, both activities, strong user authentication and transaction authorization is done by using security mechanisms implemented in the mobile application.

Also, compared to some LSP (Large Scale Pilot) projects, e.g. STORK (https://www.eid-stork.eu/) and STORK 2.0 (https://www.eid-stork2.eu/), where some very complex interoperability authentication model is proposed, our proposed model could be more comprehensive and complete since the STORK models are mostly based only on user authentication mechanisms and their interoperabilities in cross-border usage. Unfortunately, there are no much discussions about possibilities of transaction authorization in the cross-border case.

Besides the above mentioned references, the authors of this paper could not find similar works in the literature related to m-healthcare systems based on Web services and Android clients. Thus, unfortunately, the presented experimental analysis does not contain a comparative experimental analysis to other achievements from the literature.

Secure Mobile Web Service Client Application

The proposed secure mobile Web service client application could comprise of following functionalities:

- **Graphical User Interface (GUI)** for presenting business functionalities to the end user. The GUI object of the proposed mobile Web service application is responsible to show user interface that enable calling of function for authentication of the end user and presenting the core functionalities to the end user. According to this, the GUI object communicates with following modules:
- User Authentication module for mobile client application of the Security module
- User PKI Registration module (XKMS module) of the Security module
- User Authentication and Authorization module for the m-government platform (SAML module) of the Security module
- Business functionalities
- **Business (core) functionalities** of the application – m-healthcare functionalities. Business functionalities have links to Security and Communication modules of the secure mobile Web service application.
- **Security functionalities.** The Security module of the considered secure mobile Web service application is responsible for overall application-level security functionalities.
- **Communication.** The communication module is responsible for establishment of secure communication between patients and medical/insurance organizations.

The security functionalities of the proposed Secure Android Mobile Client application consist of the following modules:

- **Authentication module** of the secure mobile application. User authentication for the secure mobile application should be two-step process:
- The first step would be a combination of username/password for accessing the application (password should be changeable by the user). This should be done immediately after the application starts. These credentials will be generated during the user registration process. During the initial phase of the registration application, the user will obtain the username and default password. The application has to force the user to change the initial password on the first application start.
- The second step will be in presenting a corresponding PIN code for accessing the asymmetric private key just before digital signing different m-healthcare requests.

The generation of user asymmetric public/private key pair and corresponding digital certificate should be done through user registration function of the XKMS protocol. The User Authentication module is called from the GUI object.

- **XKMS module.** XML Key Management Specification enables to simplify the use of PKI by mobile client systems.
- **STS module.** The STS module is responsible for the communication with the STS server in order to receive a SAML assertion (token) that will be used afterwards to enable access to the business functionalities by the client. The user first sends a RequestSecurityToken message to the STS (Security Token Service) server by using a SAML protocol. A protection is done by using WS Security mechanisms. After successful authentication of the user based on the client's X.509v3 digital certificate, the STS server issues a SAML token to the user which is digitally signed by the STS server. This token is securely communicated to the end user by using the WS security mechanisms.
- **XML security module.** XML security module is responsible for implementation of standard XML signature and XML encryption components. XML security module consists of:
- Implementation of the RSA private key operation for creating digital signature, as well as a function for signature verification.
- Implementation of hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512).
- Implementation of different symmetrical cryptographic algorithms (3DES, AES).
- Implementation of the RSA private key operation for decryption of encrypted symmetric message key in digital envelope.
- Implementation of the RSA public key operation for encryption of symmetric message key in digital envelope.
- **WS-Security module.** Web Service (WS) Security module is implemented as standard security mechanisms for protection of SOAP messages. WS-Security module is very important module of the Security module since it is used for protection:
- Communication with STS server.
- Communication with the proposed SOA-Based m-healthcare platform.

This way, the WS-Security module communicates with SAML module of the Security object as well as with Business functionalities object. The SAML module communicates with WS security module of the Security object as well as with the Communication object.

- **Time-Stamping module.** This module is responsible for communication with the TSA. A time-stamping service supports assertions of proof that a datum existed before a particular time. The user's application requests a timestamp token by sending a request to the TSA. As the second message, the TSA responds by sending a response, i.e. actual timestamp, to the requesting entity.

The secure mobile Web service application could secure communicate with all mentioned external entities in Section 4, i.e. it has all security functions mentioned implemented:

- Secure mobile Web service application sends Request for Security Tokens to the STS server by using WS-Secured (WS-Signature and WS-Encryption) SOAP communication.
- Secure mobile Web service applications sends digitally signed (XML signature) m-healthcare request to the Web service of the proposed m-

healthcare platform by using WS-Encrypted SOAP communication. The sent request includes the SAML token issued and signed by the STS server.
- The request is timestamped by sending a timestamp request and obtaining the corresponding timestamp response (digitally signed by the TSA).
- The secure mobile Web service application also receives the signed and timestamped response from the m-healthcare platform through WS-Encrypted communication and performs all necessary signature verifications and certificate validations (by help of the XKMS server) actions.

Optimization of Cryptographic Algorithms in Secure mobile Web Service Client Application

The Android platform ships with a cut-down version of Bouncy Castle - as well as being crippled. It also makes installing an updated version of the libraries difficult due to class loader conflicts. Different versions of Android operating system have implemented different versions of Bouncy Castle library releases. In order to avoid lack of interoperability between different devices that have implemented different operating systems and get more flexible code we used Spongy Castle functions (http://rtyley.github.com/spongycastle/). A simplified package structure of the Spongy Castle package is illustrated in Figure 2.

The Spongy Castle package contains low-level lightweight API implementing all the underlying cryptographic algorithms and a provider for the Java Cryptography Extension (JCE) and the Java Cryptography Architecture. The basic package that supports the cryptographic algorithms and padding schemes is the org.spongycastle.crypto package. The org.spongycastle.asn1 package supports the parsing and writing ASN.1 objects, which is useful in processing X.509 certificates. The utility classes in org.spongycastle.util can be used for producting and reading Base64 and Hexadecimal strings. The utility is useful if the ciphertext is required to be displayed as a Base64 string.

In order to achieve smaller and faster implementation we have partly modified Spongy Castle functions. The modification of Spongy Castle funtions is achieved in org.spongycastle.jce package. We don't want to use JCE functionalities of genuine Spongy Castle implementation because that adds a significant memory overhead. In order to avoid using the heavyweight provider for the JCE that contains implementation of many unnecessary functions we cut off a lot of functions and implement only the necessary ones. We directly call necessary Spongy Castle functions without using java.security.Provider functionalities at all. Using this approach we got smaller and faster code.

Because mobile devices have limited resources, an application designed for mobile devices should be as compact as possible. An obfuscator is a useful tool for minimizing the size of an application. We used

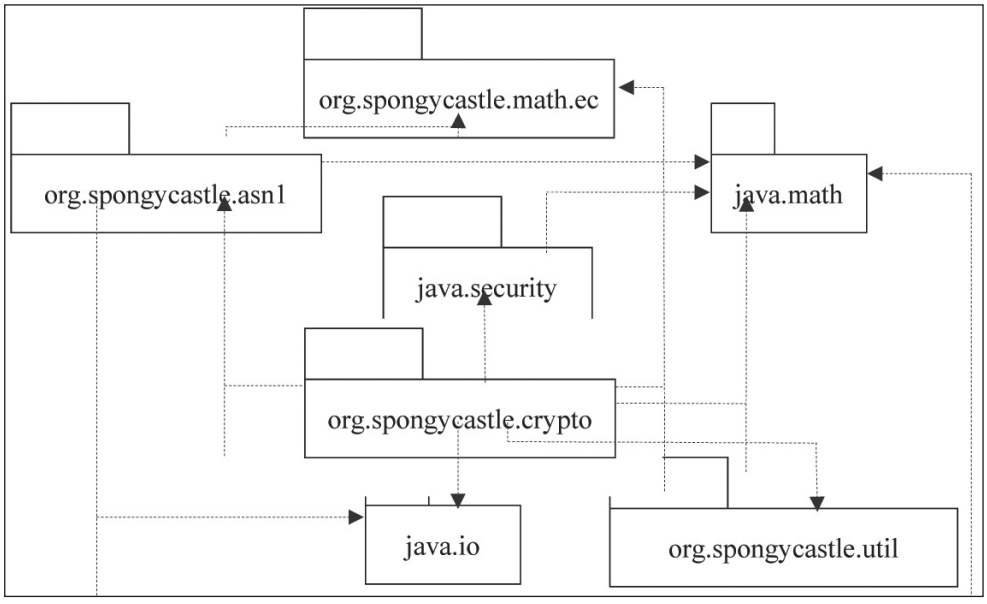


Figure 2: *Lightweight Spongy Castle API Package structure*

ProGuard obfuscator that shrinks, optimizes, and obfuscates code by removing unused code and renaming classes, fields, and methods with semantically obscure names. The result is a smaller sized .apk file that is more difficult for being reversely engineered.

In order to addionally improve performanse we have considered possibility of implementation of private key RSA operations (creation of digital signature, open digital envelope) using native code in Android Native Development Kit (NDK). A basic reason for this decision was a fact that the native code is compiled to binary code and run directly on mobile phone OS. We implemented native code on a basis of usage of OpenSSL package. In this case, a lot of cryptographic functions are implemented using C programming language. In order to additionally speedup operations with RSA private key we implemented some functions directly in assembler code. One of implemented functions in assemler code is procedure of Montgomery modular multiplication. Montgomery multiplication is a method for computing $a*b$ mod m for positive integers a, b and m. It reduces execution time on a CPU when there are a large number of multiplications to be done with same modulus m, and with a small number of multipliers. In particular, it is useful for computing a^n mod m for a large value of n. The number of multiplications modulo m in such computation can be reduced to a number substantially less than n by successively squaring and multiplying according to the pattern of the bits in the binary expression for n ("binary decomposition").

Experimental Analysis

This Section is dedicated to the experimental analysis of the cryptographic operations implemented on Android mobile phone, i.e. smart phones with Android operating system [9], as a possible example of the proposed secure mobile client application that could be used in the proposed m-healthcare model. Also, the proposed model and presented experimental results on Android mobile operating systems represent m-healthcare extension compared to the discussion presented in [1]. The presented experimental results are generated using devices (mobile phone, tablet, PC laptop and PC desktop) described in [7].

Experimental results that are presented in this section are based on the modified version of Spongy Castle functions as well as partly modified version of OpenSSL native code. In Tables 1, 2, 3, 4, a row with title 'Native code' is shown with results where operations with RSA private key are done by using native code (C code + assembler). During testing phase we have measured average time by using some number of iterations. The actual number of iterations used are shown in each table. The same code and packages are used during testing procedure in all devices. Throughout this Section, all presented experimental results are given in miliseconds – ms. In order to evaluate the possibility of using the mobile phone for secure mobile Android-based client application in m-healthcare systems based on Web service we measured times needed for creation X509 v3 self-signed certificate comprising a creation of PKCS#10 certificate request (Table 1). As a signature algorithm we used SHA-1 hash algorithm and RSA asymmetric cryptographic algorithm. Then we measured time for creation of XML-Signature and Web Service (WS) Signature (Table 2, Table 3), respectively. In all these experiments, we used a file of 1KB, RSA asymmetric algorithm and SHA-1 hash function. We also analyzed possibility of WS Decryption mechanisms (Table 4).

Some observations of the presented experimental analysis are:

Table 1: *Create X509 v3 self-signed certificate*

Device 512		RSA private key length (bits), n=50000 iterations				
		1024	2048	3072	4096	
Mobile Phone	SpongyCastle	18.11	27.41	84.41	216.89	467.95
	Native code	13.48	21.26	73.48	206.53	426.34
Tablet		34.49	46.27	116.05	283.22	548.40
PC Laptop		1.78	9.01	58.07	180.97	414.14
PC Desktop		1.33	6.78	43.92	137.36	312.90

Table 2: *XML-Signature creation*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	29.64	38.15	95.87	228.20	479.10
	Native code	25.01	32.01	84.94	217.84	437.49
Tablet		59.73	73.78	144.08	319.65	586.54
PC Laptop		2.12	9.38	58.50	181.54	414.74
PC Desktop		1.57	7.05	43.85	137.87	312.79

Table 3: *WS-Signature creation*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	63.76	74.51	131.00	266.29	507.47
	Native code	59.13	68.36	120.07	255.93	465.86
Tablet		126.99	147.68	216.81	384.48	663.93
PC Laptop		2.79	10.07	59.18	182.1	415.19
PC Desktop		2.02	7.50	44.57	138.03	311.66

Table 4: *WS-Decryption mechanism*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	34.96	44.20	102.48	232.75	486.20
	Native code	30.33	38.05	91.55	222.39	444.59
Tablet		80.91	119.74	169.87	339.54	609.42
PC Laptop		2.41	9.67	58.88	181.79	415.98
PC Desktop		1.77	7.28	44.36	138.01	313.88

- The creation of the self-signed X.509v3 digital certificate with 2048 bits key by using the mobile phone takes 84.61 ms and even 73.48 by using optimized native code which is similar to the results obtained by PC computers.
- The operation of digital signature of XML message (XML-Signature and WS-Signature mechanisms), using 2048-bit private RSA key, takes on mobile phone 95.87 and 131 ms, respectively, and in optimized native code version 84.94 and 120.07 ms, respectively, which are comparable to the results obtained by other devices..
- The operation of decryption of WS-Encrypted message using 2048-bit private RSA key, takes 102.48 ms and in the optimized native code version 91.55 ms. It means that in one second can be implemented about 10 operations of decryption WS-Encrypted message using 2048-bit RSA private key.

These observations could lead to the conclusion that mobile phone could be used in real time for implementation of RSA private key operations in times comparable to the ones obtained on PC computers, especially when the optimized native code is used.

Conclusions

In this Paper, we presented an overview of possible secure model of m-healthcare systems as well as an analysis of possibility and feasibility of using secure Android-based web service mobile client application in it.

First, this paper is related to the consideration of some possible SOA-based m-healthcare online systems, i.e. about secure mobile communication between patients and medical professionals with medical and insurance organizations.

Second, the paper presented a possible example of an Android-based secure mobile client application that could be used in the described m-healthcare model and which is experimentally evaluated. An emphasis is given on possible optimization techniques of cryptographic algorithms implemented on the Android platform. In this sense, we give two approaches of possible optimization of RSA private key operations. The proposed optimization techniques are experimentally verified in the paper

Presented experimental results justify that security operations related to RSA private key operations (creation of X.509v3 digital certificate, XML/WS digital signature, WS-Encryption) are feasible for usage on some current smart phones. Thus, we could conclude that this application could serve as a basis for implementing secure m-healthcare system based on the model described in this paper. Also, presented experimental analysis justifies the usage of the proposed optimization of cryptographic techniques implemented on a basis of C and assembler code.

REFERENCES

[1] Braga, A. M., Nascimento, E. N.: Portability Evaluation of Cryptographic Libraries on Android Smartphones, Cyberspace Safety and Security, Lecture Notes in Computer Science, Volume LNCS-7672, 2012, pp 459-469.

[2] Kumar, M., Hanumanthappa, M., Reddy, B. L.: Security Issues in mGovernment, H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.), ICGeS 2008, CCIS 12, pp. 265-273, 2008, Springer-Verlag, Berlin Heidelberg, 2008.

[3] Lee, Y., Lee, J., Song, J.: Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. Computer Communication. 2007. 30 (4): 893-903.

[4] Marković, M., Đorđević, G.: On Possible Model of Secure e/m-Government System. Information Systems Management. Taylor & Francis Group, LLC. 2010. 27:320-333.

[5] Marković, M., Đorđević, G.: On Secure SOA-Based e/m-Government Online Services, in Handbook "Service Delivery Platforms: Developing and Deploying Converged Multimedia Services", (pp. 251 – 278, Chapter 11), Taylor & Francis, 2011.

[6] Marković, M., Đorđević, G.: On Secure m-government and m-banking model, in *Proc of 6th International Conference on Methodologies, Technologies and Tools Enabling e-Government*, July 3 – 5, 2012, Belgrade, Serbia, pp. 100-111.

[7] M.Marković, G.Đorđević: Secure Android Application in SOA Based Mobile Government Systems, in Proc of 7th Int. Conference on Methodologies, Technologies and Tools Enabling e-Government, Luis Alvarez Sabucedo and Luis Anido Rifon (Eds.), Oct. 17 – 18, 2013, Vigo, Spain, pp. 117-126.

[8] Marković, M., Savić, Z, M., Kovačević, B.: Secure Mobile Health Systems: Principles and Solutions, chapter in the book *M-Health, Emerging Mobile Health Systems*, Series: International Topics in Biomedical Engineering Istepanian, Robert; Laxminarayan, Swamy; Pattichis, Constantinos S. (Eds.) 2006, XXX, 624 p. 182 illus., Hardcover, ISBN: 0-387-26558-9, pp. 81-106.

[9] Reto Meier, P.: Professional Android 4 Application Development, John Wiley & Sons, Inc., Indianapolis, Indiana, 2012.

Submitted: October 18, 2019
Accepted: December 3, 2019

ABOUT THE AUTHORS

Goran V. Đorđević was born 1972 in Novi Sad, Serbia. He received a BSc in Computer Science at the Technical Military Academy in 1996. Afterwards he did his post-graduate studies, at the Faculty of Electrical Engineering of University of Belgrade where he received a MSc. Currently employed as a senior software developer in AET Europe. His main areas of interest are smart card security and smart card applications, security protocol design, mobile devices, tokens, Internet of Things and information security.

Milan Marković received B.S.E.E., M.S.E.E., and Ph.D. degrees in electrical engineering from Faculty of Electrical Engineering, University of Belgrade, Serbia, in 1989, 1992, and 2001, respectively. He is an Associate Professor on College of Information Technology, Pan-European University of Apeiron in domain of information security courses. His research interests are mainly in public key infrastructure, information security, cryptographic algorithms, mobile security, identity management, secure e/m-banking and e/m-government, trust services, ISMS, Blockchain, etc. He has published more than 320 scientific papers.

FOR CITATION

Đorđević G., Marković M., On Possible Cryptographic Optimization of Mobile Healthcare Application, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:80-88, (UDC: 004.056.55:621.39), (DOI: 10.7251/JIT1902080DJ), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

New Approach of Storing and Retrieving Large Data Volumes

Nedeljko Šikanjić[1], Zoran Ž. Avramović[2]

[1]*PhD student at Pan-European University Apeiron, Banja Luka, Bosnia and Herzegovina*

[2]*Pan-European University Apeiron, Banja Luka, Bosnia and Herzegovina*

A General Survay

DOI: **10.7251/JIT1902089S** UDC: **004.6:658.4]:519.8**

Abstract: In today's world of advanced informational technologies, society is facing a huge amount of data that is just getting impossible to store, process and analyze. In these big data volumes, some of the important information is being lost, that could help us improve the quality of personal and business life. This paper focus is on finding the best possible way of approaching this issue to find a feasible solution in increasing the efficiency and quality of data.

Keywords: Data Warehouse, Data Lake, Lambda architecture.

Introduction

When it comes to every day of people's lives, including the social and business perspective of it, it generates various types of data every second. The internet, different tracking and transaction logs, various documents, emails, numerous business applications such as ERP or CRM, IoT systems and devices, they all produce a high volume of data. In this data, is hidden right information for the right process, which might be used depending on the need of the system, organization or person. In this paper analysis is made on the existing solutions, their benefits, and their faults or disadvantages, to find a better approach or solution for coping with a large volume of data.

Data Warehouse

When people think about structured data, the first thing that comes in mind is data warehouses. This approach with data warehouses is since the 1990s emerged as a need to have a solution for storing a large volume of data. William H. Inmon has created the term data warehouse and contributed to creating and developing data warehouse architecture [9].

The data warehouse is well known for its structured data and schema. The schema represents the way of how data will be grouped and organized, including a well-structured hierarchy. In this way, we have the benefit and disadvantage of knowing before time what data and in what format the data will be stored. These data warehouses are optimized for reading in terms of query performance, and therefore it is a performance-based big advantage in using these data warehouse systems. When we compare with transactional database models (OLTP), in data warehouses it is being used as an analytical model approach (OLAP) where the reading of data is a key factor.

This data warehouse for storing large volumes of data approach was good enough but just for a time being as information society developed, so did data also. We are faced with different types of data coming in like data from IoT (internet of things), social media data that was well unstructured, so this has

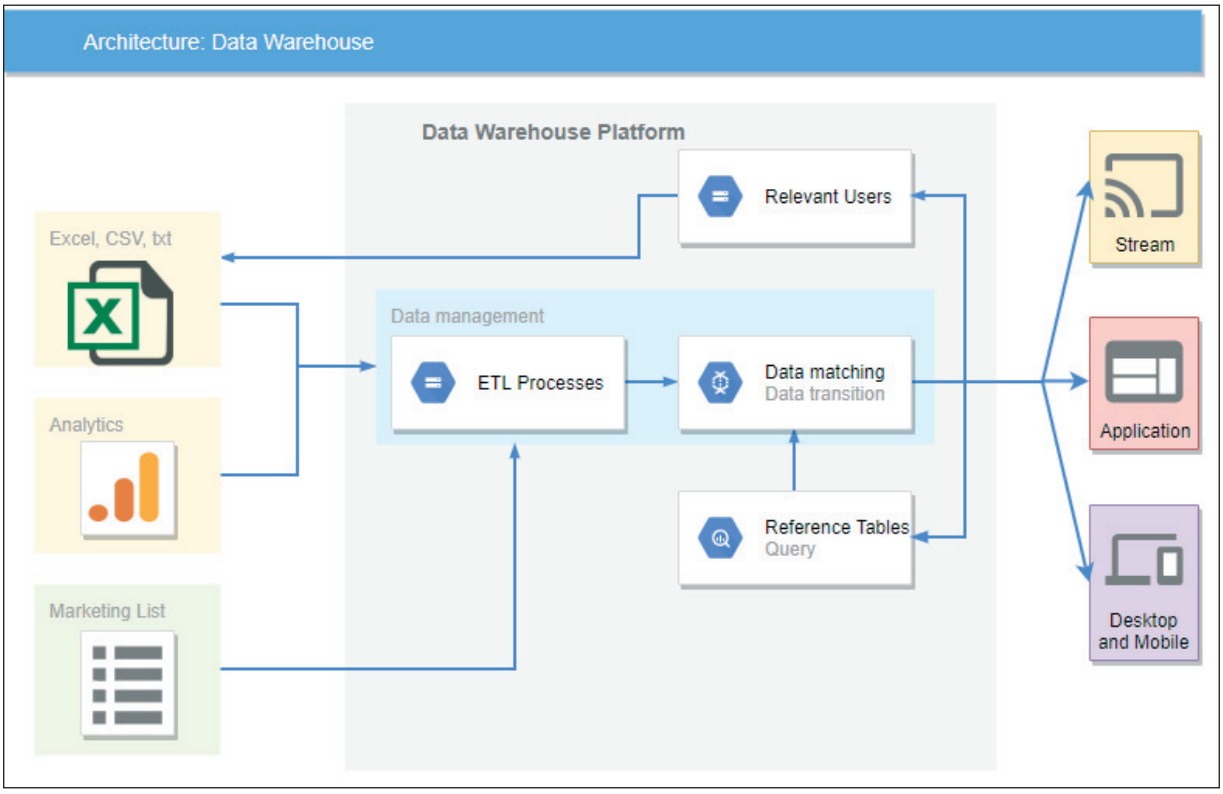


Figure 1. *Data warehouse architecture*

imposed huge pressure on existing data warehouse in order to cope with this kind of new data.

The benefit of the data warehouse is that has proven itself on the market for a long time, that human resources are well-skilled, that is has matured over time in the term of stability and reliability. Performance is another key aspect of the data warehouse as it is based on good structure and great query engines that are fully optimized for reading and are supporting various incremental changes of the data. Another great characteristic is usability as users may not be familiar with how to get information from source data, but with the analytical approach of the data warehouse, users can by transforming, filtering or slicing the data to find the information they need. In this way, users are getting a single source of data, instead of matching various sources of data, trying to find the information they are looking for. With the coming of cloud services, data warehouse systems are very well adapted to new technology in this way, where we have the flexibility of having on-premise or in the cloud the data while keeping this architecture.

Speaking of some of the downsides of data warehouses, we must mention storage cost as this kind of data model or data architecture is requiring lots of storage resources. As we already have explained the benefit of reading time, that does come with a certain price in terms of time. Time is required by preparing the processes and components that are needed in order to pre-structure the source data that is coming into the data warehouse. As we know what structure of data we are looking for, we might lose some data that could be useful in the long run, as we remove this data in ETL (extract, transform, load) processes. Another disadvantage of the data warehouse as it is not designed for the large volume of various data or better known as big data that includes the internet of things and social media for example.

DATA LAKE

The other competitor in storing large data volumes is data lake. The first term of data lake was introduced by James Dixon, where he has compared data lake as a large whole of water stored in a natural state [2]. This concept was created as it was noticed that only part of data has been visible and processed, as data has attributes that are predefined and after data is aggregated, subset levels of data are not seen

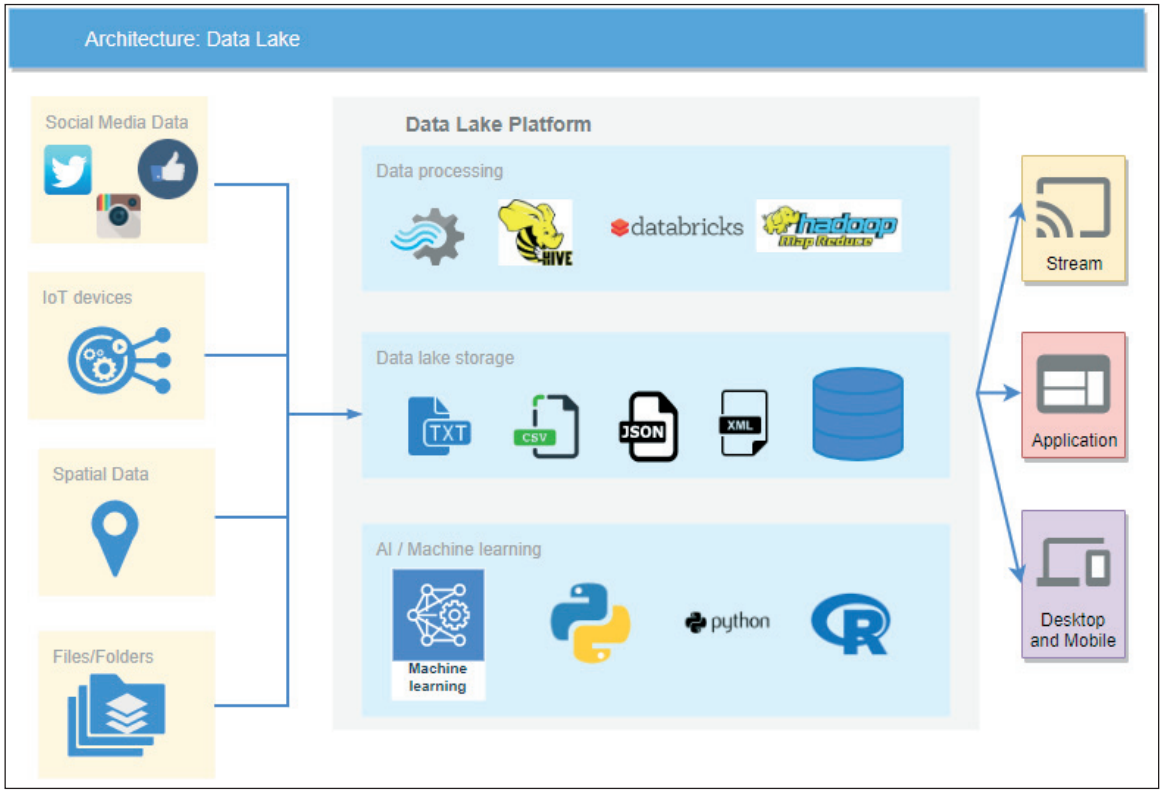


Figure 2. *Data lake architecture*

more. In order to keep all the data, we have or generate, with data lake we will keep them in their original form, and then we will introduce the processing of data we require in that specific moment.

When it comes to the data lake, the big advantage is that we can store all kinds of data in it. For example, we can store structured data, semi-structured of unstructured data. Here we don't have a predefined schema, so it means that we can put or save data in its raw format, without losing any time on preparing the data for storing. Because of this, we don't have a data model in the term of transactional or analytical only, but it is more organized in the way of storing data based on different types of data that we are trying to save in the data lake.

If we would like to make it sounds simplified, we could say that it would be enough to store our data into date lake and at end of the process, we could have some sort of reporting or analysis services, that would be responsible for a representing the data at our end users or clients.

However, there is, of course, more refinements that would need to be implemented, such as security and data governance, to have a sustainable and reliable solution for managing our data.

Some of the disadvantages of data lakes that we need to mention are human resources with skills that are needed to process this data within the data lake environment, then there is an issue with knowing how this data flow will fit in within the organization, that is implementing this approach or has already a data warehouse processes established. Also, as a benefit of saving the data results in low cost in storage, the downside is that will increase the performance cost of implementing the complex queries on the data from the data lake.

Proposed Solution

In most cases, it is not a question if it is an only data warehouse or a data lake approach, but it is determined on the need for the project or organizational infrastructure.

The best approach to have a full potential of both data implementation solution is an integration of both systems in a hybrid solution. With this approach, we can leverage the full capabilities of storing large sets of data while preserving the functionality of data processing, data quality and securing the data.

Here we will analyze the approach of ETL (extract-transform-load) and ELT (extract-load transform).

ETL is a process where is most common when we know what structure we have forehand, so in this way, we can prepare data for the questions we already know to provide the answer.

For the ELT process, it works perfectly in the environment where we want to take advantage of data, which we would like to find answers to the questions that might come up in the future.

For some approaches, we can use a combination of machine learning and artificial network algorithms [4] to automate processes.

LAMBDA APPROACH

Lambda architecture [3] is data processing architecture created on the need of speeding up the processing of data regarding large data volumes or big data implementation. When using the data processing algorithm, we will put data coming in batches. This means that this data will be grouped so we can then try to set some operations based on these batches of data, to get information from this data. Once we get data in batches, we will try to query the data. However, we have some batches of data finished and ready for processing but data that are still coming in are in the middle of preparing batches. This means that we are missing this data in real-time. This is the moment when we implement streaming. Streaming data means that we will take the same data that are coming into batches and make it available for the querying. After the corresponding batch is finished with the processing of data, we will clear the data list that is in the streaming process, to prevent duplication of the data.

Table 1. *Simplified Lambda process flow*

Input data	Batch	Output data
	Speed	

To implement the best practice approach, we will try using lambda processing data flow.

In our sample test case, we will have sample data from the AirVisual meteorological web site. Here we will use data that we will stream into our data lake and then we will process it to see the behavior of the proposed system. For the tools used in this test case, we will use a Microsoft Azure cloud platform, as this is one of the fastest growing online cloud platforms that supports various big data systems and big data platforms.

So, once we get data inside of our system, we will store this data into the data lake store. Data lake store is based on HDFS (Hadoop Distributed File System). Data will be distributed on more nodes, which means that we will have more copies of our data and access to it will be faster because this approach supports the parallel reading of data.

For the batch process, where we process our data, we will use a new approach with U-SQL [8] procedural language. This language is a new way of supporting unstructured data. It is a mixed technology approach of supporting C# programming language and a standard SQL language. Based on our needs we can transform the data in structured data, or we can output it also as unstructured data. This approach gives great flexibility in serving data to the end-users. The component that we will use is called data lake analytics.

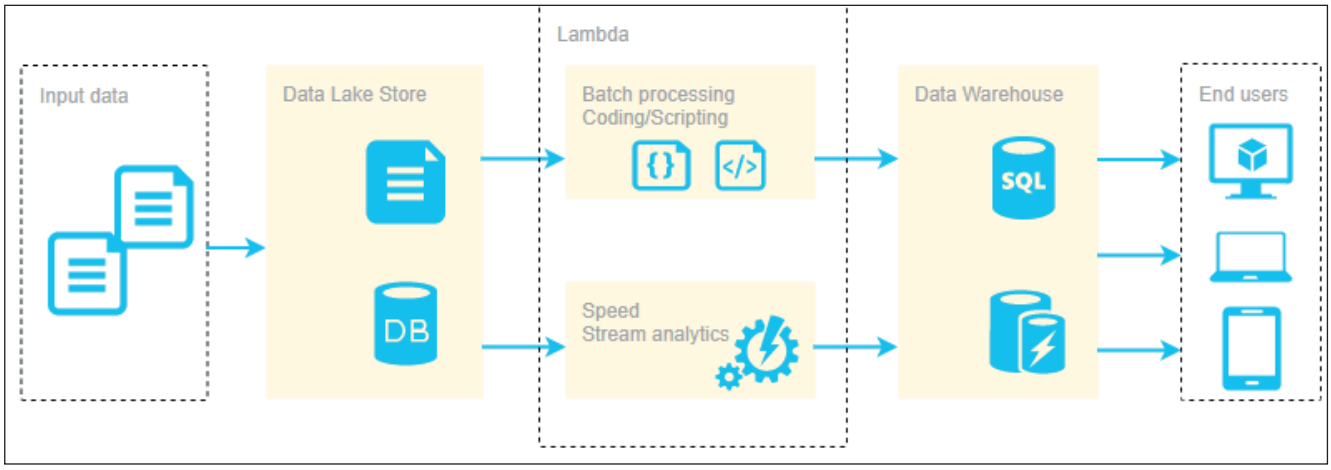


Figure 3. *Diagram of Lambda architecture with data lake and data warehouse*

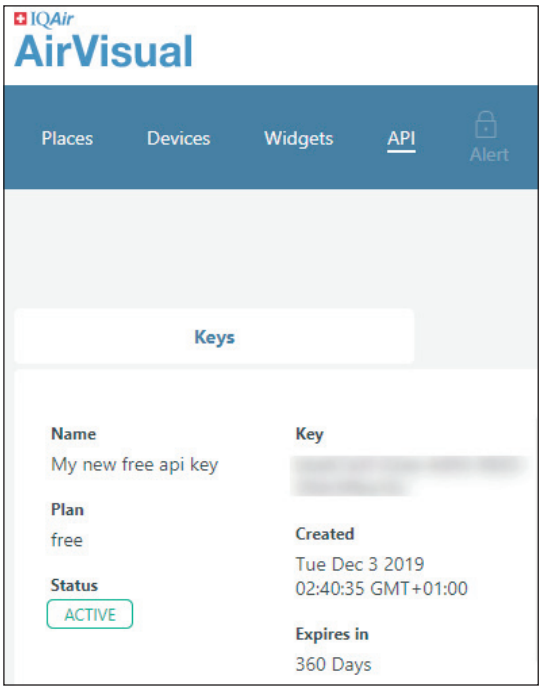


Figure 4. *AirVisual credential page*

For the speed layer, we will use the streaming analytics component, as this is excellent in terms of supporting standard SQL language, supports vertical partitioning and can write to more than one output at the same time.

Before we send data to the users, we will use the data warehouse component, as this is where our end data will be processed and stored. This represents a combination of two different systems we try to combine, to have the best result from both data systems [5].

To implement this solution, we will first set up an event hub, which will act as an IoT input point, which will receive information from the AirVisual website.

First, we test the API of AirVisual, so we are sure to set the right call from the event hub using an API testing tool.

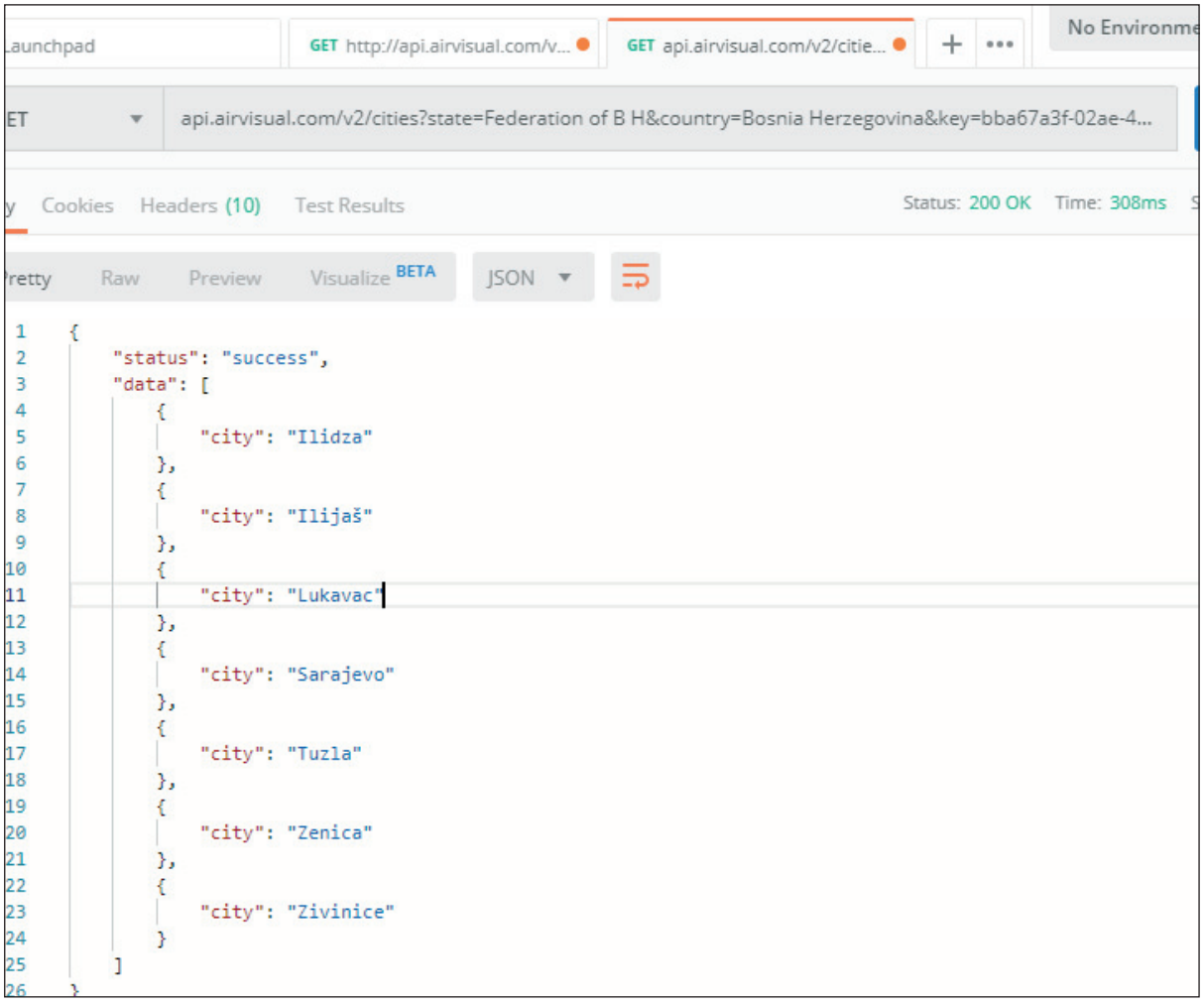


Figure 5. *Data structure of response from Web API*

After having an input data source, we will set up a streaming job, where we set a source for our streaming job.

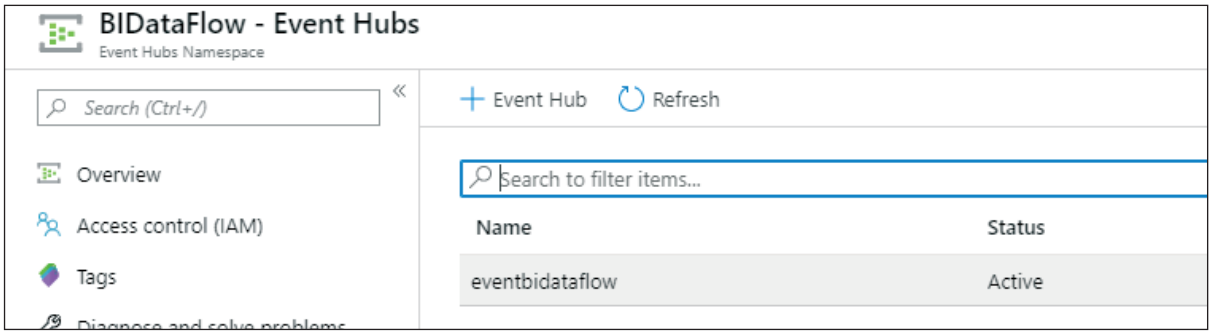


Figure 6. *Event Hub for data input*

For each of our data sources, we will set the output of this component to a data lake store.

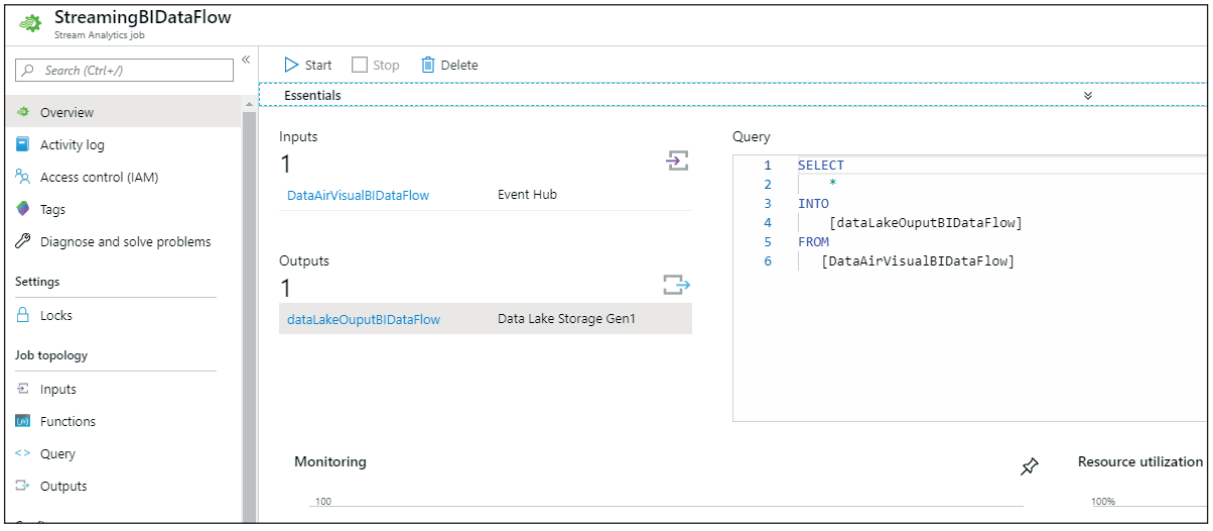


Figure 7. *Streaming analytics for speed layer*

For the batch processing, we will use a data lake analytics, where we will be doing the processing of our data. At the end of each processing of data, we will be having an output flat files, in this case in CSV (Comma-separated values) format.

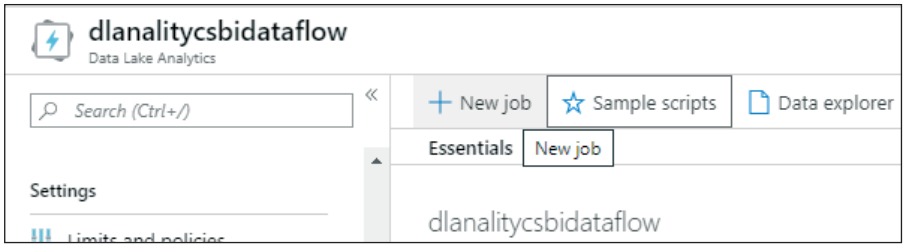


Figure 8. *Data lake analytics for batch processing*

Just go a little bit back to our first step of loading the data, let's examine the data we are interested in. This important to show how we integrate this into the existing lambda architecture we have created. The data is coming in JSON (JavaScript Object Notation) format.

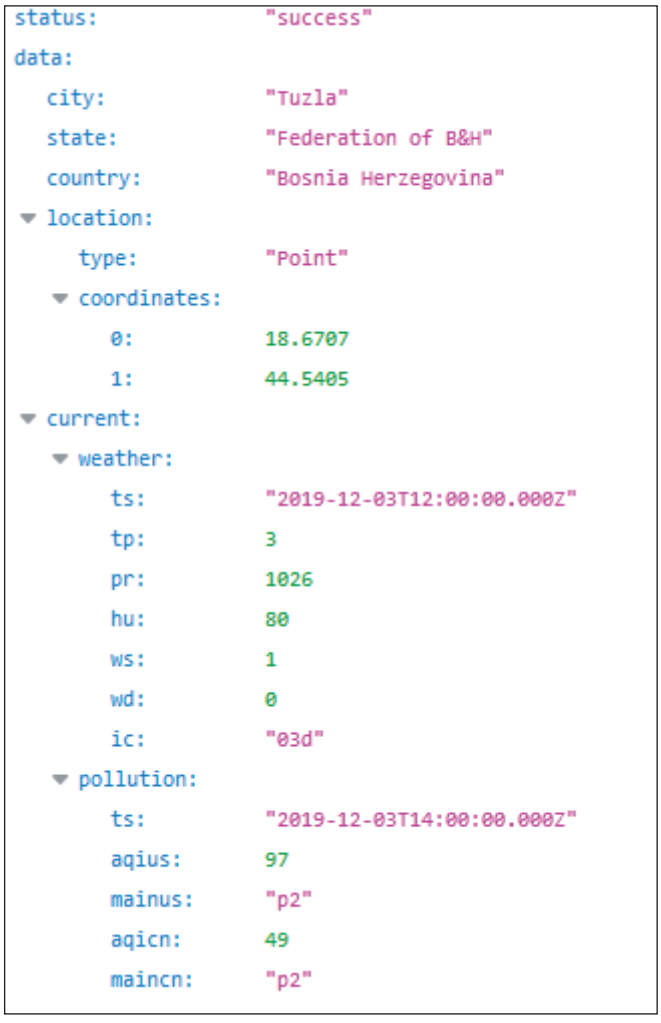


Figure 9. *JSON structure of raw data*

So, as we can see on the JSON result above, we need to have a value for pollution "aqius" - AQI value based on US EPA standard [6]

Based on this data, we have structured our U-SQL query as it follows:

```
DECLARE @InputDirectory string ="/SourceData/{FileName}.csv"; //source files
DECLARE @OuputDirectory string = "/OutData/Polution.csv";     //output file

@RawData=
    EXTRACT City string,
                Aqi int,
                TS DateTime
FROM @InputDirectory
    USING Extractors.Csv(skipFirstRows:1);

@OutputData =
    SELECT City,
           SUM(Aqi) as TotalAQI
    FROM @RawData
    GROUP BY City;
OUTPUT @OutputData TO @OuputDirectory USING Outputters.Csv();
```

Figure 10. *U-SQL for batch processing*

When it comes to the data warehouse, we will be using a tool called PolyBase [1]. With the PolyBase approach, we will set the source of our queries using a table that is dynamically connected with underlying flat files. Then we can use a query that we can use to merge the results from these outputs of batch processing and speed processing, following a lambda architecture design process flow.

As we are doing implementation on the Azure platform, we are using an Azure Synapse Analytics (formerly known as SQL Data Warehouse). When working with the Cloud applications, then security is one of the key prerequisites. We will be setting an OAuth2 authorization framework [7] as this is the best security option when working with cloud applications and web applications in general.

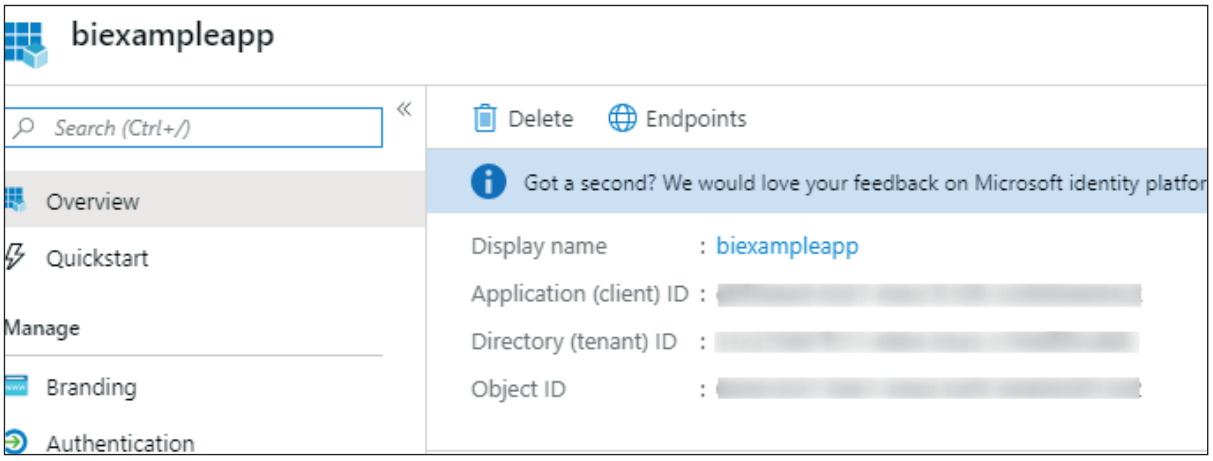


Figure 11. *OAuth credential generation*

Then it is quite straightforward to implement these credentials within our data warehouse.

```
create database scoped credential azureDataLakeCredential
with
identity='                                    2@https://logi
secret='f                                     T';


create external data source DataLake
with (
type=hadoop,
location='adl://datalakebidataflow.azuredatalakestore.net',
credential=azureDataLakeCredential
)
```

Figure 12. *Usage of generated OAuth credentials*

What is important to know, that we can separate the level of access to individual objects into the data lake. We can allow read to some objects as CSV files in our case and we can even allow higher-level permissions, depending on the scenario we would like to implement. This resembles in granular functionality where we can have great control over the security in general.

Here we see the implementation of the PolyBase data lake source file query, where we propagate the location on to the Hadoop system. With this approach, we can use a data warehouse as a central point for the serving layer in our lambda architecture.

Based on this we will get data to the end-users. We can use various tools to analyze this data and excel

```
create external table dbo.SpeedProcess
(
CityName nvarchar(100),
AQI int,
MAINS int,
AQICN int,
MAINUS nvarchar(2),
MAINCN nvarchar(2),
dateTS nvarchar(100)
)
with
(
location='SourceData/AllAirPolutionInputData_20191125_151606.csv',
data_source=DataLake,
file_format=csvfile,
reject_type=Value,
reject_value=0
)

SELECT
cityName,
case when AQI<=50 then 'Good'
when AQI between 51 and 100 then 'Moderate'
when AQI between 101 and 150 then 'Unhealthy for Sensitive Groups'
when AQI between 151 and 200 then 'Unhealthy'
when AQI between 201 and 300 then 'Very Unhealthy'
end as DegreeOfPoluttion,
AQI,
datets as DateCollected
FROM
(
select cityName, AQI, dateTS from dbo.BatchProcess
union
select cityName, max(AQI) as AQI, dateTS from dbo.SpeedProcess
GROUP BY cityName,dateTs
) as t
```

Figure 13. *Server layer output query with data lake and data warehouse*

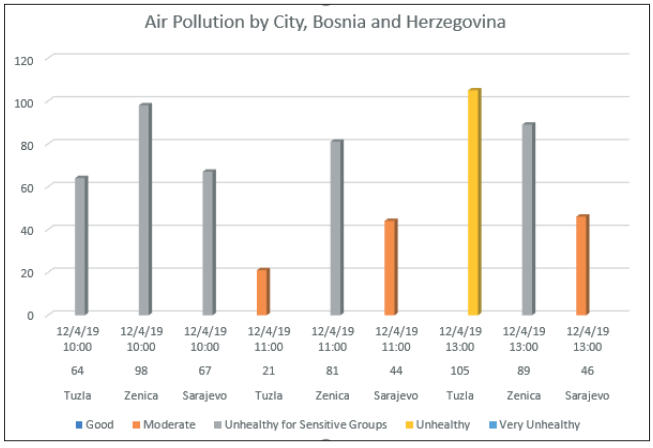


Figure 14. *Reporting analytics for end users*

with data connectors presents a powerful solution as it is easy to use and rich with data analyzing features.

As it can be seen from the graph, here is shown data that is coming simultaneously and data that is being processed in batches. This way, we don't miss out on the data while waiting for being processed and served to the client or user service.

Conclusion

This paper has shown how to implement the approach of lambda architecture into the latest technologies while combining the best features from big data and standard database models. Presented re-

search explains how advanced it is possible to go in the term of getting the most out of the data processing while keeping data integrity and minimizing the time of response, from the input data to the serving the data to the end-users. Also, as people as a society in general, are moving into cloud and internet applications in every segment of everyday lives, this paper has demonstrated how to implement big data solutions in terms of data consistency while keeping the focus on the security as one of the important factors as well.

REFERENCES:

[1] Benjamin Weissman, "PolyBase in SQL Server 2019 – The End of ETL?", https://www.red-gate.com/simple-talk/sql/data-platform/polybase-in-sql-server-2019-the-end-of-etl/ (accessed on 23.10.2019)

[2] James Dixon, "Pentaho, Hadoop, and Data Lakes", https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/ (accessed on 28.09.2019)

[3] Nathan Marz, "Big Data: Principles and best practices of scalable realtime data systems", Manning publication Co ISBN-13: 978-1617290343

[4] Nedeljko Šikanjić, Zoran Ž. Avramović, Esad F. Jakupović, "Implementation of the Neural Network Algorithm in Advanced Databases", JITA – Journal of Information Technology and Applications, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 8(2018) 2:54-63, (UDC: 004.738.5:551.588:551.506)

[5] Simon Whiteley, "A Guide to Azure SQL DataWarehouse", https://adatis.co.uk/a-guide-to-azure-sql-datawarehouse/ (accessed on 18.10.2019)

[6] The AirVisual API description, https://api-docs.airvisual.com/?version=latest#detailed-response-example (accessed on 23.10.2019)

[7] The OAuth 2.0 Authorization Framework, https://tools.ietf.org/html/rfc6749 (accessed on 25.10.2019)

[8] U-SQL Language Reference, "A Guide to Azure SQL DataWarehouse", https://docs.microsoft.com/en-us/u-sql/ (accessed on 17.10.2019)

[9] William H. Inmon, "Building the Data Warehouse", Wiley Computer Publishing ISBN: 0-471-08130-2

Submitted: October 16, 2019
Accepted: November 13, 2019

ABOUT THE AUTHORS

Nedeljko Šikanjić holds a Magister degree in Informatics and Computer Science and has worked for more than 15 years as a Software and Database Architect/Engineer. His main fields of studies are in the area of advanced Databases and Software Architectures. He has been a holder of an active Microsoft Certified Trainer Certificate since 2012 and has been teaching courses on various topics in Information Technologies. Doctoral studies of the third degree enrolled in the academic 2017/2018.

Zoran Ž. Avramović was born in Serbia (Yugoslavia) on September 10th, 1953. He graduated from the Faculty of Electrical Engineering, University of Belgrade. At this Faculty he received a Master's degree, and then a PhD in technical sciences. He is:

- Academician of the Russian Academy of Transport (RTA, St. Petersburg, Russia, since 1995),
- Academician of the Russian Academy of Natural Sciences (RANS, Moscow, Russia, since 2001),
- Academician of the Yugoslav Academy of Engineering (YAE, Belgrade, Serbia, since 2004) (today: Engineering Academy of Serbia, EAS)
- Academician of the Academy of Electrotechnical Sciences of the Russian Federation (AES of the Russian Federation, Moscow, Russia, since 2007)

Scientific Secretary of the Electrical Engineering Department of the Engineering Academy of Serbia.

FOR CITATION

Šikanjić N., Avramović Ž. Z., New Approach of Storing and Retrieving Large Data Volumes, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:89-98, (UDC: 004.6:658.4]:519.8), (DOI: 10.7251/JIT1902089S), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

Reduction of Ict Security Risks Using Level Based Approach

Ivo Džakula[1], Branko Latinović[2]

[1]PhD Student at Pan-European University Apeiron, Banja Luka, Bosnia and Herzegovina, dzakula.ivo@gmail.com

[2]Pan-European University Apeiron, Banja Luka, Bosnia and Herzegovina, branko.b.latinovic@apeiron-edu.eu

Case Study

DOI: **10.7251/JIT1902099DZ** UDC: **006.3:[004.738.5:316.774**

Abstract: Security controls are certainly one of the most preferred ways of controlling the environment in which our system is "alive". But although they are heavily represented and used in practice, security controls tend to become the same and not change after they are introduced. To try to make the most of the opportunities that this approach provides, this paper will explain the importance of implementing ICT security controls and propose a new approach by adding emergency ICT control. This approach gives us the ability to integrate the entire organization into the development of control by providing a better, more accurate and faster basis for managing the security risks of ICT technology.

Keywords: ICT – Information and communications technology, Risk, Security controls.

Introduction

Business processes in the modern age depend largely on the degree of development of computer systems. The integration of sophisticated software solutions, the transfer of business data through computer networks and the creation of a cyber environment have proven to be very useful in the business world. But if we look at the other side, it is sure that the risk of data alienation is getting bigger and bigger. Cybercrime is a problem of a modern age that is causing headaches to companies around the world.

Like all other branches of business, an accelerated process of computerization through business processes did not pass by ICT. ICT resource management and in time reaction are key to the success and preservation of the process.

However, in order for the reaction to be timely, it is necessary to take steps that not only give promises but also results.

Risk Assessment and Systems

Risk is a product of a probability of an event and an impact on the event. With regard to the security risk of information systems, we can conclude that this risk definition is difficult to apply directly because of the intentional impact on the event and the unpredictability of threats, and is often approximate to the relative risk of comparing the likelihood of a security attack successfully executed against an asset on another asset. It follows that security risk is a combination of threats, possible system vulnerabilities to the threat, and consequences after a successful attack. Thus, the threat is generally accepted as part of the assessment associated with determining further probabilities.

Information Attack Method

The method of information attack is a method that is deliberately directed, causing a damaging impact on the confidentiality, integrity and/or availability of information assets. Security data deals

with the protection of its confidentiality, integrity, and availability. Informational Attack Method treats the following elements:

- Confidentiality is important for information that is sensitive to reputation, competitive advantage, or security. Theft or copying may compromise the confidentiality of the data.
- Data integrity refers to their accuracy. Information is useful if one can believe it is true. Without this element, the value of information is drastically reduced.
- The availability of information is taken care of by delivering the data to the correct destination in a timely manner. If information reaches your destination late, it will be considered that it was not available when needed.
- Authentication means that the information is true and original (the information is neither fabrication nor copy) - it should be borne in mind that falsification can also be done without the principle of breach of confidentiality (counterfeit uses own account), possession of information (some data is taken out of control) or integrity (information is a product of criminogenic activity). Hence, information assets are subject to threats of confidentiality, integrity, availability, and authenticity. The exact nature or causes of this threat will depend on a particular property issue.

Methods of an attack on information assets can be done physically (by stealing or property damage), by cyber-attacks, or by using electromagnetic spectrum interference suppression devices. For example, a physical attack method claims a copy of the information may be stolen or copied without permission and may potentially affect their confidentiality.

Similar information jeopardizes integrity, an attack of dissatisfied or forcible employees, deliberately or virtually exchanged through a computer virus.

ISO 27005 Information security risk management provides specific guidance on the risk management of information protection within the organization.

To begin with, it is most important to determine critical points that are potentially at risk of attack. It is also important to emphasize that poor asset management, using obsolete software and hardware, lack of device compatibility, lack of alternative solutions, and lack of adequate human factors are a very important component in risk assessment.

The classic threat model is a very good communication tool. The threat to the organization or system is visible when it is displayed in a clear, easy to understand, and graphical representation. The multifaceted, hierarchical development of the Model of threats allows those with no technical or non-security expertise to immediately assess where threats come from and identify which assets are attacked, and experts and operators point to the need for adequate security control. The graphic nature of the model facilitates its understanding and increases its communication advantages. Furthermore, this model offers common definitions and language for security threats, influences and controls to enable communication. The threat model allows you to identify property threats that could cause a major impact on process activities. It, therefore, enables the risk assessment organization to focus and resources on the asset that requires further testing.

Obviously, some security threats can and do a prolonged or delayed impact, and would be useful if this could be proven. The performance display procedure over a given period of time should be incorporated into the risk assessment methodology itself. This gives you additional benefit not only that you are able to communicate about the influence of time aspect, but also encourages contemplation of countermeasures that are time-constrained.

Means of Threats / Sources of Threats

Traditional sources of threats

Traditional threats in the narrow sense include espionage, sabotage, terrorism and subversion, and the definitions that can be found below briefly describe each of these threats:

- Espionage - Espionage is an act in which certain foreign accesses or takes information secretly or illegally through foreign forces, and for further goals has a subversive political goal.
- Sabotage - Sabotage is an unauthorized act where a certain party intentionally causes consequences that would slow down or stop

processes in the injured party in order to assist certain hostile groups or to further pursue the political goal.
- Terrorism - Terrorism is an act by which a certain party through the use of violence or intimidation for the outcome has a political goal.
- Subversion - activities that endanger the security or well-being of the State and are intended to undermine or abolish political ideology by industrial, political or violent means.

Non-traditional sources of threats

The number of non-traditional threats is on the rise and there are the following examples:
- Crime - Theft is a worrying rise especially for ICT and facilities with large budgets that are at risk of fraud of dissatisfied workers or criminal groups. Criminal activity may range from physical theft of equipment, computers, computer parts, back-up materials, etc. This activity also includes blackmail, illegal access, or corruption of IT data for fraud or crime purposes.
- Protesting Groups - Protest groups are conducting demonstrations, due to various causes, against a wide spectrum of facilities whether they are state or airport facilities and systems. They are mostly peaceful and democratic protests, but extreme elements can involve the pursuit of attacks against individuals or property and can pose a threat and be as significant as part of terrorism.
- Research journalists - Research journalists can try to get information on certain works, critical information, program data, and even the structure of the whole system for better research. Such a type of non-traditional threat can lead to disturbances in daily operations, such as airport operations, and can seriously affect the company's reputation.
- Industrial espionage - Industrial espionage is a type of unlawful act which through the appropriation of information secretly or illegally works to help the competition.

ICT security controls

In order to adapt to the Security System, security controls should be grouped into six levels as shown in Figure 1 – ICT security control levels. The key difference is at the risk level of a particular ICT system depending on each organization. The level of risk varies depending on the criticality of the service provided by these vulnerabilities of the ICT system and the nature of threats depending on the systems.

ICT security control can be organized at levels depending on the assessment of ICT system vulnerability. The lowest level of risk will require the lowest level of basic control; the highest level of risk will require the highest level of basic control.

International practice is the establishment of six levels of control: Level 1 to Level 6 are cumulative and meet the basic requirements of ICT control for organization. The degree of control depends on the complexity of the ICT system or the level of assessment of the vulnerability of ICT assets. For example, Level 1 is the lowest level of security and is appropriate for organizations with a limited and isolated ICT system. Level 6 is the highest level, requiring the implementation of all control requirements (from Level 1 to Level 6). The key difference is at the risk level of a particular ICT system. The level of risk varies depending on the criticality of the service provided by the organization, the vulnerability of the ICT system and the nature of threats.

It is necessary to create categories - tables for certain organizational functions and in detail to clarify each level. Since this kind of organization can not be categorized as a classical one, it is necessary for each and every individual before setting up control to determine critical assets depending on the organization's business processes. This means that the ICT assets that are not critical to the operation will fall into lower risk, while critical assets will be included in the highest level of risk and therefore control. Within each table, levels of control in the rising order from levels 1 to level 6 are described. Levels are cumulative, which means that a higher level of control contains all that is listed below.

Control levels are designed so that the organization is balanced Certainty will have similar levels of control in each of the organizational functions. The organization may request the revision of ICT security, assessing the level of control for each of the above-mentioned categories. This assessment may point to areas where controls are inconsistent at their levels.

Level	Information	Scope	Critical system isolation	Threats
1	Manage sensitive information	Critical	Isolated	Common threats (eg hacker attacks or potential criminals)
2	Manage sensitive information	All	Highly-connected IT system	Common threats (eg hacker attacks or potential criminals)
3	For sensitive information	Adds a medium level of control to the security system	Exposure to a larger area of threat is little compared to the overall ICT system within the organization	More modern and better equipped potential attackers (eg those dealing with serious and organized crime - cybercrime, including terrorist organizations)
4	For sensitive information	Medium level control for the entire organization	Highly Integrated Information System	More modern and better equipped potential attackers (eg those dealing with serious and organized crime - cybercrime, including terrorist organizations)
5	Information is of great value to the organization and potential attackers	High level of control is characteristic of risks and assets	Relatively isolated	The most powerful potential attackers. These types of attacks are in most cases associated with hostile governments (eg government-sponsored terrorism, industrial espionage or some highly capable offenders engaged by a criminal organization)
6	Information is of great value to the organization and potential attackers	High level of control for the entire organization	The distribution of assets can not be sufficiently isolated	The most powerful potential attackers. These types of attacks are in most cases associated with hostile governments (eg government-sponsored terrorism, industrial espionage or some highly capable offenders engaged by a criminal organization)

Figure 1. *ICT security control levels*

It is important to know that multiple business-critical networks and multiple non-critical networks can emerge at the organization level. This type of organization poses many different security requirements to us and it is very difficult to put everything in the same bin. Namely, it is a miracle to find yourself in a situation where all levels and all controls are applicable to all networks of the organization. To properly address this issue and set up valid security controls, you must do the following:

- Categorizing the importance of networks and network infrastructure
- Categorizing the importance of data
- Determining the points of contact between critical and non-business networks

For each of the above requirements, it is necessary to develop security controls that will be adequate for each individual network category. Particular attention should be paid to cases where these two types of differently categorized networks meet. In these cases, priority is given to controls over critical networks. Network staff categorized as critical to the network will always have "superiority" over staff working on a network of lesser importance to the organization. This is not to say that one network or staff is more dominant than another, but that in the event of a network crash, being categorized as critical would have a greater impact on the profitability and reputation of the organization.

In order to meet the requirements of international regulations, local Laws and provisions of international standards, which are increasingly implemented by organizations, it is necessary to develop a set of controls that will meet all of these requirements, and in addition, meet the needs of the organization and ensure confidentiality, integrity, and availability of data. All of these regulations, as well as international standards, give us requirements that must be met as well as guidelines for satisfying them. Although compliance with the provisions is considered to be a harmonized security system, in many cases there is a lack of security controls, which is visible only after conducting an audit, control or penetration test. In order for an organization to ensure that controls are fully aligned with operational requirements, it is necessary to enter into every message of the organization and examine the weakest links. From the human resources, the IT sector of the security staff, and even to the administrative staff itself, there is a certain degree of responsibility for conducting security controls.

The fact is that risk assessments cannot be accurate unless there is accurate input from all stakeholders, both inside and outside the organization. Given the importance of risk assessment, it is crucial to ensure accurate and timely information. If

there is no quality input or it is learned during the risk assessment that a particular part of the organization has failed or is unable to provide accurate information, then that same part of the process can be viewed as a risk.

Proposal for emergency security controls

It would be a good idea, when establishing security controls, to establish a mechanism for adopting emergency security controls that would serve as a coercive mechanism as well as a mechanism to protect certain organizational processes. In cases where certain organizational units are unable to carry out activities and thus place themselves in a situation of becoming a security vulnerability, this approach could provide additional security measures for a predetermined period of time. This type of control could be considered as the highest level and would only relate to processes that have proven to be vulnerable when assessing risk. Adopting emergency security controls would allow for faster response and would target a smaller target since they can only be adapted to one process as opposed to the previous approach in which controls are divided organizationally or by categorization of networks and processes.

We can also look at emergency security controls as a complement to process or system-dependent security controls. They could also be set up as a set of predefined controls that are only valid under certain conditions or within a specified period of time. Although all this can be achieved by establishing a well-known control system, by making precise provisions for each individual system or process, they would make such a large set of controls that, in the case of generalization, would be violated with itself. Therefore, we suggest that in addition to the already known system of security controls, it should be supplemented with controls depending on the process and the system and with a defined time period or activity that activates them.

Application of emergency security controls

We can see the application of this approach to security management during emergencies. In the event of an emergency, controls in the already prepared set should come into effect and not used until then. For example, let us say that at level 6, human resources control does not, in normal situations, contain specifically defined provisions on the prohibition of access to facilities with critical ICT systems. Should an emergency response event occur, an emergency plan should be in place. An Emergency Plan is a plan of measures that an organization must take to respond, reduce the consequences, or prevent hacker attacks. This applies exclusively to the operational part and covers strictly prescribed activities that must be fully complied with. But what about policies and security controls? They remain unchanged in this situation. Emergency controls should focus on access policies, ensure smooth operation, but at the same time tighten employee access.

During the period of validity of emergency security controls, they should be revised and their applicability checked in real-time. This approach would require a team of internal auditors to conduct an internal audit on the applicability of emergency provisions at predetermined periods of time. The same could be done through checklists.

System Control via Check Lists

Checklists are a tool to quickly and easily determine whether work processes are in accordance with the requirements. By using this tool, the examiner can prove in a very short time whether the processes are running smoothly. Controlling the network's operating system through a checklist requires constant updating and alignment of checklist issues with security requirements. For example, in the case of a high-level security checklist, the checklist should be filled in as short a time interval as possible and the width of the questions should be as narrow as possible. This means that any question that is put in the checklist must be directly question-free.

Good control and information gathering through checklists:

- The speed of collecting more information
- Possibility to set the pitch
- Possibility of changing issues with each internal control
- Broad-spectrum of interviewees (from technical to other staff)
- The ability to use data from checklists as a

data source to modify or supplement security controls

Poor control and information gathering via checklists:

- The accuracy of the information obtained
- Professional qualifications of respondents to answer questions of expert nature
- The accuracy of the data from the checklists as a data source for the risk assessment methodology
- Disclosure of matter by the examiner (resulting in a bad question, which leaves the possibility for the wrong answer of the interviewee)

From the above, we can see that the checklists can be used to check in a very short time interval the possibility of implementing the set of ICT security controls. Based on the checklist, it is possible to conclude that further adaptation of a certain level of security controls to the system is required.

Information systems audit

Audit of information systems represents the process of checking the success of information systems in accordance with business requirements, ie the process of analysis and verification of their accuracy, efficiency, efficiency, and reliability. It is a collection of complex management, auditing, and technology activities that examine (check) the effects, but also the risks of using information systems and ultimately evaluate their impact on business.

This is a complex process of collecting and evaluating evidence that can be used to assess the success of a business information system, whether to determine whether a business information system is in the function of asset retention, whether data integrity is maintained, whether it is effective to achieve business goals and use are the resources of the system in an effective way.

An information system audit is a systematic process for assessing whether IT complies with business operations to what extent it effectively and effectively supports the business objectives and the practice (maturity) of management and control of information systems at various hierarchical levels.

The audit information system is systematically and thoroughly inspecting controls across all parts of the information system, and the basic task is to evaluate its current state (maturity, performance level), detect risk areas, assess the level of risk, and give recommendations to management to improve its management practices.

Combining all the steps from above and making them meet the requirements of a specific organization, we will make sure that our controls are put in such a manner that will be effective and in time. The only thing left to do is making sure that our personnel is appropriate for tasks they are assigned for.

Conclusion

Given that the use of security controls is governed by regulations and international standards, practice shows that the benefits they provide are very rarely fully utilized. The globalization of IT systems and the pursuit of business activities in the virtual world increases the risk of information alienation or attack on systems. The use of security controls covers almost the entire organization and increases confidence in the system. However, as with other branches of the economy, the development of an IT system requires the development of a security system, and therefore a further modification of security controls that must at all times justify its reason for being.

Introducing emergency security controls can contribute to improving the security system and improving management's handling of the security system, which gives us an increased dose of confidence in an age when nobody is safe online.

Bibliography

[1] EUROCONTROL Manual for National Security Oversight 03 October 2013
[2] Frameworks for audit of an information system practice Dalibor Drljača Branko Latinović JITA 6(2016) 2:78-85
[3] Industry Consultation Body - Industry Developments in Cybersecurity October 2016
[4] The Complete Guide to Cybersecurity Risks and Controls: Anne Kohnke, Dan Shoemaker, Ken E 978-1-4987-4057-9

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

Ivo Džakula was born on March 4th, 1989 in Čapljina, Bosnia and Herzegovina. A joint master's degree program at the Faculty of Information Technologies of Pan-European University "Apeiron" in Banja Luka in 2014. He is currently a doctoral student. Adress: Čeljevo BB, Čapljina 88300, B&H

Branko Latinović was born on April 28, 1956 in Prijedor, Bosnia and Herzegovina. He graduated from the Faculty of Economics in Banja Luka in 1980. At the same faculty he enrolls a master's degree that ends in 1994, and in 1997 successfully defended his doctoral dissertation. She works as a dean of the Dean of the Faculty of Information Technologies of Pan-European University "Apeiron" in Banja Luka.

For citation

Džakula I., Latinović B., Reduction of Ict Security Risks Using Level Based Approach, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:99-105, (UDC: 006.3:[004.738.5:316.774), (DOI: 10.7251/JIT1902099DZ), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

DESIGN, DEVELOPMENT AND IMPLEMENTATION OF DATABASES IN PHARMACEUTICAL AND MEDICINE

Boris Kovačić[1], Nedim Smailović[2]

[1]The Agency for Medicinal Products and Medical Devices Bosnia and Herzegovina,

[2]Pan-European University "APEIRON", Banja Luka, Republic of Srpska, Bosnia and Herzegovina

Critical Review

DOI: **10.7251/JIT1902106K** UDC: **004.056.55:614]:004.738.5**

Abstract: This paper presents-the design and implementation of databases in pharmacy, points out the most common problems that may be encountered, and describes practical solutions. The paper also describes the structure in terms of linking multiple applications to one single database in terms of achieving business automation.

Keywords: Pharmacy and medicine database design, business automation, multiple applications to one database, SQL.

INTRODUCTION

When talking about pharmacy one immediately thinks of the drug, the pharmacist, and the patient. Complexity in this area of healthcare is evident, since pharmaceuticals requires a good knowledge of chemistry and the human being itself. This brings us to another question: is it possible to record data in this field and in what way? This area is being much more regulated lately, with the development of new international standards and regulations. The answer leads us to three possible segmentations of records.

One of the records is the record of medicines that can be marketed in the country (for which the record is being made), the second is the record of healthcare system patients', and the third record is the record of professionals, which in our case is a–graduated pharmacist or a master of pharmacy. Namely, through the institution's registries certain records of these professionals are being created. In the recent history, we have had a situation where we have lacked this personnel and this record was very important because it prevented the misuse of a pharmacist's professional qualification license. Theoretically, it could happen that one graduated pharmacist worked full-time jobs in 3 wholesales in 3 different cities, which is impossible in practice.

To automate logging in this area, software's with various solutions are created. These software's are made up of an application and databases from which applications pull data and enter new or modify existing ones.

LEGAL REGULATIONS AND STANDARDS

In order to become familiar with the subject of the inspection and construction of the database, we need to familiarize ourselves with the relevant legislation and standards in the Bosnia and Herzegovina.

Bosnia and Herzegovina is regulated in such a way that the national Agency for Medicinal Products and Medical Devices of Bosnia and Herzegovina controls the manufacturing, transportation and wholesale distribution of medicines and medical devices, while the entity ministries and the Brcko District control the retail sale.

Relevant national legislation in Bosnia and Herzegovina includes:[2]

- Law on Medicines and Medical Devices (Official Gazette of Bosnia and Herzegovina, No. 58/08);
- Rulebook on the Type, Amount and Method of Payment of Expenses for Performing the Activities of the Agency for Medicinal Products and Medical Devices of Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina", No. 70/09);
- Order on payment account for payment of costs provided by the Law on Medicinal Products and Medical Devices ("Official Gazette of Bosnia and Herzegovina", No. 72/09);
- Order on Amendments to the Payment Accounts for Administrative Fees (Official Gazette of Bosnia and Herzegovina No. 84/13);
- Rulebook on Manner of Quality Control of Medicinal Products ("Official Gazette of Bosnia and Herzegovina", No. 97/09);
- Rulebook on the manner of monitoring defects in the quality of the medicinal product (Official Gazette of Bosnia and Herzegovina, No. 97/09);
- Rulebook on Clinical Trials of Medicines and Medical Devices ("Official Gazette of Bosnia and Herzegovina", No. 4/10);
- Rulebook on Medical Devices (Official Gazette of Bosnia and Herzegovina, No. 4/10);
- Rulebook on Procedure and Manner of Granting Marketing Authorization ("Official Gazette of Bosnia and Herzegovina", No. 75/11);
- Rulebook on Good Manufacturing Practice (GMP) for Medicines ("Official Gazette of Bosnia and Herzegovina", No. 24/10);
- Rulebook on the manner of advertising medicines and medical devices ("Official Gazette of Bosnia and Herzegovina", No. 40/10);
- Rulebook on the Content and Method of Labeling of the Outer and Inner Packaging of the medicinal product (Official Gazette of Bosnia and Herzegovina, No. 40/10);
- Rulebook on Conditions, Circumstances and Procedure for Engaging Authorized Laboratories ("Official Gazette of Bosnia and Herzegovina", No. 60/10);
- Decision on the manner and scope of implementation / selection of parameters for quality control of each batch of imported medicinal product (Official Gazette of Bosnia and Herzegovina No. 60/10);
- Rulebook on the Method of Conducting Pharmaceutical Inspection (Official Gazette of Bosnia and Herzegovina, No. 23/11);
- Ordinance on the disposal of pharmaceutical waste (Official Gazette of Bosnia and Herzegovina, No. 23/11);
- Rulebook on Conditions for Importation of Medicines Not Authorized for Marketing in Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina", No. 23/11);
- Rulebook on Pharmaceutical Inspector Exams ("Official Gazette of Bosnia and Herzegovina", No. 59/11);
- Decision on the program and content of the Pharmaceutical Inspector exam;
- Decision on the procedure for obtaining a license for the import of risk medicines licensed for placing on the market in Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina", No. 23/11);
- Medicines and Medical Devices Policy in Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina", No. 55/11);
- Rulebook on the manner of reporting, collecting and monitoring adverse reactions to medicinal products (Official Gazette of Bosnia and Herzegovina, No. 58/12);
- Rulebook on monitoring of adverse events related to medical devices (vigilance of medical devices) ("Official Gazette of Bosnia and Herzegovina", No. 58/12);
- Guidelines for Good Clinical Practice in Clinical Trials ("Official Gazette of Bosnia and Herzegovina", No. 19/12);
- Rulebook on the Manufacture and Wholesale of Medical Devices ("Official Gazette of Bosnia and Herzegovina", No. 71/12);
- Corrigendum to the Rulebook on Manufacture and Wholesale of Medical Devices ("Official Gazette of Bosnia and Herzegovina", No. 64/13);
- Rulebook on Amendments to the Rulebook on the Content and Method of Labeling of the Outer and Inner Packaging of the medicinal product (Official Gazette of Bosnia and Herzegovina, No. 36/13);

- Rulebook on Good Distribution Practice (GDP) for Medicinal Products for Human Use ("Official Gazette of Bosnia and Herzegovina", No. 75/13);
- Decision of the Expert Council on Delaying the Application of Data Exclusivity (Official Gazette of Bosnia and Herzegovina, No. 57/13);
- Rulebook on Conditions for Carriage of Wholesale Medicines ("Official Gazette of Bosnia and Herzegovina", No. 49/14);
- Instruction on the procedure for import of medicinal products and medical devices of humanitarian character for the territories of Bosnia and Herzegovina endangered by natural or other disasters;
- Rulebook on the Method and Procedure for Classifying Medicines ("Official Gazette of Bosnia and Herzegovina", No. 69/14);
- Rulebook on Conditions for Production of Medicinal Products ("Official Gazette of Bosnia and Herzegovina", No. 73/14);
- Rulebook on the method of price control, the method of pricing medicines and the manner of reporting drug prices in Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina", No. 3/17);
- RULES ON GOOD MANUFACTURING PRACTICES FOR MEDICAL GAS (Official Gazette of Bosnia and Herzegovina No. 49/18);
- RULES ON GOOD DISTRIBUTION PRACTICE (GDP) OF MEDICAL RESOURCES ("Official Gazette of Bosnia and Herzegovina", No. 75/18);
- Law on Prevention and Suppression of Narcotic Drug Abuse (Official Gazette of Bosnia and Herzegovina, No. 8/06) - with lists;
- Decision on the Designation of International Border Crossings for the Transboundary Movement of Substances and Plants in Tables II, III and IV of the List of Narcotic Drugs, Psychotropic suspensions, Narcotic Drugs and Precursors (Official Gazette of Bosnia and Herzegovina, No. 58/08);
- Decision on amendments to the list of narcotic drugs, psychotropic substances, plants from which narcotic drugs can be obtained and precursors ("Official Gazette of Bosnia and Herzegovina", No. 103/08);
- Decision on amendments to the list of narcotic drugs, psychotropic substances, plants from which narcotic drugs can be obtained and precursors ("Official Gazette of Bosnia and Herzegovina", No. 51/11);
- Decision to exempt preparations from the application of control measures (Official Gazette of Bosnia and Herzegovina, No. 20/10);
- Security requirements for issuing a license for the production and marketing of narcotic drugs and psychotropic substances ("Official Gazette of Bosnia and Herzegovina", No. 69/13).

In addition to these regulations, there are entity and Brcko District regulations.

The entity's new responsibility is retailing and retail pricing towards end users, patients. Entity and Brcko District regulations are located at the following links:

1. Brcko District [6]
2. Federation of Bosnia and Herzegovina [7]
3. Republic of Srpska [8]

Standards and legislation applicable at national level include part of EU standards and regulations. In the EU countries European Medicines Agency (EMA) has competence in addition to national institutions.

The European Medicines Agency (EMA) is in the process of implementation of the standards developed by the International Organization for Standardization (ISO) for the identification of medicinal products (IDMP).

The ISO IDMP standards specify the use of standardized definitions for the identification and description of medicinal products for human use.

Their purpose is to facilitate the reliable exchange of medicinal products' information in a robust and consistent manner. They help to ensure wide interoperability across global regulatory and healthcare communities, which is critical in ensuring accurate analysis and unambiguous communication across jurisdictions.

Commission Implementing Regulation (EU) No 520/2012 (articles 25 and 26) obliges European Union (EU) Member States, marketing authorization holders and EMA to use the ISO IDMP standards. This will affect many areas of the pharmaceutical regulatory environment, both in the EU and other regions.

Scope of the ISO IDMP standards [3]

The five standards provide data elements and structures to uniquely identify and exchange information about:

- substances (ISO 11238);
- pharmaceutical dose forms, units of presentation, routes of administration and packaging (ISO 11239):
- units of measurement (ISO 11240);
- regulated pharmaceutical product information (ISO 11616);
- regulated medicinal product information (ISO 11615).

These standards cover the following to describe a medicinal product for human use:

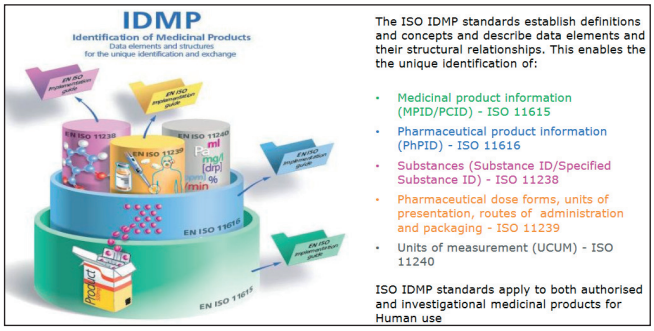
- medicinal product name;
- active substances;
- pharmaceutical product (route of administration, strength);
- marketing authorization;
- clinical data;
- packaging;
- manufacturing.

Medical devices are products or equipment intended generally for a medical use. They are regulated by the national competent authorities, but the European Medicines Agency (EMA) is also involved in the assessment of certain categories of medical device under European Union (EU) legislation.

The adoption of Regulation (EU) 2017/745 on Medical Devices (MDR) and Regulation (EU) 2017/746 on In-Vitro Diagnostic Devices (IVDR) changed the European legal framework for medical devices, introducing new responsibilities for EMA and for the national authorities. Both Regulations entered into force in the May 2017 and have a staggered transitional period.

The MDR has a transition period of three years and will fully apply from 26th May 2020. The IVDR has a transition period of five years and will fully apply from 26th May 2022.

During the transition period, manufacturers can place devices on the market under the currently applicable EU Directives (93/42/EEC, 98/79/EC and 90/385/EEC) or under the new Regulations if they fully comply with these. [4].



Picture 1. *Page 6 of presentation Introduction to SPOR data services Source: https://www.ema.europa.eu/en/documents/presentation/presentation-introduction-spor-data-services_en.pdf visited: 11/28/2019. [5]*

Designing Databases

The tools I used to create the database are an MS-SQL server with MS SQL Management Studio, MS Access with ODBC drivers for connecting to the database and data loading. In addition, I used MS Excel to purify the data and to plan the construction of the database by normalizing it. This enabled the Excel worksheet visibility of the duplicated data and thus prevented duplication of records in the database. This web-based solution for Internet data displaying via a web server currently captures read-only database data.

The first version of the database contained an application with a database that included institution's registries. The database of this application is on the MSSQL platform, while the application in Access pulls data through the ODBC driver.

A second database was then implemented on the MYSQL platform with an application that was written in the PHP programming language. The latter database and application belong to the Inspectorate and was separated from the former for the confidentiality reasons. This led to the need for data reload due to the different technology used for the application and due to the disconnection of the databases themselves.

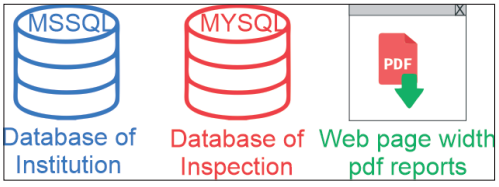
Reports were extracted from the application first and second for the website and periodically modified in PDF format.

The basic idea for the reconstruction of the database and the accompanying applications, was to create 3 applications with a common database, where everyone could use their part, which will be visible to him and will have the possibility to update

in the required segment of the database. In addition, a third application will be used to capture the data and display it on the website automatically after the data input.

In this way, we will avoid tipping over and enable more efficient business operations, while achieving automation of the business process. This transition will take place in 4 phases.

The first phase will be data purification, upgrade and preparation of the database design according to user development requirements.

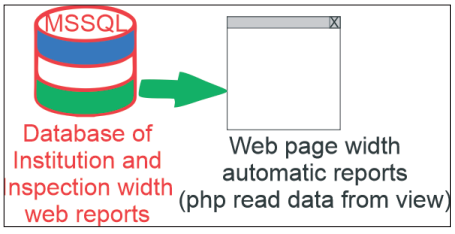


Picture 2. *Phase 1, consolidation and cleaning data*

The second phase will be the reconstruction of the existing database by adding an inspection data, with the migration of existing data.

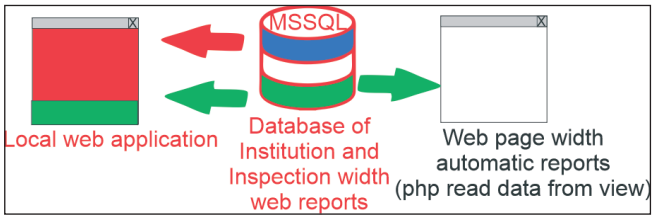
Picture 3. *Phase 2 database upgrade with inspection data migration*

The third phase will be publishing of the data from MSSQL View via the PHP platform to the web site.



Picture 4. *Phase 3 Same database width 2 application, and automatic web reporting site width data form database*

The fourth and the final phase will involve the creation of a web-based local application with local user authority segmentation.



Picture 5. *Database width local web application and automatic web reporting data from database*

After this phase, they could go a step further and enable online users to submit online applications. However, this requires further analysis due to the security aspect. Security testing is a type of software testing which purpose is detecting system's vulnerabilities. It checks whether the system data is protected from unauthorized access, during which data could be altered or deleted.[1]

Data input

With the data input we will divide basic data and inspection data.

Namely, the basic information entered by the officials is about the registration of a wholesale distributors or manufacturers of medicines or medical devices.

The inspector who performs the inspection of all these legal entities can see all the above-named data, and have possibility to modify them. He can also enter additional amount of data about inspection control, as well as the ordered measures. Further upgrading of the database could allow the automatic download of data about the drugs from the Drug Database, or the automatic download of data about medical devices from the Medical Devices Database. This is not currently automated, but there is possibility for further development of the base.

Processing

In order to compare the difference, I will show the main table.

Namely, in the first phase, this table contained almost all data about the legal entity. This later changed in such a way that only the basic data remained, because the primary key rjesenjeID has taken other data from table Rjesenje that can be changed by the institution when changing the solution. In addition, the field of inspection was added.

Table 1. *MAIN TABLE Institution on Phase 1 – list of data*

Name	Field type	Allowed blank	Primary key
UstanovaID	Int	Unchecked	yes
RegistarskiBroj	Int	Checked	no
VrstaUstanoveID	Int	Checked	no
Ustanova	nvarchar(50)	Checked	no
Adresa	nvarchar(50)	Checked	no
MjestoID	Int	Checked	no
Telefon	nvarchar(10)	Checked	no
Telefax	nvarchar(10)	Checked	no
[E-mail]	nvarchar(30)	Checked	no
BrojRjesenja	nvarchar(21)	Checked	no
DatumRjesenja	datetime	Checked	no
OblikSvojine	nvarchar(100)	Checked	no
DatumPrestankaRada	datetime	Checked	no
Napomena	Ntext	Checked	no
Dokumentacija	Ntext	Checked	no
IDStatus	Int	Checked	no

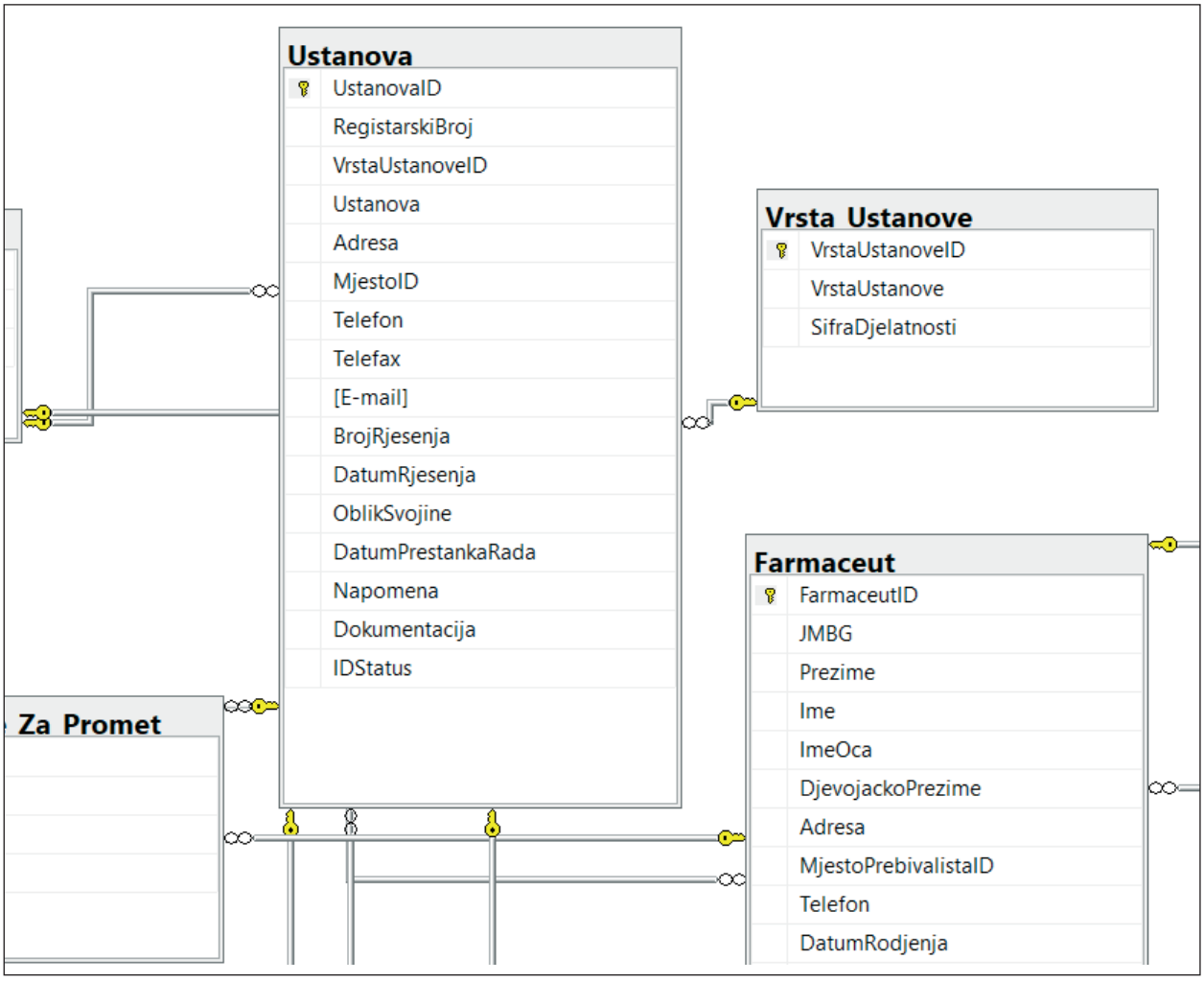
```
USE [ru]
GO

/****** Object: Table [dbo].[Ustanova] Script Date: 28.11.2019. 14:19:39 ******/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

CREATE TABLE [dbo].[Ustanova](
	[UstanovaID] [int] IDENTITY(1,1) NOT NULL,
	[RegistarskiBroj] [int] NULL,
	[VrstaUstanoveID] [int] NULL,
	[Ustanova] [nvarchar](50) NULL,
	[Adresa] [nvarchar](50) NULL,
	[MjestoID] [int] NULL,
	[Telefon] [nvarchar](10) NULL,
	[Telefax] [nvarchar](10) NULL,
	[E-mail] [nvarchar](30) NULL,
	[BrojRjesenja] [nvarchar](21) NULL,
	[DatumRjesenja] [datetime] NULL,
	[OblikSvojine] [nvarchar](100) NULL,
	[DatumPrestankaRada] [datetime] NULL,
	[Napomena] [ntext] NULL,
	[Dokumentacija] [ntext] NULL,
	[IDStatus] [int] NULL,
 CONSTRAINT [PK_Ustanova] PRIMARY KEY CLUSTERED
(
	[UstanovaID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_
LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

GO
```



Picture 6. *Main table at database diagram - Phase 1*

Table 2. *MAIN TABLE Institution on Phase 2 – list of data*

Name	Field type	Allowed blank	Primary key
UstanovaID	Int	Unchecked	yes
RegistarskiBroj	Int	Checked	no
RjesenjeID	Int	Checked	no
InspekcijaID	Int	Checked	no
IDStatus	Int	Checked	no

```
USE [ru]
GO

/****** Object: Table [dbo].[Ustanova] Script Date: 28.11.2019. 23:45:35 ******/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO
```

```
CREATE TABLE [dbo].[Ustanova](
	[UstanovaID] [int] IDENTITY(1,1) NOT NULL,
	[RegistarskiBroj] [int] NULL,
	[RjesenjeID] [int] NULL,
	[InspekcijaID] [int] NULL,
	[IDStatus] [int] NULL,
 CONSTRAINT [PK_Ustanova] PRIMARY KEY CLUSTERED
(
	[UstanovaID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_
LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[Ustanova] WITH CHECK ADD CONSTRAINT [FK_Ustanova_Mjesto] FOREIGN
KEY([InspekcijaID])
REFERENCES [dbo].[Mjesto] ([MjestoID])
GO

ALTER TABLE [dbo].[Ustanova] CHECK CONSTRAINT [FK_Ustanova_Mjesto]
GO

ALTER TABLE [dbo].[Ustanova] WITH CHECK ADD CONSTRAINT [FK_Ustanova_Status] FOREIGN
KEY([IDStatus])
REFERENCES [dbo].[Status] ([IDStatus])
GO

ALTER TABLE [dbo].[Ustanova] CHECK CONSTRAINT [FK_Ustanova_Status]
GO

ALTER TABLE [dbo].[Ustanova] WITH CHECK ADD CONSTRAINT [FK_Ustanova_Vrsta_Ustanove] FOREIGN
KEY([RjesenjeID])
REFERENCES [dbo].[Vrsta_Ustanove] ([VrstaUstanoveID])
GO

ALTER TABLE [dbo].[Ustanova] CHECK CONSTRAINT [FK_Ustanova_Vrsta_Ustanove]
GO
```

Output data

The output contains a report.

We have four reports in the phase 1, but in the phase 2 we have 13 reports. In the phase 3 we have 14 reports.

List of reports in the phase 1:

1. REGISTRY OF DRUG MANUFACTURERS IN BOSNIA AND HERZEGOVINA
2. REGISTRY OF MEDICAL DEVICES MANUFACTURERS IN BOSNIA AND HERZEGOVINA
3. REGISTRY OF MEDICINAL PRODUCTS WHOLESALE DISTRIBUTORS IN BOSNIA AND HERZEGOVINA
4. REGISTRY OF MEDICAL DEVICES WHOLESALE DISTRIBUTORS IN BOSNIA AND HERZEGOVINA

List of reports in the phase 2:

1. REGISTRY OF DRUG MANUFACTURERS IN BOSNIA AND HERZEGOVINA
2. REGISTRY OF MEDICAL DEVICE MANUFACTURERS IN BOSNIA AND HERZEGOVINA LICENSED FOR THE CLASS I MEDICAL DEVICE MANUFACTURING AGENCY

3. REGISTRY OF MEDICAL DEVICE MANUFACTURERS IN BOSNIA AND HERZEGOVINA AUTHORIZED FOR THE CLASS II MEDICAL DEVICE AND OTHER/LOWER CLASSES OF MEDICAL DEVICES MANUFACTURING
4. LIST OF RESPONSIBLE PERSONS FOR PLACING THE MEDICINE ON THE MARKET IN BOSNIA AND HERZEGOVINA
5. REGISTRY OF MEDICINAL PRODUCTS WHOLESALE DISTRIBUTORS WITH A LICENSE FOR IMPORT AND MARKETING OF MEDICINES IN BOSNIA AND HERZEGOVINA
6. REGISTRY OF MEDICINAL PRODUCTS WHOLESALE DISTRIBUTORS IN BOSNIA AND HERZEGOVINA WITH LICENSE FOR NATIONAL WHOLESALE
7. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED TO WHOLESALE ALL MEDICINAL PRODUCTS
8. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF MEDICAL DEVICES
9. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS I MEDICAL DEVICES
10. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS II MEDICAL DEVICES
11. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS II AND OTHER LOWER CLASSES OF MEDICAL DEVICES
12. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED SOLELY FOR THE TRANSPORT OF MEDICAL DEVICES
13. LEGAL ENTITIES WITH A PERMANENT OR TEMPORARY PROHIBITION OF ACTIVITIES

List of reports in phase 3:

1. REGISTRY OF DRUG MANUFACTURERS IN BOSNIA AND HERZEGOVINA
2. REGISTRY OF MEDICAL DEVICE MANUFACTURERS IN BOSNIA AND HERZEGOVINA LICENSED FOR THE CLASS I MEDICAL DEVICE MANUFACTURING AGENCY
3. REGISTRY OF MEDICAL DEVICE MANUFACTURERS IN BOSNIA AND HERZEGOVINA AUTHORIZED FOR THE CLASS II MEDICAL DEVICE AND OTHER/LOWER CLASSES OF MEDICAL DEVICES MANUFACTURING
4. LIST OF RESPONSIBLE PERSONS FOR PLACING THE MEDICINE ON THE MARKET IN BOSNIA AND HERZEGOVINA
5. REGISTRY OF MEDICINAL PRODUCTS WHOLESALE DISTRIBUTORS WITH A LICENSE FOR IMPORT AND MARKETING OF MEDICINES IN BOSNIA AND HERZEGOVINA
6. REGISTRY OF MEDICINAL PRODUCTS WHOLESALE DISTRIBUTORS IN BOSNIA AND HERZEGOVINA WITH LICENSE FOR NATIONAL WHOLESALE
7. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED TO WHOLESALE ALL MEDICINAL PRODUCTS
8. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF MEDICAL DEVICES
9. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS I MEDICAL DEVICES
10. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS II MEDICAL DEVICES
11. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED FOR THE TRANSPORT OF CLASS II AND OTHER LOWER CLASSES OF MEDICAL DEVICES
12. REGISTRY OF WHOLESALE DISTRIBUTORS AUTHORIZED SOLELY FOR THE TRANSPORT OF MEDICAL DEVICES
13. LEGAL ENTITIES WITH A PERMANENT OR TEMPORARY PROHIBITION OF ACTIVITIES
14. ADMINISTRATIVE PROHIBITION MEASURES IMPOSED DURING INSPECTION SUPERVISION AS OF 01.01.2015

Registry of manufacturers of Medicinal Products in Bosnia and Herzegovina

SELECT UstanovaID, RegistarskiBroj, VrstaUstanoveID, Ustanova, Adresa, MjestoID, Telefon,

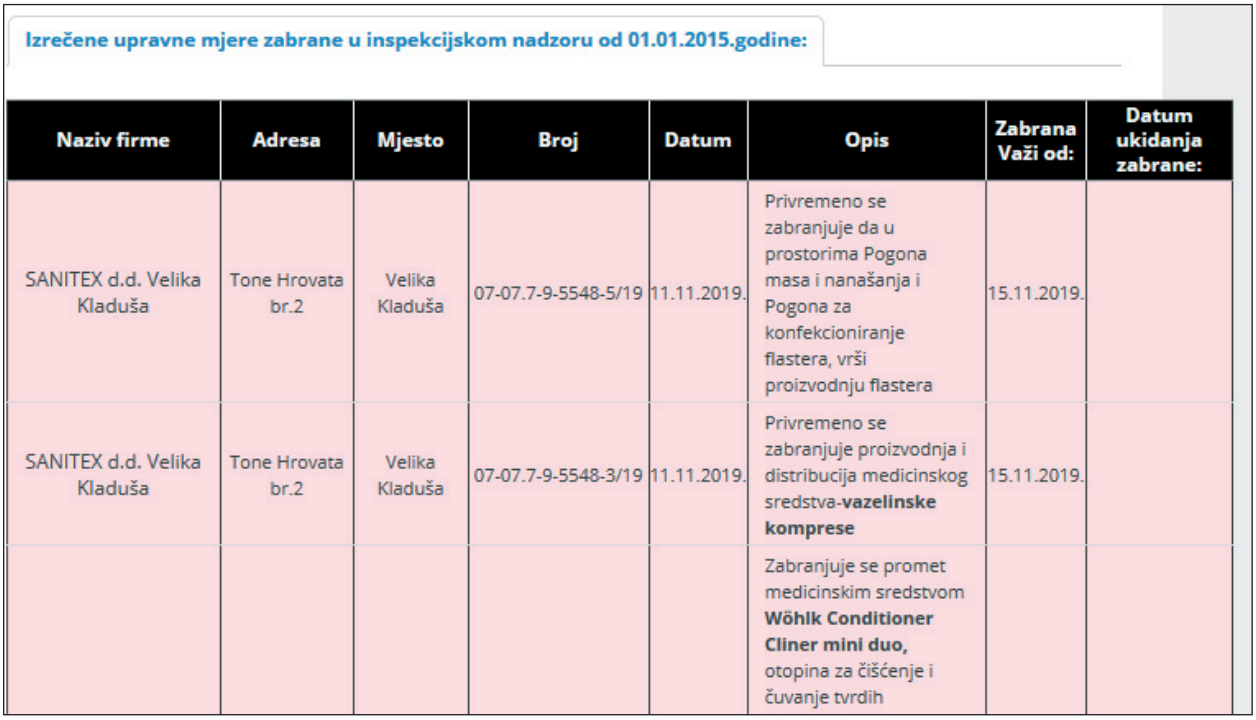
Telefax, [E-mail], BrojRjesenja, DatumRjesenja, OblikSvojine, DatumPrestankaRada, Napomena, Dokumentacija, IDStatus,
DatumPrestankaRada AS Expr1, VrstaUstanoveID AS Expr2
FROM dbo.Ustanova
WHERE (VrstaUstanoveID = 10) AND (DatumPrestankaRada > { fn NOW() })

Registar proizvođača lijekova

srijeda, 12. jun 2019.

Reg br.	Vrsta ustanove	Naziv ustanove	Adresa	Mjesto	Telefon	Telefax	E-mail	Broj rješenja	Datum rješenja	Rješenje važi do:
Banja Luka										
10	Proizvođač lijekova	HEMOFARM D.O.O.	Novakovići bb	Banja Luka	051 331650	051 331623	infobl@hemofarm.com	10-07.12-7-8160-3/17	17.12.2018.	20.12.2023.
Lukavac										
1	Proizvođač lijekova	ZADA PHARMACEUTICALS	Bistarac Donji b.b.	Lukavac	035 551140	035 551150	zada@zada.ba	10-07.12-7-63-1/15	17.02.2015.	16.02.2020.
Sarajevo										
15	Proizvođač lijekova	AMSAL PHARMACEUTICALS	Igmanska 38,Vogošća	Sarajevo	033 580730	033 580740	info@amsal.ba	10-07.12-3-3095-1/19	10.06.2019.	09.06.2024.
11	Proizvođač lijekova	BOSNALIJEK	Jukićeva br.53	Sarajevo	033 254400	033 664971	info@bosnalijek.ba	10-07.2-3-6205-3/16	14.10.2016.	13.10.2021.
2	Proizvođač lijekova	FARMAVITA	Igmanska br. 38	Sarajevo	033 476320	033 476321	farmavita@farmavita.ba	10-07.12-7-3300-1	06.07.2015.	05.07.2020.
Široki Brijeg										
14	Proizvođač lijekova	NATURA PHARM D.O.O.	Gornji Mamić bb,Kočerin	Široki Brijeg	033 852115	033 852114	info@natura-pharm.ba	10-07.12-3-10278-1/18	26.12.2018.	25.12.2023.
Travnik										
13	Proizvođač lijekova	PHARMAMED	Dolac na Lašvi bb	Travnik	030 515005	030 515007	GC@PHARMAMED.BA	10-07.12-3-2328-1/18	13.04.2018.	12.04.2023.
	UKUPAN BROJ	7								

Picture 7. *Report Registry of manufacturers of Medicinal Products in Bosnia and Herzegovina source: http://www.almbih.gov.ba/_doc/proizvodjaci/rpl.pdf?5*



Izrečene upravne mjere zabrane u inspekcijskom nadzoru od 01.01.2015.godine:

Naziv firme	Adresa	Mjesto	Broj	Datum	Opis	Zabrana Važi od:	Datum ukidanja zabrane:
SANITEX d.d. Velika Kladuša	Tone Hrovata br.2	Velika Kladuša	07-07.7-9-5548-5/19	11.11.2019.	Privremeno se zabranjuje da u prostorima Pogona masa i nanašanja i Pogona za konfekcioniranje flastera, vrši proizvodnju flastera	15.11.2019.	
SANITEX d.d. Velika Kladuša	Tone Hrovata br.2	Velika Kladuša	07-07.7-9-5548-3/19	11.11.2019.	Privremeno se zabranjuje proizvodnja i distribucija medicinskog sredstva-**vazelinske kompresе**	15.11.2019.	
					Zabranjuje se promet medicinskim sredstvom **Wöhlk Conditioner Cliner mini duo,** otopina za čišćenje i čuvanje tvrdih		

Picture 8. *Administrative prohibition measures imposed in the inspection supervision as of 01.01.2015: Source: http://www.almbih.* ***gov.ba/inspektorat/ visited:*** *28.11.2019.*

CONCLUSION

Establishing a database in the control of the pharmaceutical market in Bosnia and Herzegovina will facilitate cooperation and business in the field of classification and supervision of legal entities engaged in the wholesale distribution of pharmaceutical and medical products.

Namely, databases in pharmacy are important for the classification of data and for the monitoring of the traceability of administrative proceedings and penalties against legal and natural persons who make offenses. We have seen in the paper that, in addition to being tracked, wholesale owners are also classified by the type. Sometimes we have a situation where the owner tries to maximize profits at the expense of noncompliance and does not want to comply with the minimum legislative requests. Sometimes we have a situation where a healthcare professional, pharmacist or a doctor tries to maximize profits by breaking the rules. In both cases, there is a procedure that first points to the need to eliminate deficiencies and return within legal frame, and if he fails to comply with repressive measures in the form of penal provisions and other sanctions, and even prison sentences. Namely, repressive sanctions are rigorous because the health of the population is threatened.

REFERENCES

[1] Ksenija Živković, Ivan Milenković, Dejan Simić (2016) USING OPEN SOURCE SOFTWARE FOR WEB APPLICATION SECURITY TESTING. Journal of Information Technology and Applications, 87(1), 86–92.

[2] http://www.almbih.gov.ba/dokumenti/regulative/, [Accessed: 28. November 2019].

[3] https://www.ema.europa.eu/en/human-regulatory/overview/data-medicines-iso-idmp-standards-overview, [Accessed: 28. November 2019].

[4] https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices, [Accessed: 28. November 2019].

[5] https://www.ema.europa.eu/en/documents/presentation/presentation-introduction-spor-data-services_en.pdf, [Accessed: 28. November 2019].

[6] http://skupstinabd.ba/ba/zakon.html, [Accessed: 28. November 2019].

[7] http://www.fmoh.gov.ba/index.php/zakoni-i-strategije/zakoni/zakon-o-lijekovima-fbih, [Accessed: 28. November 2019].

[8] http://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/MZSZ/dokumenti/Pages/Farmacija.aspx, [Accessed: 28. November 2019].

Submitted: November 3, 2019
Accepted: November 24, 2019

About the authors

Boris Kovačić was born in Bihac in 1979. He finished elementary and technical school in Banja Luka. He graduated at the Faculty of Information Technology and the Faculty of Business Economics at Pan-European Apeiron University. He has a master's degree in economics from Pan-European Apeiron University.
He is employed in The Agency for Medicinal product and Medical Devices of Bosnia And Herzegovina as IT consultant.

Nedim Smailović was born in Tuzla. He has been living in Banja Luka since 1973. He graduated from the Faculty of Electrical Engineering, department of Telecommunications. Since 1982 he has worked in RO PTT traffic of Bosnia and Herzegovina, and a series of organizational transformation it is now called Mtel doo Banja Luka. His first work experience was in designing and maintaining the PTT capacities. He obtained his Master's degree from Pan European University 'Aperion' Banja Luka, in 2005. There he also defended his doctoral thesis titled: Computer information graphics in presenting Bosnia and Herzegovina on the road to accessing the European Union. He was elected Associate Professor in 2013 and he has been teaching since in three universities in Bosnia and Herzegovina subjects relating to computer technology. He is an author and co-author of several books from the field of information technology and mathematics. He is married, father of two daughters.

For citation

Kovačić B., Smailović N., Design, Development and Implementation of Databases in Pharmaceutical and Medicine, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:106-117, (UDC: 004.056.55:614]:004.738.5), (DOI: 10.7251/JIT1902106K), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

ANALYSIS OF USING CLOUD BUSINESS IN BOSNIA AND HERZEGOVINA AND THE REGION

Mihajlo Travar[1], Igor Dugonjić[2], Saša Ristić[3]

[1]Regulatory Commission for Energy of Republic of Srpska, Trebinje

[2]University Clinical Centre of the Republic of Srpska, Banja Luka

[3]Lanaco-Information technologies, Banjaluka

A General Survay

DOI: **10.7251/JIT1902118T** UDC: **004.735.8:004.6(497.6)**

Abstract: Cloud business is the basic support to operations of modern companies. It enables companies to be more agile and innovative. Such form of digital transformation improves business and company productivity and solves business problems in innovative ways. On one hand, Cloud business makes possible for users to get the best expertise possible which they cannot develop independently. On the other hand, it offers possibilities to reduce the costs related to hardware and software to a reasonable level. The time value of money present in Cloud business is also significant. Namely, companies no longer need to invest large sums of money in equipment or software solutions; it is sufficient to rent those and use revenues for future business investments. Cloud solutions mean that users, using modern technology, access their business software solution through a web browser (web application) thus completing their business processes and accessing the database. Expansion of business leads to a new phenomenon – users are no longer tied to a physical location. In this way, users more frequently work from home or on the move by using different mobile devices. We all use a number of applications (Gmail, outlook.com, Facebook, LinkedIn, Twitter etc.) and take advantage of the Cloud business without being aware of it. We do not install any of the mentioned applications on our devices but access those using an internet browser. Given the lack of IT experts due to economic migrations, as is the situation here, insufficient supply and enormous demand for IT professionals, the traditional model of using business information systems will become practically unsustainable. In this paper, following introductory and general remarks on Cloud business, an analysis was made of using Cloud business IT systems in RS/BH, Serbia and the EU.

Keywords: Cloud business, Business IT systems ICT, Cloud, Digitalization of business.

INTRODUCTION

The modern business environment is characterized by digitalization, development of the Internet of Things, customer support, risk management and the application of sophisticated technology. Therefore, more and more questions are being asked how to respond to the challenges ahead and how technology will affect the business. It is estimated that there were 31 billion devices interconnected through the internet in 2018. According to global projections, there will be 80 billion interconnected devices by the end of 2020. The same estimates suggest that, in two years, each resident on the planet will have 6.5 devices connected to the Internet. Processes aiming to introduce new or, better to say, modern ways of organizing business and social environments can be called the process of digital transformation. Global analyses show that only 10% of companies in the world are completely digitally transformed and ready to operate in an IoT environment. This is to say that one of the most significant manifestations of digital transformation is the use of the so-called Cloud.

Today everyone talks about Cloud computing and there are many definitions from various authors. In 2011, the American National Institute of Standards

and Technology (NIST) published a definition often cited and considered one of the simplest ones: 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[6]. The RAD Lab publication by Berkeley University of California published a definition that has become very popular: 'Cloud business also applies to applications delivered as online services, and to hardware/software systems in the data centres providing those services'[5].

How does Cloud function as a contemporary business model? The system consists of two physically separate parts. The first, user-controlled part is the so-called front end, while the second part is the service provider's infrastructure called back end. For the system to work, both parts need to be connected into one unit, which is enabled through an internet connection. This use of technology enables companies and individuals to reduce initial investment in equipment and investment in the application. Besides, users may adapt the technology to their own needs in a quick, simple and innovative way. One of the basic differences between the standard business concept and Cloud business is that the load carried by personal computers or servers is shifted to the Cloud provider's servers. The service provider's servers have supreme performances, which enables fast execution of applications, data storage and a special data storage process – backup. Most often it is about storing the same data in several different locations, and copying the same data is done on a daily, weekly and monthly basis.

History and Properties of Cloud Business

The history of Cloud business, especially in the region, is short – it is closely related to the development of the internet and business technologies. In the last century, specifically in the 1960s, Joseph Carl Licklider coined the term 'Cloud business.' Thus, he may be said to represent one of the most significant figures in this field. The history of Cloud business was also influenced by one of the most significant events in 1999 when company Salesforce introduced a new concept of delivering business applications through a website. In 2002, Amazon launched its web services such as human intelligence computing through Amazon Mechanical Turk services. After that, in 2006, Amazon launched a Cloud called 'Elastic Compute Cloud', which allowed businesses or private users to rent computers for running personal computer applications. Following Amazon, many other companies like IBM, Microsoft, Oracle etc. started to develop their Cloud business services. As a result, users today have a wide choice of these services. [8]

Cloud business is intended not only for businesses but also for private users with resources available from service providers. Accordingly, the computer industry has identified models to connect millions of users and make state-of-the-art software solutions available to them. All this will completely suppress traditional approaches of using applications on personal computers and using them in On-premise format.

The difference in the very concept of Cloud business is whether it is used by IT experts or ordinary users. Ordinary users will define it as a new and less expensive way to use software solutions to be hired as needed, while IT professionals define it as a new business model or a new technology platform for storing, launching and using state-of-the-art technology. [2]

A publication titled 'Benefits and Challenges of Cloud ERP Systems – a Systematic Literature Review' published in 2017 by Mohamed Ali Abd Elmonem, Eman Nasr and Mervat H. Gheith comprises 31 papers published in the period 2011 – 2016. A systematic analysis of the papers shows the advantages and disadvantages of Cloud business given in the table below.

Table 1. *Advantages and disadvantages of Cloud business [3]*

ADVANTAGES	DISADVANTAGES
Lower initial costs	Subscription costs
Lower operating costs	Safety risks
Faster implementation	Performance risk (long implementation)
Scalability	Limited scalability and integration with other on-premise applications
Focus on key competences	Strategic risks
Use of advanced technology	Compliance risk

Fast update/upgrade	Loss of IT competence
Advanced accessibility, mobility and usability	Limited functionalities
Easier connection with Cloud services through the internet connection	Service Level Agreement (SLA) issues
Improved system availability and disaster recovery	Information sensitivity
Cost transparency	Control of ERP in Cloud
Sales automation	Hidden contractual costs
Use of safety standards	Loss of technical skills
Demo versions	Choice of ERP in Cloud
	Need for service standards and ERP regulations
	Knowledge about Cloud
	Organizational challenges

SERVICE PROVISION DISTRIBUTION MODELS AND TYPES OF CLOUDS

As for Cloud business, these are the following three different service provision models:

- Software as a service (SaaS) platforms.

SaaS is software offered by a third party – remotely configured service provider available on-demand, most often through the internet. SaaS is a model where an application is hosted as a service to users accessing it through the internet. When software is hosted off-site (in a user-independent location), users are not required to provide maintenance and support. This type of a Cloud service offers a complete functionality of an application covering everything from basic applications (e-mail, Office 365 etc.) to applications like ERP system (EcoOne by Lanaco).

- Platform as a Service (PaaS) enables users to develop new applications using the API (Application Programming Interface). The offered platforms have development tools, configuration management and platforms for development and application.

Some examples of PaaS services are Microsoft Azure, Force and Google App Engine.

- Infrastructure as a Service (IaaS)

IaaS provides virtual machines and other abstracted hardware and operating systems controllable through API service. Some examples of IaaS are Amazon EC2 and S3, Terremark Enterprise Cloud, and Windows Live SkyDrive in Rackspace Cloud.

Types of Clouds

- Public Cloud – a Cloud that is based on Cloud computing service provider renting their resources to users and charging them by the scope of use. The resources include the processing power, data storage space and applications that exist on the Cloud. Depending on the provider and type of service, the applications may be free of charge or charged as used. The resources are shared among users and accessed through the Internet.
- Private Cloud – a type of Cloud created for a single client only. The infrastructure is virtualized with additional elements making it user-friendly, manageable and compatible with other Clouds. This is a system that entirely belongs to the user and is controlled and handled by the user's IT service.
- Joint Cloud – it has the same infrastructural properties as the public Cloud but is created as a closed solution for a certain community i.e. group of companies. The community usually gathers companies with common needs, safety requirements and other properties. A good example is a school Cloud or public companies' Cloud. This type of Cloud is managed by companies alone or the service provider.
- Hybrid Cloud – this solution allows the user who has his/her private Cloud to expand the existing infrastructure with certain services from the public Cloud to form an integrated entity. This makes it impossible for service users to detect which part of the infrastructure is used by individual services. In addition, this ensures complete mobility of the service between the private and public part as well as the integrated management of the available infrastructure.

ANALYSIS OF USING CLOUD BUSINESS IN BOSNIA AND HERZEGOVINA, SERBIA AND THE EUROPEAN UNION

Most companies in the environment are still underusing the benefits of the Cloud business. Despite

having the software bought from the same IT supplier, regional companies do not have integrated financial management on the corporate level. Their data exchange is still executed via Excel sheets and emails. The use of Cloud business would enable those companies to save significant resources for sharing and consolidating financial data for reporting across the group. The challenges faced by regional companies operating in the international market are numerous, one of the most important ones being the establishment of an integrated business and information system and a centralized database by using Cloud technology. The technological conditions for deploying Cloud technology do exist but need to be implemented. This would provide a simpler and faster financial analysis of the regional markets i.e. companies could perform daily analysis of inventory and receivables. It is also very important for BH companies with subsidiaries in the region and vice versa to establish an appropriate level of control. For example, if the controlling function in the parent company can directly access the financial information in the subsidiary, which the Cloud business certainly enables, any irregularities can be more easily detected and corrected. The irregularities in operation do not have to be intentional; however, they demonstrate that the accounting staff of the subsidiary lack know-how and skills, which needs to be improved. Cloud business would also provide these companies with additional security in terms of data storage. We have witnessed many tragic events in this turbulent area. Such unforeseeable circumstances, as well as natural disasters, conflicts and the like, may lead to the mother company suffering losses and damages of not just material nature (loss of stocks, damages etc.) but also immaterial damages such as the loss of financial data and documents in its subsidiaries. If such companies choose to operate using Cloud business, electronic data and document archiving for the whole group can be carried out at the mother company or another safe location.

Bosnia and Herzegovina

Cloud business is slowly becoming a part of our everyday life here. According to the BH Statistical Institute [1], the use of online Cloud services is a relatively new technology in the country, used by only 13% out of the total number of observed companies in Bosnia and Herzegovina. Based on the data obtained by analysing the use of information and communication technologies in Bosnia and Herzegovina – the subject of research was the use of Cloud services – we concluded that only 5.1% of companies use Cloud services.

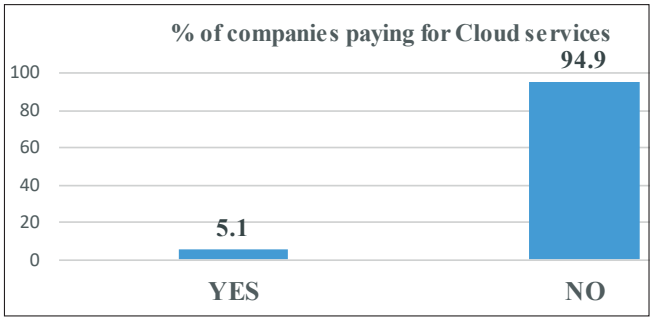


Figure 2: *Percentage of companies paying for Cloud services*

When reviewing the above analysis of companies using the Cloud, it is important to distinguish between the sizes of the companies. The largest companies are always the main drivers of new technologies as they possess the human and technical resources allowing them to adopt new technological advances. Below is an overview of Cloud technology users based on the size of companies.

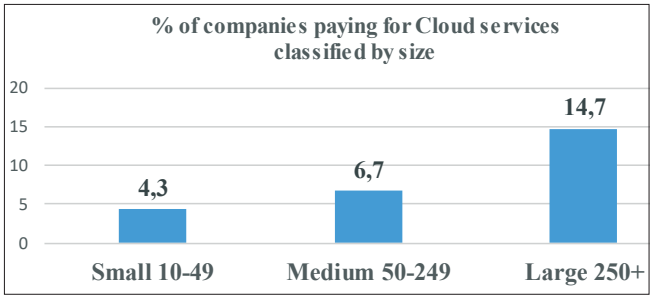


Figure 3: *Percentage of companies paying for Cloud services (by size)*

The use of Cloud technology in Bosnia and Herzegovina is still very poor. There are many reasons to be recognized as indicators for such situation. Some of the key reasons are the low level of technology, lack of information and lack of staff dealing with information and communication technology.

Serbia

Unlike Bosnia and Herzegovina, where the use of services is at an extremely low level, the situation in

Serbia is significantly different. The number of companies subscribed to Cloud services is considerably larger, which is also confirmed by the fact that the number of observed companies in Serbia is much higher.

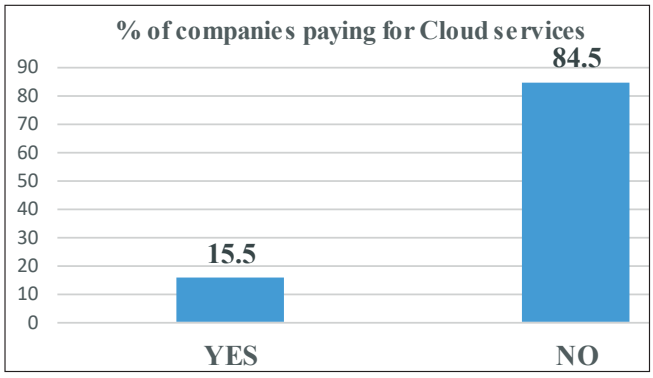


Figure 4: *Percentage of companies paying for Cloud services*

According to the Serbian Statistical Institute 2018 survey [7], 31.5% of surveyed companies (each having over 250 employees) declared to pay for Cloud service, which is significantly higher compared to 2016, with only 13.2% companies being subscribed to Cloud. This indicates that an increasing number of companies consider Cloud an integral part of the modern business rather than mere business optimization facilitator. The main reason for this is the multiple benefits this solution offers to the company business.

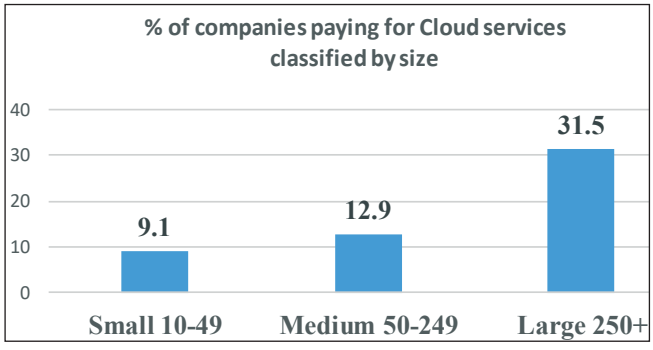
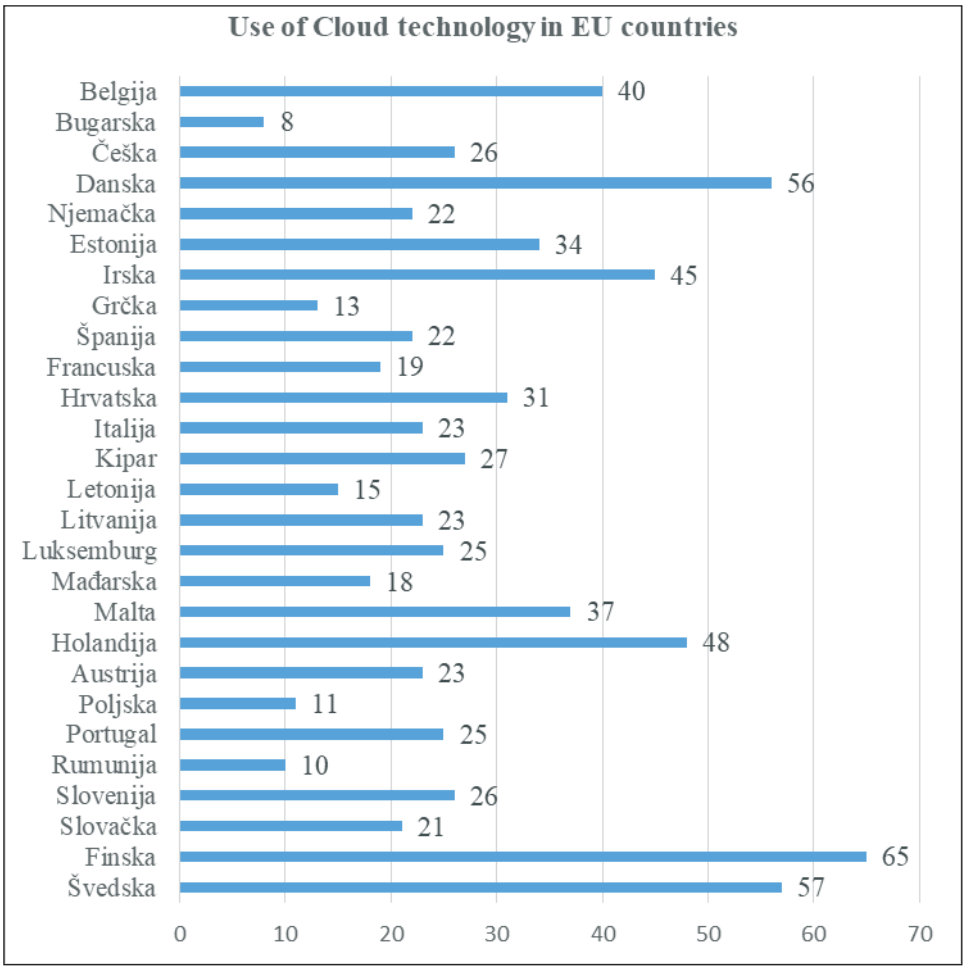


Figure 5: *Percentage of companies paying for Cloud services (by size)*

Although the use of Cloud technology in Serbia is above the percentage recorded in Bosnia and Herzegovina, this is still significantly below European countries. This means that many different measures need to be taken to make Cloud business an integral part of daily life. An important feature of using such forms of distribution is the legislative framework that allows the use of technology. The GDPR adopted at European Union level guarantees the protection of EU citizens' data. As to using solutions via Cloud distribution model, there are limiting factors for non-EU countries such as Bosnia and Herzegovina or Serbia. Namely, the GDPR further complicates the situation given that EU citizens' data must be stored on the territory of the European Union. Another important feature is that there are not many Data Centres in the region that can adequately respond to the needs of Cloud Business in terms of data protection security and adequate data storage.

European Union

According to Eurostat data for 2018, 26% of companies in the European Union with at least 10 employees used Cloud services [4]. The use of Cloud services has increased in recent years compared with 2014 and 2016 when only 19% and 21% of the respective companies used such services. Companies with more than 250 employees tend to use Cloud business more than companies with 10 to 49 employees (56% compared to 23%). In the last four years (2014 – 2018), the major increase in the use of Cloud services was reported in large enterprises (+21%) compared with +12% and 6% in medium and small enterprises respectively. In regional terms, the Cloud business is most used in Nordic companies (over 50%); 65% in Finland, 7 % in Sweden and 56 % in Denmark. The countries with the lowest percentage of companies using Cloud services are Bulgaria (only 8 %) and Romania (10 %). Below is an overview of EU countries using Cloud technology (in %). For our region to keep up with EU countries, it is necessary to align domestic legislation to EU norms and regulations in the future. Another important thing is permanent training and informing both citizens and businesses to recognize the benefits of using Cloud services.



Examples of Large Global Companies Transferring Their Operations to Cloud

We are already surrounded by many examples of Cloud business changing the world of business forever. The Japanese automotive manufacturer Toyota has recently transferred its whole organization of 200,000 employees to the Cloud. Toyota's CTO Yack Hicks said they had done it to do something important for their clients and their business. By doing so, Toyota created more room for their IT staff to focus on cost-effective projects rather than deal with data storage, maintenance and upgrade. This resulted in the following important innovations: semi-autonomous vehicles that can assist the elderly with transportation, a steering wheel that measures the vital signs of the driver and transmits them to a health facility, cars that can alert the police that the driver's health is ill, vehicles that offer many connected online applications, search for parking spaces and the like. The famous media giant Netflix, which accounts for nearly a third of North American internet traffic on an average weekend night, operates in the Cloud. It may sound strange that a company involved in selling print and digital document products is on the list, but Xerox has also recognized the Cloud business trend. In addition to offering Cloud printing service a few years ago, they now have their Cloud service. One of the fastest-growing social networks, Pinterest, has been operating in the Cloud right from the very start as well as Instagram, which has been doing business in the Cloud since 2010 when it began to grow to an undreamed-of level. Apple also opted for the Cloud when developing Siri. Although the majority of users recognize Siri due to its voice, the real magic takes place in the Cloud, where all questions to be answered by Siri are directed. Three out of five companies in the USA applies new knowledge in using Cloud technology.

It is anticipated that it will be impossible to operate without Cloud in five to ten years and that all relevant global companies will follow Toyota's example. Moving to Cloud has begun and this is why

companies in the region should consider transferring their business to Cloud if they want to keep up with other companies.

Conclusion

IT trends show an increased use of Cloud applications. The number of mobile technology users is growing and, consequently, the number of Cloud-customized applications. The value of public Cloud services in the world in 2019 is USD 214.3 billion. Gartner predicts that the value of public Cloud services will rise to USD 331.2 billion by 2022. The same reports indicate that 'Software as a Service' will rise from USD 94.8 billion to USD 143.7 billion in the same period. Cloud business application developers are offering new functionality on a daily basis. However, companies using such business systems need to be convinced of the functionality of such a service and evaluate their business value before fully embracing it. Cloud business information systems will enable lower initial costs, rapid system responsiveness, easier integration with other technologies and global connectivity for organizations. Given the importance of the Internet in every business, one of the biggest benefits of using this type of service is that the user pays the service provider a fee according to how much service is used, as opposed to purchasing their resources but not using them in full. Cloud business is ideal for start-ups because they do not have to invest in their infrastructure as they use Cloud services. It is particularly important to emphasize that the costs of using such technology are acceptable to the smallest users. Given all this, Cloud could be considered a revolutionary solution, and its application in our region will increase in the future. By following the trends of highly developed countries, working and using technology in this way will undoubtedly become commonplace.

Cloud business in Bosnia and Herzegovina is just about to grow and therefore companies need to be more informed about Cloud services. It is also necessary for the competent authorities to adopt a Cloud business strategy. To successfully manage finances, especially in the case of international business and corporate governance, companies in Bosnia and Herzegovina need to provide up-to-date financial information, the application of adequate business communication tools and the coordination of synchronized financial reporting activities. These reasons – financial management and control – are the very benefits of deploying a Cloud business, which primarily reflects in user-friendliness of an integrated business information system and centralized database for analysis, planning and reporting.

Owing to the advantages of Cloud computing, the initial investment in IT has nowadays been significantly reduced and the benefits are multiple. The service provider guarantees the system availability and is likely to provide a 24/7 technical support 365 days a year. The end price is several times lower than the price of own information system. Today, every serious IT company emphasizes the development and sales of products and services related to Cloud.

We hope we have brought closer one of the fastest-growing trends in the IT industry and business in general. Cloud business is still a growing technology which is used for business and private purposes every day. Cloud business will, by all means, become more and more available and simple for end-users and, at the same time, the range of services on offer will become wider. It certainly remains to be seen how successfully RS/BH companies will be able to keep up with the present trends.

References

[1] BH Statistical Institute: http://www.bhas.ba
[2] Cert Carnet (2010) Cloud Computing, available at: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-03-293.pdf
[3] Elmonem, M., Nasr, E. and Geith, M. (2017) Benefits and challenges of Cloud ERP systems – A Systematic Literature Review. Cairo, Egypt: Future Computing and informatics Journal 1, 1-9
[4] Eurostat: https://ec.europa.eu/eurostat
[5] Group of authors (2009) Above the Clouds: A Berkeley View of Cloud Computing
[6] National Institute of Standards and Technology (NIST)
[7] Serbian Statistical Institute, available at http://publikacije.stat.gov.rs/G2018/Pdf/G201816013.pdf
[8] Simonović, (2013) Cloud Computing Technology

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

MihajloTravar earned his PhD at the Faculty of Mechanical Engineering, University of Belgrade. He is a member of Regulatory Commission for Energy of the RepublikaSrpska. Mr Travar is Associate Professor at the 'University of Business Studies' in Banja Luka, where he gives lectures on the following subjects: Databases, Software Engineering, CASE Tools, Design Engineering and ERP Systems. He has written more than forty scientific papers in ICT, mechanical engineering and business organisation.

Igor Dugonjić earned his Master's degree in computer science at the Faculty of Electrical Engineering, University of Banja Luka. He is doing his PhD at Pan-European University 'APEIRON' in Banja Luka. Mr Dugonjić works as a medical equipment programming and maintenance engineer at the University Clinical Centre of the Republika Srpska as well as a senior teaching assistant at the Pan-European University "APEIRON". He has written several scientific papers on medical ICT research.

Saša Ristić graduated on Faculty of Economics in Banja Luka. Currently he is on master studies on University of Banja Luka, department Accounting and audition. For several years he has been working at the largest IT company in region on software solutions in SaaS distribution model. Besides that, he lectures on the seminars of Association of Accountants and Auditors of RS on the subject Information technology. He has written a few scientific works about ERP systems, electrical administration and IT technology.

For citation

Travar M., Dugonjić I., Ristić S., Design, Analysis of Using Cloud Business in Bosnia and Herzegovina and the Region, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:118-125, (UDC: 004.735.8:004.6(497.6), (DOI: 10.7251/JIT1902118T), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

Instructions for Authors

The *Journal of Information Technology and Application (JITA)* publishes quality, original papers that contribute to the methodology of IT research as well as good examples of practical applications.

Authors are advised that adherence to the Instructions to Authors will help speed up the refereeing and production stages for most papers.

- Language and presentation
- Length of submissions
- Submission
- Contact details/biographies
- Title of the paper
- Abstract and keywords
- Figures and tables
- Sections
- Footnotes
- Special characters
- Spelling
- References
- Proofs
- PDF offprint
- Copyright and permissions
- Final material
- Correspondence
- Publication ethics

Language and presentation

Manuscripts should be written in English. All authors should obtain assistance in the editing of their papers for correct spelling and use of English grammar. Manuscripts should have double spacing, with ample margins and pages should be numbered consecutively. The Editors reserve the right to make changes that may clarify or condense papers where this is considered desirable.

Length of submissions

Papers should not normally exceed 12 Journal pages (about 8000 words). However, in certain circumstances (e.g., review papers) longer papers will be published.

Submission

Manuscripts must be submitted through the JITA online submission system.

Please read the instructions carefully before submitting your manuscript and ensure the main article files do not contain any author identifiable information.

Although PDF is acceptable for initial submission original source (i.e. MS Word) files will be required for typesetting etc.

Contact details/biographies

A separate file containing the names and addresses of the authors, and the name and full contact details (full postal address, telephone and e-mail) of the author to whom correspondence is to be directed should be uploaded at the time of submission (you should select Contact details/Biographies as the file type). This file is not shown to reviewers. This file should also contain short biographies for each author (75 words maximum each) which will appear at the end of their paper.

The authors' names and addresses must not appear in the body of the manuscript, to preserve anonymity. Manuscripts containing author details of any kind will be returned for correction.

Title of the paper

The title of the paper should not be longer than 16 words.

Abstract and keywords

The first page of the manuscript should contain a summary of not more than 200 words. This should be self-contained and understandable by the general reader outside the context of the full paper. You should also add 3 to 6 keywords.

Figures and tables

Figures which contain only textual rather than diagrammatic information should be designated Tables. Figures and tables should be numbered consecutively as they appear in the text. All figures and tables should have a caption.

Sections

Sections and subsections should be clearly differentiated but should not be numbered.

Footnotes

Papers must be written without the use of footnotes.

Special characters

Mathematical expressions and Greek or other symbols should be written clearly with ample spac-

ing. Any unusual characters should be indicated on a separate sheet.

Spelling

Spelling must be consistent with the Concise Oxford Dictionary.

References

References in the text are indicated by the number in square brackets. If a referenced paper has three or more authors the reference should always appear as the first author followed by et al. References are listed alphabetically. All document types, both printed and electronic, are in the same list. References to the same author are listed chronologically, with the oldest on top. Journal titles should not be abbreviated.

- Journal

[1] Avramović Z.Ž. (1995). Method for evaluating the strength of retarding steps on a marshalling yard hump. *European Journal of Operational Research*, 85(1), 504–514.

- Book

[2] Walsham G. (1993). Interpreting Information Systems in Organizations. Wiley, Chichester.

- Contributed volume

[3] Huberman A.M. and Miles M.B. (1994). Data Management and analysis methods. In Handbook of Qualitative Research (Denzin NK and Linkoln YS, Eds), pp 428-444, Sage, Thousand Oaks, California.

- Conference Paper

[4] Баранов Л.А. (2017). Принципы построения и алгоритмы интеллектуальных автоматических систем управления движения поездов, функционируемых в рамках городских транспортных систем. In G. Radić & Z.Ž. Avramović (Eds.), *Proceedings of a IX International Scientific Conference "Information Technology for e–Education"*, (pp.9-18). Pan-European University APEIRON, Banjaluka, 29–30.9.2017. Republic of Serpska, B&H

- Unpublished reports/theses

[5] Nandhakumar J.J. (1993). The practice of executive information systems development: and in-depth case study. PhD Thesis, Department of Engineering, University of Cambridge.

Proofs

Proofs of papers will be sent to authors for checking. Alterations to diagrams should be avoided where possible. It will not be possible to accept major textual changes at this stage. Proofs must be returned to the publishers within 48 hours of receipt by fax, first-class post, airmail or courier. Failure to return the proof will result in the paper being delayed.

PDF offprint

Corresponding authors will receive a PDF of their article. This PDF offprint is provided for personal use. It is the responsibility of the corresponding author to pass the PDF offprint onto co-authors (if relevant) and ensure that they are aware of the conditions pertaining to its use.

The PDF must not be placed on a publicly-available website for general viewing, or otherwise distributed without seeking our permission, as this would contravene our copyright policy and potentially damage the journal's circulation. Please visit http://www.jita-au.com to see our latest copyright policy.

Copyright and permissions

The copyright of all material published in the Journal is held by Pan-European University APEIRON. The author must complete and return the copyright form enclosed with the proofs.

Authors may submit papers which have been published elsewhere in a foreign language, provided permission has been obtained from the original publisher before submission.

Authors wishing to use material previously published in JITA should consult the publisher.

Final material

All final material must be submitted electronically in its original application format (MS Word is preferred). The file must correspond exactly to the final version of the manuscript.

Correspondence

Business correspondence and enquiries relating to advertising, subscriptions, back numbers or reprints should be addressed to the relevant person at:

Pan-European University APEIRON
Journal JITA
Pere Krece 13, P.O.Box 51
78102 Banja Luka
Bisnia and Hercegovina / RS

Publication ethics

We take an active interest in issues and developments relating to publication ethics, such as plagiarism, falsification of data, fabrication of results and other areas of ethical misconduct. Please note that submitted manuscripts may be subject to checks using the corresponding service, in order to detect instances of overlapping and similar text.

JITA

PUBLISHER
Pan-European University APEIRON, Banja Luka
College of Information Technology
Banja Luka, Republic of Srpska, B&H
www.apeiron-uni.eu
Darko Uremović, Person Responsible for the Publisher
Aleksandra Vidović, PhD, Editor of University Publications

ISSN 2232-9625
9 772232 962005