VOLUME 9 NUMBER 1 BANJA LUKA, JUNE 2019 (1-48) 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
indexcopernicus.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 1 BANJA LUKA, JUNE 2019 (1-48)

Contents

The content of this issue of JITA consists of five papers.

The first paper, entitled "Statistical Analysis of Texts of the Balkans Electronic Media Columnists" by Nedim Smailović, presents results of statistical analysis of some segments in texts of the four columnists in the Balkans electronic media: Bosnia and Herzegovina – Dnevni avaz (Muhamed Filipović), Serbia – Politika (Aleksandar Apostolovski), Croatia – Jutarnji list (Miljenko Jergović) and Montenegro – Vijesti (Miodrag Lekić). They write about different themes, in different language styles, but statistical analysis clearly points to large similarities in certain segments, such as number of particular alphabet letters, most common combinations of two or three words, etc.

The second paper is "Digitalization of Railways – ICT Approach to the Development of Automation" by Zoran Avramović, Dražen Marinković and Igor Lastrić. The concept of digital railway is defined in the European Initiatives, which started in 2016. The basis for this technical development and improvement plan is the Shift^{2}Rail and the Roadmap for Digital Railways, presented by the Community of European Railways and Infrastructure Managers (CER), the International Rail Transport Committee (CIT), the Association of European Rail Infrastructure Managers (EIM), and the International Union of Railways (UIC).

The next paper is "Digital Signature and Organization of Decentralized Authentication in Business Environment", by Tijana Talić, Zoran Avramović and Gordana Radić. Modern electronic communication is fast and efficient. It has never been easier to change the document's content. This paper explains and shows practical work on how it is possible to protect the data sent electronically in business communication by using decentralized authentication systems.

The forth paper in this issue is "Safety Analysis of Reverse Algorithm Encryption in Databases" by Branko Latinović, Zoran Avramović and Mahir Zaimović. Encryption provides security for databases. This paper provides a new encryption algorithm "Reverse Encryption Algorithm (REA)". The safe and successful proposed encryption algorithm REA is evaluated and compared with the most common encryption algorithms. The designing of the REA algorithm also improves the security of data encryption. Experimental results show that the proposed encryption algorithm REA surpasses other encryption algorithms in performance and security of databases.

The next paper is "The Importance of Information Technologies in Managing Human Potentials of the Logistic Centers of Republika Srpska" by Nataša Đalić, Edit Terek, Mina Paunović and Mihalj Bakator. At the time of great technological innovations, the human resources management plays an important role in achieving the competitive advantage of logistics centers on the market. With the development of new technologies, there are also changes in the way human resources management is handled within companies. The theme of this paper is the research of the connection between the importance of information technologies in managing human potentials and the performance of logistics centers.

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.

Editors, Gordana Radic, Editor-in-Chief, Zoran Avramović, Dušan Starcevic

Statistical Analysis of Texts of the Balkans Electronic Media Columnists

Nedim Smailović

Pan-European University "APEIRON", Banja Luka, Republika Srpska, Bosnia and Herzegovina

Contribution to the state of the art

DOI: **10.7251/JIT1901005S** UDC: **659.3/.4:316.776]:004.738.5**

Abstract: This paper presents results of statistical analysis of some segments in texts of the four columnists in the Balkans electronic media: Bosnia and Herzegovina – *Dnevni avaz* (Muhamed Filipović), Serbia – *Politika* (Aleksandar Apostolovski), Croatia – *Jutarnji list* (Miljenko Jergović) and Montenegro – *Vijesti* (Miodrag Lekić). They write about different themes, in different language styles, but statistical analysis clearly points to large similarities in certain segments, such as number of particular alphabet letters, most common combinations of two or three words, etc. These results leave space to conclude that it is one polycentric language, which is not a rare phenomenon in the modern world. Naturally, the final judgement about this should be given by the linguists.

Keywords: linguistics, language, electronic media, text analysis, visualization of data.

Introduction

Researching the speech and writing systems is a field that receives large attention nowadays. It is understandable, since quality transmission of the verbal signal is impossible without good knowledge of properties of speech. The significance of linguistic works is best confirmed by the fact that highly expensive projects of researching the speaking is financed by the military. Such activity received a large impulse during the WW2. A lot is being done on studying the psychology of listening, understanding the speech and its resilience to interference, synthesis and analysis of speech, translation of encoded messages and foreign language.

What are the touching points, and where do the linguists and the technicians get apart? The linguists are interested in the correctness of content, while the technicians take care of the optimal signal transfer. A linguist wants highest possible intelligibility, while a technician will settle to a minimum intelligibility to satisfy the economical principle. Language terms, such as: rhythm of words, vowels, consonants, stress, length, gender, number and case of each noun and adverb, agreement of sounds in words, words in a sentence, etc. – all these serve the language system to increase intelligibility, secure undisturbed transfer of information and enhance expressivity. Means that improve resilience to interference in language are called redundancy. It is believed that languages contain up to 50% of redundancy, i.e. one half of language means contains the necessary information, while the role of the other half is to enable more secure transfer and receipt of information.

How much redundancy is there in a language is shown in the following example, where, with a little effort, it is possible to understand the meaning of the following text, in which most of the vowels are left out:

I WLD NT B MPSSBL T NDRSTND VN A TXT LK THS, WHCH S WTHT VWELS AND WTHT SPC N TH PLC F TH VWELS.

IT WLD B TH SMPLST ND MST PRCTICL IF W WLD LVE VWELS NLY T TH STRT F WRDS, N IMPRTNT PRFXS ND SFXS. W CLD SVE A LT F TM ND SPC. THAT IS HW IT S MAINLY DNE IN STNOGRAPHY, NT TO MNTION ARAB OR HEBREW WRITING.

Though at first glance it looks like some kind of game, solving such linguistic problems receives a great atten-

tion in the world today, since the roots of contemporary machine and automated translations, and even certain segments of artificial intelligence can be found there.

FREQUENCY OF LETTERS IN EUROPEAN LANGUAGES

Language can be described as a system of symbols that serves for communication among people. [9]. It is a form that mankind expresses itself as a thinking being, uncovering its essence and its difference compared to other living beings. [9].

Linguistics deals with internal order among units of language. Different languages usually have different sets of voices and different sets of letters to write them down. Frequency of use of particular letters is different in every language, as well as in comparison between languages.

In the given languages, there are 84 different letters used, and those are: a, á, à, â, ä, ã, å, ą, æ, b, c, ĉ, ç, č, ć, d, ď, ð, e, ě, é, è, ê, ë, ę, f, g, ğ, ĝ, h, ĥ, i, ı, í, ì, î, ï, j, ĵ, k, l, ł, m, n, ň, ń, ñ, o, ó, ò, ô, ö, õ, ø, œ, p, q, r, ř, s, ś, ŝ, ş, ß, š, t, ť, þ, u, ŭ, ú, ù, û, ü, ů, v, w, x, y, ý, z, ź, ż, ž.

Table 1. *Relative frequences of use of letters in some European languages (descending towards English)*

Letter	English	French	German	Spanish	Esperanto	Italian	Turkish	Swedish	Polish	Danish	Czech
e	12.702%	14.715%	16.396%	12.181%	8.995%	11.792%	9.912%	10.149%	7.352%	15.453%	7.562%
t	9.056%	7.244%	6.154%	4.632%	5.276%	5.623%	3.314%	7.691%	2.475%	6.862%	5.727%
a	8.167%	7.636%	6.516%	11.525%	12.117%	11.745%	12.920%	9.383%	10.503%	6.025%	8.421%
o	7.507%	5.796%	2.594%	8.683%	8.779%	9.832%	2.976%	4.482%	6.667%	4.636%	6.695%
i	6.966%	7.529%	6.550%	6.247%	10.012%	10.143%	9.600%*	5.817%	8.328%	6.000%	6.073%
n	6.749%	7.095%	9.776%	6.712%	7.955%	6.883%	7.987%	8.542%	6.237%	7.240%	6.468%
s	6.327%	7.948%	7.270%	7.977%	6.092%	4.981%	3.014%	6.590%	5.224%	5.805%	5.212%
h	6.094%	0.737%	4.577%	0.703%	0.384%	0.636%	1.212%	2.090%	1.015%	1.621%	1.356%
r	5.987%	6.693%	7.003%	6.871%	5.914%	6.367%	7.722%	8.431%	5.243%	8.956%	4.799%
d	4.253%	3.669%	5.076%	5.010%	3.044%	3.736%	5.206%	4.702%	3.725%	5.858%	3.475%
l	4.025%	5.456%	3.437%	4.967%	6.104%	6.510%	5.922%	5.275%	2.564%	5.229%	3.802%
c	2.782%	3.260%	2.732%	4.019%	0.776%	4.501%	1.463%	1.486%	3.895%	0.565%	0.740%
u	2.758%	6.311%	4.166%	2.927%	3.183%	3.011%	3.235%	1.919%	2.062%	1.979%	2.160%
m	2.406%	2.968%	2.534%	3.157%	2.994%	2.512%	3.752%	3.471%	2.515%	3.237%	2.446%
w	2.360%	0.049%	1.921%	0.017%	0	0.033%	0	0.142%	5.813%	0.069%	0.016%
f	2.228%	1.066%	1.656%	0.692%	1.037%	1.153%	0.461%	2.027%	0.143%	2.406%	0.084%
g	2.015%	0.866%	3.009%	1.768%	1.171%	1.644%	1.253%	2.862%	1.731%	4.077%	0.092%
y	1.974%	0.128%	0.039%	1.008%	0	0.020%	3.336%	0.708%	3.206%	0.698%	1.043%
p	1.929%	2.521%	0.670%	2.510%	2.755%	3.056%	0.886%	1.839%	2.445%	1.756%	1.906%
b	1.492%	0.901%	1.886%	2.215%	0.980%	0.927%	2.844%	1.535%	1.740%	2.000%	0.822%
v	0.978%	1.838%	0.846%	1.138%	1.904%	2.097%	0.959%	2.415%	0.012%	2.332%	5.344%
k	0.772%	0.074%	1.417%	0.011%	4.163%	0.009%	5.683%	3.140%	2.753%	3.395%	2.894%
j	0.153%	0.613%	0.268%	0.493%	3.501%	0.011%	0.034%	0.614%	1.836%	0.730%	1.433%
x	0.150%	0.427%	0.034%	0.215%	0	0.003%	0	0.159%	0.004%	0.028%	0.027%
q	0.095%	1.362%	0.018%	0.877%	0	0.505%	0	0.020%	0	0.007%	0.001%
z	0.074%	0.326%	1.134%	0.467%	0.494%	1.181%	1.500%	0.070%	4.852%	0.034%	1.503%

Source table at the address: *https://en.wikipediam.org/wiki/Letter_frequency [4] also contains data on frequency of use of other letters being used in each of the given 11 languages*

Table 2. *Eleven languages and sorted set of letters used in them*

Letter	English	Letter	French	Letter	German	Letter	Spanish	Letter	Esperanto	Letter	Italian	Letter	Turkish	Letter	Swedish	Letter	Polish	Letter	Danish	Letter	Czech
e	12,70%	e	14,72%	e	16,40%	e	12,18%	a	12,12%	e	11,79%	a	11,92%	e	10,15%	a	10,50%	e	15,45%	a	8,42%
t	9,06%	s	7,95%	n	9,78%	a	11,53%	i	10,01%	a	11,75%	e	8,91%	a	9,38%	i	8,33%	r	8,96%	e	7,56%
a	8,17%	a	7,64%	s	7,27%	o	8,68%	e	9,00%	i	10,14%	i	8,60%	n	8,54%	e	7,35%	n	7,24%	o	6,70%
o	7,51%	i	7,53%	r	7,00%	s	7,98%	o	8,78%	o	9,83%	n	7,49%	r	8,43%	o	6,67%	t	6,86%	n	6,47%
i	6,97%	t	7,24%	i	6,55%	r	6,87%	n	7,96%	n	6,88%	r	6,72%	t	7,69%	n	6,24%	a	6,03%	i	6,07%
n	6,75%	n	7,10%	a	6,52%	n	6,71%	l	6,10%	l	6,51%	l	5,92%	s	6,59%	w	5,81%	i	6,00%	t	5,73%
s	6,33%	r	6,69%	t	6,15%	i	6,25%	s	6,09%	r	6,37%	ı	5,11%	i	5,82%	r	5,24%	d	5,86%	v	5,34%
h	6,09%	u	6,31%	d	5,08%	d	5,01%	r	5,91%	t	5,62%	d	4,71%	l	5,28%	s	5,22%	s	5,81%	s	5,21%
r	5,99%	o	5,80%	h	4,58%	l	4,97%	t	5,28%	s	4,98%	k	4,68%	d	4,70%	z	4,85%	l	5,23%	r	4,80%
d	4,25%	l	5,46%	u	4,17%	t	4,63%	k	4,16%	c	4,50%	m	3,75%	o	4,48%	c	3,90%	o	4,64%	l	3,80%
l	4,03%	d	3,67%	l	3,44%	c	4,02%	j	3,50%	d	3,74%	y	3,34%	m	3,47%	d	3,73%	g	4,08%	d	3,48%
c	2,78%	c	3,26%	g	3,01%	m	3,16%	u	3,18%	p	3,06%	t	3,31%	k	3,14%	y	3,21%	k	3,40%	k	2,89%
u	2,76%	m	2,97%	c	2,73%	u	2,93%	d	3,04%	u	3,01%	u	3,24%	g	2,86%	k	2,75%	m	3,24%	m	2,45%
m	2,41%	p	2,52%	o	2,59%	p	2,51%	m	2,99%	m	2,51%	s	3,01%	v	2,42%	l	2,56%	f	2,41%	u	2,16%
w	2,36%	v	1,84%	m	2,53%	b	2,22%	p	2,76%	v	2,10%	b	2,84%	h	2,09%	m	2,52%	v	2,33%	p	1,91%
f	2,23%	é	1,50%	w	1,92%	g	1,77%	v	1,90%	g	1,64%	o	2,48%	f	2,03%	t	2,48%	b	2,00%	í	1,64%
g	2,02%	q	1,36%	b	1,89%	v	1,14%	g	1,17%	z	1,18%	ü	1,85%	u	1,92%	p	2,45%	u	1,98%	z	1,50%
y	1,97%	f	1,07%	f	1,66%	y	1,01%	f	1,04%	f	1,15%	ş	1,78%	p	1,84%	ł	2,11%	p	1,76%	j	1,43%
p	1,93%	b	0,90%	k	1,42%	q	0,88%	b	0,98%	b	0,93%	z	1,50%	ä	1,80%	u	2,06%	h	1,62%	h	1,36%
b	1,49%	g	0,87%	z	1,13%	ó	0,83%	c	0,78%	h	0,64%	g	1,25%	b	1,54%	j	1,84%	å	1,19%	ě	1,22%
v	0,98%	h	0,74%	ü	1,00%	í	0,73%	ĝ	0,69%	à	0,64%	h	1,21%	c	1,49%	b	1,74%	ø	0,94%	y	1,04%
k	0,77%	j	0,61%	v	0,85%	h	0,70%	ĉ	0,66%	q	0,51%	ç	1,16%	å	1,34%	g	1,73%	æ	0,87%	ý	1,00%
j	0,15%	à	0,49%	p	0,67%	f	0,69%	ŭ	0,52%	è	0,26%	ğ	1,13%	ö	1,31%	ó	1,14%	j	0,73%	á	0,87%
x	0,15%	x	0,43%	ä	0,58%	á	0,50%	z	0,49%	ú	0,17%	c	0,96%	y	0,71%	ę	1,04%	y	0,70%	b	0,82%
q	0,10%	z	0,33%	ö	0,44%	j	0,49%	š	0,39%	w	0,03%	v	0,96%	j	0,61%	h	1,02%	c	0,57%	c	0,74%
z	0,07%	è	0,27%	ß	0,31%	z	0,47%	h	0,38%	í	0,03%	p	0,89%	x	0,16%	ś	0,81%	w	0,07%	ž	0,72%
		ë	0,22%	j	0,27%	é	0,43%	ĵ	0,06%	y	0,02%	ö	0,78%	w	0,14%	ć	0,74%	z	0,03%	š	0,69%
		y	0,13%	y	0,04%	ñ	0,31%	ĥ	0,02%	j	0,01%	f	0,46%	z	0,07%	ż	0,71%	x	0,03%	é	0,63%
		ç	0,09%	x	0,03%	x	0,22%			k	0,01%	j	0,03%	q	0,02%	ą	0,70%	q	0,01%	č	0,46%
		k	0,07%	q	0,02%	ú	0,17%			x	0,00%					ń	0,36%			ř	0,38%
		û	0,06%			w	0,02%									f	0,14%			ů	0,20%
		ù	0,06%			ü	0,01%									ź	0,08%			g	0,09%
		â	0,05%			k	0,01%									v	0,01%			f	0,08%
		w	0,05%																	ú	0,05%
		î	0,05%																	x	0,03%
		ô	0,02%																	ó	0,02%
		œ	0,02%																	w	0,02%
		ë	0,01%																	ď	0,02%
		ï	0,01%																	ň	0,01%
																				ť	0,01%

If we present the usage frequency of those letters for each language in the descending order, we get the following table:

The following figures present the data from the table above, visualized by Treemap type of charts. Letter usage frequency is proportional to the corresponding surface on the chart. This kind of presentation clearly shows dominance (higher frequency) of particular letters compared to other letters. Below each chart there is a descending order of letters for that language, left to right.

Table 3. *Graphical presentation of letter usage frequency in particular languages*

Columnists

a i o e n r s t u j k v m d l p g z b č c š n j h ć ž lj f đ dž

English

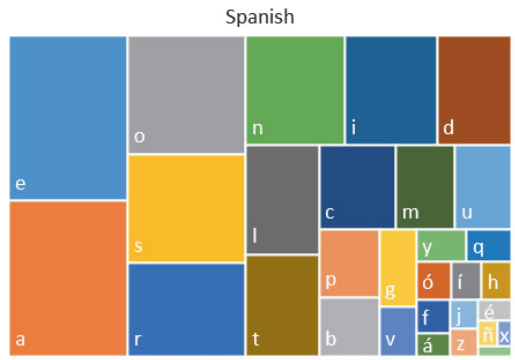
e t a o i n s h r d l c u m w f g y p b v k j x q z

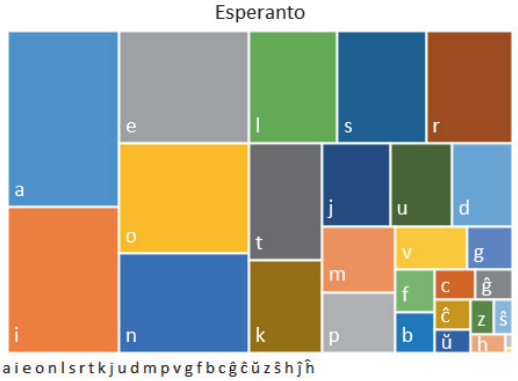
French

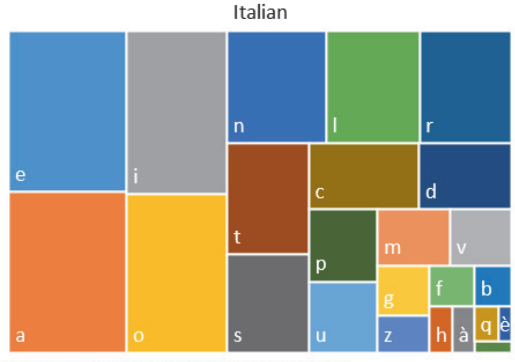
e s a i t n r u o l d c m p v é q f b g h j à x z è ê ê y ç k û ù â w î ô œ ë ï

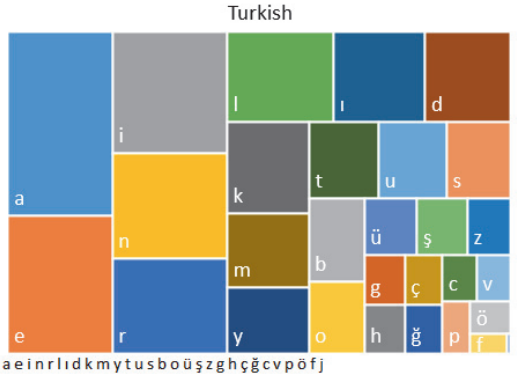
German

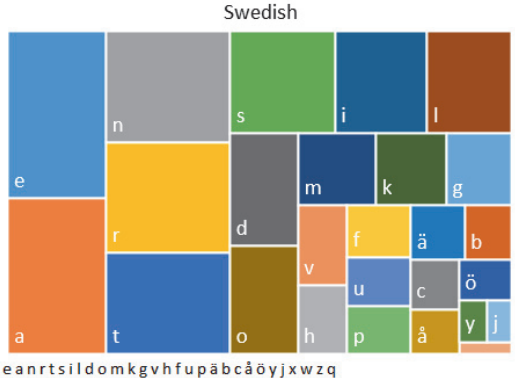
e n s r i a t d h u l g c o m w b f k z ü v p ä ö ß j y x q

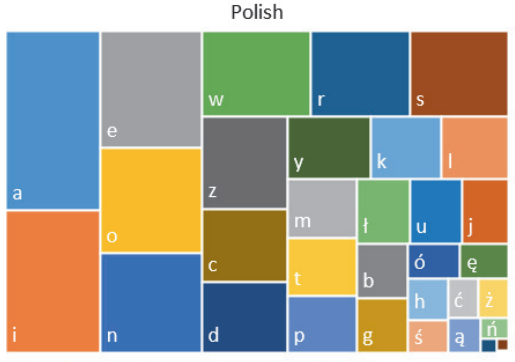


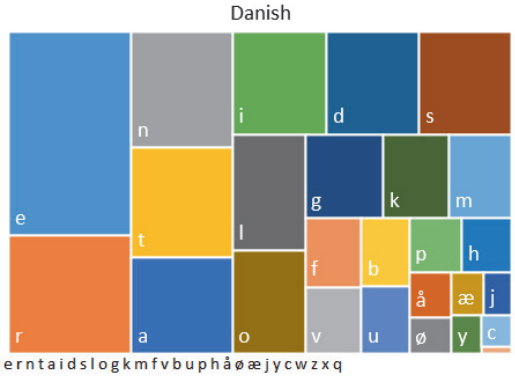


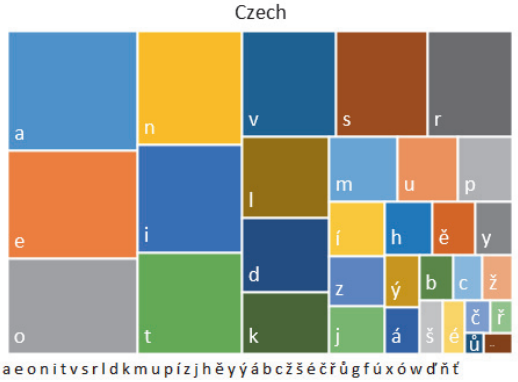












For easier remembering of the order of letter usage frequency, the bibliography offers the first twelve most frequently used letters given in two (non-existing) six-letter words. For our eleven languages, those words are:

English	etaoin shrdlc
French	esaitn ruoldc
German	ensria tdhulg
Spanish	eaosrn idltcm
Esperanto	aieonl srtkju
Italian	eaionl rtscdp
Turkish	aeinrl ıdkmyt

Swedish	eanrts ildomk
Polish	aieonw rszcdy
Danish	erntai dslogk
Czech	aeonit vsrldk

World statistics confirms that there are over 7100 spoken languages today. It is not easy to establish the exact number of languages as there are no clear boundaries between certain languages and dialects. Besides, some languages are disappearing. In the course of the 20th century, 110 languages were proclaimed extinct, while 12 languages have disappeared in this century.

Published scientific linguistic works, printed and electronic, analyze language and its characteristics in many places. Naturally, such analyses usually refer to dominant world languages: Chinese, Spanish, English, Hindi, Arab, Bengali, Portuguese, Russian, Japanese… [1]

This list of the largest (by number of people speaking) world languages is different, if sorted according to their impact in trade and industry, social, political and economy circles. English language is on top of that list, followed by French, which is an official language in 25 countries. There are 2303 languages spoken in Asia, while in Europe there are 285.

Language is a living organism. It is constantly changing. Some words emerge, some get into a language from other languages, some words change their meaning, and some become archaic over the time and disappear. Therefore, new analyses should be done in continuity, while that job is significantly alleviated with new IT tools.

Statistical Analysis of Text in Selected Columns

A smaller or larger sample is necessary for any analysis. The samples for this analysis were taken from texts by four columnists in the Balkans electronic media: Bosnia and Herzegovina – *Dnevni avaz* (Muhamed Filipović), Serbia – *Politika* (Aleksandar Apostolovski), Croatia – *Jutarnji list* (Miljenko Jergović) and Montenegro – *Vijesti* (Miodrag Lekić). [2] [3] [7] [8] All of them still write for the mentioned media, so we can say that this analysis deals with modern language.

In order to be able to make a comparative analysis of language of aforementioned columnists, it is necessary to compare samples of equal length, so the texts were selected and merged to be equal in number of characters (without blanks). In all examples, the merged set of columns for each columnist had exactly 148.232 characters (without blanks). Among these characters there are also letters not used in the columnists' alphabets (such as w, q and similar). For the said number of characters, it took: 23 columns by Miljenko Jergović, 32 columns by Filipović, 34 columns by Apostolovski and 25 columns by Lekić. In some tables, we analyzed a summary-merged text of all columnists, which gives a sample of over half a million characters.

Table 4. *Framework statistics of text samples*

	ALL	JERGOVIĆ	FILIPOVIĆ	APOSTOLOVSKI	LEKIĆ
No. of pages	163	40	46	41	36
No. of words	109.707	27.976	28.857	27.509	25.365
No. of characters without blanks	592.928	148.232	148.232	148.232	148.232
No. of characters with blanks	701.032	175.893	176.607	175.417	173.115
No. of paragraphs	1.936	323	565	425	623
No. of lines	7.997	1.953	1.946	2.161	1.937
No. of sentences	5.519	1.301	1.140	1.503	1.575

It is important to say that in this paper we did not analyze standpoints or opinions of columnists or their editors, but exclusively statistical analysis of the text produced.

The authors have their style of writing, and some combinations occur more often than others. In the following table, we gave three-words combinations that occur with each author over five times.

In a joined text of all columnists, "ono što je" (which is) was the most often repeated combination of three words.

Individually, it was as follows:

Jergović: "ono što je" (13 times), Filipović: "Bosne i Hercegovine" (24 times), Apostolovski: "da li je" (12 times) and Lekić: "u Crnoj Gori" (25 times).

Table 5. *The most often repeated combination of three words*

3 words together	ALL	3 words together	JERGOVIĆ	3 words together	FILIPOVIĆ	3 words together	APOSTOLOVSKI	3 words together	LEKIĆ
ono što je	33	ono što je	13	Bosne i Hercegovine	24	da li je	12	u Crnoj Gori	25
i da se	30	koji su se	12	Bosni i Hercegovini	23	se da je	10	s druge strane	10
s druge strane	29	i to je	11	a to je	19	kako bi se	10	o Crnoj Gori	9
u Crnoj Gori	27	a onda i	11	u Bosni i	18	da li će	9	u isti mah	9
Bosne i Hercegovine	26	ne samo da	10	ono što je	18	kao da je	8	Crnoj Gori i	8
ono što se	25	u vrijeme kada	8	s druge strane	18	ne može da	7	i da se	6
Bosni i Hercegovini	25	je riječ o	8	i da se	15	kao što je	6	SAD i Rusije	6
kao što je	23	prije nego što	8	na taj način	13	i da se	6	radi se o	6
tako da je	23	ono što se	7	kao što je	12	je da je	6	na međunarodnom planu	6
a to je	22	tako da se	7	da je to	12	je reč o	6	u svakom slučaju	6
koji su se	22	tako da je	7	tako da je	12	saveza za s Srbiju	6	i da je	5
kao što su	21	kao što su	6	Bosna i Hercegovina	12	u kojoj je	6	u vezi sa	5
da je to	20	a zatim i	6	da se ne	11	pravoslavne nove godine	6	u kojem je	5

Table 6. *The most commonly repeated combination of two words*

2 words together	ALL	2 words together	JERGOVIĆ	2 words together	FILIPOVIĆ	2 words together	APOSTOLOVSKI	2 words together	LEKIĆ
da je	418	da je	86	da se	171	da je	127	da je	63
da se	395	što je	78	da je	140	da se	100	da se	59
što je	210	da se	63	i da	90	da su	48	pa i	44
koji je	174	je u	60	što je	86	koji je	43	crnoj gori	39
je u	167	i u	47	koji je	73	su se	36	je u	36
i da	157	su se	39	koji su	55	je u	36	koji su	28
koji su	134	kao i	37	to je	54	da će	36	i u	27
i u	127	što se	37	ono što	45	koji se	36	koji je	27
su se	127	koji su	32	koja je	43	da li	32	u crnoj	26
da su	126	ono što	32	je bio	42	je to	30	je bio	26
to je	113	koji je	31	tako da	41	je da	30	i to	23
je to	107	bi se	30	zbog toga	41	se u	30	je i	21
što se	102	je to	29	da će	40	se da	29	su se	20

In a joined text of all columnists, "da je" (that is) was the most often repeated combination of two words – 418 times. With authors individually, two most commonly words used together were: Jergović: "da je" (86 times), Filipović: "da se " (171 times), Apostolovski: "da je" (127 times) and Lekić: "da je" (63 times).

Looking at individual words, it is noticeable that among the most frequently used ones in a joined text there were no nouns, verbs, adjectives, numbers… The dominating were connections, auxiliary verbs, prepositions (non-lexical, function words).

It is interesting that: **i**, **je**, **u**, **da**, **se**, **na** with all authors were among the first six most frequent words.

In that sense, we could perform a separate analysis of lexical density in the columns, measuring how informative the text is.

Remark:

Lexical density is defined as a number of lexical words (or content words) divided by a total number of words. Lexical words give meaning to a text. Those are nouns, adjectives, verbs and adverbs. Other types of words (functional words), such as auxiliary verbs, prepositions or conjunctions, are more of grammatical nature and they give little or no information about the subject matter.

With individual authors, the most frequent nouns were: Jergović: "vrijeme" (time) and "godina" (year) (47 times), Filipović: "države" (state) (67 times) and "ljudi" (people) (65 times), Apostolovski: "godine" (year) (66 times) and Lekić: "istorije" (history) (62 times) and "rata" (war) (52 times).

Table 7. *The most frequent words*

the most frequent word	ALL	the most frequent word	JERGOVIĆ	the most frequent word	FILIPOVIĆ	the most frequent word	APOSTOLOVSKI	the most frequent word	LEKIĆ
i	4603	i	1389	i	1153	je	1033	i	1137
je	3889	je	1058	je	1098	i	924	u	873
u	3390	u	827	da	1088	da	847	je	700
da	2796	se	520	u	859	u	831	da	407
se	1986	da	454	se	580	se	539	se	347
na	1551	na	416	na	389	na	412	na	334
su	1223	su	323	sam	319	su	365	su	243
za	768	što	297	su	292	za	235	sa	184
što	692	ne	224	to	262	kao	200	za	174
to	684	a	196	a	241	od	176	o	144
ne	678	kao	196	koji	232	koji	165	od	132
a	673	s	195	što	230	a	160	iz	116
koji	663	od	190	ne	182	ne	156	ne	116
kao	652	nije	188	za	176	ali	147	koji	115
od	622	za	183	s	165	će	145	to	111
o	562	to	181	kao	161	s	138	kao	95
s	528	bi	171	o	158	bi	137	nije	81
nije	515	o	164	mi	141	to	130	a	76
bi	452	koji	151	bio	130	nije	128	treba	72
sam	440	ali	136	od	124	iz	114	dakle	69
iz	439	ili	134	koja	119	što	111	do	67
će	421	će	117	nije	118	o	96	pa	65
ali	401	iz	115	on	108	kako	91	bio	63
ili	353	tako	96	tako	108	ili	79	istorije	62
sa	337	samo	95	odnosno	102	kada	76	već	61
bio	330	ni	94	će	101	–	74	koje	60
koja	277	bilo	94	bi	96	bio	72	će	58
kako	273	nego	88	koje	95	već	70	bez	57

koje	272	po	83	iz	94	sa	66	sve	57
tako	268	sve	82	bilo	92	godine	66	ili	56
bilo	257	te	79	smo	92	ga	65	što	54
samo	257	kada	73	ja	88	po	65	rata	52
kada	245	kako	68	bih	86	li	62	ali	51
sve	242	koja	68	jer	86	mu	60	uz	49
do	236	biti	66	ili	84	jer	60	koja	49
po	228	koje	65	kako	79	ako	58	zemlje	49
pa	223	bio	65	nego	78	samo	58	bi	48
ni	218	pa	63	do	75	sve	56	još	48
mi	214	ga	62	toga	75	posle	55	po	45
jer	212	do	57	tome	71	koje	52	kada	45
on	201	jer	54	kad	71	ni	50	poslije	41
nego	193	onda	51	rekao	70	dok	50	sam	41
već	190	bila	51	ali	67	pa	49	dvije	40
ga	189	ono	49	države	67	još	49	između	40
te	180	on	48	samo	65	jedan	47	crnoj	40
biti	167	vrijeme	47	ljudi	65	tako	44	gori	39
smo	167	godina	47	šta	62	više	43	samo	39
ako	165	može	46	vrlo	62	koja	41	godine	39
li	158	ona	46	način	61	on	40	kako	35
bila	158	ništa	45	prema	59	sam	39	države	35

Digrams, or digraphs, from Greek δίς dís, "twice, two times" and γράφω gráphō, "to write", are combinations of at least two written units, letters (graphemes) to mark a single phoneme in a language. A digraph is not the same as two characters pronounced consecutively. Digraphs are often present in foreign languages, for example: qu, ch, ph, ee, cs, dz, dzs, gy, ly, ny, sz, ty, zs, dh, gj, ll, nj, rr, sh, th, xh, zh. When a digraph is capitalized, both letters are in capital character.

In Bosnian, Serbian, Croatian and Montenegrin language, which were treated as single Serbo-Croat language prior to the fall of SFR Yugoslavia, the digraphs were dž, lj and nj.

Each author has his own style of writing, characterized by different properties. In the analyzed

Table 8. *Frequency of words according to number of characters*

svi		Jergović		Filipović		Apostolovski		Lekić	
Broj karaktera u riječima	Frekvencija (%)	Broj karaktera u riječima	Frekvencija (%)	Broj karaktera u riječima	Frekvencija (%)	Broj karaktera u riječima	Frekvencija (%)	Broj karaktera u riječima	Frekvencija (%)
1	8,9	1	9,9	1	8,9	1	7,8	1	9,0
2	17,1	2	16,8	2	19,5	2	18,0	2	13,7
3	6,6	3	6,8	3	7,6	3	6,7	3	5,0
4	10,9	4	11,8	4	11,5	4	10,1	4	10,1
5	10,4	5	10,5	5	11,0	5	10,0	5	10,0
6	10,1	6	10,1	6	8,8	6	11,1	6	10,8
7	9,3	7	8,6	7	9,5	7	9,5	7	9,7
8	7,8	8	7,5	8	7,3	8	8,0	8	8,6
9	6,2	9	6,1	9	5,5	9	5,7	9	7,5
10	4,8	10	4,5	10	4,0	10	4,8	10	6,0
11	3,5	11	3,2	11	3,1	11	3,4	11	4,2
12	1,8	12	1,7	12	1,6	12	1,8	12	2,3
13	1,1	13	1,1	13	0,8	13	1,0	13	1,4
14	0,7	14	0,7	14	0,4	14	0,8	14	0,9

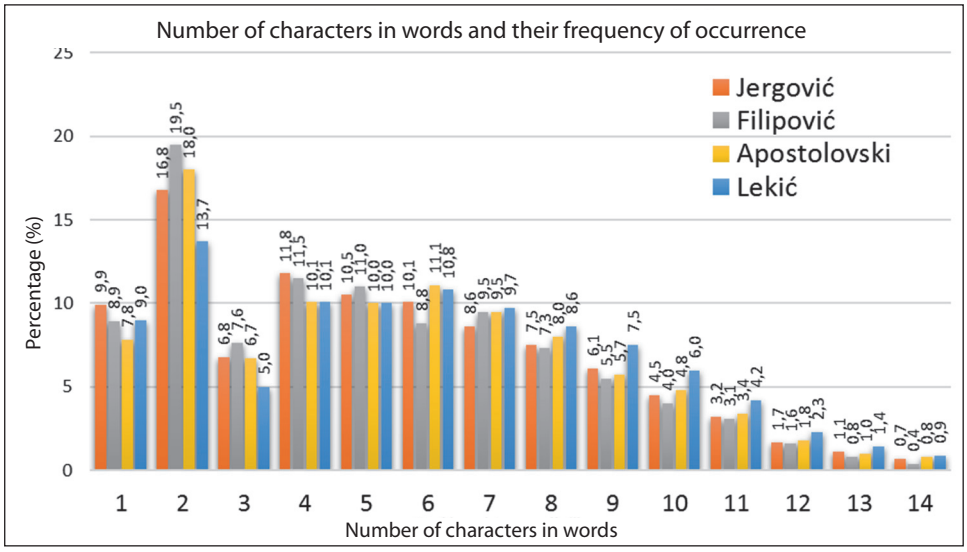


Figure 1. *Frequency of words according to number of characters*

Table 9. *The most frequent combinations of two consecutive letters in analyzed columns*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
je	na	ra	ko	ni	st	ij	no	an	li	ti	da	po	ta	ka	re	ov	ne	ja	to	pr	ma	en	va	ri	im	oj	al	nj	vi

texts of all authors, words of up to 14 characters make over 99% of text, and their frequency per number of characters is given in the following table and chart.

There were more and less frequent combinations of two consecutive letters in the texts. Some of them were even words, such as: iz, na, li, on, to, mi and similar. In the sample texts there were even combinations of the same letters one next to another, but mostly because the authors were citing original transcription of names, or were using foreign words.

In Bosnian, Serbian, Croatian and Montenegrin language, there are rare examples of two consecutive letters which are the same. They appear in compounds, such as: najjači, najjasniji, narodnooslobodilački, prekookeanski, kooperativan etc.

Table 10. *An overview of frequency of combinations of two consecutive letters*

	a	b	c	č	ć	d	dž	đ	e	f	g	h	i	j	k	l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž		rank
a	5	1114	755	743	591	5644	33	314	168	225	1626	261	72	4495	4816	3603	613	4430	8525	882	74	1576	7689	2787	562	5079	178	4378	3019	746	a	65.003	1
b	290	0	5	0	0	164	10	0	610	2	2	2	110	55	0	36	1	154	10	0	1533	0	314	10	0	55	378	0	402	75	b	4.218	22
c	1248	0	6	2	0	1	0	0	287	0	0	0	1467	29	168	32	2	27	460	3	277	37	172	128	0	10	167	81	0	0	c	4.604	19
č	1083	0	0	0	0	0	0	0	375	0	0	0	1707	16	13	2	0	6	45	0	571	8	34	1	29	2	632	11	0	0	č	4.535	20
ć	196	0	0	0	0	0	0	0	963	0	0	0	947	0	8	0	0	8	2	0	203	57	13	0	122	0	598	1	0	0	ć	3.118	23
d	2560	15	1	0	0	1	0	0	3034	0	144	5	607	58	0	48	19	40	456	0	3682	1	210	15	0	21	827	79	173	103	d	12.099	15
dž	30	0	0	0	0	0	0	0	6	0	0	0	16	17	0	0	0	0	2	0	5	0	6	0	0	0	17	0	0	0	dž	99	30
đ	378	0	0	0	0	0	0	0	542	0	0	0	25	0	0	0	0	0	0	0	216	0	75	0	0	0	82	0	0	2	đ	1.320	28
e	50	860	790	938	1143	1728	39	450	7	231	389	201	51	14848	1517	1983	868	2621	4725	1862	37	639	4759	2975	771	2689	71	3062	577	932	e	51.813	2
f	156	0	0	0	0	0	0	0	153	3	0	0	100	4	1	49	0	13	109	0	119	0	16	39	0	6	16	0	0	0	f	784	29
g	605	0	9	0	0	174	0	0	1460	3	2	0	494	10	2	23	0	0	161	0	3592	0	219	1	0	0	795	13	202	0	g	7.765	16
h	229	3	59	0	0	0	0	0	84	0	1	0	2054	5	1	1	0	0	5	0	95	19	95	87	0	0	137	0	0	0	h	2.875	25
i	166	2831	2652	1368	829	2570	40	91	50	480	530	230	2	2755	1750	5927	331	1743	6820	700	103	934	4253	1141	512	5702	27	3845	1127	848	i	50.355	3
j	2522	211	60	30	0	433	0	0	205	0	0	0	6186	4	2	2677	0	353	3873	0	4077	194	88	268	1	92	516	616	49	21	j	22.478	7
k	3007	2	36	1213	23	0	0	0	1868	1	0	5	2309	126	0	62	21	8	343	1	1212	13	272	3040	357	327	557	50	0	0	k	14.853	13
l	4054	401	10	84	0	212	0	0	2184	32	684	25	2797	20	591	24	0	328	4	0	2092	388	237	1751	251	13	688	752	331	12	l	17.965	10
lj	302	59	1	0	0	21	0	0	375	0	2	0	227	2	108	0	0	230	2	0	273	76	25	132	80	36	20	389	1	12	lj	2.373	26
m	2625	1	0	2	0	101	0	25	2575	0	45	18	4179	72	15	102	0	4	0	0	3802	2	277	680	12	25	650	3	319	9	m	15.543	12
n	5939	193	0	640	116	1970	0	0	4386	2	62	25	3535	478	253	715	122	346	21	0	2822	58	881	982	364	695	673	1241	817	247	n	27.583	5
nj	1267	3	0	13	4	165	0	0	490	0	10	0	268	12	195	0	1	38	0	0	26	7	20	0	276	28	20	4	0	37	nj	2.884	24
o	1975	1173	70	199	48	1966	21	53	488	309	2770	446	1876	614	7181	2702	23	2740	6007	93	39	5292	2959	568	55	4445	130	3454	302	44	o	48.042	4
p	772	0	0	0	0	6	0	0	458	0	0	0	337	47	4	13	0	239	15	0	1008	1	248	894	18	112	706	0	0	0	p	4.878	18
r	2950	797	366	0	0	1538	0	0	2578	207	1101	309	1251	8	1076	0	0	175	30	0	3392	4432	13	574	2	2129	613	1237	130	34	r	24.942	6
s	1697	3	0	0	0	406	0	0	1732	20	2	1	2802	448	306	84	57	110	974	28	3703	383	500	30	0	79	1189	109	0	0	s	14.663	14
š	1022	1	0	0	0	1	0	0	554	0	0	0	812	15	7	3	6	11	9	0	721	104	202	0	0	1	837	88	0	0	š	4.394	21
t	3037	0	21	0	0	2	0	0	2334	6	11	63	2926	47	549	267	2	15	1245	0	1351	80	436	6661	1782	22	837	5	1	0	t	21.700	8
u	289	433	316	304	218	778	7	479	140	104	536	44	0	2687	1592	897	523	871	1113	298	76	568	1670	2002	110	1456	5	553	382	89	u	18.540	9
v	3605	14	18	9	0	424	0	0	1274	0	17	160	1708	116	442	11	0	1	23	0	4728	0	562	1766	27	1203	293	0	450	6	v	16.857	11
z	1275	35	0	0	0	12	0	0	806	2	20	0	2213	47	1	2	0	1	101	0	662	0	100	0	0	24	433	0	7	0	z	5.741	17
ž	528	0	0	0	0	0	0	0	236	0	0	0	188	0	0	2	0	0	12	0	514	0	541	0	0	0	305	0	0	0	ž	2.326	27
	a	b	c	č	ć	d	dž	đ	e	f	g	h	i	j	k	l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž		
	43.862	8.149	5.175	5.545	2.972	18.317	150	1.412	30.422	1.627	7.954	1.795	41.266	27.035	20.598	19.265	2.589	14.512	35.092	3.867	41.005	14.869	26.886	26.532	5.331	24.251	12.397	19.971	8.289	3.215		474.350
rank	1	18	22	20	25	13	30	29	5	28	19	27	2	6	10	12	26	15	4	23	3	14	7	8	21	9	16	11	17	24		

The following table gives frequency of all combinations of neighboring letters in a unified text of all authors and columns. The table is read by first looking at the column, and then at the row. The cross section gives the number of those combinations in the text. For example, the combination "do" was found 1966 times. Fields with number of noticed combinations were conditionally colored in a way that in each column the least frequent are red, and as the frequency increases, the color proceeds into white, and finally into green. In the table, it is easy to distinguish, by red color, combinations of two letters that do not appear at all, or very rarely, and those in green, which are the most frequent ones (in a column).

It may be noticed that two consecutive letters most often have letter "a" as the first (43.862 times),

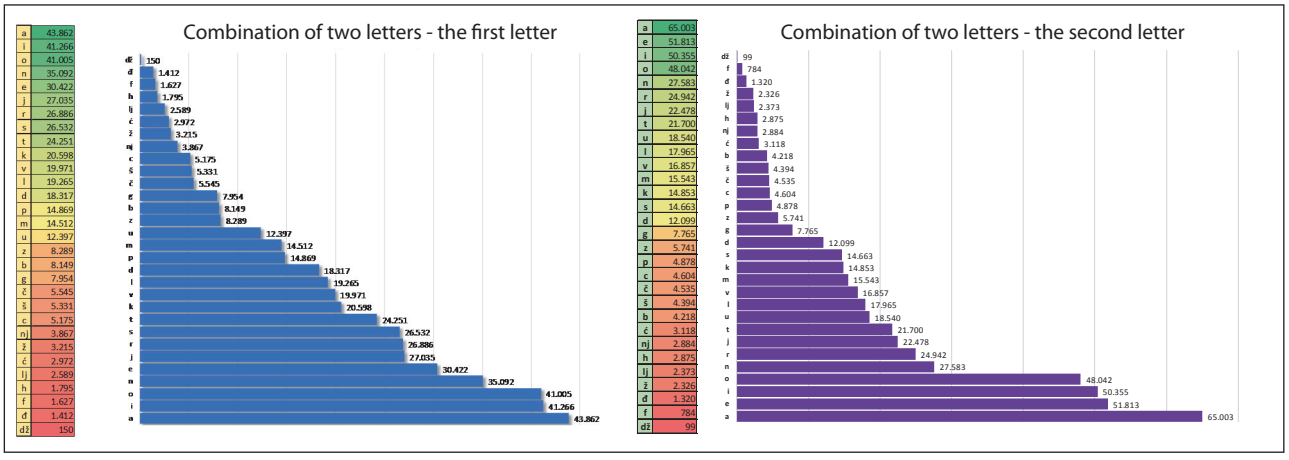


Figure 2. *Order of combinations of two consecutive letters*

followed by i, o, n, e, j, etc., while least frequent were letters: dž (150 times), đ, f, h, lj, etc.

In combination of two consecutive letters, the most frequent second letter is "a" (65.003 times), followed by e, i, o, n, r, etc., and least frequent were letters: dž (99 times), f, đ, ž, lj, h, etc.

Table 11. *Frequency of letters of individual columnists – alphabetically and in descending order*

			Filipović	Jergović	Apostolovski	Lekić	SVI
1	a	A	17.213	15.795	17.140	16.067	66.215
2	b	B	2.168	1.952	2.266	1.748	8.134
3	c	C	1.132	1.248	1.445	1.549	5.374
4	č	Č	1.269	1.610	1.419	1.355	5.653
5	ć	Ć	961	809	1.227	630	3.627
6	d	D	5.506	4.359	5.271	4.616	19.752
7	dž	Dž	53	21	56	28	158
8	đ	Đ	371	293	404	345	1.413
9	e	E	11.923	12.619	12.539	12.807	49.888
10	f	F	422	341	372	545	1.680
11	g	G	2.426	2.412	2.504	2.553	9.895
12	h	H	1.025	1.129	800	823	3.777
13	i	I	14.615	15.252	14.051	14.503	58.421
14	j	J	6.000	5.960	4.600	5.451	22.011
15	k	K	5.062	5.471	5.646	5.239	21.418
16	l	L	3.913	4.070	4.624	4.241	16.848
17	lj	Lj	612	804	584	701	2.701
18	m	M	5.333	5.036	4.469	5.047	19.885
19	n	N	8.048	8.497	8.019	8.605	33.169
20	nj	Nj	949	1.027	841	1.056	3.873
21	o	O	14.294	13.591	13.509	12.784	54.178
22	p	P	3.465	3.432	4.075	3.911	14.883
23	r	R	6.426	6.356	7.173	7.896	27.851
24	s	S	6.973	6.818	6.822	6.853	27.466
25	š	Š	1.412	1.528	1.399	971	5.310
26	t	T	6.651	6.965	5.974	6.615	26.205
27	u	U	5.806	5.564	6.141	5.843	23.354
28	v	V	4.974	5.102	5.233	4.748	20.057
29	z	Z	2.238	2.203	2.291	2.386	9.118
30	ž	Ž	913	885	752	642	3.192
			142.153	141.149	141.646	140.558	**565.506**

sort

		Filipović
a	A	17.213
i	I	14.615
o	O	14.294
e	E	11.923
n	N	8.048
s	S	6.973
t	T	6.651
r	R	6.426
j	J	6.000
u	U	5.806
d	D	5.506
m	M	5.333
k	K	5.062
v	V	4.974
l	L	3.913
p	P	3.465
g	G	2.426
z	Z	2.238
b	B	2.168
š	Š	1.412
č	Č	1.269
c	C	1.132
h	H	1.025
ć	Ć	961
nj	Nj	949
ž	Ž	913
lj	Lj	612
f	F	422
đ	Đ	371
dž	Dž	53
		142.153

sort

		Jergović
a	A	15.795
i	I	15.252
o	O	13.591
e	E	12.619
n	N	8.497
t	T	6.965
s	S	6.818
r	R	6.356
j	J	5.960
u	U	5.564
k	K	5.471
v	V	5.102
m	M	5.036
d	D	4.359
l	L	4.070
p	P	3.432
g	G	2.412
z	Z	2.203
b	B	1.952
č	Č	1.610
š	Š	1.528
c	C	1.248
h	H	1.129
nj	Nj	1.027
ž	Ž	885
ć	Ć	809
lj	Lj	804
f	F	341
đ	Đ	293
dž	Dž	21
		141.149

sort

		Apostolovski
a	A	17.140
i	I	14.051
o	O	13.509
e	E	12.539
n	N	8.019
r	R	7.173
s	S	6.822
u	U	6.141
t	T	5.974
k	K	5.646
d	D	5.271
v	V	5.233
l	L	4.624
j	J	4.600
m	M	4.469
p	P	4.075
g	G	2.504
z	Z	2.291
b	B	2.266
c	C	1.445
ć	Č	1.419
š	Š	1.399
ć	Ć	1.227
nj	Nj	841
h	H	800
ž	Ž	752
lj	Lj	584
đ	Đ	404
f	F	372
dž	Dž	56
		141.646

sort

		Lekić
a	A	16.067
i	I	14.503
e	E	12.807
o	O	12.784
n	N	8.605
r	R	7.896
s	S	6.853
t	T	6.615
u	U	5.843
j	J	5.451
k	K	5.239
m	M	5.047
v	V	4.748
d	D	4.616
l	L	4.241
p	P	3.911
g	G	2.553
z	Z	2.386
b	B	1.748
c	C	1.549
č	Č	1.355
nj	Nj	1.056
š	Š	971
h	H	823
lj	Lj	701
ž	Ž	642
ć	Ć	630
f	F	545
đ	Đ	345
dž	Dž	28
		140.558

sort

		SVI
a	A	66.215
i	I	58.421
o	O	54.178
e	E	49.888
n	N	33.169
r	R	27.851
s	S	27.466
t	T	26.205
u	U	23.354
j	J	22.011
k	K	21.418
v	V	20.057
m	M	19.885
d	D	19.752
l	L	16.848
p	P	14.883
g	G	9.895
z	Z	9.118
b	B	8.134
č	Č	5.653
c	C	5.374
š	Š	5.310
nj	Nj	3.873
h	H	3.777
ć	Ć	3.627
ž	Ž	3.192
lj	Lj	2.701
f	F	1.680
đ	Đ	1.413
dž	Dž	158
		565.506

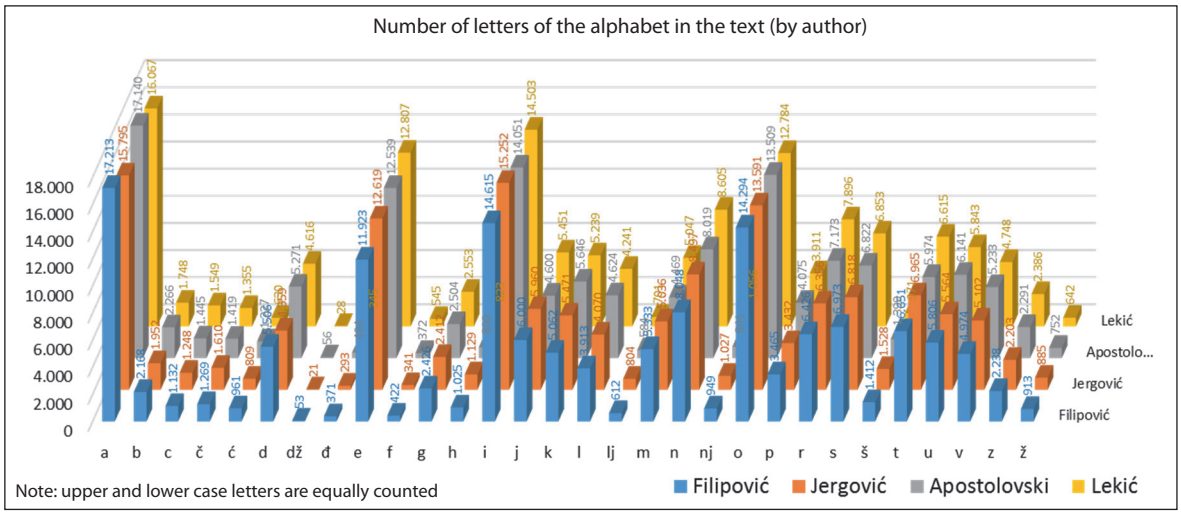


Figure 3. *Number of particular alphabet letters in texts of the column authors*

Analysis of Frequency of Certain Letters in a Text

Frequency of particular letters in a text may depend on several factors. Among them are: language of use, type of text (prose, poetry, technical text…), theme of the text, author's style and the usual fund of words the author uses, etc. In the Internet, one can find pages [6] and programs to get the number of particular letters in the given text, but a great deal of those tools does not recognize our characters č, ć, dž, đ, lj and nj. In that case, possibilities offered by text processors may be used.

Here is the analysis of frequency of particular letters for each of the columnists separately.

Order of letters per individual author:

Filipović:	aioenstrjudmkvlpgzbščchćnjžljfđdž
Jergović	aioentsrjukvmdlpgzbčšchnjžćljfđdž
Apostolovski	aioenrsutkdvljmpgzbcčšćnjhžljđfdž
Lekić	aieonrstujkmvdlpgzbcčnjšhljžćfđdž
ALL	aioenrstujkvmdlpgzbčcšnjhćžljfđdž

It is indicative to compare these orders with the orders given in Table 3: Graphic presentation of frequency of letters in particular languages.

Conclusion

Linguistics deals with language (French *linguistique,* from Latin *lingua* – language), which may be subdivided to: phonetics (science of sounds), phonology (science of function of sounds), morphology (science about forms of language units), syntax (science about organization of sentence), semantics (science about meanings in language), etc. Linguistics is multidisciplinary science, and therefore its specialized branches emerged in the 20th, such as: mathematical linguistics, psycholinguistics, sociolinguistics, neurolinguistics. In this paper we statistically analyzed the language of four distinguished columnists in electronic media. They wrote about different topics, with different language styles, but there were noticeable large similarities in some segments. Such results give space to conclude that it is one, single, polycentric language, which is not a rare phenomenon in the modern world. Naturally, the final word about this should be given by linguists. Polycentric languages are English (Great Britain and the USA), German (Germany, Austria, Switzerland), French (France, Canada (Québec), Belgium), Spanish (Spain, Argentina, Mexico), Persian (Iran, Afghanistan, Tajikistan), Portuguese (Brazil, Portugal), Arabic (Saudi Arabia, Iran, Iraq, Tunisia, Egypt…), etc. Each of the variants of any polycentric language has its standard national variation, grammar and orthography, distinguishable according to some differences. [5]

There are also monocentric languages, such as Japanese or Russian, which do not have more standardized variations.

Modern electronics enables language analyses that could not be imagined until recently, which will probably impact the creation of new branches of linguistics and new findings about the language.

REFERENCES

[1] Ethnologue: Jezici svijeta, sedamnaesto izdanje. Dallas, Teksas: SIL International. Online verzija: http://www.ethnologue.com.
[2] http://www.politika.rs/scc/authors/texts/901
[3] https://avaz.ba/tag/4975/muhamed-filipovic
[4] https://en.wikipediam.org/wiki/Letter_frequency
[5] https://hr.wikipedia.org/wiki/Policentri%C4%8Dni_standardni_jezik
[6] https://norvig.com/mayzner.html
[7] https://www.jutarnji.hr/autori/miljenko-jergovic
[8] https://www.vijesti.me/autor/miodrag-lekic
[9] Jahić, Dž. (1999). Trilogija o bosanskom jeziku. Knj. 3, Školski rječnik bosanskog jezika Sarajevo: Ljiljan biblioteka Linguos.

Submitted: May 20, 2019
Accepted: May 24, 2019

ABOUT THE AUTHORS

Nedim Smailovic 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

Nedim Smailović, Statistical Analysis of Texts of the Balkans Electronic Media Columnists, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:5-16, (UDC: 659.3/.4:316.776]:004.738.5), (DOI: 10.7251/JIT1901005S), Volume 9, Number 1, Banja Luka, june 2019 (1-48), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

Digitalization of Railways – ICT Approach to the Development of Automation

Zoran Ž. Avramović, Dražen M. Marinković, Igor T. Lastrić

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

Contribution to the state of the art

DOI: **10.7251/JIT1901017A** UDC: **656.2:[621.313:681.5**

Abstract: The concept of digital railway is defined in the European Initiatives, which started in 2016. The basis for this technical development and improvement plan is the Shift²Rail and the *Roadmap for Digital Railways*, presented by the Community of European Railways and Infrastructure Managers (CER), the International Rail Transport Committee (CIT), the Association of European Rail Infrastructure Managers (EIM), and the International Union of Railways (UIC).

Keywords: ATO, automatic train operations, digital railway, ERTMS, ETCS.

Introduction

There are numerous options for modernizing the railways using digital technologies in train management [1], [5-7]. In the context of digitization, train management involves automated traffic management (including support for decision-making and train speed regulation), signal transmission to the machine driver's cab (European Train Control System - ECTS), Automated Train Operations (ATO), related advisory systems (CDAS), and appropriate supporting telecommunication network [2], [4].

The introduction of digital solutions will increasingly be the focus of modern and future efficient railways. It will improve connectivity and help people move faster and safer. The current traditional signaling infrastructure is gradually becoming history with increasing security risks and possible delays [3].

State and Development Concepts

Digital technologies, such as the transmission of signal signs to the cab of the machine operator and intelligent railway traffic management systems, are becoming more and more important in raising the capacity of the existing rail network, and in particular to meet the prospective growth needs.

The European Railways have made a number of recommendations based on the transport needs and possibilities of the modern industry in the area of signaling and management of rail traffic with the aim of introducing digital signalization and operational technology (Table 1).

The recommendations were based on the conclusion that improvements in signaling and traffic control technology are needed to expand the network of railroads of the highest class. The idea is to speed up the development of the European Train Control System (ETCS), as well as traffic management software and driver support.

The introduction of digital signaling technology suggests a greater dependence on a reliable mobile network. This initiates the need to build a SWIFT (Superfast Wi-Fi In Carriage for Future Travel) project, which will be a good example of a harmonized partnership in technology, railways and mobile networks.

The SWIFT project is designed to provide free Wi-Fi services for travelers through a dedicated infrastructure installed along the railway network. It

Table 1. *Global trend of information development*

Research and innovative solutions under development	IPID 2020	EU White Paper	Shift 2Rail	US FRA Strategic Plan
Increased safety based on intelligent systems	☑	☑	☑	
Reduction of risks related to the human factor	☑			☑
Increased business efficiency and streamlining of logistics	☑	☑	☑	☑
Development of multimodal transportation	☑	☑	☑	
Harmonization of service-related requirements. "One stop"	☑	☑		
Development of virtual and cloud-based client services	☑	☑	☑	
Computerization and digitalization of traffic management processes	☑	☑	☑	☑
High-speed traffic development	☑	☑	☑	☑
New rolling stock	☑	☑	☑	☑
Increased energy efficiency	☑	☑	☑	☑
New power plants. New types of energy resources	☑	☑	☑	☑
Focus on rational environmental management	☑	☑		
Infrastructure development	☑	☑		☑
Unmanned technologies	☑		☑	☑

**IPID – Investment Projects Implementation Department*

will be used by existing Network Rail Telecoms networks to provide good connectivity and speed for the user.

Projects for the introduction of digital signalization and management technology should be jointly developed by the owners of the railway infrastructure in partnership with the appropriate companies for the transport of passengers and goods.

DEVELOPMENT RIGHTS

Digital Rail is itself an integral set of technologies between railroad and train. Therefore, the topic requires cross-sectoral approach, which is reflected in the competent team for cross-sectoral development of the digital railway, its users and management (Figure 1).

DEVELOPMENT STRATEGY

The digitalization of the railways emphasizes the current global trend of adopting digital technologies and processes, including the deep penetration of digital technologies in the transport sector. It is also expected to take advantage of the significant experience of the European railway sector for innovative development.

Although it has the potential to be a driver of the game for the rail industry, digitalization is not an end in itself. It provides unique tools to increase the efficiency of rail transport that can stimulate the transition to a new level of industry development.

For example, the widespread use of next-generation low-pass wireless networks, such as LoRa, as well as the enormous processing capability offered by cloud-based technologies, can open the way for the development of an integrated technology platform that supports decision making for all industrial processes. (LoRa – Low power Radio technology – wireless RF technology used in WAN for M2M and IoT applications thanks to low power consumption and secure data transmission).

In an effort to maintain the achieved market share while ensuring continued sustainable development, European railways have developed their own innovative development plans for the immediate prospective period. These plans envisage the widespread use of digital technologies in all company business, including fleet and infrastructure monitoring, communications, traffic management and trains management.

At the heart of today's transition, new digital business data is based on data based on the auto-

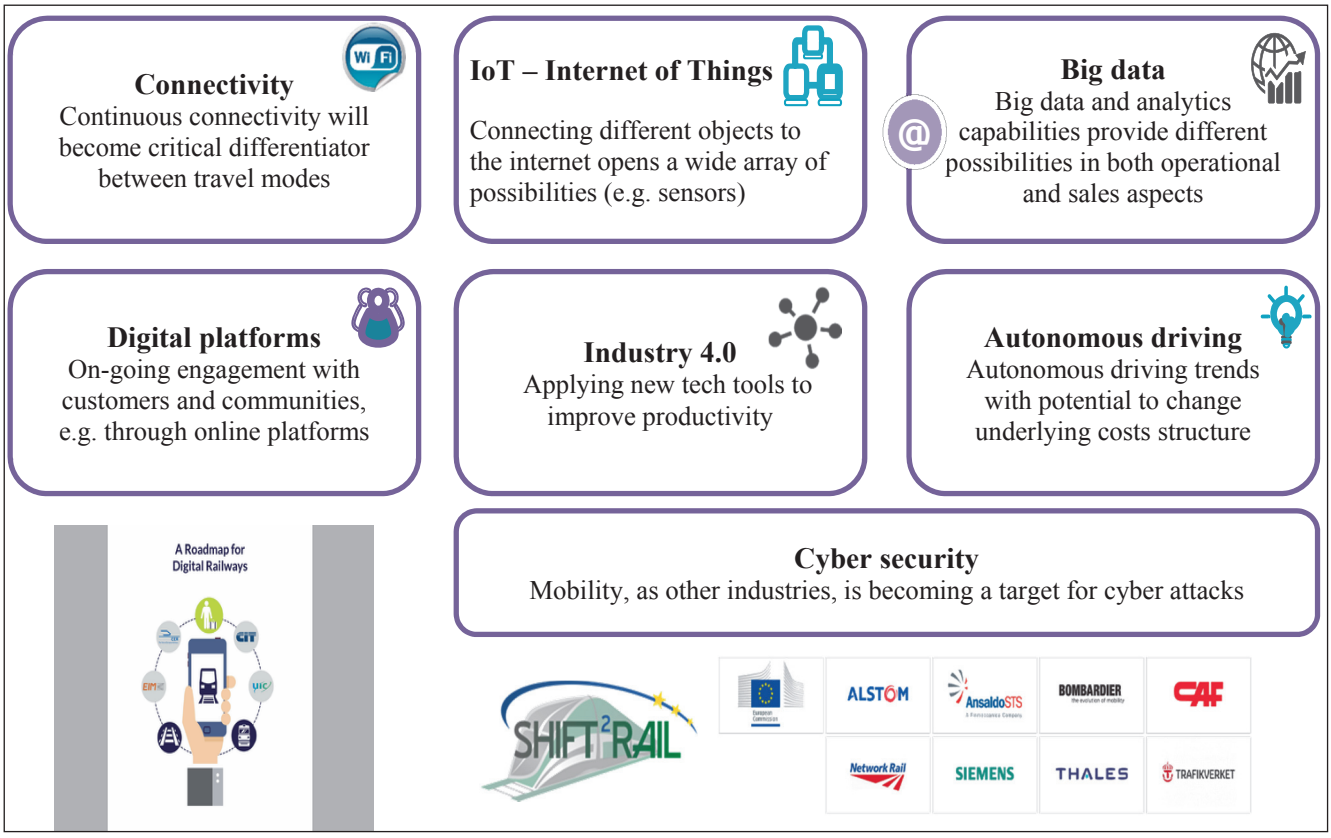


Figure 1. *Today's challenges. Tomorrow's opportunities*

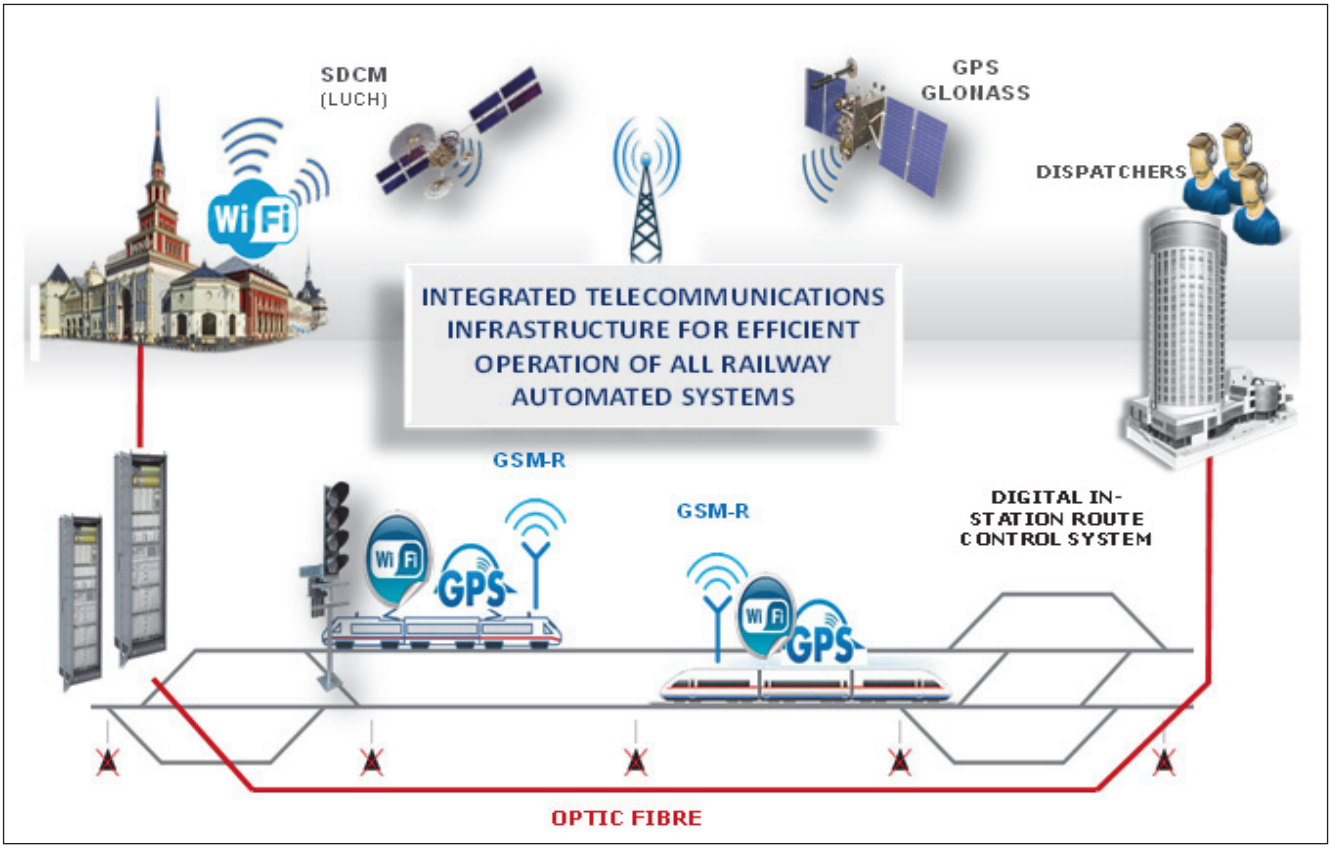


Figure 2. *Integrated Telecommunications*
SDCM System for Differential Corrections and Monitoring (component of GLONASS), Luch - family satellites

mation of data collection from specific work parameters and industrial processes.

In the rail context, this implies the development and improvement of digital or virtual images of objects and processes. Digital images help solve the whole spectrum of problems.

For example, analyzing and simulating the behavior of a digital image of a device, which is made using information collected by specialized monitoring and diagnostic sensors throughout the device's lifecycle, provides access to accurate information about vital device parameters, such as: work safety, resilience/robustness and longevity (Figure 2).

PRACTICAL SOLUTIONS

The concept of a digital railway is inevitably linked to fully automatic trains without a driver. The so-called smart locomotives and smart trains are considered to be the future of rolling stock, and many railways are actively developing this technology, along with prototypes that already pass tests on some test pieces.

In several world examples, the operation of automatically guided locomotives has been successfully tested at marshalling yards.

Here, the speed of the track is controlled via a digital radio block with continuous automatic monitoring of their location using GPS / Glonass satellite navigation with differential correction. The purpose of this project is to develop a procedure for the simultaneous control of several shunting units from one remote workstation.

Another innovative solution, developed for positioning trains, is the use of monitoring of vibration acoustic paths. In this system, train presence detection is based on an optical sensor for identifying precise coordinate positioning of trains on open lines between stations.

This technique requires the conversion of the backup fiber into an optical cable into a spatially distributed sensor, which works on the basis of determining changes in signal reflection from the cable while the train passes along the line. This is done using a measuring gauge located on the periphery with the differences between the reflecting branches that provide an accurate measurement of the position of a particular vehicle. The system permits the monitoring of the vehicle fleet within 40 km of the gauge - reflectors and locations of the central computer unit with a positioning accuracy not less than 15 m.

The techniques that work in accordance with the concept of the Industrial Internet of Things (IIoT), which is increasingly accepted throughout the rail world, have greatly applied. Today, a large number of technical and technological solutions at the IIoT base go through tests on various parts and objects of the world rail network.

Railways today are considering and testing other low-voltage wireless communication solutions. It also tests and uses a wide range of applications that use wireless sensors to collect information and realize remote transmission in the rail environment as part of the IIoT concept. Promising results of wireless sensors for automation systems for railways, such as signals, relay groups and cabinets, tracking equipment and overheating detection systems, are expected.

All information pertaining to the operation of the railway facilities collected by the distributed sensor network is transmitted to the appropriate automated control systems of the railways that are connected to a reliable corporate communications network.

A special feature of the selected IIoT concept is the deep vertical and horizontal integration of automated industrial control systems. European railways have developed RDBMS as a platform for the integration of all automated traffic management systems. The platform is complemented daily and perfected by passing through the concepts based on a multi-agent approach. This improvement relies on the principles of artificial intelligence, developed to integrate and process large amounts of data from traffic processes. This may include the current status of signaling systems, speed and weight of trains, location of locomotives, trains, cars, speed limits per line sections, as well as the technical condition of rolling stock and automation devices.

The RDBMS project assumes that the fleet acts as a sensor. It should be noted that its source is seen in the first solutions in the world based on equipping the fleet with a train protection system integrated with GPS / Glonass satellite receivers, which are able to transmit the position of the train and other data through the radio link to the traffic control center.

In addition, the latest generation of EMU solutions, such as Lastochka and Sapsan [5], are equipped with special information and measure-

ment systems for diagnostics and monitoring, which provide complete automatic control over the state of the infrastructure during everyday tasks.

This includes LoRa, which provides guaranteed wireless communication channels in a range of 15 km in poorly populated and 5 km in densely developed urban areas. It has been proven that the LoRa-based communication network has sufficient robustness at a high level of interference and an unfavorable electromagnetic environment.

Reliable information about the state of the railway infrastructure and facilities is one of the key components of intelligent data processing and analysis systems. This also implies the development and implementation of decision support solutions at the highest level.

New Access to Diagnostics and Monitoring

New equipment for diagnostics and monitoring of accessories is installed on the existing fleet without overlapping with the existing classical equipment.

Diagnostic activities do not interfere with the traffic process, and at the same time provide high frequency traffic monitoring of high speed trains.

Diagnostics of the condition is carried out without interruption of the work of the rolling stock, the railway infrastructure and the contact line.

Full automation of all control equipment for diagnostics, measurement, processing and monitoring has been realized (does not require presence of operator).

Diagnostics makes it easier to apply a new approach to maintenance of rail infrastructure and rolling stock based on the collected data. In addition, various wireless sensors installed on a fleet, which include a wide range of digital subsystems, including acoustic sensors and technical modes, can be supplemented by fixed, integrated inspection stations. As a result, the technology not only identifies the wear or critical state of the components, units and plants, but also provides a supported forecast of equipment deterioration, as well as full information when deciding on the allocation of maintenance activities (Figure 3).

A high-quality, modern diagnostic hardware-software platform has already implemented some, but also all the following features, based on the automation of data collection and application:

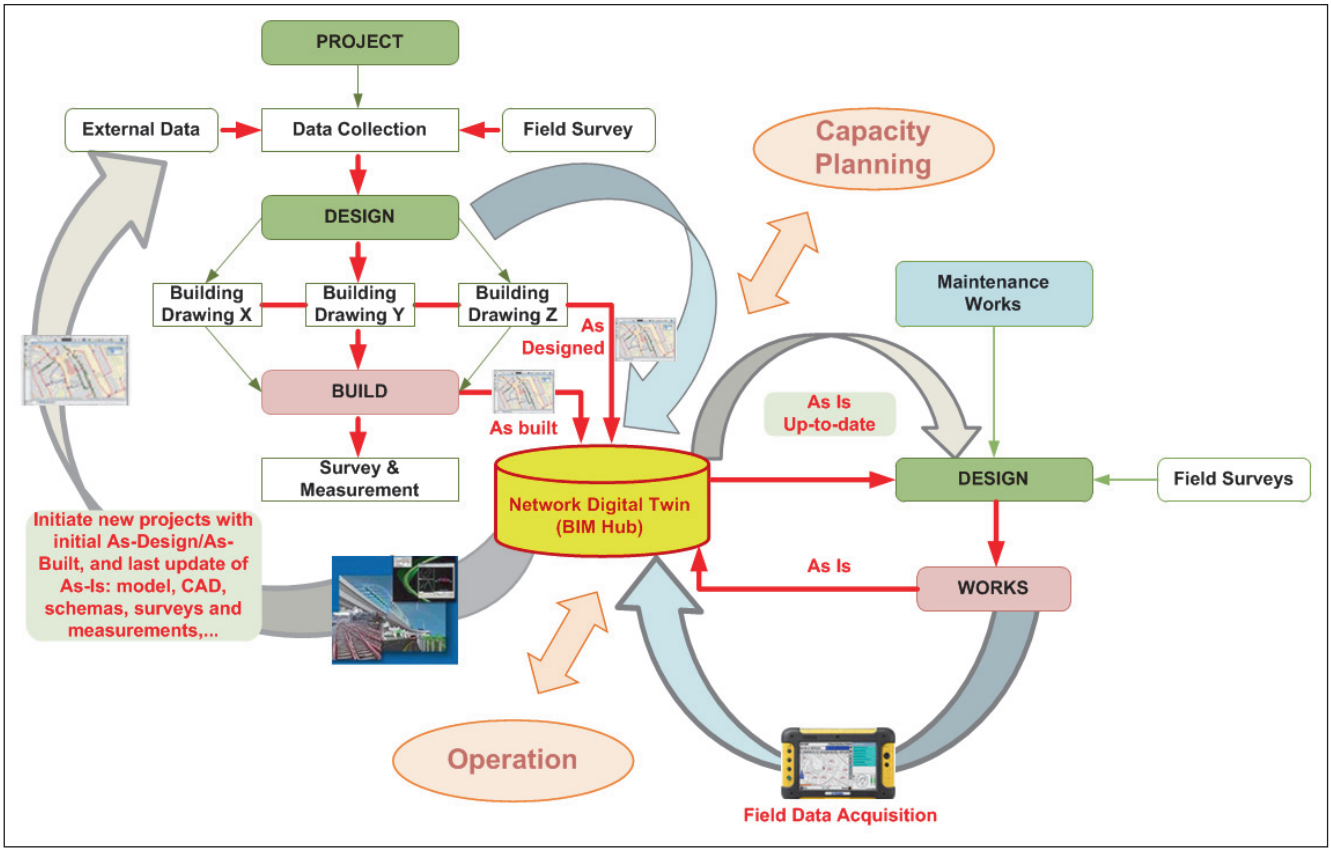


Figure 3. *UIC RailTopoModeL (RTML)*

- automation of the initial processing of statistical data on railway infrastructure and the failures of the equipment of the vehicle fleet,
- identification of quantitative values of operational reliability and safety indicators of infrastructure objects,
- quantitative assessment of infrastructure and service activities that are the subject of failure and organization of maintenance and operation of infrastructure facilities,
- monitoring, comparing and supporting the activities of associated business units based on operational reliability and safety indicators,
- assessment of compliance of real performance indicators and work safety within standard norms,
- preparation of estimated data to support recommendations for risk reduction,
- identification of vulnerable objects based on risk assessment,
- drafting work plans for the maintenance of infrastructure and rolling stock, and
- preparing investments in projects for those railway facilities that are the biggest problem.

Geographic Information Systems

One of the priorities set before digitization in the modern rail industry is the use of geographic information systems in the widespread application, automatic generation and updating of digital models of a dotted, linear or parallelogram type with a rich set of precise data.

For several years, this technology has been tested in a range of operating environments. For example, the use of digital rail models that offer precise coordination of coordinate infrastructure facilities has enabled the automation of maintenance and mapping procedures that have significantly reduced costs and improved the quality of the activities carried out. This approach, in addition, offers the possibility of assigning maintenance operations with an accuracy of the order of cm, which advanced railways encourages to introduce this technology into their network.

Further development is based on an integrated system of spatial data of railway infrastructure, which is in development phase, with a highly precise coordinate system, which is primarily intended for the design, construction, maintenance and exploitation of infrastructure.

One such solution was used in a large and extensive project of reconstruction of the Moscow Ring Railway.

The reconstruction project involves the management of mixed passenger and freight traffic. For these purposes, a complex system for train separation has been developed, which is based on an automatic rail block and uses circular streams of audio frequencies integrated with computer blocking on stations and ATP systems on trains.

This enabled the automatic separation of trains using the principle of a mobile block, and can operate in two ways: a mode of operation with light signals for organizing the operation of freight trains of a certain mass and length and a light signal without a working mode for operation at higher EMU speeds with a minimum interval of three minutes.

The system provides automatic train guidance to the specified target and automatically identifies and resolves possible conflicts by calculating and performing an alternative approach. In the event of train delay, this process attempts to compensate for lost time. The position and speed of the train are determined by using GSM-R, and the integrated positioning system based on satellite navigation devices is part of the train protection system.

Conclusion

Real-time rail traffic management will reduce disruptions, increase safety, improve reliability and enable a better response to new passenger demands.

It should be noted that in a large number of applications on the rail network traditionally used track circuits, as a basic element of railway automation and telemechanics. With them, we detect the presence of a moving structure on some part of the track and the whole of the rail.

Although still a very reliable element, its improvement is being investigated. Today, the rail power circuit serves as the primary channel for transmitting information on signal aspects and the allowed speed of the train.

Track circuits are not an ideal solution. This channel is inferior to the digital radio. Track circuits are very sensitive to interference. However, they are more reliable than radio links in terms of cyber threats. Further development of the track circuits is seen as a kind of combination of these media with

the improvement of cyber security. Track circuits are already becoming digital, with digital generators and filters that provide high functionality and availability.

In any case, the concept of a multilayer security system is being promoted today in the world. It is intended that the entire railway territory is fully covered by the digital generation of the latest generation. GSM-R is slowly becoming an outdated solution with its known limitations.

We need a new broadband digital radio communication for the digital railway.

References

[1] Department for Transport, Ministerial Group (2016), Digital Railway, www.gov.uk/dft (1.5.2018)
[2] Ozerov Alexey Valeryevich (2017), Digital Technologies for Railways, X International Conference "Traffic Safety Systems", 20-23. April 2017, Ljubljana, Slovenia, collection of works on CD, JSC NIIAS, Moscow, Russia, www.vniias.ru (April 12, 2018)
[3] Friend Matej (2017), Digitalization of operational communications on Railways, X International Conference "Traffic Safety Systems", 20-23. April 2017, Ljubljana, Slovenia, collection of works on CD, IskraUralTEL, Yekaterinburg, Russia, www.iskrauraltel.ru (April 12, 2018)
[4] Rozenberg Efim Naumovich, Ozerov Alexey Valeryevich (2017), Wide-reaching program of "digitalization" its Russian Railways network, IX international scientific-expert meeting "Information technologies for e-education - ITeO 2017", Pan-European University APEIRON, Banja Luka, Republika Srpska, BiH, 29-30. September 2017, a collection of works on CD, pages 141-147, (published as a whole) (ISBN 978-99976-34-13-9), (COBISS.RS-ID 6139416).
[5] Rozenberg Efim Naumovich (2017), New Digital Technologies for Railways, X International Conference "Traffic Safety Systems", 20-23. April 2017, Ljubljana, Slovenia, collection of works on CD, JSC NIIAS, Moscow, Russia, www.vniias.ru (April 12, 2018)
[6] Rozenberg Efim Naumovich (2017), Цифровая железная дорога: современные задачи развития автоматизации, X International Conference "Traffic Safety Systems", 20-23. April 2017, Ljubljana, Slovenia, collection of works on CD, JSC NIIAS, Moscow, Russia, www.vniias.ru (April 12, 2018)
[7] UIC – International Union of Railways, High Speed Rail – Fast Track to Sustainable Mobility, Passenger Department, (author Michel Leboeuf), ISBN 978-2-7461-2700-5, may 2018

Submitted: January 27, 2019
Accepted: April 4, 2019

About the authors

Zoran Ž. Avramović is the Rector of PanEuropean University "APEIRON" Banja Luka. He was born in Municipality of Loznica, in Serbia (Yugoslavia). He graduated from the State University of Belgrade - Faculty of Electrical Engineering, with an average grade of 9.72 (out of 10). He received his master's degree at this faculty (average grade 10 out of 10), and then received a PhD in technical sciences (1988). He studied mathematics at the Mathematical faculty in Belgrade. He was the champion of Serbia in mathematics ("first prize") and Yugoslavia in electrical engineering ("gold medal"). He is: full member of the Russian Transport Academy, of the Russian Academy of Natural Sciences, of the Engineering Academy of Serbia, of the Academy of Electrotechnical Sciences of the Russian Federation.

Dražen M. Marinković was born in Banja Luka, Republika Srpska - Bosnia and Herzegovina. He finished elementary school in Prnjavor. He finished secondary school of Electrical Engineering in Prnjavor. He graduated at the Faculty of Information Technologies at Pan-European University "APEIRON" in Banja Luka. Master studies completed in 2015. Doctoral studies of the third degree enrolled in the academic 2015/2016. He lives and works in Prnjavor.

Igor Lastric, assistant on Pan-European University "APEIRON". He is a CEO at "software solution d.o.o.", Banja Luka based company and chief of software development at "RND Software Services", New York based software development company. He graduated from "Paneuropean University Apeiron" with bachelors degree in Computer Sciense and currently working on Master degree under mentoring of professor Zoran Z. Avramovic.

For citation

Avramović Z.Ž., Marinković D.M., Lastrić I.T., Digitalization of Railways – ICT Approach to the Development of Automation, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:17-23, (UDC: 656.2:[621.313:681.5), (DOI: 10.7251/JIT1901017A), Volume 9, Number 1, Banja Luka, june 2019 (1-48), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

DIGITAL SIGNATURE AND ORGANIZATION OF DECENTRALIZED AUTHENTICATION IN BUSINESS ENVIRONMENT

Tijana Talić, Gordana Radić, Zoran Ž. Avramović

Pan-European University APEIRON, Banja Luka, Republika Srpska, Bosnia and Herzegovina,
tijana.z.talic@apeiron-edu.eu

Contribution to the state of the art

DOI: **10.7251/JIT1901024T** UDC: **316.77:004.773]:658.14**

Abstract: Modern electronic communication is fast and efficient. It has never been easier to change the document's content. In this paper, we explain and show through practical work how it is possible to protect the data sent electronically in business communication by using decentralized authentication systems.

Keywords: authentication, digital signature.

INTRODUCTION

Security is a matter of trust. Should you take your security into your own hands or let someone else take care of it?

The problem of security and protection of computer systems is slowly becoming a business, actually, a service that is sold to you by companies outside your firm. This releases companies from employing professional staff and partially relieves their costs. These services often include: the purchase of a part of the hardware, especially firewalls, the software that works on them, installing and maintaining antivirus programs, various types of data backups, and even storing cloud databases that are maintained by specialized hardware, software, and team of experts. This is very interesting for our BiH conditions, especially when electricity goes down. This brings us back to the eternal question of who controls the controllers, or how much we can trust those companies. Even if these systems function properly, the fact is that a lot of damage can be caused by the lack of sender's authentication or the credibility of the electronic message.

Violating privacy, tracking the users and recording their habits is a perpetual topic in electronic communication. On the other hand, the presence of various kinds of malicious programs imposes the need to pay attention to security in every form of communication.

Modern electronic communication is fast and efficient. At the same time it has never been easier to change the document's content. This can be applied not only to electronic messages, but also to printed documents that are not particularly protected, for example, with a dry stamp, using special paper or in a similar manner. It is enough just to digitize the document, make a change in one of the available editors, and print it again. We had the opportunity to see how officers usually check the credibility of the stamps on paper by 'licking' them. This tells us more clearly that in the new age we have to use new techniques of signing and credibility verification.

Authentication

One of the main elements of authentication in electronic communication is a digital signature, whereby we need to distinguish the meaning of terms electronic and digital signature. One of the definitions states that an electronic signature is any sound, symbol or process that is electronically linked to a document-contract or record adopted by the signatory, indicating his or her intention of signing. The digital signature replaces the personal signature and confirms the sender's identity as well as the credibility of the sent message and is based on cryptographic algorithms and keys. Connecting a public key and identifying the person using it is one of the major issues in authentication. There are two approaches to solving this problem:

- Use of certification authorities (centralized system)
- Use of decentralized systems

WoT

The most well-known decentralized model of trust is the "Web of Trust" (WOT). WOT is a concept used in PGP and other OpenPGP compatible systems, best known as GnuPG (GPG) [4]. It does not rely on the certification authority hierarchy, but users sign certificates among themselves to confirm the public key connection with the person or entity specified in the certificate.

Key K is considered valid if two conditions are fulfilled:

1. It is signed with enough valid keys which means:
   b. It was signed by you personally,
   c. It was signed by a fully reliable key,
   d. It was signed by three keys with marginal trust.
5. The path's length of the signed keys that leads from the key K back to your key is five steps or shorter.

Besides signing a public key, each user must also be determined the level of trust (owner-trust) in the way he signs other keys. There are four levels of trust:

- unknown
- none
- marginal
- full

It is possible to adjust the length of the path, the number of marginally trusted keys and the number of fully trusted keys. The above listed numbers are default values used by GnuPG. The setting parameters are: marginals-needed, completes-needed, and max-cert-depth for the path's length from the key K back to your key.

It is important to note that the level of trust in user (owner-trust) must always be entered on our own, while the key validity can be calculated using the above mentioned method.

Web of Trust has a flexible approach to the problem of secure public key exchange. This approach allows you to configure GnuPG to reflect how it is used. In the extreme case, it is possible to request a multiple, shorter path from your key to key K. On the other hand, you may be satisfied with a longer path and perhaps with a shorter path from your key to key K as well. Requiring multiple short paths is a powerful guarantee that the key K is really valid.

The main problem is that if we need to confirm a large number of keys or we need to communicate with people, we do not know that this procedure requires user's immense engagement.

Therefore, the main problem of the WoT network is the validation of keys in case we want to establish communication with a large number of people. In this case, in order to provide less perfect but effective security solution, it is suggested to slightly loose the threat model instead of using theoretically perfect but practically very difficult rules. We achieve this by using the TOFU model (*trust on first use*).

TOFU

The TOFU model memorizes the key during the first contact and remembers the key usage statistics [5]. In the case that the key is changed, the TOFU declares both the key (old and new) as conflicting and requests interaction with the user to determine whether it is an attack or a regular key update. In the case of an attack, the attacking key will be declared defective, communication will be denied and, if necessary, other measures will be taken as well. If we find that it is a regular update of the sub keys in contact with the sender, both keys will be accepted as correct.

TOFU will also warn us on the first contact and we can easily recognize whether it's a mimicry attack or a real new contact.

WEB Key Directory

Web Key Directory is a new public keyword detection scheme that allows you to detect PGP keys by using an email address.

For example, if you are looking for the key of tijana@example.org, the key will be delivered from the following location:

https://example.org/.well-known/openpgpkey/hu/1xnth55nm69yzufx5jbdyh5hjzcbecbr

The web directory provides an easy way to discover public keys via HTTPS. It provides an infrastructure that significantly improves user's experience while sharing secure email and file messages.

Unlike the public key server, Web Key Directory does not publish email addresses. This is the authoritative source for your own domain.

It works in the following way:

- The sender's mail client checks the "well-known" URL on the recipient's domain.
- If the public key is available for this email address, it will be downloaded via HTTPS.
- The public key can now be used without further user's interaction.

The use of WKD is implemented in GPG from version 2.1.12 as well as by adding it to the main e-mail clients: Thunderbird / Enigmail 2.0, KMail from Version 5.6, Outlook with GpgOL from version 2.2.0, Mailvelope from version 3.0.0

The Web Key Directory is generally created and maintained through the web key service, but organizations or individuals can host only the web key directory without the web key service.

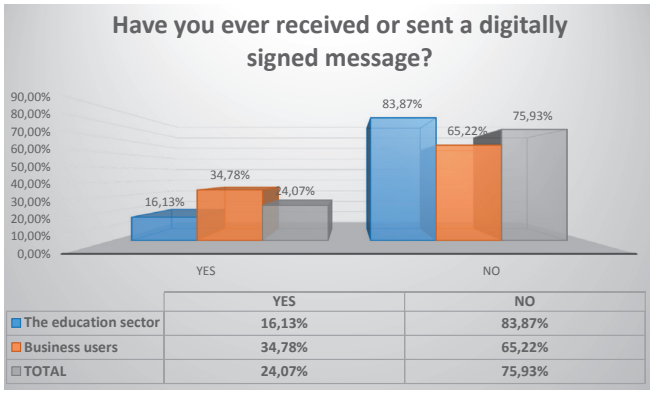
This is accomplished by using a flat file structure that should be re-created if the public message changes.

The thing is that files, whose hash address name is from corresponding domain, are created for each address of the corresponding domain with the help of GPG. It is necessary to have control over the web server of that domain. Created files are set up on the path. well-known / openpgpkey / hu / on the web server's domain. This is set up on the HTTPS server. It is necessary for the web server to be configured appropriately and to enable HTTPS communication and protect the directory from direct browsing. The client calculates hash addresses and searches for a file with that name on that path. If he finds it, then the matching public key is imported.

WKD is set up only for addresses from that domain and represents a unique authoritative key server of that domain.

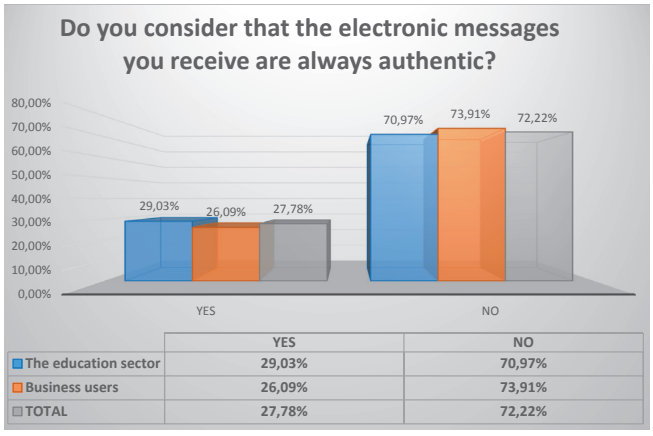
Current situation

The use of digital signatures in the business environment of BiH can easily be seen from the research diagram conducted in the work [1]. The survey covered two groups of business users: employees in the education sector and employees in the civil service.



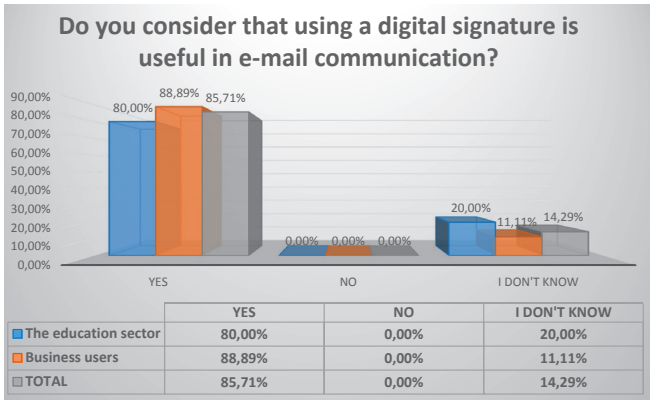
	YES	NO
The education sector	16,13%	83,87%
Business users	34,78%	65,22%
TOTAL	24,07%	75,93%

Figure 1. *Use of digital signature in business environment*



	YES	NO
The education sector	29,03%	70,97%
Business users	26,09%	73,91%
TOTAL	27,78%	72,22%

Figure 2. *Authenticity of electronic messages*



	YES	NO	I DON'T KNOW
The education sector	80,00%	0,00%	20,00%
Business users	88,89%	0,00%	11,11%
TOTAL	85,71%	0,00%	14,29%

Figure 3. *The importance of using a digital signature in electronic communications*

From Figure 1 we can conclude that a small number of business users use a digital signature. On the other hand, it is clear from Figures 3 and 4 that electronic communication is not always safe and messages sent electronically are not always authentic. The survey also shows that over 85% of respondents in our business environment agreed that the induction of authentication by using digital signatures makes business communication easier and more secure.

Organization Model in a Business Environment

Our model is based on a combination of web of trust and trust for first use (TOFU). This solution does not cover the entire world, but we will limit ourselves to everyday business communication in which we have the definite number of participants. Construction begins as WOT. In the case of a business entity, we will form the key that is related to the company. Although email is a strong identifier, we can create this key without using an email. We can also omit the encryption sub key so that this key is for signature and certification only. Let us call this key the main key of the company. With the main key we will sign all employees' keys. By signing the main key with complete trust, all employees will have mutually valid keys. The connection of the main key and employees' key is two-way and with full confidence. In this way, we saved the users within the company from a part of the work about the signing and certification.

We should not forget that all these keys must be synchronized with the key server.

Employees will deposit their secret keys and revocation keys in a secure location. Depositing private keys and keys for revocation to a secure location is extremely important as well as remembering the pas-phrase key. This is especially noteworthy since, during the performance of the experiment, we noticed that users are prone to lose keys or passwords for private key.

Let us observe the other organization that was arranged in the same way. It would be desirable that, if there is a business link between these two organizations, the administrators sign and certify the main keys with full confidence. Of course, the administrators will do this with detailed checks. What did we get with this?

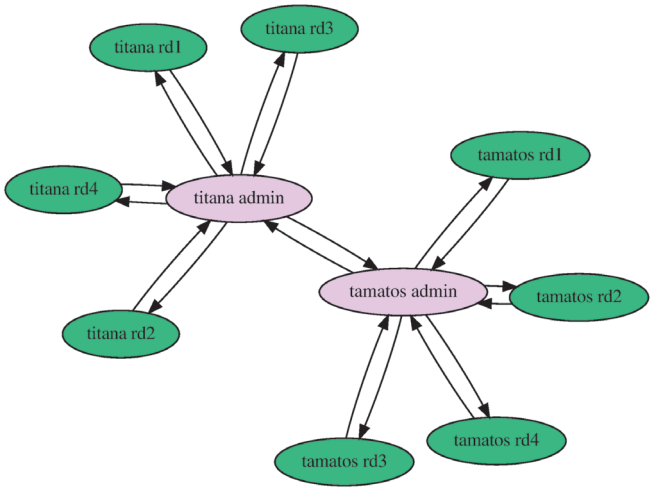


Figure 4. *The signature structure for Titana and Tamatos companies*

If a user from one company imports the main key of another company, WoT will automatically certify the main key of another firm. This key will be associated with unknown trust. If the user makes more effort and gives fully trust to the main key of another firm (based on a check made by administrators among them), then all users of another company certified with its main key are placed on the path shorter than 5 steps and signed with enough valid keys. In this way, we used WoT to identify known associates from close companies. In order to join a third company in this scheme, the previous steps should be repeated.

Automating and increasing reliability using WKD

Using the WKD, it is possible to automate the process of key manipulation additionally. New versions of GPG have built-in support for WKD application. Add-ons of the well-known mail clients are set to automatically check the existence of a key on WKD. After entering the recipient's address, these add-ons on Enigmail (Mozilla Thunderbird) and GpgOL (Outlook) automatically detect the keys to the WKD. This further reduces user's interaction.

Of course, IT administrators have to create web key directories and maintain them up-to-date. Combination of the automatization provided by WKD and web of trust increases the level of resistance to sophisticated attacks. When applying automation, we need to distinguish the way in which we

have come up with the appropriate public key. If a user explicitly enters an email address (for example, when encrypting), we know that the user intended to enter exactly that email address. On the other hand, if we get the key through the WKS to check the signature (for example, we use WKS to find the key for varalica@example.org), then we should not be convinced that the key is reliable and the message is authentic.

The third engine of this system is TOFU. It practically checks the system all the time. It also tracks and collects key usage statistics and most importantly, it detects the conflict. In case of TOFU conflict detection, both keys are declared defective and user's interaction is necessary.

This can be applied in organized systems with an IT administration. Of course, this is often not the case. In such, and in all other situations, we will use the TOFU scheme. It is necessary to emphasize the importance of establishing the first contact. It is desirable that the keys exchange is performed with a secure channel, or by combining multiple communication modes.

Our solution requires from customers to use the TOFU + PGP settings to validate the keys. This setting calculates validity according to WoT and TOFU rules and sets the higher one. In some cases it is advisable to set the settings so that the TOFU does not provide any evaluation of the key validation, and the TOFU is only used for conflict detection. The result is an increase of the interaction level.

The defense of persistent and targeted attacks is not easy. Although this system has a high level of automatization, a certain level of user's training is needed to see some signals when it comes to targeted pirate attack or CEO fraud.

Conclusion

This model uses three essential components: WOT with its strict and precise rules is loosened by the usage of TOFU models and it is automatized by the usage of WKD. The model is not demanding to the end user.

Interaction with the user is reduced to a minimum. The purpose of this model is its usage in everyday communication where it gives a solid level of reliability, especially when defending from *man in the middle* attack and facilitating the detection of mimicry. For areas where communication reliability requirements are much higher, it is necessary to use different models and probably other tools.

The use of this model requires the existence of IT administrators, whether they are directly present in a business entity or engaged from outside, as well as a minimum education of users.

Bibliography

[1] Talić, T., "The use of digital signature in electronic communication in BiH - Research," *JITA - Journal of Information Technology and Applications*, vol. 7, no. 1, pp. 20-23, June 2017.

[2] Darxus,. (2002) sig2dot GPG/PGP Keyring Graph Generator. Available at: http://www.chaosreigns.com/code/sig2dot/, [Last accessed 01 May 2019]

[3] Talić, T., Decentralizovani sistemi autentifikacije u savremenoj komunikaciji, 2019, (Doctoral dissertation, PanEuropien University APEIRON, Banja Luka).

[4] wiki.gnupg.org,. (2018, Jun) *Automated Encryption.* Available at: https://wiki.gnupg.org/AutomatedEncryption, [Last accessed 10 May 2019]

[5] Walfield, H N. and Koch Werner, "TOFU for OpenPGP," in *EuroSec '16 Proceedings of the 9th European Workshop on System Security*, London, 2016.

[6] Gambetta, D., ""Can we Trust Trust?"," in *Trust: Making and breaking coopeative relations*.: Department of Sociology, University of Oxford, 2000, ch. 13, pp. 213–237.

[7] Böhme, R. and Grossklags Jens, "The security cost of cheap user interaction," in *Proceedings of the 2011 Workshop on New Security Paradigms Workshop, NSPW '11,* New York, 2011, pp. 67-82.

Submitted: May 24, 2019
Accepted: May 30, 2019

For citation

Talić T., Radić G., Avramović Z.Ž., Digital Signature and Organization of Decentralized Authentication in Business Environment, *JITA – Journal of Information Technology and Applications Banja Luka,* PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:24-28, (UDC: 316.77:004.773]:658.14), (DOI: 10.7251/JIT1901024T), Volume 9, Number 1, Banja Luka, june 2019 (1-48), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

Safety Analysis of Reverse Algorithm Encryption in Databases

Branko Latinović[1], Zoran Ž. Avramović[1], Mahir Zajmović[2]

[1]PanEuropien University APEIRON, Banja Luka, B&H

[2]PhD Student at University "VITEZ", Vitez, B&H

General Survey

DOI: **10.7251/JIT1901029L** UDC: **004.7.056.55:004.432.2**

Abstract: Encryption provides security for databases. This paper provides a new encryption algorithm ,"Reverse Encryption Algorithm (REA)". Furthermore, designing a REA algorithm has improved data encryption security. Safe and successful proposed encryption algorithm REA is evaluated and compared with the most common encryption algorithms. The designing of the REA algorithm also improves the security of data encryption. Additionally, the safety and the performance of the suggested encryption algorithm REA represents evaluation and enhancement with the most common encryption algorithms. Experimental results show that the proposed encryption algorithm REA surpasses other encryption algorithms in performance and security of databases. All in all, the proposed encryption algorithm REA achieves a balance between security and efficiency.

Keywords: encryption, cryptography, databases, algorithm, REA.

Introduction

Cryptography is the science of data encryption. Cryptographs create algorithms which use input data, called plain text and convert it into encrypted output. Encryption is much more than just moving letters or changing some letters. After a suitable cryptographic encryption, the output is indistinguishable or output looks like a random order of data. For data protection in electronic form new protocols are needed to ensure secrecy as much as the old protocols. There we have a unique opportunity for progress and increased security [7].

Database encryption is a well-established technology for sensitive data protection. Unfortunately, the integration of existing encryption techniques with database systems causes undesirable performance degradation. This is a main technique in safety mechanisms of databases. The database encryption solution is specialized and complex although the internal resources do not have cryptographic expertise in relation to the database environment, external expertise should be used to ensure superior efficiency and strong safety. [1]

A new innovative encryption algorithm REA has been proposed. The algorithm is efficient and secure. It has achieved the safety and is fast enough for the most used software. The proposed algorithm REA limits additional time costs for encryption and decryption and at the same time does not degrade the system performance of the database. Therefore, the safety analysis and the performance factors which are used are safe and efficient: such as key space, key sensitivity, data security from the attack, calculating speed, information entropy and the correlation coefficients. [3

This paper looks at the method for assessing the security and efficiency of the proposed REA encryption algorithm and is compared with the most common encryption algorithms: DES, 3DES, RC2, AES and Blowfish. Comparison will be shown for these encryption algorithms during the encryption and decryption. The comparison for the safety value will also be shown (used for the measurement if information entropy).

Furthermore, another safety measure is a coefficient of correlation of coded fields with proposed encryption algorithm REA. Results of the experiment show that the encryption and decryption time of proposed encryption algorithm REA has very good performances comparing to the other encryption algorithms. The results from safety measures (information entropy) show that the proposed encryption algorithms REA and AES are safer than DES, 3DES, RC2 and Blowfish.

Compared Algorithm Performance

To give more information about the compared algorithm performances, gathered results from other resources are being considered in this paper. It is concluded that the AES is faster and more efficient than other encryption algorithms.[2] As far as the data transfer is considered , there is a slight difference in the performances of different symmetric key schemes (the most of the resources are spent on the data transfer , not for computing). Even if we have the scenario of data transfer, it would be necessary to use AES scheme if the encrypted data are being saved on the other end and are decrypted several times.

The study shows the safety measure levels for Web programming, considers performance measures of the encryption process in the programme language script with Web browsers. After that, a test simulation follows to get the best encryption algorithm compared to the Web browser. [3] It has been shown that Blowfish and AES have the best performances among the others. Both have better encryption (are stronger against data attack) than the other two. [9]

The study is carried out for various popular algorithms such as DES, 3DES, AES and Blowfish. They are implemented and their effect is compared with the encryption of input data of different content and sizes. Algorithms have been tested on two different hardware platforms to compare their performances.

The testing has been performed on two different machines: PII 266 MHz and P4 2.4 GHz. The results showed that Blowfish had very good performances compared to the other algorithms. Also, it has been showed that AES has better performances than 3DES and DES. We can conclude that 3DES has almost 1/3 throughput from DES-a, or in other words DES needs three times more to process the same amount of data. [5]

Rea Algorithm

New encryption algorithm REA is recommended because of its simplicity, efficiency and safety. It can surpass competitive algorithms. The proposed algorithm REA is a symmetric stream code that can be efficiently used for encryption and data protection. A changeable length key is required, which makes it ideal for data security.

Encryption Algorithm Rea

Algorithm steps for encryption REA are shown through:

- Step 1: Text and key input.
- Step 2: Adding the text key.
- Step 3: Converting previous text into the ASCII code.
- Step 4: Converting previous ASCII code into binary data.
- Step 5: Reverse the previous binary data.
- Step 6: Obtain all 8 bits from previous binary data and obtain ASCII code from it.
- Step 7: Divide previous ASCII code by 4.
- Step 8: Obtain the ASCII code from previous distribution and place it as one sign.
- Step 9: Obtain the rest of the previous distribution and place it as a second sign.
- Step 10: Returning the encrypted data.

INPUT: Plaintext (StrValue), Key (StrKey).
OUTPUT: Ciphertext (EncryptedData).

1. Add the key to Text (StrKey + StrValue) → full string (StrFullVlaue).
2. Convert the Previous Text (StrFullVlaue) to ascii code (hexdata).
3. Foreach (byte b in hexdata).
   a. Convert the Previous ascii code (hexdata) to binary data (StrChar).
   b. Switch (StrChar.Length).
      Case 7 → StrChar = "0" + StrChar.
      Case 6 → StrChar = "00" + StrChar.
      Case 5 → StrChar = "000" + StrChar.
      Case 4 → StrChar = "0000" + StrChar.
      Case 3 → StrChar = "00000" + StrChar.
      Case 2 → StrChar = "000000" + StrChar.
      Case 1 → StrChar = "0000000" + StrChar.
      Case 0 → StrChar = "00000000" + StrChar.
   c. StrEncrypt += StrChar. (where, StrEncrypt= "")
4. Reverse the Previous Binary Data(StrEncrypt).
5. For i from 0 to StrValue.Length do the following:
   a) if (binarybyte.Length == 8).
      I. Convert the binary data (StrEncrypt) to ascii code and,
      II. Divide the ASCII by 4 -A the result(first character) and,
      III. The remainder of the previous A second character.
6. Return (EncryptedData).

Algorithm steps for decryption are shown through:

- Step 1: Enter the text encryption and the key.
- Step 2: Circle the encrypted text to get the ASCII sign code and ad the next sign.
- Step 3: Multiply ASCII code first sign by 4.
- Step 4: Add the next digit (the rest) to the multiplication result operation.
- Step 5: Convert the previous ASCII code into the binary data.
- Step 6: Reverse the previous binary data.
- Step 7: Obtain all 8 bits from previous binary data and obtain ASCII code from it
- Step 8: Convert the previous ASCII code into the text.
- Step 9: Remove the key from the text.
- Step10: Return decrypted data.

```
INPUT: Ciphertext (EncryptedData), the Key (StrKey).
OUTPUT: Plaintext (DecryptedData),
  1. For (i = 0; i < EncryptedData. Length; i += 2)
     a. Get the ascii code of the encrypted text
     b. newascii = (EncryptedData[i] * 4) + the next digit(remainder)[i+1].
  2. Foreach (byte b in newascii).
     a. Convert the Previous ascii code (newascii) to binary data (StrChar).
     b. Switch (StrChar.Length).
        Case 7 → StrChar = "0" + StrChar.
        Case 6 → StrChar = "00" + StrChar.
        Case 5 → StrChar = "000" + StrChar.
        Case 4 → StrChar = "0000" + StrChar.
        Case 3 → StrChar = "00000" + StrChar.
        Case 2 → StrChar = "000000" + StrChar.
        Case 1 → StrChar = "0000000" + StrChar.
        Case 0 → StrChar = "00000000" + StrChar.
     c. StrDecrypt += StrChar.
  3. Reverse the Previous Binary Data(StrDecrypt).
  4. For i from 0 to StrDecrypt.Length do the following:
     a. if (binarybyte.Length == 8).
        I.  Convert the binary data (StrChar) to ASCII code (hexdata) and,
        II. Convert the previous ASCII code (hexdata) to the text
            (StrFullVlaue).
  5. Remove the key from the text (StrFullVlaue - StrKey) → (StrValue).
```

Safety Factor And Work Analysis

The following factors are used as safe and efficient criteria: key space, key sensitivity, data safety from the attack, computing speed, information and correlation coefficient. [4]

Key Space Analysis

Key space is the total number of different keys that can be used in cryptographic system. Algorithm safety (strength) is the key length function. The longer the key is, the algorithm is more resistant to a successful brutal attack. Key length is universally expressed as the number of bits. [4]

Key length of the N-bit has the key space 2n possibility. From the cryptography point, the size of the key space should not be less than 2100 to ensure a high level of security. [6]

The secret key of the proposed encryption algorithm REA is 256 bit long, can be increased, the key space has about 2256 (1.16x1077) different combinations of secret key. Long key space is sufficient for reliable practical use.

Key sensitivity analysis

Good encryption should be vulnerable to a small change in secret keys. Proposed encryption algorithm REA is vulnerable to a small change in secret keys. If the secret key changes a bit, decrypted data are not performed. [8]

Attack analysis

There are well-known attack methods, as well as brutal force that determines the number of steps and time needed for a successful attack.

I. Attack steps

The attack steps are defined as a number of steps needed for performing the most famous attack. The number of steps can help in deterring the time which could be needed for a successful attack using a specific processor, without the need to actually attack the algorithm. Proposed encryption algorithm REA using the key length 256 bit, can be increased and the attack steps are about 2256 (1.16x1077).

II. Time of the attack

The attack time is defined as the time needed to perform the most famous attack on a certain processor. For an example, machine that works on 2000 (Mops) multiply 60 (seconds/minutes) multiply 24 (hours/day) 365 (days/year) equals 6.3072x1016 operation/year. The attack time in years is performed by dividing the attack steps by the pilot Mtop annually (6.3072x1016 operation in a year). Since the proposed algorithm REA used 256-bit, then the time of attack is approximately 1.839x1060 years.

Speed analysis

This is an important tool for evaluating the efficiency of encryption algorithms that measures the time it takes to encrypt and decrypt the process. Encryption and decoding time of the proposed encryption algorithm REA is shown in experimental results and it is fast enough. [3]

RESULTS

This section examines a typical case study that evaluates the security and efficiency of the proposed encryption algorithm REA and compares it to the most common encryption algorithms: DES, 3DES, RC2, AES and Blowfish. Comparisons were made for these encryption algorithms at computing speed (encryption and decryption time) and secure analysis such as the information entropy and the correlation coefficient. To minimize encryption and decryption time, the cryptosystem should be optimized. Practically, information entropy of the encrypted data is smaller compared to the ideal case. Also, if the correlation coefficient is equal to zero, this means that the encryption text is completely different from the original.

All of the experiments were performed on the laptop IV 2.0 GHz Intel processor with 1 MB cache memory, 1 GB memory and one 120 GB disk. The operating system used was Microsoft Windows 7 Professional. Results were made based on the Microsoft SQL Server 2008 database "Northwind", which contains eight tables. Program Tasks were made by Microsoft Visual C # 2008. In the experiments, using two databases from the database "Northwind", the results are:

a. NorthwindPlaintext does not have encrypted fields, but it is used for encryption and decryption of some fields (Table 1) using the most common algorithms for encryption: DES, 3DES, RC2, AES, Blowfish and proposed algorithm REA.
b. Northwind REA has encrypted fields (Table 1) using proposed encryption algorithm REA.

Table 1. *Name of the encrypted fields*

	Field name	Table name
F1	Contact name	Suppliers
F2	Price per unit	Products
F3	Boat address	Orders
F4	Freight	Orders
F5	Price per unit	Order details
F6	Quantity	Order details
F7	Description	Categories
F8	Notes	Employees
F9	Contact name	Buyers
F10	Contact title	Buyers

The keys used in the encryption data keep confidentiality in the encrypted table with the proposed encryption algorithm REA. This table contains five StrTable fields (encrypted table name), StrField (the name is encrypted field), StrKey (is the encrypted key used in the encryption process, StrAlgo (the name of encryption algorithm) and StrFieldType (type of encrypted field), where the first three fields are encrypted with the proposed REA algorithm. Only the administrator will get these keys using the password.

After the administrator enters the password and selects the required database, he needs to look at the encrypted keys table in the "NorthwindREA" database.

Table - dbo.Key | Summary

StrTable	StrField	StrKey	StrAlgo	StrFieldType
#3#3$3%2&2#1#0	303132/0$0$1"3...	3031321231302...	REA	nvarchar(4000)
303132,0#1&3&...	303132.1#1&2...	3031322223213...	REA	money
303132+3#1$0...	303132*2$1%2...	3031321212213...	REA	money
303132,0#1&3&...	303132*2$1%2...	3031321333213...	REA	money
303132,0#1&3&...	303132+2"2"2$1...	3031322012333...	REA	smallint
303132.2$2#3$...	303132,1$0"3&...	3031323312333...	REA	ntext
303132/0"2#0"3...	303132/0$0$1"3...	3031323112333...	REA	nvarchar(4000)
303132/0"2#0"3...	303132/0$0$1"3...	3031322122202...	REA	nvarchar(4000)
303132,0#1&3&...	303132+0%3%...	3031323312132...	REA	nvarchar(4000)
303132/0"2"3&2...	303132.3&2#0'...	3031322033132...	REA	ntext
NULL	NULL	NULL	NULL	NULL

Figure 1. *Table of encrypted keys with proposed REA algorithm in „Northwind_REA" database.*

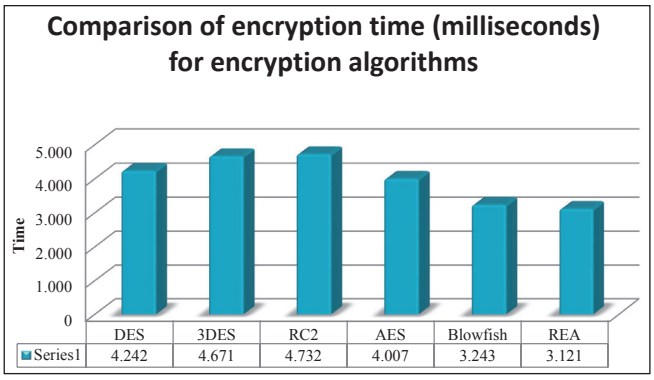
The experiments were encrypted and decrypted in ten different fields (table 2) with the proposed encryption algorithm REA and the calculated execution time for each of them. Then, the average execution time is calculated for each encryption and decryption process.

The comparison results are shown in Table 2 in the encryption time and Table 3 at decoding time.

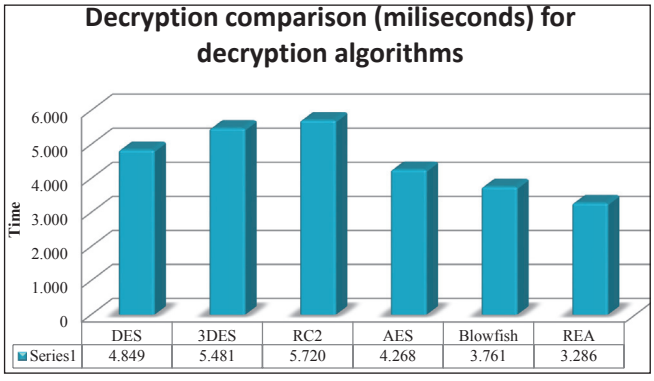
a. First point: The results show the superiority of the REA algorithm compared to other algorithms in terms of encryption and decoding time.
b. Second Point: Blowfish requires less encryption and decoding time than all algorithms except REA.
c. Third point: AES has the advantage compared to the other 3DES, DES i RC2.
d. Fourth point: 3DES has low performances in terms of encryption and decoding time com-

Table 2. *Encryption time comparison (milliseconds) for encryption algorithms*

	DES	3DES	RC2	AES	Blowfish	REA
F1	0.141	0.263	0.342	0.109	0.116	0.104
F2	0.359	0.419	0.395	0.329	0.296	0.266
F3	3.609	4.484	4.594	3.047	2.671	2.521
F4	4.063	4.469	4.513	3.297	2.544	1.718
F5	14.194	14.968	15.234	14.000	11.304	11.297
F6	15.906	17.547	17.328	15.484	12.452	12.360
F7	0.344	0.453	0.449	0.331	0.274	0.265
F8	2.960	3.203	3.531	2.688	2.051	2.005
F9	0.422	0.463	0.487	0.403	0.376	0.335
F10	0.421	0.438	0.442	0.386	0.346	0.334
Average	**4.242**	**4.671**	**4.732**	**4.007**	**3.243**	**3.121**



Graph 1. *Graphical presentation for encryption time comparison (milliseconds) for encryption algorithms*



Graph 2. *Graphic representation of decryption time comparison (milliseconds) for decryption algorithms*

Table 3. *Decryption comparison (milliseconds) for decryption algorithms*

	DES	3DES	RC2	AES	Blowfish	REA
F1	0.125	0.141	0.156	0.135	0.137	0.121
F2	0.343	0.359	0.384	0.344	0.322	0.271
F3	4.672	4.992	5.172	4.212	3.816	3.445
F4	4.313	4.625	4.516	4.103	3.417	1.654
F5	16.687	19.156	20.281	14.266	12.963	12.687
F6	17.797	20.313	21.406	15.125	13.761	11.030
F7	0.359	0.404	0.426	0.359	0.318	0.281
F8	3.312	3.891	3.906	3.319	2.175	2.743
F9	0.443	0.478	0.499	0.421	0.381	0.318
F10	0.438	0.447	0.456	0.398	0.315	0.308
Average	**4.849**	**5.481**	**5.720**	**4.268**	**3.761**	**3.286**

pared to DES. It has also been established that RC2 has low performance in terms of encryption and decryption time compared to other five algorithms.

Overall, the results have shown that the proposed encryption algorithm REA has very good performance compared to other encryption algorithms. It has also been shown that Blowfish and AES have better performance than DES, 3DES and RC2. For the factor information (Security Analysis), secure encryption algorithm should perform a condition about information entropy and this means that the encrypted text should not provide any information about pure text.

Table 4. *Secure (entropy) values comparison for the encryption algorithms.*

	DES	3DES	RC2	AES	BF	REA
F1	5.577	6.678	6.948	7.504	3.861	7.817
F2	4.765	5.872	6.354	7.415	3.801	7.181
F3	5.805	6.878	7.165	7.845	4.405	7.604
F4	4.748	5.847	6.451	7.423	3.791	7.255
F5	4.751	5.846	6.234	7.423	3.783	7.053
F6	4.769	5.841	6.587	7.656	3.799	7.154
F7	5.666	6.754	7.078	7.772	4.212	7.631
F8	5.258	6.339	6.975	7.583	4.163	7.735
F9	5.632	6.702	7.025	7.608	3.998	7.577
F10	5.623	6.667	6.952	7.801	4.358	7.684
Average	**5.259**	**6.342**	**6.777**	**7.603**	**4.017**	**7.469**

The experiments result in safe (entropy) values of encrypted fields with the proposed REA encryption algorithm and comparison with the most common algorithms: DES, 3DES, RC2, AES and Blowfish. The results for this comparison are shown in Table 4, on secure (entropy) values.

Secure (entropy) of encrypted data with the proposed encryption algorithm REA (about 7.469) is less than the ideal case. Therefore, REA design is the data encryption security.

Conclusion

Encryption of sensitive data in databases becomes increasingly important in protection against intruders who bypass the conventional mechanisms of access control and have direct access to the database. The effect and security of the new scheme must be studied systematically. For this purpose it was suggested that these issues be considered in this paper and to contribute to the following:

- We are introducing a new encryption algorithm REA, transferring its advantages and functions compared with other similar encryption algorithms. This limits the costs of added time on encryption and decryption, so the performance of the database system was not reduced.
- Evaluating the efficiency of the proposed REA encryption algorithm and comparing it with the most common encryption algorithms, namely: DES, 3DES, RC2, AES and Blowfish shows the speed of the encryption and decryption process.

The results show the superiority of the REA algorithm compared to other algorithms in terms of encryption and decryption time.

- The safety comparison has been shown (used to measure entropy of information). The results show that safe (entropy) of the encrypted data proposed by the REA encryption algorithm (about 7.469), which is smaller than the ideal case.

Therefore, designing a REA algorithm provides a powerful safety in database encryption.

References

[1] Castano S, Fugini M, Martella G, Samarati P (1995) Database Security, Addison - Wesley, pp. 11.-14.
[2] El – Fishawy N (2007) Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms, Proceedings International Journal of Network Security, pp. 5.
[3] Idrus S, Aljunid A (2008) Performance analysis of encryption algorithms text length size on web browsers, International Journal of Computer Science and Network Security, vol.8, pp. 25.
[4] Musheer A, Shamsher M (2009) A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping , International Journal on Computer Science and Engineering, pp. 46.-48
[5] Salama D, Abdual - Kader H, Hadhoud M (2011) Studying the Effects of Most Common Encryption Algorithms, International Arab Journal of e- Technology, pp. 16.
[6] Weerasinghe T (2012) Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms, International Journal of Information & Network Security, pp. 79.

[7] Zajmović M (2017) Cryptographic data protection methods in databases - example Oracle, Proceedings, University of Novi Sad, Faculty of Applied Management, Economics and Finance Belgrade, Republic of Serbia, pp. 77
[8] Zeghid M, Machhout M, Khriji L, Baganne, Tourki R (2007), A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology, pp. 206.

Submitted: May 31, 2019
Accepted: June 10, 2019

About the authors

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. He completed his master studies at the same faculty in 1994, and successfully defended his doctoral dissertation in 1997. He is the Dean of the College of Information Technologies of Pan-European University "Apeiron" in Banja Luka.

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.

Mahir Zajmović was born on July 10, 1986 in Mostar, Bosnia and Herzegovina. He graduated from the Faculty of Information Technologies at the University "Džemal Bijedić" in Mostar in 2010. He successfully completed a joint Master's degree program at the Faculty of Information Technologies of the University "Džemal Bijedić" in Mostar and the Faculty of Economics of the University of Sarajevo in 2014. He is currently a doctoral student.

For citation

Latinović B., Avramović Z.Ž., Zajmović M., Safety Analysis of Reverse Algorithm Encryption in Databases, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:29-35, (UDC: 004.7.056.55:004.432.2), (DOI: 10.7251/JIT1901029L), Volume 9, Number 1, Banja Luka, june 2019 (1-48), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

THE IMPORTANCE OF INFORMATION TECHNOLOGIES IN MANAGING HUMAN POTENTIALS OF THE LOGISTIC CENTERS OF THE REPUBLIC OF SRPSKA

Nataša Đalić[1], Edit Terek[2], Mina Paunović[2], Mihalj Bakator[2]

[1]University of East Sarajevo, Faculty of Transport and Traffic Engineering, Republic of Srpska, djalic.natasa@gmail.com

[2]University of Novi Sad, Technical Faculty "Mihajlo Pupin" in Zrenjanin,

terekedita@gmail.com, minapaunovic91@gmail.com, mihaljbakator@gmail.com

Critical Review

DOI: **10.7251/JIT1901036DJ** UDC: **005.96(497.6):[659.23:004.738.5**

Abstract: Information technologies within logistic systems and their impact on economic, social and personal development have become an important subject of scientific research over the past decades. Theoretical and empirical research has shown the need to achieve and exploit positive outcomes (organization expansion, efficiency, effectiveness, competitive position) adoption and implementation of information technologies in logistics centers. At the time of great technological innovations, the human resources management plays an important role in achieving the competitive advantage of logistics centers on the market. With the development of new technologies, there are also changes in the way human resources management is handled within companies. The theme of this paper is the research of the connection between the importance of information technologies in managing human potentials and the performance of logistics centers. Information technologies have a growing presence in the management of human resources within logistics centers, and therefore their application achieves a great competitive advantage on the market. The aim of this paper is to use the analysis and descriptive methods to find a solution to the importance of information technologies in human resources management within a logistics center with the greatest focus on ERP systems.

Keywords: information technology, human resources management, logistics center, ERP system.

INTRODUCTION

The global processes of globalization, social knowledge and economic effects of the existence of separate countries, organizations and individuals, as well as the rapid development of information technologies have greatly influenced the changing of the existing business structure and ways of communication, and the fact is that the adoption and implementation of information technologies is the basis of competitiveness and economic growth for companies, organizations and countries that are able to use them [18].

Information technologies and their impact on economic, social and personal development have become an important subject of scientific research over the past decades. According to the data from Ollo-Lopez and Aramendia-Munte (2012), numerous studies focused on the analysis of how the adoption of information technologies affects logistics centers [9].

The development and use of information and communication technologies have transformed modern society into an »information society«. Its main characteristic is that information and communication technologies play the most important role in both production and the economy, as well as in all other spheres of life of individuals and society as a whole [13].

In a business environment, the basic resource of each company is made up of people with their abilities, which enable them to solve their tasks, and thus achieve the common goals of the company.

In the companies and countries that assimilate new technologies and innovations, rapid changes are expected. There are different studies analyzing ICT, especially factors that impact ICT adoption. Analysis of ICT effects in private sector is significant only after thorough analysis of conditions that should be satisfied in order to successfully adopt ICT – expectations towards positive impacts of ICT and characteristics of individual company (financial, technological, personnel resources, flexibility of structures etc.) are closely linked. According to Alam and Noor (2009) the adoption of the ICT "is considered to be a means to enable businesses to compete on a global scale, with improved efficiency, and closer customer and supplier relationships". Therefore, the adoption of ICT is recognized as crucial condition enabling SMEs to consider information and communication technology as an important implement in their business to take competitive advantage from the global markets.

Global competition encourages companies to make steady and rapid progress in order to survive against the new demands posed by globalization. If the company has good human potential, i.e. quality and educated human resources, it is possible to respond to the challenges and demands that it is constantly facing. Human resources are the most important component of any organization. Human resources have the treatment of the most important capital - human capital.

Human resource management is a management activity that focuses on human resources. Human potentials include the total knowledge, skills, abilities, creative possibilities, motivation and loyalty that an organization (or society) has at its disposal. It is the total intellectual and psychological energy an organization can engage in achieving goals and developing a business [11].

The ability of logistics centers for efficient and effective functioning, at the time of the global expansion of information technologies in the world, depends on the support of various information technologies within the logistics center itself. The basic motive for the application of information technologies in the management of logistics and supply chains is in their ability to collect a multitude of data and information, as well as savings arising from sophisticated analysis of these data [16].

Information technologies can be used to manage and monitor business processes within an enterprise, or to transfer information between different businesses or individuals. The application of information technologies within the logistics center itself will increase the competitive advantage of the center on the market. Many companies provide value-added services to their users by applying modern information technology, and at the same time it is a means of their differentiation on the market, and, on the basis of this, the way of conducting business contributes to the development of strong and long-lasting connections with its users.

At the time of major changes and the daily introduction of modern technologies into all business segments, the most important part of each logistics system is the information flow, which includes the exchange of information between parts of the internal transport system and between the enterprise and the external system.

The importance of information as a new production factor in the conditions of increased competition, the opening of new markets, the shortening of the product life cycle and the globalization of the market has grown remarkably. This is due to the fact that, without the use of a modern information system that would allow the introduction of a flexible and time-optimized business concept, many companies would not be able to successfully to do business or to exist and survive on the market.

The use of modern information technologies is the mperative for the successful operation of logistics centers on a global basis.. The reason for this is the fact that information technologies, which are constantly in great expansion, contribute to the process of creating a new way of doing business in all its segments.

Development of human resources management, at a time when globalization of the market has reached its stagnation, shows that this activity takes its place in the development of companies that want to maintain their leading position on the market or achieve greater competitiveness [12].

Strategic goals of logistics centers are trying to be realized through better connections with the organizational structure of the company. Personal interests of individuals and teams must be in line with organizational goals, which achieve the strategic goals of the company. A very important link in the chain is human potential, which, with their knowledge and possibilities, help achieve goals.

Using the analysis and the descriptive method in this paper, we find a solution on the importance of information technologies in human resources management within the logistics center and in order to gain a certain competitive advantage in the market.

PROCESSES OF MANAGEMENT OF HUMAN RESOURCES IN LOGISTIC CENTERS

Human resource management is one of the most important sectors of each company, and so in logistics centers, as it is precisely the human resources managers that determine whether the logistics center will achieve the set goals and tasks in its business, and therefore whether it will be competitive on the market or not. Logistic centers daily notice that people are their biggest capital, which gives them a competitive advantage on the market. Increasing the complexity of logistic processes within the logistics centers requires a high-quality, competent and educational staff capable of responding to all the requirements [7].

Human Resources Management relates to the practice and policies necessary to perform managerial tasks in relation to personal issues, and in particular the recruitment, training, assessment and rewarding of employees in the company and the provision of a secure, ethically acceptable and just environment for them. Human resources management is very important for companies, as the last thing the manager wants is to choose the wrong candidate for the job, and thus endanger the performance of a particular sector, and the entire company [8].

With the development of globalization, there is a growing competition and companies are constantly facing new challenges to reduce costs and increase productivity. In addition to globalization, technological progress is very important, that is, human resources management has to find a way to quickly apply new technologies in order to improve its own work and efficiency. A competitive advantage on the market is achieved with an adequate workforce that is able to respond to market needs and changes that are happening [13].

Human resource planning must be dynamically linked to the needs of creating staff assumptions, timely and successful realization of tasks, or goals of logistics centers.

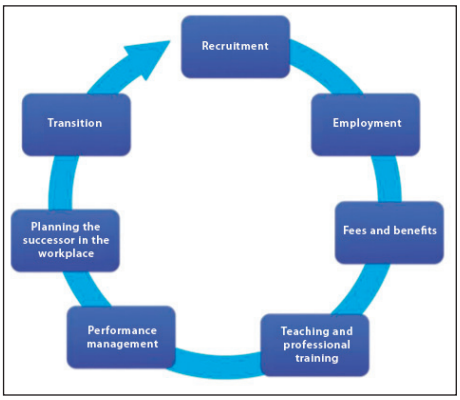


Figure 1. *Life cycle of employees in logistics centers [6]*

This cycle allows logistics centers to make choices and employ the best potentials, develop employee skills, harmonize employee aspirations with business goals, measures and rewards employee results, plan future exchanges in key locations, and ensure the transition of employees through retirement and exit from the company [6].

Recruiting management is a module used at the earliest stage of the employee's life cycle to attract the most talented candidates who will become successful employees within the center [7].

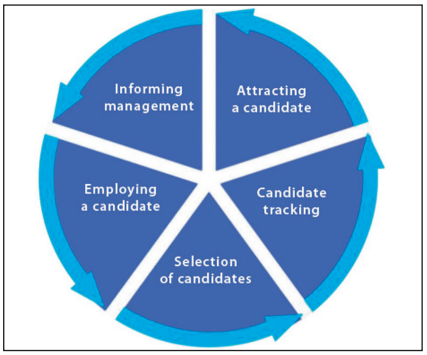


Figure 2. *The life cycle of employees in human resource management [7]*

INFORMATION SYSTEM FOR THE MANAGEMENT OF HUMAN RESOURCES OF THE LOGISTIC CENTER

The most common segment of information systems is information that can be defined by Shannon and Viver as "the amount of reduction in uncertainty when a message is received."

This creates the need for an explanation of the concept of data that can be defined as the raw material of the system it receives through the procedures and used to generate information. According to one

of the definitions of the information system, several forms of resources are used, so apart from people as one of the most important resources, there are also resources that fall into hardware such as appliances that are used and resources that are part of the software, for example, guidelines for activities, procedures and the like. In this way, the organization of resources takes the data, processing, output, storage and control of data, and then they turn into products of information nature [18].

Modern technology plays a very important role in human resource management, facilitates and improves its functionality, but it also modernizes, accelerates and improves the work of the human resources department of each logistics center.

In order to maximize the management of the human potentials of various individual logistics centers, it is necessary to have a special organizational unit for human resources that develops the methodology, obtains, analyzes and stores data on employees and proposes to the superiors in the hierarchical system determined. In addition to such systemic hierarchical forms, it is also necessary to use modern IT solutions designed specifically for the management of human potentials.

The Human Resources Management Information System is used for decision making in management, launching initiatives for improvement in human resources management, and adopting regulations in the field of human resources. The most important functions of the system are updating employee data, maintaining organizational scheme of the company, integrating with other relevant systems, analyzing and creating job descriptions or their structure, producing statistical reports and analyzes, recruiting, analyzing needs for additional training and education, developing training plans and education, assessment of work results and analysis of employee performance and career planning.

Implementation of information systems is one of the most important processes of every company that seeks to improve its business and constantly develops its information system.

Logistic information systems supported by computers are defined as a unique and harmonized system of hardware, software, data, networks and staff that serves logistic planning, implementation, management and control in all activities that are carried out in order to accomplish the necessary tasks [15]. According to the decision-making method, information systems can be divided into several groups depending on the level of hierarchy in the company. Planning, managing and monitoring the information system as a whole with all interaction influences provides optimal use of synergy and efficient management of current and segmented processes.

Today there is a very large number of information systems that can be found on the market, and whose introduction improves and facilitates the entire business system business, that is, the process of human resources management in companies.

Resource Planning in Corporations (ERP) is a process in which business resources are planned, and in the very implementation of this process, one of the business information systems (commercial software package) is mainly included. Application of certain software packages can contribute to a significant improvement in the quality of services and products.

ERP is a strategic tool that enables the integration of all organizational parts and the synchronization of isolated business functions in the organization into related business processes of a single information system.

What is very important for ERP systems is that they have a number of application advantages because they consist of a set of standardized software solutions for business processes. As a consequence, the implementation of these systems leads to the reorganization of existing business processes within logistics centers. Given the difficult adaptation of existing business processes to the ERP system, its implementation is always closely linked or almost inseparable from reengineering [14].

In response to the needs of logistics centers of all sizes to redefine their business processes, ERP (Enterprise Resource Planning) software packages are developed that integrate and process information based on business process monitoring in an organization.

Considering the trend that is actual in our country and in the world, where there is the rule that an organization has to have a wide spectrum and a large volume of its business if it wants to be successful, competitive and above all to provide support from the public interest through the use of current and modern information technology, the conduct of such business and its planning must in many ways be performed through some of the modern ERP solutions [17].

ERP systems as standard, complex, software packages were developed to meet the business requirements of organizations as a whole and as such have incorporated the experience and skills taken from organizations, as well as previous ERP solutions users [17].

Adequate implementation of the ERP system in companies enables efficient and effective job management in a number of fields. ERP systems are a combination of managing the entire company's business and modern technology, which makes it easier to manage.

Within each ERP system there are specific modules, and a module that supports human resources management contains information about employees, collecting and archiving information about their skills, their positions, and the like. The modules can have exactly the same content, but the different names, and vice versa [4].

ERP systems consist of modules representing standard processes in organizations, such as financial modules, human resource modules and logistic modules.

The ERP system for new technologies and the Internet integrates new modules, such as SCM (Wsupply Chain Management), CSM (Customer Relationship Management), Sales Force Automation (SFA), Advanced Planning and Scheduling (APS), Business Intelligence (BI) and e-Business.

The most important characteristics of the ERP system are flexibility, independence, comprehensiveness, modularity, openness, flexibility and experience.

The flexibility of the ERP system implies its ability to respond to every set request in the organization in line with changes in the business environment.

The independence of the ERP system implies independence from the hardware, operating system, and database management system.

The ERP system, through its comprehensive feature, supports all types of business functions and business organizations of all types of activities [17].

The structure of the ERP system is globally comprised of subsystems and modules, but it must also be ensured that each of the modules can be added to the subsystem or removed from it, thus reflecting the characteristics of the ERP system modularity.

The openness characteristic implies that the ERP system must support different hardware platforms, but also provide links to applications from other software vendors.

Each organization does not need all modules of the system, so it is necessary to adapt the system to the requirements of each organization, and in this we will look at the characteristics of the ERP system of flexibility.

The ERP system is an experience for all business processes, as well as solutions that have shown the best results in the practice so far.

One of the most important advantages of ERP is in linking work units within the enterprise, which contributes to effective communication and rapid response capabilities [2].

As technology developed, the influence on strategic human resource planning has also grown. Human Resource Management Information Systems can be defined as systems that group data in databases for easier access and analysis. Certain information systems provide the possibility of automating the process as in the case of calculating tax rates, while in others it is done in order to reduce the need for manual data entry, which improves accuracy and efficiency. As one of the functions in the human resources sector that benefits from the use of human resources management information systems, there is a system of total rewards for the model of overall compensation, including benefits and wages. These information systems provide more efficient monitoring and planning of salaries, insurance, pensions and other aspects. System monitoring of current costs and others [16].

In the very creation and development of human resources management, information systems for human resources management were primarily used for administrative and operational procedures. Collecting data on requests for leaving the company, compen- sation and possible accidents, as well as wage reimbursement was carried out. During the 1970s and 1980s, due to some factors, there was a change in access to these information systems. Given the complexity of the payment system, there is a need for greater flexibility and the use of information systems as a result of the development of the use of hardware and software systems. In larger organizations, the payment processing system was separated from other human resources functions, and some organizations delegated those responsi-

bilities to associates outside companies because of their expertise in the area [16].

Information systems for human resources management are used to collect, store, manipulate, analysis of information on human resources of the organization. The purpose of these systems is to implement and provide support for tactical operational decision-making, program evaluation, procedures or day-to-day operations [17.

Goals of the Application of Information Systems in Logistic Centers

Logistics information system can be defined as a structure of interaction between people, equipment and procedures that together provide relevant information to the logistics manager for the purpose of planning, implementation and control.

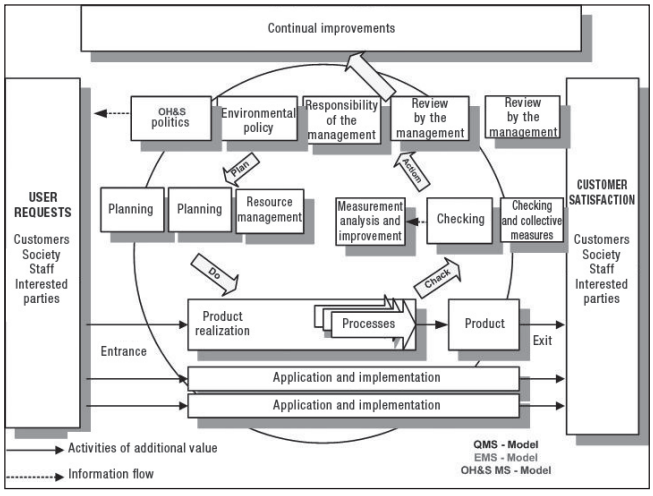


Figure 3. *Logistic information system [17]*

One of the most important goals of application of information systems within the logistics center is to connect all members from the place of supply of raw materials or semi-finished products for the production process to the place of delivery or ordering, whereby synchronization of the information flow with the goods flow is necessary. In this way, it is possible to plan, monitor and determine the time from the occurrence of a request (order) to the final realization on the basis of real data. Each participant in the chain should have access to information on where the appropriate product is located [1].

Based on the structure of the chain, different flows of goods and information can be defined. Respecting the needs of chain members for different types of information, the question of the availability of the requested information is raised. The availability of information on the status of raw materials and products is the basis for making appropriate decisions. In the event that there is a delay in the delivery of raw materials, which may significantly influence the realization of the production program, the task of the information system is to forward this information to relevant stakeholders in order to make appropriate correction in the production process (delay of the planned production plans or consideration of alternative sources of raw materials).

Moreover, one of the essential goals of the application of information systems, which is to satisfy conditions in terms of information, can be accessed from anywhere, and that information has the same content for all users of that system.

The third goal of information systems application in logistic centers is to analyze data in order to achieve a state of overall functioning within the logistics center. In addition to the possibilities of analysis, the information system should support finding the most efficient ways of production, assembly, storage and product ditribution. On the basis of the information received, operational, tactical and strategic decisions within the center can be made[1].

Previous studies have shown that the priority of each logistics center should be logistics elements such as deliveries on time, stock levels, orders, tracking, ordering, ordering, downloading from customers and the possibility of replacement. All activities are in the domain of logistics managers, and their successful implementation depends largely on the exact flow of information, and this is successfully achieved through the use of information systems [3]. The goal of all of the above is that information solutions, that is, the use of information systems that are maximally convenient and easy for users, support all business functions, i.e. To maximally facilitate the work of the employees within the logistics center.

There is no information technology or type of information system without contribution to human resource management. In one area, some systems do it in a good and productive way, while in another system their performance is not so impressive. On the other hand, some systems have completely opposite benefits and impacts. The best measure of

availability of information capital in human resources management is the level of development of online transaction processing systems [12].

APPLICATION OF ERP SYSTEM IN LOGISTIC CENTERS OF THE REPUBLIKC OF SRPSKA

A survey on the importance of information technologies in the management of human potentials of logistics centers on the market was conducted on a representative sample of 136 economic entities in the territory of Republika Srpska.

The relatively high return rate of correctly filled questionnaires (68% - 136 questionnaires) can be explained by the fact that the questionnaire is sent to experienced officials who are familiar with the issues of this research. Survey questionnaires were sent to respondents mostly via e-mail, post or in person. The survey process was carried out in the period from the beginning of February to the end of May 2018.

The significance of information technologies in the management of human resources of logistics centers in the Republic of Srpska, in the conditions of the global crisis, has a number of other advantages reflected in the modernization of business activities with a reduction in the number of employees, better financial performance of the company, more rational use of resource capacities as well as better distribution of materials and goods. In the Republic of Serbia, 93% of respondents of business entities confirmed that they use modern information technologies in their business.

The questionnaire is addressed to managers who are intensely using information technology in carrying out everyday tasks. Using the modern methods of descriptive and quantitative statistics, the data submitted are processed.

The aim of this research is to obtain data in order to define the importance of information technologies in the management of human potentials of logistics centers in the Republic of Srpska in the conditions of the global crisis. In addition to the stated main goal of this research, there were other goals of the research related to the impact of information technologies on reducing the need for hiring of employees, automation and faster recording of business events, improvement and development of financial reporting, improvement and development of accounting analysis, increase of productivity of labor, the development of logistics operations in the near future, and more. In the first part of the questionnaire, general data on surveyed entities were collected, such as name, activity, ownership and number of employees.

Distribution of surveyed subjects according to the activities they perform are shown in the following chart.

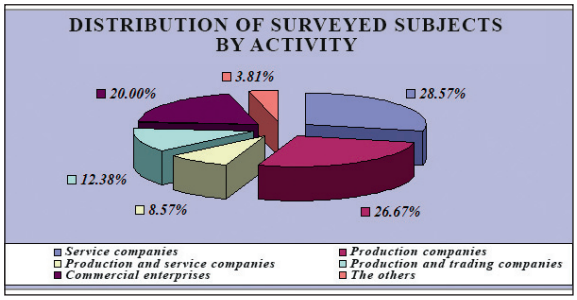


Figure 4. *Distribution of surveyed subjects by activity*

Modern information technologies are quick steps towards improving all business activities in logistics centers. Modernization of business activities in the company in order to increase the competitiveness of logistics centers on the market is achieved by reducing the number of employees and consequently by reducing the costs related to employees. A part of the research conducted for this purpose has confirmed that the application of information technologies has a great impact on the number of employees, and consequently also on the labor force, and the standard of work of workers is becoming more and more complex in the process. Based on the very rapid development of information technology, the results of the research related to the contribution of information technologies to the reduction of employees in logistics centers confirmed a significant contribution to reducing the demand for work force. As much as 75.55% of the surveyed subjects confirmed that the introduction of information technology indicates the need to reduce the number of employees in logistics centers.

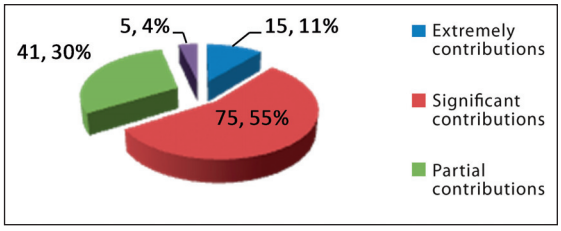


Figure 5. *Influence of information technology on the reduction of labor demand*

An empirical research on the impact of information technology on the competitive advantage of companies in the market in the conditions of the global crisis has confirmed their significant influence on maintaining a competitive position on the market. The conducted research is shown in Figure 6 where it is clearly seen that the majority of subjects surveyed, as much as 66%, agree that information technologies make a great contribution to achieving and maintaining the competitive position of logistics centers on the market.

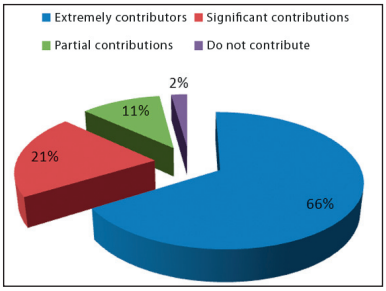


Figure 6. *Influence of information technologies on achieving and maintaining the competitive advantage of the company*

The conducted research has shown that the management of logistics centers in the Republic of Srpska is aware of the role and importance of information technologies for improving the business results, for achieving a competitive position in the market, and at the same time the introduction of information technologies in the company is seen as a long-term investment.

An important segment of the conducted research is the views of users of information systems who believe that the application of information technologies is extremely important and necessary in the everyday work of the company. They believe that the business problems will be overcome with their application, and they will meet the habits, needs and expectations of the customers, and therefore will also achieve the competitive position of the companies on the market in times of crisis.

In the world, ERP systems represent a powerful management tool for daily resource management of modern logistics centers.

It is evident that logistics centers that use ERP are in great advantage compared to competition due to transparency of data, rationalization of costs and time, optimization of business functions, automation of business activities and better planning of resources.

The situation in the Republic of Srpska is not very favorable.

Statistical Office of the Republic of Srpska conducted a survey on the use of information and communication technologies within logistics centers.

It could also be said that in our country, the initial introduction of the ERP system started in companies that had to now increase their value for sale or privatization, as well as in companies that wanted to work with large foreign partners at the same level.

Enterprise size analysis shows that of the total number of large companies, the ERP system owns 27%, 11.6% of medium-sized enterprises, while 8.4% of small businesses have an ERP system.

Banks and insurance companies mostly use the ERP system (24.1%), followed by companies in the field of Transport, storage and communication (24%).

Based on the research, it was concluded that the number of companies using the ERP system decreased by 6.4% compared to 2007. The reason for this is most likely a poor information about the ERP system. The following data is also supported by this:

In 2008, even 16.9% of companies declared that they did not know if they had an ERP system, while this figure for 2007 was much smaller and amounted to 4.4%

It could also be said that in our country, the initial introduction of the ERP system began in companies that had to now increase their value for sale or privatization, as well as in companies that wanted to work with large foreign partners at the same level.

Conclusion

The intensity of changes and qualitatively changed business conditions emphasize the special importance of the communication system in order to facilitate the interaction and connection of all elements of the system and the environment. We are witnessing a daily increase in the use of information technology in logistics centers for the easier operation of these.

The model as a whole ensures that each user performs tasks more easily, more precisely and more efficiently with the provision of data and tools for the realization of his functions.

The application and project solutions of this model greatly contribute to the development and

improvement of accounting information through the following:

- creation of accounting information for the needs of decision making,
- improvement and development of the business accounting functions of the company,
- creating new and improving existing project and application solutions,
- development of modern forms of accounting information and the like.

The presented model represents a set of practically possible solutions based on the scientific understanding of information systems that influence the process of creating a competitive advantage in a global context. Taking into account the above, it can be concluded that this model influences the development and improvement of:

- planning and management of employment of accounting officers,
- planning and management of costs,
- profitability of the product,
- financial reporting,
- audits of accounting information systems.

By creating timely and quality information systems, the model significantly contributes to the development of the business decision-making process and business in general. Therefore, it can be concluded that the existing solutions provide the following:

- performing a significantly larger scope of tasks in a very short period,
- improving the efficiency and effectiveness of business operations,
- providing new services and creating new opportunities for more efficient management enterprise,
- the growth and development of the accounting profession,
- increase the productivity of the work of accounting officers,
- better information support for users.

Considering the above, it can be noticed that the advancement and development of information technologies in the process of crushing competitive advantage greatly contributes to increasing the profitability of business, ie strengthening the competitive position of companies on the domestic and international market in the conditions of the global crisis.

After the introduction of the ERP system into logistics centers, it can be concluded that the quality of business has been raised to a significantly higher level.

Logistic centers that use ERP are of great advantage over the competition due to transparency of data, rationalization of costs and time, optimization of business functions, automation of business activities and better planning of resources.

The time of big technological changes and the daily introduction of new information technologies led to the fact that the traditional appearance of the company changed under the influence of numerous changes. The business environment has also experienced major changes in terms of stronger and more modernized competition in the market, new customer demands, and thus all of this reflected and human resources management within logistics centers.

Logistic centers are forced to rely on the knowledge, abilities and skills of employees within it, and with the use of information technologies in the management of human potentials occupy a significant competitive position on the market, and therefore most logistics centers now see information systems as an area of strategic importance.

Human resource management is an extremely complex business, but in the logistic centers it is essential to investigate whether the introduction of certain innovations in the domain of information technology is cost-effective. It is very important that every company analyzes how each component can contribute to its development and take a competitive position in the market.

REFERENCES

[1] Alam, S. S., & Noor, M. K. M. (2009). ICT adoption in small and medium enterprises: an empirical evidence of service sectors in Malaysia. International Journal of Business and Management, 4(2), 112–125.

[2] Alfes, K., Shantz, A., & Truss, C. (2012). The link between perceived HRM practices, performance and well-being: the moderating effect of trust in the employer. Human Resource Management Journal, 22(4), 409-427. doi: 10.1111/1748-8583.12005

[3] Barac, N., Milovanović, G., (2003), Menadžment poslovne logistike, Ekonomski fakultet Niš,

[4] Bowersox, D.J. and Daugherty, P.J. (1995), "Logistics paradigms: the impact of information technology", Journal of Business Logistics, Vol. 16 No. 1, pp. 65-80.

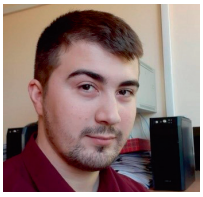
[5] Bowersox, D.J., Closs, D.J. and Stank, T.P. (1999), "21st century logistics: making supply chain integration a reality", Supply Chain Management Review, Vol. 3 No. 3, pp. 17-28.
[6] Bradford M. (2015): „Modern ERP, Select, Implement & use today`s advanced business systems, Raleigh, NC, Copyright 2015, 200
[7] Bradford M. (2015): „Modern ERP, Select, Implement & use today`s advanced business systems, Raleigh, NC, Copyright 2015, 204.
[8] Christopher, Martin L. (1992), Logistics and Supply Chain Management, London: Pitman Publishing.
[9] Hall, B. H., Lotti, F., & Mairesse, J. (2013). Evidence on the impact of R&D and ICT investments on innovation and productivity in Italian firms. Economics of Innovation and New Technology, 22(3), 300–328. http://dx.doi.org/10.1080/10438599.2012.708134
[10] Koh, C.E. and Nam, K. (2005), "Business use of the internet: a longitudinal study from a value chain perspective", Industrial Management & Data Systems, Vol. 105 No. 1, pp. 82-95.
[11] Lai, F., Zhao, X. and Wang, Q. (2006), "Taxonomy of information technology (IT) strategy and its impact on the performance of 3PLs in China", International Journal of Production Research (in press).
[12] Lajšić, H., (2017) Komparativna analiza HRIS i ERP modula u podršci upravljanju ljudskim resursima. Financing. 2017, Vol. 7 ISSUE 3, P45-53. 8P.
[13] Meade, L., & Sarkis, J. (1998). Strategic analysis of logistics and supply chain management systems using the analytical network process1. Transportation Research Part E: Logistics and Transportation Review, 34(3), 201-215.
[14] Mistry, J.J. (2006), "Differential impacts of information technology on cost and revenue driver relationships in banking", Industrial Management & Data Systems, Vol. 106 No. 3, pp. 327-44
[15] Porter, Michael (1985), Competitive Advantage, New York: The Free Press
[16] Tan, K. C., Kannan, V. R., Handfield, R. B., & Ghosh, S. (1999). Supply chain management: an empirical study of its impact on performance. International journal of operations & production Management, 19(10), 1034-1052.
[17] Vasiljević, M (2015). Logistika u saobraćaju, Univerzitet u Istočnom Sarajevu, Saobraćajni fakultet Doboj,
[18] Vehovar, V., & Lesjak, D. (2007). Characteristics and impacts of ICT investments: perceptions among managers. Industrial Management & Data Systems, 107(4), p. 537–550. http://dx.doi.org/10.1108/02635570710740689

Submitted: May 31, 2019
Accepted: June 07, 2019

About the authors

Nataša Đalić is employed at the University of East Sarajevo as a teaching assistant. He finished her Master's degree in 2010 and graduated as an engineer of informatics - master. He is currently a student of the third cycle, doctoral studies at the University of Novi Sad, Technical Faculty "Mihalo Pupin" Zrenjanin. Research fields are: information technology, management information systems, leadership, competitiveness.

Edit Terek is an assistant professor at department of Management, University of Novi Sad, Technical Faculty "Mihajlo Pupin", Zrenjanin, Serbia. She graduated at the Technical faculty "Mihajlo Pupin" in Zrenjanin (University of Novi Sad) in 2008. She defended her PhD thesis entitled: "*The impact of media relations on certain organizational and business performances in companies in Serbia*", in 2017 at the Department of Engineering management at University of Novi Sad. Her basic fields of interest are public relations and organizational behavior. She published more than 80 papers from which 10 papers in journals with impact factors.



Mihalj Bakator has M.Sc. degree in engineering management at the University of Novi Sad, Technical faculty "Mihajlo Pupin", in Zrenjanin, Republic of Serbia. Currently, he is a Research Associate and Ph.D. student of engineering management at the University of Novi Sad, Technical faculty "Mihajlo Pupin" Zrenjanin. Areas of research interest are: marketing management, quality management, entrepreneurship, consumer behaviour and competitiveness.

Mina Paunović is Ph.D. student at University of Novi Sad, Technical faculty "Mihajlo Pupin" in Zrenjanin, Serbia. (department of Management). After finishing FMK and DTM, she finised Master on Faculty of organisation sciences-department marketing. Since 2015. she works as assistent in The College textile – design, technology and managment –DTM, Serbia.

For citation

Đalić N., Terek E., Paunović M., Bakator M., The Importance of Information Technologies in Managing Human Potentials of the Logistic Centers of the Republic of Srpska, *JITA – Journal of Information Technology and Applications Banja Luka,* PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:36-45, (UDC: 005.96(497.6):[659.23:004.738.5), (DOI: 10.7251/JIT1901036DJ), Volume 9, Number 1, Banja Luka, june 2019 (1-48), 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, fax 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 (50 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 spacing. 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

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

Book

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

Contributed volume

Huberman AM and Miles MB (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

Huberman AM and Miles MB (1994) Data Management and analysis methods. In Handbook of Qualitative Research (Denzin NK and Linkoln YS, Eds), pp 428-444, Sage, Thousand Oaks, California.

Unpublished reports/theses

Nandhakumar JJ (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.apeiron-journals.com/JITA/authors/rights_and_permissions.html** to see our latest copyright policy.

Copyright and permissions

The copyright of all material published in the Journal is held by Paneuropean 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.

For citation

Bestemyanov Petr Filimonovich, Evaluation of the period of sensors motion parameters of the train, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 8(2018) 1:14-17, (UDC: 656.08:352.07), (DOI: 10.7251/ JIT1801014B), Volume 8, Number 1, Banja Luka, june 2018 (1-44), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004

About the authors - Biographies

Authors should submit their short biographies up to 100 words at the end of their work and, possibly, an picture.

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:

Paneuropean University APEIRON
Journal JITA
Pere Krece 13, P.O.Box 51
78102 Banja Luka
Bosnia 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,
College of Information Technology
Banja Luka, Republic of Srpska, B&H
www.apeiron-uni.eu
Darko Uremović, Person Responsible for the Publisher
Aleksandra Vidović, Editor of University Publications

ISSN 2232-9625
9 772232 962005