ICT AND MANAGEMENT 754

ICT AND MANAGEMENT

COMPARATIVE ANALYSIS OF SCRUM AND KANBAN METHODOLOGIES FOR MANAGING INFORMATION SYSTEMS DEVELOPMENT

Ognjen Pantelić*[1], Vedrana Gajić[1], Ana Pajić[1]
[1]Faculty of Organizational Sciences, University of Belgrade
* Corresponding author, e-mail: pantelic.ognjen@fon.bg.ac.rs

Abstract: *Understanding of customer demands was always the weakest point in information systems development. Due to the inadequat understanding and defining business demands, numerous projects end up not being successfully finished. Being aware that client demands are changing, many companies decide to use agile methodologies which generally contribute to faster and more efficient information systems development. However, there are many tools and methodologies which are considered to be agile. Companies decide to use two or more methodologies for managing projects of information systems development, in order to use their advantages and adjust them to their business model. The goal of this paper is comparative analysis of Scrum and Kanban methodologies, as well as their tools, with the idea to integrate these two methodologies in order to use their best practices. The analysis shown in this paper is used for developing software tool called „ScrumbanTool", which presentation is going beyond this paper.*

Keywords*: agile methodologies, scrum, kanban, information systems development, project management*

1. INTRODUCTION

Information systems development consists of all activities related to analysis, design, development, and deployment. Considering the fact that technologies change with time, organisations need new systems or significant changes in the old ones, in order to fulfil their goals. This points out the fact that the information systems development is complex and continuous process.

Throughout software development, different methodologies developed that help information systems development. Numerous factors influence the choice of methodology, one of them being the support of methodology in managing the project of the information systems development. Project management is not only significant scientific discipline needed in every organization, but is also considered to be necessary for the survival of any company. Due to the changes in client's demands, many companies decide to use agile development methodologies which enable better focus on client's problems, shorter time for project realisation and faster and easier adjustment to changeable environment (Moniruzzaman & Hossain, 2013).

It is not so rare the companies decide to combine two or more methods for project managment, in order to use these methods in the best possible way and adjust them to their business model. With the development of agile methodologies, numerous software tools that enable easy survey of project and it's managing, are also developed. The goal of this paper is comparative analysis of Scrum and Kanban agile methodologies.

2. AGILE SOFTWARE DEVELOPMENT METHODOLOGIES

In the late 1990-ies, a group of designers (Ken Beck, Alstair Cockburn and others, founded Agile Alliance) was the creator of agile approach in the information systems development. Supporters of agile software development methodologies bring in 2001 Agile Software Development Manifesto trying to emphasize the role the flexibility could have in more skilled and faster development of software product (Padavić, Velić, & Ljubobratović, 2011).

According to the Agile Manifesto (Fowler & Highsmith, 2001), some of the principles of agile methodologies are:

- The highest priority is to satisfy customer through early and continuous product delivery
- The change in demands is normal, even in the late project phases
- Software product that works, is delivered every few weeks or months
- The team periodically tests good and bad procedures, and tries to repair them for the next period

The principles represent conceptual framework which should be used during development of software product. Agile methodologies are subset of iterative and evolutional methods, and are based on iterative enhancement, while iterations (repetitions) are short in order to give correct information to project team.

Understanding of customer demands has always been the weakest point in the information systems development. Due to inadequate understanding and defining of business demands, some software development projects failed to fulfill customer expectations. Management of demands consists of activities which are dealing with detecting demands, following and controlling of versions and changes in demands. The change in demand is every change of the existing demand or new demand that can influence the existing demands.

Demand changes happen due to the changes in business environment or customer needs. Defining demands, according to the traditional methodologies, goes through phases of analysis, documentation and check. For many organizations, this is a process of few weeks or even months. Unlike traditional, agile practice deals with smaller parts of demands, which are developed and tested during one sprint (iteration) and, in the end, being presented to final customer, for demand validation. Identifying and development of agile demands is done during agile planning, development and delivery (Milanov & Njegus, 2012):

- Agile planning. Agile teams develop demands according to their business values, i.e.: profit increase, cost decrease, service improvement, harmonizing legislation, accomplishing market goals etc. Agility means focusing on the actual values and discarding everything that is not of great importance. Planning covers not only „current view“ (current iteration), but as well the review of the solutions and „big view“(the vision and the map of product development). Product owners are doing agile planning, by constantly reconsidering demand priorities and by validating risks and dependencies.
- Agile development. Agile development team estimates, develops, tests and demonstrates demands to final users. Before the beginning of Sprint, development team sketches data model, condition diagrams or interfaces, which also represents mini specification of the solution.
- Agile delivery. Demands are often dependent on one another. Agile teams analyze and optimize dependencies of the demands.

Predetermined length of the iteration is used as a time frame for the development team. According to the length of the iteration, the scope of the problems to be solved is being determined. The main difference between agile and iterative methodologies is the length of a single iteration. While the length of the iteration for iterative methodologies is three to six months, with agile approach the interval decreased to one to four weeks, and the most 30 days.

Some methodologies for information system product development based on agile principles are (Abrahamsson, Warsta, Siponen, Ronkainen, & Ronkanen, 2003), (Hiranabe, 2007):

- eXtreme Programming – XP
- Scrum
- Feature Driven Development – FDD
- Crystal family of methodologies
- Dynamic Systems Development Method – DSDM
- Adaptive Software Development – ASD
- Kanban

2.1. Scrum development methodology

The term „scrum“ originates from rugby and represents „throwing the ball back into the game“. This methodology is fast, adaptable and more and more popular among IT companies.

Initially, this agile methodology was developed as a set of management recommendations and suggestions for managing the information systems development project. Project development with Scrum methodology is done iteratively, and iteration is called Sprint. Sprint has to be predetermined and is recommended to last between two and four weeks (Pichler, 2010). After one Sprint, one draft version is ready for delivery, while the whole project can be done through three to eight sprints.

According to Scrum, complete system development is divided into three groups of activities: pregame, game and post-game (Gorakavi, 2009). Through pregame, demands and development priorities are being defined, and value of newly built increments is being estimated. Throughout the game, the development and functionality implementation are done iteratively, and in post-game period, testing and integration (Figure 1).

Scrum tools are making processes and activities of this methodology much easier. Many vendors are offering their versions of tools for project management that support Scrum, and some of them are with open code. Some of Scrum tools are: Agile Tracking Tool, Scrumwise, ScrumDo, Scrumy, Agilito, Agilo for Scrum, PangoScrum, Scrumpad, Rally Dev, Jira etc.

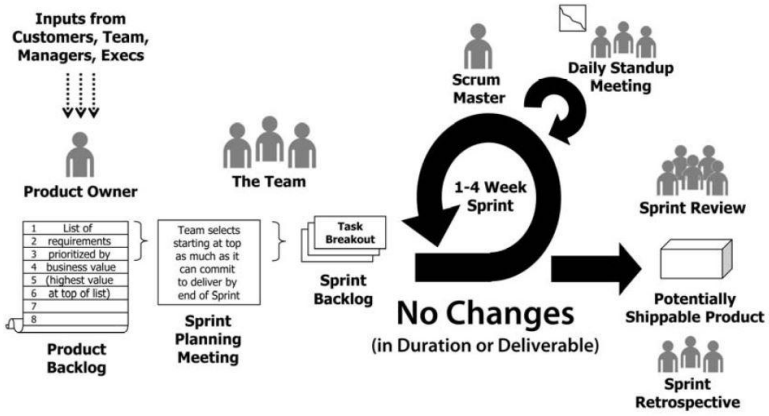


Figure 1: Scrum methodology through phases (Deemer & Benefield, 2010)

Jira is one of the best known Scrum tools. It is the product of Atlassian, and is used for project management. It is written in Java program language, and it also has its free version for projects with the open code (Atlassian, 2005). It is often used with systems for version control, such as SVNili Mercurial, and with Bamboo build server. The system enables communication within development team, as well as with a buyer or owner.

With very intuitive control board, it is possible to:
- Create, set projects
- Set schemes and workflow
- Work with tasks, as a main project unit
- Track task length and status
- Give priority and person in charge for every task
- Sort backlog etc.

2.2. Kanban development methodology

Kanban agile methodology of information systems development is following Lean software development. The term „lean“ represents the motive to spend less amount of time, less human effort, less investment, less effort and less finances during development.

Kanban spread through production industry in the world, as the tool for Lean Manufacturing, and in agile information systems development, it is the way of project visualization by placing cards with assignments on the board, by which just in time – JIT development strategy is achieved (Wagener, Schmit, Mandal, & Vaishnavi, 2012). In Japanese vocabulary „kan“ means „signal“ while „ban“ means „card“ or „board“.

Lean Kanban strategy is generally more focused on job being finished in time, instead of being focused on who did it. People work together, but they do not work with the same speed, they do not have the same knowledge and skills, so they have to synchronize (Anderson, 2010). In Kanban, the work is organized by tasks or processes, and allows team members to change on their own the workflow in the most productive way.

The rules of Kanban do not consider important demands that are not needed at the moment by anyone, do not write more specifications than can be programmed, codes are written in the amount that can be tested, and according to that, only what can be released is tested (Anderson, 2010). Kanban system in engineering is done in a way that all demands which are waiting in line are passing through few phases, until they are finished. When demand is in a phase „Finished“ than it goes to the next phase.

The advantages of Kanban, compared to traditional „push“ systems, are (Topić, 2012):
- Simple and understandable process
- Gives fast and precise information

- Low costs of transferring information
- Possible fast reply to changes
- Limited capacity in process
- Avoids hyper production
- Minimizes waist
- Easier control maintaining

Main Kanban principles which are continuously followed by the team are: visual control (Kanban board), Limit Work in Process – WIP, card pull, fix Kanban backlog. The usage of colored cards and their availability for different types of work, can enable development team too quickly:
- See what is currently being worked on (the cards give value to a certain job)
- Easily see blocker tasks
- Estimate how good was the analysis
- Do easy tracking (how many tasks exceeded time limit etc.)

If there is emergency case concerning support demands or mistake in software product (software bug) during production, than an empty space in Kanban board is used, under the name „Urgent". The tasks that are solved in this way are not being put into backlog, but the aim is to solve them as quickly as possible.

The advantage of Kanban board is visibility of the following (Hiranabe, 2008):
- The work of individual
- Is the individual overloaded with work
- Where is bottleneck
- Where problems in work occur
- What is being blocked

Some of the well-known web-based Kanban tools are: Lean Kit Kanban, Kanboard, Axosoft, Kanbanery, AgileZen, Flow, FogBugz Kanban, GreenHopper, Hansoft, LeanKit Kanban, Lino, Qanban, SilverCatalyst and others.

3. COMPARATIVE ANALYSIS OF SCRUM AND KANBAN METHODOLOGIES

- Comparison by the number of rules

These two methodologies can be compared by the number of rules they possess. If a certain methodology has more obligatory rules, that methodology is called prescriptive methodology. On the other hand, if methodology does not possess any rule, it is called adaptive methodology. Completely prescriptive methodology gives all the guidelines and rules, so everything organization needs to do is follow the rules, without any other efforts during project management, while completely adaptive methodology leaves everything to organization without any rule. Both extremes are very risky (Kniberg & Skarin, 2010).

Agile methodologies are generally referred to as light weight methodologies, because they are less prescriptive from traditional methodologies. Both Scrum and Kanban methodology are very adaptive, but compared to one another, Scrum is more prescriptive. Scrum possesses more limits and therefore has fewer options. For example, Scrum expects usage of time-limited iterations (sprints), while Kanban does not.

- Comparison by roles

There are three different types of roles in Scrum: Product owner, Development team and Scrum leader. There are no different roles for different members of team, in other words, there are no specific roles. This does not mean that the team organised around the project should not have its owner, but rather that it is not necessary.

On the other hand, both Scrum and Kanban are open to adding any other type of role if necessary. But there has to be precaution, in order to add new value to the product by adding new role, and not only conflicts with other elements of the process. Companies often add Project Manager to the team, who synchronises teams and product owner. However, since the global motto of both methodologies is „less is more", if organisation is having a dilemma, the recommendation is to start with less number of roles in a team.

- Comparison by meetings

Scrum team is having a short meeting every day at the same time and place. The goal of these daily meetings is to exchange information about development, plans for the next day and to point out any major problem if there is any.

Kanban does not imply daily meetings, but nevertheless most of Kanban teams have this habit. It is a great technique for any methodology.

Scrum form of meetings is mainly about people, since every person gives a report, one after another. Kanban teams use more Kanban board, and are focused on the problems that are visible on the board. The problem of this way occurs when many teams use the same board and have daily meeting together, because it is not always necessary to listen to other team's problems (Kniberg & Skarin, 2010).

- Comparison by time planning

Scrum is based on time-limited iterations. The team itself determines the length of iteration, but it is important that iteration always has the same length through the complete project development, or at least, one long period of time.

At the beginning of each iteration a plan is being formed, team plans certain and definite number of orders from backlog, based on the priorities of product owner. During iteration, team is focused on finishing orders that had been planned at the beginning of the iteration, while at the end of the iteration the team presents potentially finished product to stakeholders and gives a retrospective/discussion in order to improve complete process.

One Scrum iteration is time-limited sequence which combines three different activities (Kniberg & Skarin, 2010):

- Planning
- Continuous process improvement (retrospective)
- Releasing the product of iteration into production

When using Kanban methodology, the iterations are not predetermined. The team can decide at any moment when to plan, improve the process or release application into production. It can decide on one of the basic tactics, such as releasing application into production on Mondays, or when client demands, or i.e. only when application undergone significant changes or improvements (whenever something useful can be released).

- Comparison by boards (Scrum and Kanban board)

In Scrum, backlog of iteration shows everything that should be done during current iteration. This information is often shown by using cards on the wall, which is called Scrum or Task board.

Both Kanban and Scrum board follows numerous demands as an improvement or workflow. Let us say that both boards have three columns that represent condition of demands: To do, Ongoing, Done. Both methodologies do not limit teams concerning in which condition can demands be put in, so they can choose conditions that are more suitable for their process.

The difference between these two charts is that Kanban limits the number of orders per column. For example, in the column „Ongoing", there can be only 3 requests at the same time. Scrum does not have the rule that as prevention limits the team to put many requests at the same time in one column. On the other hand, Scrum limits the number of orders in the chart, because at the beginning of each iteration, the number of orders is being defined. Therefore both methodologies are limiting requests but in a different way.

Considering the fact that Scrum methodology functions with fixed number of requests within iteration, if a client wants to add a request in „To do" column, it would not be possible. If the team uses Kanban methodology, the request would be accepted only if the capacity of the column is not already full. Otherwise, the previous requests from that column would have to be finished first. Of course, none of these two approaches is exclusive. Scrum team can, as well, decide to allow product owner to change priorities in the middle of sprint, but it is considered an exception.

Another difference is that Scrum board is reset after each iteration, in other words, it is deleted after every sprint. New iteration starts after planning where the team will work, on a completely new Scrum board with new requests. In Kanban, the chart is mainly persistent, and there is no need for reset.

- Comparison by teams

Scrum team is functional team which consists of members who have necessary knowledge to solve any request in iteration (Figure 2). In Kanban, a team like that is only an option. It is important that requests can be fulfilled, but it is not important that every team member can solve every request (Figure 3).

Agile methodologies generally contribute to faster and more efficient information systems development. However, there are many tools and methodologies that are considered agile. That is why the choice of methodology that will be used is very important, and it should be taken into consideration if the methodology can be applied to all projects within organization.

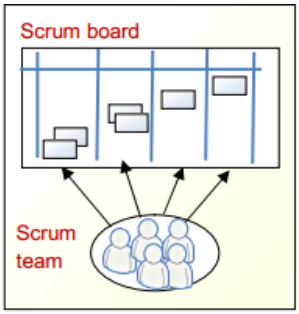


Figure 2: Necessary knowledge of Scrum development team (Kniberg & Skarin, 2010)

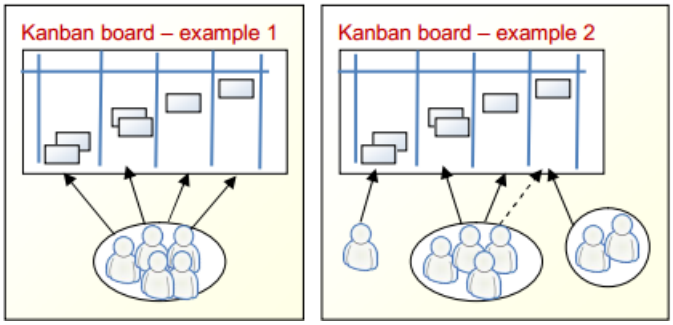


Figure 3: Kanban development team (Kniberg & Skarin, 2010)

Based on the comparison, it can be concluded that there is high number of advantages while using any of these two methodologies. Both methodologies are highly used and popular in the world and in IT companies in Serbia. Summarized overview of the most important differences in Scrum and Kanban approach is shown in Table 1.

Table 1: Differences in Scrum and Kanban methodology

Scrum	**Kanban**
Iterations are time limited	Time limited iterations are only an option
Uses speed and velocity measuring as metric	Uses lead time as metric
Team members have to be functional between themselves	Team members can be experts for only one necessary field of work
Time estimations are necessary	Time estimations are not determined
Forbids adding new requests if iteration is in progress	Enables adding new requests as long as capacity allows
Defines three types of roles	There are no predefined roles for team members
Scrum board is being reset after every iteration	Kanban board is persistent

Organizations have as well the possibility of combining these two methodologies. Teams can use those recommendations which are more suitable and helpful, making combination of Scrum and Kanban. Many Scrum teams decide to limit waiting lines, which is recommended by Kanban methodology. On the other hand, many Kanban users have daily meetings, like every Scrum team does.

4. CONCLUSION

Agile methodologies emphasize the importance of flexibility in more efficient information systems development. Product is being adjusted to the changes in user's requests, during development process itself. Changes in requests are normal and they happen after changes in business environment or user needs. Therefore the user is being more involved in product development process, after each iteration when smaller part of complete implemented requests is being validated.

This paper presented Scrum and Kanban methodologies for managing information system development, which are widely accepted and being used today. Lean Kanban strategy is more focused to have the job

finished in time, while there are no time limited iterations. By using special way of visualization, Kanban board, the project is being observed and focus is put on the problems on the board. Therefore this methodology does not imply characteristics of teams and daily meetings, unlike Scrum method. Scrum method is more rigorous and requests daily reports from every team member. It functions with fixed number of requests during iteration, which disables client to add any new request during the iteration. This situation can be overcome by Kanban method, so new request could potentially be accepted if there is enough capacity.

Based on the comparative analysis of Scrum and Kanban methodologies, as well as their tools, it can be concluded that these two methodologies can be used together successfully, by using only the best recommendations from both. Teams can use those recommendations that are suitable and helpful, by making a mixture of Scrum and Kanban methodology. Many Scrum teams decide for work in progress (WIP limit), which is Kanban recommendation. On the other hand, many Kanban users organize daily meetings like every Scrum team. It should be mentioned that a new software tool that gives the opportunity to combine Scrum and Kanban methodology by the name „ScrumbanTool“, has been developed.

REFERENCES

Abrahamsson, P., Warsta, J., Siponen, M. T. M. T., Ronkainen, J., & Ronkanen, J. (2003). New Directions on Agile Methods: A Comparative Analysis. In *Proceedings of the International Conference on Software Engineering* (pp. 244–254). Portland, Oregon, USA. doi:10.1109/ICSE.2003.1201204

Anderson, D. J. (2010). *Kanban: Successful Evolutionary Change for Your Technology Business*. United States of America: Blue Hole Press.

Atlassian. (2005). JIRA User ' s Guide. Retrieved from http://apply07.grants.gov/apply/opportunities/instructions/oppMARWAN-020610-cfda00.000-cidMARWAN-020610-instructions.pdf

Deemer, P., & Benefield, G. (2010). *The scrum primer (An Introduction to Agile Project Management with Scrum)*. *Goodagile-Scrum Training in India and Asia, (1.04)*. Retrieved from http://www.rallydev.com/documents/scrumprimer.pdf\nwww.goodagile.com

Fowler, M., & Highsmith, J. (2001). The Agile Manifesto. *Software Development*, *9*, 28–35. doi:10.1177/004057368303900411

Gorakavi, P. K. (2009). Build Your Project Using Scrum Methodology. *IPMA USA*, pp. 1–5. Retrieved from http://www.ipma-usa.org/articles/A3_AboutScrum.pdf

Hiranabe, K. (2007). Visualizing Agile Projects using Kanban Boards. Retrieved from http://www.infoq.com/articles/agile-kanban-boards

Hiranabe, K. (2008). Kanban Applied to Software Development: from Agile to Lean. Retrieved from http://www.infoq.com/articles/hiranabe-lean-agile-kanban

Kniberg, H., & Skarin, M. (2010). *Kanban and Scrum-making the most of both* (Vol. 1). United States of America: C4Media Inc., Publisher of InfoQ Enterprise Software Development.

Milanov, G., & Njegus, A. (2012). Upravljanje izmenama zahteva u skladu sa modifikovanim Scrum procesom. In *Proceedings of Telecommunications Forum (TELFOR), 2012 20th*, 1685–1688. Belgrade.

Moniruzzaman, A. B. M., & Hossain, D. S. A. (2013). Comparative Study on Agile software development methodologies. *Global Journal of Computer Science and Technology*, *13*(17), 1–25.

Padavić, I., Velić, M., & Ljubobratović, D. (2011). Agilni razvoj programskih proizvoda agile software development. In *Proceedings of Infoteh- Jahorina Conference* Vol. 10, 466–470.

Pichler, R. (2010). *Agile Product Management with Scrum: Creating Products that Customers Love*. *AddisonWesley Professional*. United States of America. doi:10.1111/j.1540-5885.2011.00829_2.x

Topić, A. (2012). *Utjecaj Kanban agilne metodologije na razvoj programskog proizvoda*. Faculty of Electrical Engineering, University of Split.

Wagener, J., Schmit, S., Mandal, A., & Vaishnavi, R. (2012). *Project Management Using Kanban*. Retrieved from http://www.pmi.lu/event/120201-Using.pdf

APPLICATION OF MULTIMODAL BIOMETRICS IN ACCESS CONTROL SYSTEMS

Ivan Milenković, Ksenija Ţivković, Dejan Simić
Faculty of organizational sciences

***Abstract**: Access control systems are part of our everyday reality. The choice of an authentication method has a significant impact on an access control system. Topic of this paper is possible application of multimodal biometrics in access control systems. Relevant papers and solutions are analyzed, and a review of different aspects of multimodal systems is given. Analysis results show that multimodal biometric systems have some significant advantages over unimodal biometric systems and other authentication methods. However, use of multimodal biometrics as authentication method may result in increased cost and lesser system usability.*

***Keywords**: multimodal biometrics, access control, performance evaluation*

1. INTRODUCTION

Increased risk of attacks such as identity theft has raised the importance of properly implemented systems for identity and access management. Identity and access management refers to an integrated system of business processes, policies and technologies which enables organizations to simplify and control user access to online applications and resources, while protecting confidential information from different types of attack (Bogićević, Milenković and Simić, 2014).

An identity and access management process has three interdependent main activities (Milenković, Šošević and Simić, 2012) - user identification, authentication and authorization. Process of claiming user identity is called identification, while the act of verifying claimed identity is defined as authentication. Authorization is the process of asserting user rights to access some resources, such as data, computer devices or offices.

Main goal of access control is controlling the activity of the system users. According to Sandhu and Samarati (1994), access control assumes that user has been successfully verified before enforcement of access control policies. Therefore, the effectiveness of the access control systems depends on reliable authentication of its users.

There are three main types of authentication methods today. First and the most common is the use of passwords. Password is something that system user knows. However, this knowledge can be easily shared with other people, or as easily forgotten. Also, people may choose passwords of insufficient security. Some of those security problems can be solved by the use of tokens. Token is something that system user possesses. Potential danger is that tokens can be stolen and system security compromised. Third type of authentication, biometrics, tries to overcome shortcoming of other authentication methods. Biometrics uses physiological or behavioral traits of a person for authentication, something that user is.

Biometrics relies on statistical or machine learning algorithms, and algorithm output is not a definite yes/no, but a score or probability (Šošević, Milenković, Milovanović and Minović, 2013). Therefore, biometric systems can make errors. One approach to making biometric systems more precise and robust is the use of multimodal biometrics. Multimodal biometrics relies on combination of several different biometric modalities. Different combinations are possible, such as face and voice, fingerprint and iris, face, ear and palmprint.

In order to secure an access control system, it is necessary to have a secure authentication procedure. In chapter 1, introduction to biometrics and access control was given. Topic of chapter 2 is performance evaluation of biometric systems. In chapter 3 different information fusion algorithms are described, and estimates of their precision are given. Chapter 4 is concerned with security of biometric systems. In chapter

5, different applications of multimodal biometric in access control are reviewed. Conclusions and guidelines for multimodal biometrics use in access control are given in chapter 6.

2. PERFORMANCE EVALUATION

According to Phillips, Martin, Wilson and Przybocki (2000), there are three different approaches for biometric system evaluation: technology evaluation, scenario evaluation and operational evaluation. The most general type of evaluation is technology evaluation.

Technology evaluation is used to determine performance of biometric algorithms. It involves the use of the standardized database for testing purposes. Performances of different algorithms can be compared on a common set of data. All the algorithms use the data gathered by the same type of acquisition devices. Only part of a database is given to algorithm developers, and the rest of the data is used for final evaluation. An example of technological evaluation is the FERET(face recognition technology) evaluation conducted by NIST.

Open-access multimodal biometric databases suitable for technology evaluation are few. Also, they tend to have biometric data collected from a small number of individuals. Therefore, researchers who want to test multimodal algorithm have to use chimeric datasets (Poh and Bengio, 2006). For fusion algorithms that work on the match score level, there is a possible alternative in using a NIST database with face and fingerprint match scores.

Numerous published papers confirm that multimodal biometrics improve system performance. Researchers have tested their algorithms on different sets of data, because of a lack of suitable multimodal database. Sim, Asmuni, Hassan and Othman (2014) have developed a multimodal system which uses biometric modalities of iris and face. For testing, they have created their own UTMIFM dataset (Universiti Teknologi Malaysia Iris 188 and Face Multimodal Datasets). For comparison, they have also used ORL database (Samaria and Harter, 1994) for face images, and UBIRIS v.2 iris dataset (Proenca and Alexandre, 2005).

Scenario evaluations are used to determine system performance in a specific domain of application. In a scenario evaluation, we would determine if a face recognition system can be used for access control at an airport. Biometric system is being tested as whole, and both algorithms and acquisition sensors are being tested. Testers should be chosen from population of real-world biometric system users. For example, in security applications, subject may be unwilling to cooperate with the system, which is a very important distinction. System environment, such as noise or lightning should match real world scenario as close as possible. Also, data enrolment must be done under same general conditions. Results of the scenario evaluation are partly repeatable, in according to the extent of the scenario that can be controlled.

Operational evaluations are used to determine system performance for a specific application. Example for operational evaluation would be testing a face recognition system for access control on Belgrade “Nikola Tesla” airport. There is little control over testing procedure, as subject should use the system in standard way. Evaluation results are not repeatable, because each specific application environment has specific characteristics which are hard to document.

3. MULTIMODAL BIOMETRICS - ALGORITHMS AND SYSTEM PRECISION

Multimodal biometric systems integrate information gathered from different biometric modalities. Different combinations are possible, such as fingerprint and face, voice, face and ear, iris and fingerprint. To integrate information gathered from different modalities, the use of information fusion algorithm is necessary. Choice of the fusion algorithm can have a significant impact on the system precision and performance. A classification of information fusion methods is shown on picture 1.

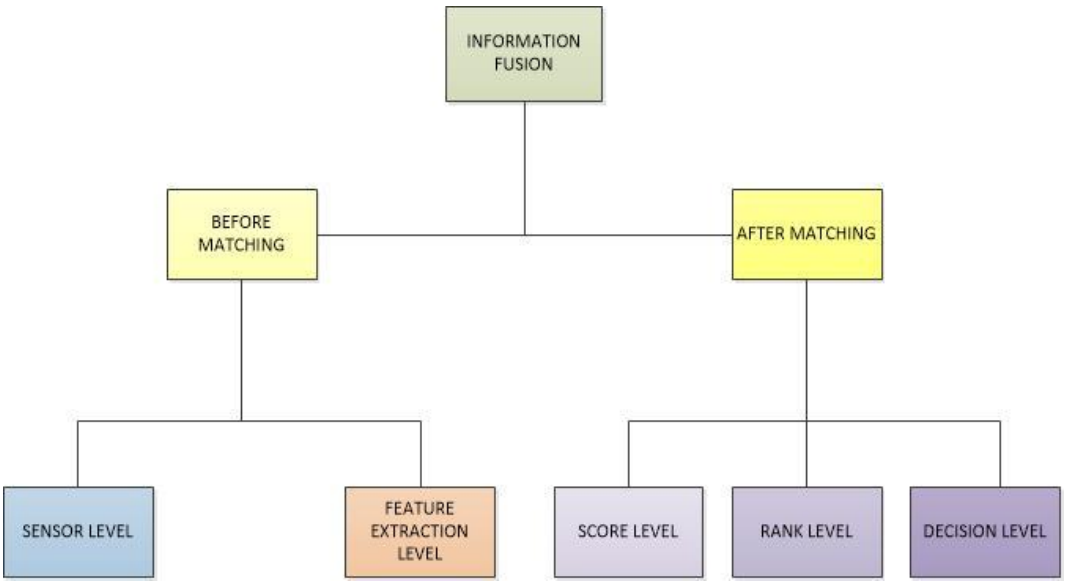


Figure 1: Different levels of information fusion in multimodal biometrics

3.1 Sensor level fusion

Data gathered from several types of sensors is integrated into single entity. At this level it is possible to fuse data from just a single biometric modality, so these methods are more likely to be considered multibiometrics than multimodal biometrics. It is important for consideration because this kind of fusion can improve system inputs.

3.2 Fusion at feature extraction level

Combining biometric characteristics extracted from several biometric modalities into a single biometric characteristic is considered as fusion at feature extraction level. Fusion methods defer from simple vector concatenation to more complex fusion methods.

Saini and Sinha (2014) describe a multimodal biometric system based on Gabor-Wigner transform. GWT is used for extraction of feature vectors. Biometric modalities used are face and palmprint, and test database had 150 subjects. Authors compare system performance with information fusion on different levels. When information fusion was employed at feature extraction level, best system EER was 3,36%. Information fusion at match score level yielded 1,89% EER.

3.3 Match score level fusion

In case of score level fusion, separate biometric characteristics are generated for each biometric modality. Each of the characteristics is matched with according template in the biometric database. The result of the matching is matching score. The greater the similarity between matched templates, the match score has the higher value. Generated match scores are used to generate new, derived match score, or are directly used to make a decision. Most of the published papers use this fusion method.

One of the first large scale evaluation of multimodal biometric system was performed by Snelick et. all (Snelik, Kisku, Bicego and Tistarelli, 2007). Prior evaluations where based on non commercial software, and smaller databases. Tests were conducted on a database of 972 system users. Fingerprint and face were used as biometric modalities. Fusion was performed on matching score level. Different combinations of score normalization and fusion techniques were applied. User weighted fusion and adaptive normalization where the most precise combination with EER of 0.63%.

Sim, Asmuni, Hassan and Othman (2014) have developed a multimodal system which uses biometric modalities of iris and face. Paper focus was toward non-ideal images, such as off-angles, reflections,

expression changes or blurred images. Information fusion is performed on score level, and matching scores weights are customized for each system user. For testing, authors have created their own UTMIFM dataset (Universiti Teknologi Malaysia Iris 188 and Face Multimodal Datasets). For comparison, they have also used ORL database for face images, and UBIRIS v.2 iris dataset. Results for multimodal approach show GAR of 95% when FAR is 0.01%, while at same FAR iris and face perform at 94% and 83% percent, respectively.

Table 1: Comparison of different fusion methods

Paper	Published	Biometric modalities	Level of fusion	Number of identities in test dataset	Unimodal systems EER	Multimodal system EER
Snelick, Uludag, Mink, Indovina and Jain, 2005	2005	fingerprint and face	Match score level	972	2.16% 3.96%	0.63%
Vatsa, Singh and Noore, 2007	2007	iris and face	Match score level	300	2%, 2.3%	0.8%
Sim, Asmuni, Hassan and Othman, 2014	2014	iris and face	Match score level	300	~7%, ~3%	~2%
Saini and Sinha, 2014	2014	face and palmprint	Feature extraction level	150	5.77%, 11.67%	3.36%
Monwar and Gavrilova, 2009	2009	face, ear, signature	Rank level	30	~5.6%, ~7.5% ~5%	1.12%

3.4 Decision and rank level fusion

If a biometrical system functions in the identification mode, it is possible to use rank method fusion. Such system could produce an ordered list of identities as an output. The first candidate on the list is the one system determined a most likely match, followed by the other candidates ranked by their match probabilities.

Some commercial unimodal biometric system function as black box systems and their only output is final decision. Integrating such unimodal systems into a multimodal recognition system requires the use of decision level fusion. Decision level fusion applies different voting algorithms to calculate the final decision. Monwar and Gavrilova (2008) describe a biometric system with decision level information fusion. Applied algorithms are AND/OR, majority voting, weighted majority voting and behavioural knowledge space.

4. SYSTEM SECURITY AND PRIVACY CONCERNS

Although using biometrics as authentication technique may result in improving system security, it does not necessarily imply that the system is secure. To achieve this desired security, various system aspects, both technological and organizational should be taken into account. Applying traditional cryptographic algorithms to secure communication channels, using biometric cryptosystems to secure biometric templates are just some of the security measures needed to be taken.

Prabhakar, Pankanti and Jain (2003) noted that biometric usage also rises some privacy concerns. Finding the balance between privacy and the public interest is a serious challenge, which has technological and legal complexity. There are debates whether biometric data should or should not be considered a "private" or "sensitive" data, and there are strong arguments for and against. For example, a company may collect fingerprint or facial data of its employees for its access control system. Company employees may use these same biometric modalities in some other system that uses biometric authentication, such as a health care

system. However, if biometric data is not properly secured, company could theoretically use this biometric data to gather information about health issues of its employees.

Adversary attacks generally exploit the system vulnerabilities at one or more modules or interfaces. Figure 2 shows eight points of attack in a biometric system.

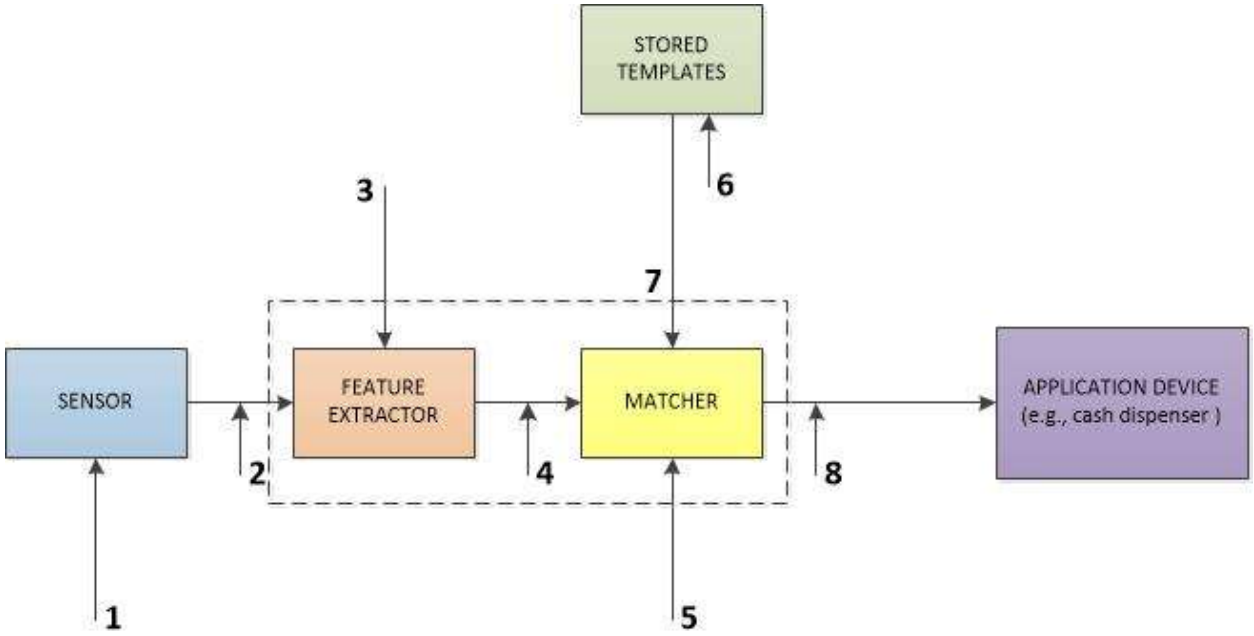


Figure 2: Points of attack in a biometric system (Ratha, Connel and Bolle, 2001)

1. Fake biometric submission at the sensor (fake finger, a copy of a signature, a face mask)
2. Resubmission of old digitally stored biometrics signal
3. Override feature extract (the feature extractor could be attacked with a Trojan horse)
4. Tampering with the feature representation (During the transmission of data between modules of extraction and corresponding modules, changing the desired set of functions)
5. Overriding matcher decision (Matcher also may be exposed to the Trojan horse)
6. Tampering with stored templates (The database of enrolled templates is available locally or remotely. The stored template attacker tries to modify one or more templates in the database)
7. Channel attack between stored templates and the matcher (attacks may change the contents of the templates before they reach the matcher)
8. Decision override (The final decision may be approved or not – YES/NO)

During the transmission of biometric data between acquisition sensor and feature extraction module there is a risk of eavesdropping. To prevent this attack, it is necessary to secure the communication channel. One approach is the use of smart cards, where the whole biometric system is integrated in such device. However, such solution is applicable only for certain scenarios of biometric verification. Some of the systems require external acquisition devices, or centralized biometric database.

A possible solution for this attack, and also other attacks which affect communication channels, is the use of cryptographic techniques. In smaller systems, where it is possible to exchange keys, symmetric cryptographic algorithms may be used. To prevent replay attacks, timestamps can be employed. In other, more complicated instances, it is necessary to protect the channel with some more complex solutions, like SSL/TLS protocol. Also, because biometric data is highly sensitive, multiple layers of protection (as used in financial transactions) should be applied.

5. APPLICATION OF MULTIMODAL BIOMETRICS IN ACCESS CONTROL

Many researchers studied multimodal biometrics in access control. Different applications of multimodal biometrics have been considered by the research community. Covered topics differ from more general, like securing access to a building or authentication for online systems, to more specific. Some of the more specific topics covered are car access control, application of multimodal biometric access control e-commerce systems access, and use of mobile devices.

Lupu (2011) proposed car access control using multimodal biometrics. System uses three biometric modalities - fingerprint, iris and voice recognition. Genuine system users are granted unlimited access to car controls. If an imposter would try to assume the car driver identity, he would be unable to drive the car. Also, the car would alarm security service or police using a GPRS system.

Maheswari et al. (2010) also used three biometric features, but instead fingerprint they used voice. Actually, they demonstrated an intelligent multimodal biometric verification system for physical access control using iris, face and fingerprint recognition. This system was created to show high security access control using multimodal biometrics. Another paper with building access control as the topic was published by Beattie et al. (2004). Paper describes a variation of sequential information fusion, based on so called path fusion algorithm. This new approach is designed for building with several authentication checkpoints. User motion through building is monitored and each system decision is influenced by previous authentications.

Common feature of the following papers is the use of hand geometry for access control. Ribaric et al. described an economical approach of multimodal biometrics in access control. They designed a prototype biometric identification system using hand-geometry, finger and palm-print. The system is based on a low-cost desktop scanner, which is used as the biometric acquisition device. Experimental analysis revealed that information fusion at the matching-score level enhances the results of the identification. Chike Obed-Emeribe (2013) stated that the palm geometry and the fingerprint are most suitable for verification. He presented implementation of multimodal biometrics as an access control tool for an e-commerce framework. Framework architecture consists of an e-commerce database server, a monitor server for transaction processing and a multimodal biometric database server.

Dehnavi and Fard (2011) proposed a multimodal biometric model for tracking students in virtual classes. Proposed model combines two behavioral biometric characteristics (mouse movements and keystroke dynamics) and a physical one (face features). This new approach allows continuous verification of student attendance. This is achieved by applying specially designed algorithm called ACT (Attendance Control Tracker). Student biometric data is continually sent to biometric server. Paper gives an architecture proposal of the described system. Testing was performed on Claroline open source LMS, and authors state that model is applicable for use with other LMS.

Trewin et al. (2012) tested usability of voice, face and gesture recognition as access control methods for mobile devices. For comparison 8-digit written and spoken PIN codes were used. Study did not take biometric system performance into account. However, because authentication causes interruption in the user's primary task flow, the impact of authentication methods on working memory was taken into account. Research results have shown that each modality has its own strengths and weaknesses. Voice was considered less usable than other modalities, because of the acquisition problems. Study participants also reported interference with the memory tasks. Combination of face and voice result in higher FTA (Failure to acquire) rate because acquisition process required more coordination.

Several commercial multimodal biometric access control systems are available on the market. One of the latest solutions in access control is Facebanx. It combines face recognition, voice recognition and document verification. For Facebanx users, first step of the registration process is adding personal data, followed by biometric data acquisition. Final enrollment step requires submitting some kind of personal ID. To prevent fraud data entered is compared to data on the identification document. Another available multimodal biometrics solution for access control is Vision-Box, the new application of biometrics for airline passengers. It is designed for automated border control at airports. It supports iris, fingerprint and facial recognition biometrics and can integrate with the advanced identity management infrastructure.

Another important area where multimodal biometrics is applied for access control are government systems, like voting or border control systems. For example, Kenya and Ghana have improved their voting systems by introducing automatic biometric recognition. Biometric modalities of fingerprint, iris and face are used for voter verification. Iris, palmprint, facial and vascular recognition are employed for voter verification. Governments of USA and Canada collect face and fingerprint data from visitors, students or temporary workers from certain countries.

6. CONCLUSION

Research papers available on the topic multimodal biometrics confirm that multimodal biometrics significantly improves system precision. However, it is difficult to compare different multimodal algorithms and approaches. Even in the case of the same combination of biometric modalities, unimodal systems and testing data often differ. Lack of multimodal databases with large number of subjects in the public domain leads to use of chimeric datasets gathered from various different sources. A framework for evaluating precision of multimodal biometric systems is still an open challenge.

Application of multimodal biometrics can remove some of the negative effects of biometric menagerie. This is achieved by applying user specific fusion, where poorly performing modalities are given lower priorities, or are not used for authentication. Therefore, the use of multimodal biometric leads to more precise and robust system.

Interoperability is still an open issue. Although there are several standards and projects, none are widely accepted for now. Some of the standards, like BioApi, depend on a specific programming language. Other, like WS-BD, target just one segment of biometric systems (acquisition). Integrating different unimodal components into a multimodal system could pose a serious challenge. However, this area is still in development.

Multimodal biometric systems share security threats of their unimodal counterparts. Some of the treats can be countered by applying standard security measures used in computer systems. However, securing biometric templates remains an open question, as all algorithms proposed so far negatively affect system precision. Multimodal biometrics can be useful here, because using several modalities improves system precision and counters some of the negative effects.

As a tool for access control, multimodal biometric systems are not yet widely accepted. There are some papers which speculate over potential use of multimodal biometrics for this purpose, however, they are not still very numerous. Although commercial multimodal biometric solutions are available on the market, they are not widely spread yet. Some governments, like USA and Canada gather several biometric modalities for border control, but resort to unimodal fingerprint recognition for most purposes.

After reviewing different aspects of multimodal biometrics, we can conclude that they have some important advantages over their unimodal counterparts, and against other authentication methods. However, when deciding whenever to apply multimodal, there are always other factors to be considered, such as implementation cost and usability. Generally, the technology is mature enough to applied, and we can expect its more widespread use in the near future.

REFERENCES

Beattie, M. et al (2004). *Building* access control using coordinated biometric verification. In *Biometrics:Challenges arising from Theory to Practice (BCTP) Workshop Proceedings*, Cambridge, UK.

Biometric scores set, NIST. Retrieved from http://www.nist.gov/itl/iad/ig/biometricscores.cfm

Bogićević, M., Milenković, I., Simić, D.(2014) Identity Management – A Survey in M. Levi-Jakšić, S. Barjaktarević, M.Martić *Innovative Management and Firm Performance*.(ch. 19). Palgrave Macmillan

Chike, O. (2013). Multimodal Biometric Technology System Framework and E-Commerce in Emerging Markets. *International Journal of Advanced Computer Science & Applications*, 4(7), 192–196.

Claroline LMS. Retrieved from http://www.claroline.net/

Dehnavi, M. K., & Peykanpour Fard, N. (2011). Presenting a multimodal biometric model for tracking the students in virtual classes. *Procedia-Social and Behavioral Sciences* 15, 3456-3462.

Facebanx multimodal biometric solution. Retrieved from http://www.facebanx.com/face-voice-document-verification.php

Face Recognition Technology, NIST. Retrieved from http://www.nist.gov/itl/iad/ig/feret.cfm

Hiew, S., Hishammuddin, A., Rohayanti, H., Razib, O.(2014) Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. *Expert Systems with Applications*, 41(11), 5390-5404. Retrieved from http://dx.doi.org/10.1016/j.eswa.2014.02.051.

Lupu, C.(2011) Car access using multimodal biometrics. *The USV Annals of Economics and Public Administration* 10(3), 368-377.

Mayank, V., Richa, S, Afzel, N.(2007) Integrating image quality in 2v-svm biometric match score fusion. *International Journal of Neural Systems*,17(5), 343-351

Monwar, M.; Gavrilova, M.L.(2009). Multimodal Biometric System Using Rank-Level Fusion Approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 39(4), (867-878)

Maheswari, U., Anbalagan, P.(2010) An intelligent multimodal biometric system for high security access. *International Journal of Biometrics*, 2(3), 295-311.

Milenković, I., Šošević, U., Simić, D.(2012) Architectures of comprehensive identity and access management. Paper presented at the *Electronic International Interdisciplinary Conference*. ISSN:1338-7871, ISBN 978-80-554-0551-3.

Monwar, M.,Gavrilova, M.L.(2008). A Robust Authentication System Using Multiple Biometrics. *Computer and Information Science Studies in Computational Intelligence*,189-201

M2SYS voting system. Retrieved from http://www.m2sys.com/automated-fingerprint-identification-system-afis-voter-registration.htm

Phillips, P.J.; Martin, A; Wilson, C.L.; Przybocki, M.(2000). An introduction evaluating biometric systems. *Computer* ,33(2),56-63.doi: 10.1109/2.820040

Poh, N.; Bengio, S.(2006) Using Chimeric Users to Construct Fusion Classifiers in Biometric Authentication Tasks: An Investigation. Presented at the *IEEE International Conference on Acoustics, Speech and Signal Processing.*

Proenca, H., & Alexandre, L. (2005). UBIRIS: A noisy iris image database. In F. Roli & 998 S. Vitulano (Eds.),Image analysis and processing-ICIAP 2005, 970–977. Berlin 999 Heidelberg: Springer. Vol. 3617

Prabhakar, S.; Pankanti, S.; Jain, A.K. (2003) Biometric recognition: security and privacy concerns. *Security & Privacy, IEEE*, 1(2), 33-42.

Proenca, H., & Alexandre, L. (2005). UBIRIS: A noisy iris image database. In F. Roli & S. Vitulano (Eds.),Image analysis and processing-ICIAP 2005, 970–977. Berlin 999 Heidelberg: Springer. Vol. 3617

Ratha, K., Connell, J. Bolle, R.M.(2001). An analysis of minutiae matching strength in the *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01*), 223–228, Halmstad, Sweden, June 2001

Rattani, A.; Kisku, D.R.; Bicego, M.; Tistarelli, M.(2007). Feature Level Fusion of Face and Fingerprint Biometrics. presented at the First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 27-29 Sept. 2007

Ribaric, S.; Ribaric, D.; Pavesic, N., (2003). Multimodal biometric user-identification system for network-based applications. IEE Proceedings Vision, Image and Signal Processing, vol.150, no.6, 409,416, 15 Dec. 2003

Ross, A., Nandakumar, K., & Jain, A. (2006). Handbook of Multibiometrics (International Series on Biometrics). Springer-Verlag New York, Inc., *Secaucus*, NJ, USA.

Ross, A., & Govindarajan, R.(2005) Feature level fusion of hand and face biometrics in Proc. SPIE 5779, Biometric Technology for Human Identification II, 196 (April 05, 2005); doi:10.1117/12.606093.

Saini, N., Sinha, A.(2014) Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction*, Pattern Analysis and Applications,* 18(4),921-932

Samaria, F. S., & Harter, A. C. (1994). Parameterisation of a stochastic model for 1017 human face identification. In Proceedings of the second IEEE workshop on 1018 applications of computer vision, 138–142.

Sandhu, R.S.; Samarati, P.(1994). Access control: principle and practice. Communications Magazine, IEEE, 32(9),40-48. doi: 10.1109/35.312842

Snelick, Robert; Uludag, U.; Mink, Alan; Indovina, M.; Jain, A. (2005). Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3),450-455, doi: 10.1109/TPAMI.2005.57

SET Secure Electronic Transaction Specification (V1.0) Book 1. Mastercard and Visa. May 1997.

Šošević, U., Milenković, I., Milovanović, M., Minović, M.(2013). Support Platform for Learning about Multimodal Biometrics. *Journal of Universal Computer Science*, 19,(11), 1684-1700.

US-Visit border control program. Retrieved from http://travel.state.gov/content/visas/english/general/border-biometrics.html

Vision-Box solution. Retrieved from http://www.vision-box.com/

OVERVIEW OF EAR BASED PERSON RECOGNITION ALGORITHMS

Sofija Krneta[*1], Uroš Šošević[1], Dušan Starčević[1]
[1] Faculty of organizational sciences, University of Belgrade,Belgrade
*Corresponding author, e-mail: sofija.krneta@mmklab.org

Abstract: *Biometric modalities in person recognition process were subject of interest for many scientists over the years. In order to make image evidences more reliable, law enforcement was the first one to see the potential in parts of the body for person recognition. One of biometric modalities that has a lot of potential but is still in developing phase is human ear. This paper explores current available algorithms, analyzes most significant ones and suggests place for improvement or focus of further research for the authors.*

Keywords*: human ear, ear based recognition, person recognition, biometric systems, multimodal biometrics*

1. INTRODUCTION

Although the beginnings of using biometric technologies are dating back to 1858 (Komarinski, 2005), their benefits are still not completely utilized. Of course some of biometric modalities already found their application in practice and are used for identification and verification of individuals in various circumstances. However, some biometric traits have not yet been researched enough to be used in real conditions. These facts represent one of the reasons why biometrics as a technology was present in only 20.5 percent of organizations that participated in the Computer crime and security survey conducted by FBI and Computer Security Institute (Richardson, 2011) on an annual basis. Most of used biometric systems rely on biometric modalities with high level of reliability such as fingerprint and iris. Unfortunately, those modalities are also highly intrusive. Immediately following these modalities are some less reliable modalities - face, ear, voice and gait. Those modalities are also subjects to occlusion and imitation which can drastically lower the reliability of the biometric system. On the other hand, they do not require that the person cooperates in recognition process. It is clear that low reliability of mentioned biometric modalities prevents wide application of biometrics. However, their unintrusiveness makes them popular for usage in applied biometric systems.

There is one popular approach that may increase the reliability of biometric systems - multimodal biometrics. Multimodal biometrics refer to usage of several biometric modalities in one biometric system. More precisely, multimodal biometrics combine information acquired with different biometric sensors in order to increase the rate of accurate recognition. Project “Multimodal biometrics in identity management”, funded by Ministry of Education and Science of Serbia (Starčević et al., 2014) is focused on application of multimodal biometrics in identity management. During the research in field of biometrics, researchers engaged in this project were exploring each of the modalities and their utilization in multimodal biometric recognition. One of the promising biometric modalities for person recognition is human ear. It is known that the structure of human ear is not only unique, but also constant as the ear does not change over the course of human life. Additionally, this biometric modality does not require person"s consent to recognition and thus it is considered as non intrusive (Pflug and Busch, 2012). In order to utilize human ear in biometric recognition process, system usually uses ear images. Ear images can be acquired on itself or it can i.e. be isolated from image of a person"s face. This fact also makes human ear an interesting biometric modality which is constantly researched in the last several years.

This paper focuses on algorithms used in person recognition based on human ear. In the next chapter, human ear as a biometric modality is presented and also ear biometric systems are described. Additionally, some applications of human ear as a modality in multimodal biometric systems are given. List of currently available ear recognition algorithms is given in third chapter. The algorithms are chronologically listed and also categorized in this chapter. Fourth chapter focuses on most popular ear recognition algorithms, their way of functioning, advantages and disadvantages. Conclusions and future work regarding the person recognition based on human ear are defined in the last chapter.

2.PERSON RECOGNITION BASED ON EAR BIOMETRIC SYSTEM

Ear biometric system can be defined as a typical pattern recognition system where the input image is reduced to a set of features that is subsequently used to compare against the feature sets of other images

in order to determine its identity (Abaza, 2013). It is a system that receives image as an input, uses details key features of human ear and gives person recognition as an output result. Person recognition can be used in two ways: Verification and Identification. Verification process uses ear features of an exact person to compare and verify person"s identity. Identification uses existing database to recognize which of existing features match features received as an input. Since identification process is iterative process through existing database, it"s duration is longer. However, the main recognition process stays the same, thus the output of person recognition process is identical - a match to a person in the existing database.

Physiological (anatomical) biometrics methods are based on the physiological features of humans. They measure and compare features of specific parts of human body in the process of recognition. So far the most interesting biometric modalities for researching are face, iris and fingerprint features since they are the most important discriminants of human identity (Perales and Draper, 2004). The advantages of anatomical biometrics can be summed into following statements:

- Acquisition of the data for input is a passive process and does not require participation of the person that is about to be included
- Acquired data is typically invariant over time, easy to acquire, and unique to each individual.

There haven"t been many efforts in application of human ear for personal authentication, even though it has proved its significant role in forensics. The main characteristics of the human ear that make it a good candidate for person recognition are (Kumar and Wu, 2011):

- rich and stable structure that is preserved since birth and is quite unique in individuals
- being invariable to the changes in pose and facial expression
- relatively immune to anxiety, privacy and hygiene problems

Human ear is highly curved 3D surface and therefore provides rich 3D features which can be used for exact feature selection and more precise person recognition. Using image processing when working with 3D images has proven to extract unique features which can"t be extracted from 3D images of other anatomical biometrics such as iris or fingerprint.

Whether the input is 2D or 3D image, it is processed to extract all the features as part of image processing and preparing input for any biometric system used for person recognition. These images are prepared for an ear biometric system.

The evolution of using person recognition based on person"s ears dates centuries back. In 1096, Richard Imhofer defined four different characteristics to distinguish 500 different persons by their ears (Imfoher, 1906). In 1949, Alfred Iannarelli determined 12 features needed for person recognition on 10000 different people (Imhofer, 1906). Iannarelli also discovered that ears are unique among twins, triplets and similar for relatives. Those discoveries made it clear that there are biometrical disadvantages of using ear for person recognition. However, studies in (Meijerman et al., 2004) and (Singh and Purkait, 2009) show by example that a person evolution, development and growth through years lead to possession of new individual characteristics. Those characteristics become unique features of the outer ear even for siblings.

There have been some questions and uncertainties about the accuracy of this modality in person recognition as standalone recognition mean. The Forensic Ear identification Project (FearID) was initiated by nine institutes from Italy, the UK and the Netherlands in 2006 (Alberink and Ruifrok, 2007). The study measured an Equal Error Rate (EER) of 4%. This error rate is satisfying even in forensics, which means that ear prints can be used as evidence in a semi-automated system. After this study, many systems implemented ear recognition as part of person recognition, but a minority of systems used it as a standalone solution, such as German police in their surveillance video analysis.

3. EAR RECOGNITION ALGORITHMS - STATE OF THE ART

During the evolution of the person recognition using ear as a biometric modality, many methods have been developed with different success on various test datasets. Main categorization could be done based on the input required for the algorithm. We can differentiate algorithms which use 2D or 3D images for recognition process.

3.1. 2D image recognition

In the list below, most of available works on 2D ear image based recognition are presented in chronological order (Pflug and Busch, 2012):

1. Burge and Burger (1998) Vornoi Distance Graphs
2. Hurley (2002) Force Field Transform
3. Moreno (2002) Geometric features with Compression Network
4. Yuizono (2002) Genetic Local Search
5. Victor (2002) PCA
6. Chang (2003) PCA
7. Abdel-Mottaleb and Zhou (2005) Modified Force Field Transform
8. Mu (2005) Geometrical measures on edge images
9. Abate (2006) General Fourier Descriptor
10. Lu (2006) Active Shape Model and PCA
11. Yuan (2006) Non-Negative Matrix Factorization
12. Yuan and Mu (2007) Full Space LDA with Outer Helix Feature Points
13. Arbab-Zavar (2007) SIFT points from ear model
14. Jedges and Mate (2007) Distorted Ear Model with feature points
15. Liu (2007) Edge-based features from different views
16. Nanni and Lumini (2007) Gabor Filters and SFFS
17. Rahman et al. (2007) Geometric Features
18. Sana (2007) Haar Wavelets and Hamming Distance
19. Arbab-Zavar and Nixon (2008) Log-Gabor Filters
20. Choras (2008) Geometry of ear outline
21. Dong and Mu (2008) Force Field Transform and NKFDA
22. Guo and Xu (2008) Local Binary Pattern and CNN
23. Nasseem (2008) Sparse representation
24. Wang et al. (2008) Haar Wavelets and Local Binary Patterns
25. Xie and Mu (2008) Locally Linear Embedding
26. Yaqubi (2008)HMAX and SVM
27. Zhang and Mu (2008) Geometrical Features, ICA and PCA with SVM
28. Badrinath and Gupta (2009) SIFT landmarks from ear model
29. Kisku (2009) SIFT from different Color Segments
30. Wang and Yuan (2009) Low-Order Moment Invariants
31. Alaraj (2010) PCA with MLFFNNs
32. Bustard (2010) SIFT Point Matches
33. De Marisco (2010) Partitioned Iterated Function System (PIFS)
34. Gutierrez (2010) MNN with Sugeno Measures and SCG
35. Wang (2010) Moment Invariants and BP Neural Network
36. Wang and Yuan (2010) Gabor Wavelets and GDA
37. Fooprateepsiri and Kurutach (2011) Trace and Fourier Transform
38. Prakash and Gupta (2011) SURF and NN classifier EER
39. Kumar (2011) SIFT GAR, FAR
40. Wang and Yan (2011) Local Binary Pattern and Wavelet Transform
41. Kumar and Wu (2011) Phase encoding with Log Gabor filters

The Force Field Transform by Hurley (2002) is one of the most frequently used methods for ear based recognition. This approach assumes mutual attraction of pixels that is proportional to their intensities and inverse to the square of the distance between them.

Structure of the outer ear proved to give extra information used for person recognition. Extraction of specific texture features can be extracted using Gabor filters. Wang and Yuan (2010) did it and then discriminately selected the most distinctive ones as they considered them to be the key information in the recognition. Kumar and Wu (2011) used Log-Gabor filters for extracting features of the local structure of the ear. Extracted features were stored in normalized grey level images. In their experiment, Log-Gabor based features had better performance than Hurley"s approach and landmark-based feature extraction approach.

Abate (2006) presented in his work generic Fourier descriptor for rotation and scale invariant feature representation. He used a polar coordinate system to transform the image into coordinates and then converted the coordinates into frequencies. The ear images had to be aligned in order to centralize the coordinate beginning before transformation into the polar coordinate system.

Wang (2010) composed six feature vectors with the help of seven moment invariants. The study showed that each of the moment invariants is invariant to changes in scale and rotation. The feature vectors were then set as input for a neural network for classification of the feature sets. Wang and Yuan (2010) then compared different feature extraction methods. They concluded that the complete accuracy of 100% is made by using moment invariants and Gabor transformation.

3.2. 3D image recognition

Recent papers focused more on 3D images in order to improve accuracy of the process. The strengths of 3D images are their immunity to rotation, scaling and translation. Shadows and special features discovered in a 3D image of an ear gave crucial addition to overall features used for person recognition. Usually, in the system where they bring more information than they take computational resources, 3D images can recognise a person based on their ear as a biometrical module only. Following algorithms gave significant results in this process:

1. Yan and Bowyer (2005) ICP using voxels
2. Chen and Bhanu (2005) ICP Contour Matching
3. Chen and Bannu (2007) Local Surface Patch
4. Liu (2007) Mesh PCA with neural network
5. Passalis (2007) Reference ear model with morphing
6. Yan and Bowyer (2007) ICP using Model Points
7. Cadavid (2008) ICP and Shape from shading
8. Islam et (2008) ICP with reduced meshes
9. Islam et (2008) Local Surface Features with ICP-Matching
10. Zheng (2010) Local Binary Patterns
11. Liu and Zhang (2011) Slice Curve Matching
12. Zhou (2011) Surface Patch Histogram and voxelization

Widely used method is ICP contour matching described in (Chen and Bannu, 2007). ICP requires double alignment of the models. They suggested extraction of point clouds from the ear contour and the registration of points with ICP (Chen, 2005).

Yan and Bowyer split the image of the ear and extracted features that give information about identity. In order to save computational resources in the recognition process, parts of the ear are indexed for faster ICP matching (Yan and Bowyer, 2005). That idea developed in direction of using Model Points in (Yan and Bowyer, 2007).

In (Cadavid, 2008) Cadavid presented a system suitable for video streaming and live image capturing, which can extract 3D models with the help of shading technique (Cadavid, Mahoor and Abdel-Mottaleb, 2009). 3D model is then set as an input in the system in order to be compared with the existing 3D images in the database.

All 3D algorithms mentioned in this paper present approaches that work satisfactorily with clear images and without occlusion. When introducing complexities such as earrings, hair etc. it has to be examined which algorithm might show best results.

4. ALGORITHMS COMPARISON

In this section of the paper we present the most important algorithms. Specifically, algorithms are presented chronologically and the way of their functioning is described briefly. 3D and 2D algorithms for ear feature extraction are separated and their advantages and disadvantages have been defined. Also, we presented recognition rates where provided by authors.

There are various research papers discussing about person recognition techniques based on human ear. Some of the papers present specific overview of algorithms used (Pflug and Busch, 2012), but none of them refers to recommendations for algorithm improvement in different segments. We believe that presenting most important algorithms for ear based person recognition and defining segments in which they can be used or improved makes room for future research in this area. In example, standardizing feature set which could lead to segmentation of ear in the recognition process. If the ear were segmented

into parts for examination, it would be possible to give significance or distinction to certain parts of the ear. Similarly, pose variations and occlusion might be partially solved by omitting occluded parts of the ear.

In case of 2D algorithms there are 5 which take precedence: Force Field Transform (Hurley, 2002), Fourier descriptor for rotation and scale invariant feature representation (Abate, 2006), Moment invariants with back propagated neural networks (Wang et al., 2010), Gabor filters (Wang and Yuan, 2010) and Local orientation features using even Gabor filters (Kumar and Wu, 2012).

Force Field Transform algorithm extracts wells and channels of the ear. It extracts a description based on the well position. It has been proven that these kind of descriptions are unique for every ear. Unfortunately, this approach has been tested on 9 subjects only, which is a setback. Room for upgrade of the algorithm could be increasing number of measures used for recognition. Additionally, by including channels into description better performance of the algorithm could be achieved. Advantages of this approach are that it is scaling invariant, it has high noise tolerance and there is no explicit ear topology description needed. No recognition rate of this algorithm has been presented by the authors.

Abate suggests Generic Fourier Descriptor for feature extraction. This algorithm is illumination and rotation invariant. Unfortunately, no testing or recognition rate information about this algorithm have been presented in the paper.

Wang, Xia and Wang recommend using improved moment invariants algorithm for feature extraction and then applying high order moment invariants for extracting 6 feature vectors. Good side of this algorithm is that it is invariant to translation, rotation and size change. By using BP neural network on 60 subjects data set, recognition of 91.8% was reached.

Gabor filter is robust and durable in case of illumination change, but Gabor features vector has immense dimensional space. Wang and Yuan use Gabor feature extraction and General Discriminant Analysis which effectively decreases dimensions of features vector. They have reached recognition rate of 99.1% on USTB database and also reported satisfying execution time - enough for real time system functioning.

Kumar and Wu achieved high performance as previous top approaches - eigen ear, force field transform, shape features. They reported recognition rate of 96.27% and 95.23% on databases containing 125 and 121 subjects, respectively. Authors used a pair of log-Gabor filters on IIT Delhi Ear Database. Disadvantage of this algorithm is that its performance has not been tested in different angles and occlusion. Testing has been done on a dataset that has small variation in image orientation and size. Thus, there is a need to test this algorithm in outdoor conditions in order to prove its performance. Outdoor conditions could greatly affect ear segmentation because of light changes and shadowing.

3D ear feature extraction algorithms that stand out are 3 algorithms presented in 2007. And 2008.

Contour matching (Chen and Bhanu, 2007) algorithm is based on contour of outer helix and uses ICP but it was improved to LSP since it has less feature points which made the process computationally cheaper. After the points were extracted, measured distances were compared to the existing ones in the database. The result was increase of recognition rate from 93.3% to 96.63% during an experiment with 302 subjects.

3D imaging (Yan and Bowyer, 2007) approach is based on contour function for describing ear shape and uses ICP with k–d tree data structure to efficiently search for closest point. The algorithm was evaluated in a large experimental study on 415 subject with accuracy rate of 97.8% and EER 1.2%.

ICP and Shape form shading (Cadavid, 2008) algorithm was presented by Cadavid as an algorithm that works well with real-time image extraction, where 3D images are modeled from CCTV images and shading technique for forming shape. Dissimilarities with existing images in the database is done by ICP. Downsides of this algorithm is its weak response to pose variations. Experiment with this algorithm on a 402 subject study showed 95% accuracy rate.

4. CONCLUSION

In this paper, there have been presented most of the available algorithms for ear based person recognition. The most important ones were applied on different databases and showed major success in accuracy. There is still a lot of room for improvement of various leading algorithms. Also,

In 2D images, pose variation and camera position change present a strong setback for most of the algorithms. Occlusion still remains the weakest link in ear based recognition. In this cases, it is indispensable to gather information about occluded parts. Occlusion caused by pose variations is especially neglected since there are no publications that tried to solve “filling the gaps” problem. There are feature extraction methods which partially solve pose variation disadvantages but they still have space for improvement.

Noticed shortcomings will be used in future works for ear based person recognition system improvement in terms of applying various algorithms in most suitable situations. Additionally, authors plan to explore possibilities for using only a visible portion of human ear in recognition process. This could be particularly useful in conditions of occlusion .

This approach might be used in all of the existing algorithms, in order to show proof of concept in improving accuracy. Also, This opens a possibility for using different algorithms on several parts of the ear.

ACKNOWLEDGMENTS

This work is a part of the project Multimodal biometry in identity management, funded by Ministry of Education and Science of Serbia, contract number TR-32013.

REFERENCES

A. Kumar, C. Wu, Automated human identification using ear imaging, Pattern Recognition (2011), doi:10.1016/j.patcog.2011.06.005

Abate AF, Nappi M, Riccio D, Ricciardi S. ’Ear Recognition by means of a Rotation Invariant Descriptor’. In: 18th International Conference on Pattern Recognition, ICPR 2006.. vol. 4; 2006. 437 –440.

Abaza, Ayman, et al. "A survey on ear biometrics." ACM computing surveys (CSUR) 45.2 (2013): 22.

Alberink I, Ruifrok A. ’Performance of the FearID earprint identification system’. Forensic Science International. 2007;166(2-3):145 – 154.

Cadavid S, Abdel-Mottaleb M. ’3D ear modeling and recognition from video sequences using shape from shading’. In: 19th International Conference on Pattern Recognition (ICPR); 2008., 1 –4.

Cadavid S, Mahoor MH, Abdel-Mottaleb M. ’Multi-Modal Biometric Modeling and Recognition of the Human Face and Ear’. In: IEEE International Workshop on Safety, Security Rescue Robotics (SSRR); 2009., 1 –6.

Chen H, Bhanu B. ’Contour Matching for 3D Ear Recognition’. In: Proceedings of the Seventh IEEE Workshop on Applications of Computer Vision (WACV/MOTION); 2005.

Chen H, Bhanu B. ’Human Ear Recognition in 3D’. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007 April;29(4):718 –737.

F.J. Perales and B.A. Draper (Eds.): AMDO 2004, LNCS 3179, 51-61, 2004

Hurley DJ, Nixon MS, Carter JN. ’Force Field Energy Functionals for Image Feature Extraction’. Image and Vision Computing. 2002;20(5-6):311 – 317.

Imhofer R. ’Die Bedeutung der Ohrmuschel f¨ur die Feststellung der Identit¨at’. Archiv f¨ur die Kriminologie. 1906;26:150–163.

Islam SM, Davies R, Mian M A S an Bennamoun. ’A Fast and Fully Automatic Ear Recognition Approach Based on 3D Local Surface Features’. In: Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems. ACIVS ’08. Berlin, Heidelberg: Springer-Verlag; 2008., 1081–1092.

Islam SMS, Bennamoun M, Mian AS, Davies R. ’A Fully Automatic Approach for Human Recognition from Profile Images Using 2D and 3D Ear Data’. In: Proceedings of 3DPVT - the Fourth International Symposium on 3D Data Processing, Visualization and Transmission; 2008.

Kumar A, Hanmandlu M, Kuldeep M, Gupta HM. ’Automatic Ear Detection for Online Biometric Applications’. In: Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG); 2011., 146 –149.

Kumar A, Wu C. ’Automated human identification using ear imaging’. Pattern Recogn. 2012 March;45(3):956–968. Available from: http://dx.doi.org/10. 1016/j.patcog.2011.06.005.

Liu H, Zhang D. ’Fast 3D Point Cloud Ear Identification by Slice Curve Matching’. In: 3rd International Conference on Computer Research and Development (ICCRD); 2011., 224.

Meijerman L, Sholl S, Conti F. D, Giacon M, van der Lugt C, Drusini A, et al. 'Exploratory study on classification and individualisation of earprints'. Forensic Science International. 2004;140(1):91 – 99.
Passalis G, Kakadiaris IA, Theoharis T, Toderici G, Papaioannou T. 'Towards Fast 3D Ear Recognition For Real-Life Biometric Applications'. In: IEEE Conference on Advanced Video and Signal Based Surveillance (AVSS 2007); 2007., 39 –44.
Pflug A, Busch C 'Ear Biometrics: A Survey of Detection, Feature Extraction and Recognition Methods' IET Biometrics, 2012.
Robert Richardson, "2010/11 CSI Computer Crime and Security Survey". Computer Security Institute. 2011
Sana PPR Anupam; Gupta. 'Ear Biometrics: A New Approach'. In: Advances in Pattern Recognition; 2007
Singh P, Purkait R. 'Observations of external ear An Indian study'. HOMO - Journal of Comparative Human Biology. 2009;60(5):461 – 472. Available from: http://www.sciencedirect.com/science/article/pii/S0018442X09001164.
Starčević et al. "Multimodalna biometrija". Faculty of organizational sciences. 2014.
Wang X, Yuan W. 'Gabor Wavelets and General Discriminant Analysis for Ear Recognition'. In: 8th World Congress on Intelligent Control and Automation (WCICA); 2010., 6305.
Wang X, Yuan W. 'Human Ear recognition Based on Block Segmentation'. In: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC); 2009., 262 –266.
Wang Xq, Xia Hy, Wang Zl. 'The Research of Ear Identification Based On Improved Algorithm of Moment Invariants'. In: Third International Conference on Information and Computing (ICIC); 2010., 58
Wang Zq, Yan Xd. 'Multi-Scale Feature Extraction Algorithm of Ear Image'. In: International Conference on Electric Information and Control Engineering (ICEICE); 2011., 528.
Yan P, Bowyer KW. 'A Fast Algorithm for ICP-Based 3D Shape Biometrics'. In: Fourth IEEE Workshop on Automatic Identification Advanced Technologies; 2005., 213 – 218.
Yan P, Bowyer KW. 'Biometric Recognition Using 3D Ear Shape'. Pattern Analysis and Machine Intelligence. 2007 August; 29:1297 – 1308.
Yuan L, Mu Z. 'Ear Recognition Based on 2D Images'. In: First IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS); 2007., 1 –5.
Zeng H, Dong JY, Mu ZC, Guo Y. 'Ear Recognition Based on 3D Keypoint Matching'. In: IEEE 10th International Conference on Signal Processing (ICSP); 2010., 1694.
Zhou J, Cadavid S, Abdel-Mottaleb M. 'A computationally Efficient Approach to 3D Ear Recognition Employing Local and Holistic Features'. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2011., 98 –105.

PREVENTION OF FRAUD IN ELECTRONIC PAYMENT SYSTEMS

Marija Bogićević Sretenović, Jasna Petković , Bojan Jovanović
Fakultet Organizacionih Nauka
marija.bogicevic@fon.bg.ac.rs

***Abstract**: Nowadays, fraud is the leading problem in electronic payment systems. The subject of this paper is a review of existing techniques for prevention of fraud in electronic payment systems. Prevention and detection of fraud are of extreme importance in the field of risk management, as well as fraud management in payment cards industry. The end goal is to reduce the number of frauds through application of multidisciplinary approach. The system for prevention of payment card frauds is a complex system that collects knowledge from more than one source. This paper shows current condition throughout the world and gives a detailed comparison of modern techniques for prevention, detection and fraud management in electronic payment systems. The paper also gives an example of possible enhancements when it comes to prevention of frauds in electronic payment systems.*

***Key words**: fraud management systems, risk management, electronic payment systems, security*

1. Introduction

One of the main problems of electronic banking is to be found in the fact that fraud transactions are increasingly showing as genuine, that is, legitimate.

As for the historical development of fraud in electronic payment systems, it could be said that stealing and forgery of cards was present during the ‘70s, but the cards were then physically stolen. In ‘80s and ‘90s, ordering by telephone/mail became a common thing. Online fraud inhabited the world scene as the Internet went live worldwide and developed into something that allows for anonymity, availability and swiftness to commit fraud on world level.

One of the fastest ways of shopping is shopping with payment cards, where one gets the goods instantly, and pays for it later. Electronic payment systems have a series of advantages, such as ordering products from far away, which allows for consumers’ conformity. However, there are disadvantages as well, such as security of data being transferred and exposure to risk of compromising data. Therefore, credit cards fraud is a serious problem encountered by all participants in this communication chain.

Today, most people use e-commerce partly due to economic reasons, and partly for conformity reasons, because there’s no need to leave home. However, card fraud is quite a serious problem indeed. Every year, card issuing organizations and the consumers themselves are exposed to significant financial costs, and potential loss of incomes. It is very difficult to cope with some techniques used by fraudsters, since some of the methods being used for authorization are genuinely wrong and inadequate. In most number of cases, the buyer himself is not aware of the process taking place in the system after he/she buys a certain product. Earlier, at time when cards with magnetic strips were used, the salesman was able to compare the signature on the slip with the signature on the back of the card. However, in case the card was stolen, the fraudster was most likely to practice the signature so that the comparison was no longer of any use. In that case, one could introduce even higher level of prevention and ask for an additional document that would confirm the identity of a person, such as ID card or driver’s license. Even higher level that was introduced later was the PIN entry, which makes the user signature unnecessary. In case of frauds, when the card is not physically present, various methods are used in an attempt to gain necessary data.The more the card is used for online shopping, the more it is exposed to attacks and compromising. In some regions, one of the methods used by fraudsters is learning the social security numbers by using social engineering techniques, and this number is used to additionally determine the person’s identity.

Banks are highly interested in processor speed that helps in detecting a fraud. Any activity can jeopardize the cardholder, and the banking institution itself. This could be either the bank in which the owner has an account tied for a card, or a processing company that supports the bank. Institutions mainly combine basic forms of prevention with more complex ones, and thus they form what is known as Fraud Management. Fraud technologies encounter the possibilities of active survey of an account in order to discover or at least sense all irregularities in transactions.

From the financial point of view, if we are to observe frauds, it’s like a recursive life cycle that illustrates a continual response to fraudsters’ behavior. Ever changing trends in the fraud development eventually led to the point where the systems are being continually developed and complex algorithms are constantly applied,

such as data mining and data analysis. The goal is to design new security protocols, as well as authentication protocols. In their response to these innovations, fraudsters develop new techniques that are to help them overcome these protective measures. New fraud patterns are identified as a result of security enhancements, including the development of new software solutions, or to be more precise, through stronger authentication and safety procedures.

2. FINANCIAL LOSSES OVER CARD FRAUD WORLDWIDE

Card fraud is becoming widely spread phenomena, which is supported by following statistical data. Namely, in 2012 alone, the abuse of credit and debit cards has caused a $ 11.7 billion loss worldwide. In the same year, the greatest number of fraudulent financial transactions over cards hit 47.3pct out of overall global transactions. Compared to 2010, up to 67pct of those exposed to frauds were the US citizens (Lindsay, 2014).

Table 1. shows regional losses caused by card frauds, where the P – predicted indicates predicted losses. Table helps us drawing a conclusion that the losses are immense, and that the prevention of fraud in electronic payment system is a problem that needs to be handled in a systematic manner.

Table 1: Regional forecast of spending and losses (Riley, 2012)

Regional spending in millions USD	2011	2012	2013	2014	2015	2016P	Annual growth
North America	$794	$794	$799	$800	$806	$816	0,5%
Europe	$444	$453	$460	$463	$465	$466	1%
Asia Pacific	$379	$416	$455	$491	$528	$564	8,3%
Latin America and the Caribbean	$98	$106	$114	$122	$130	$137	7%
Middle East and Africa	$31	$33	$34	$35	$36	$36	3,2%

2.1 Types of Fraud

According to the report of Aite Group from 2010, the frauds could be classified as follows:

1. *first-party fraud*
2. CNP (Card-not-Present)
3. counterfeit card – creating fake cards
4. lost and stolen cards
5. mail non-receipt fraud
6. card number theft / Identity theft

Figure 1. shows down the fraud losses by category according to Aite Group (Aite Group, 2012). This research has shown that the United States suffered greatest gross financial losses in 2008. CNP fraud represents the weakest spot for merchants. CNP fraud is growing faster than counterfeit fraud. Figure 1. shows that the First-party fraud is taking the greatest portion in this classification.

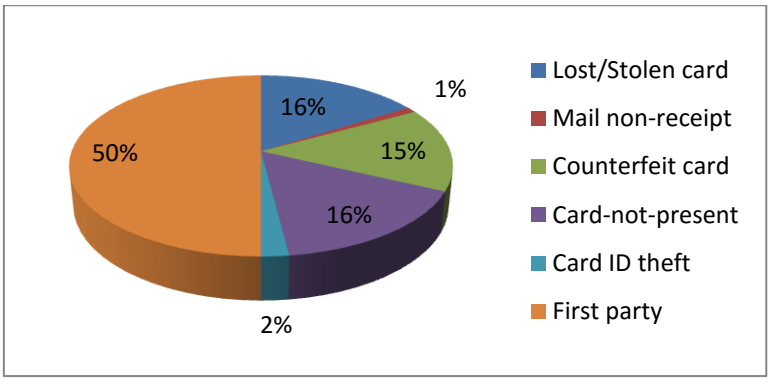


Figure 1: Portion of certain fraud types in 2012
(Aite Group, 2012)

2.2 The greatest attacks in the history of fraud management

Great attacks that happened over the last ten years, when this problem became real serious, speak of the importance of preventing credit card frauds. From July, 2005 to August, 2007, the attacks on the systems in TJX Company have exposed more than 46.5 million card details (Jones, 2013). Albert Gonzalez has been

accused of being a chief hacker who organized a group that carried out the attack. It is believed that Gonzalez, together with ten more associates, carried out this attack by using wireless scanners to find stores with vulnerable networks and them captured account information.

In August 2009, Gonzalez was again a main suspect for card fraud, or in this case, over 130 million cards that were stolen in Heartland Payment Systems, retailers 7-Eleven and Hannaford Brothers, and two unidentified companies (Godin, 2009).

In most number of cases, once the perpetrators obtained credit card data or the card itself, they pulled the money from victim's account in as short period of time as possible. This was one of the biggest ID theft case in the United States of America. The attack was carried out by using SQL injection to install sniffer software on the Heartland Payments System server to collect and intercept credit card data. This attack was a big disgrace and it hurt company's reputation badly, since the company processed more than 100 million transactions a month for more than 250.000 merchants.

In 2012, over 40 million cards have been compromised by hacking the Adobe Systems. The fact is that the total global payment-card fraud losses were $ 11.3 billion in 2012, up nearly 15% from the prior year (Economist, 2014). The United States is one of rare countries in which counterfeit-card fraud is consistently growing. Based on this, card issuers lost $ 3.4 billion in 2012 and merchants another $ 1.9 billion.

At the end of 2013 there were 1.2 billion debit, credit and pre-paid cards in circulation in America, which is more than in any other region in the world. That is nearly five cards per adult. As of 2012, 45pct of the world's payment cards and 76pct of terminals were equipped to use chip-and-PIN.

Already in July 2013, a new attack happened, and it was recorded as the 'largest hacking and data breach scheme ever prosecuted in the United States' (Benson, 2013). Russians and Ukrainians were involved in this case that took place in New Jersey, and which exposed more than 160 million credit card numbers. Those card numbers were later used for printing new plastic cards that were used for shopping. This attack resulted in hundreds of millions of dollars of losses.

Between November 27, 2013 and December 15, 2013 around 40 million cards were affected, including the cardowner name, account number, expiration date, and CVV (card verification value). The hackers hit Target Corporation, and estimates say that almost 70 million Target customers suffered losses due to this attack.

A newer attack occurred between July 16, 2013 and October 30, 2013 with Neiman-Marcus hit with a breach, when around a million of card numbers were found in their system (Wagenseil, 2014).

Recently, some banks in Indiana were also under attack. The hackers obtained card information from ATMs or through debit card payment, where more than 100 users were exposed. Transactions ranging from several hundreds to several thousands of dollars took place in Nigeria, Russia, Ukraine and Spain. A lot of cases were reported on behalf of Citibank the same year, where only two men executed hundreds of transactions and pulled around $ 750.000 from ATMs in New York. The target was a data server in Citibank. From 2007, FTC has recorded over 800,000 exposed users with total fraud loss of over $ 1.2 milliard.

In 2012, a new attack hit the payment processor company Global Payments, which resulted in exposure of 1 million cards. Visa and MasterCard payment systems were the target, and it was suspected that magnetic stripes, stripe 1 and stripe 2 were compromised. In May 2012, it became obvious that the hackers moved from Great Britain to France and Germany due to introduction of EMV in GB.

In the course of 2013, there was a great number of data breaches, when hackers used all of their abilities to take advantage of system malfunctions, as was the case with Target and Neiman-Marcus.

3. TECHNIQUES FOR PREVENTION OF PAYMENT CARD FRAUD

The development of new techniques for revealing payment card frauds is complex, mainly because of the limitations in exchange of ideas and information in this field. Once the details on fraud techniques are made public, persons in charge of the breach can use this information to avoid exposure, but at the same time these details are used for enhancing future breach techniques, by using current system faults. Set of data necessary for any of the fraud techniques is not available in public.

Techniques for fraud prevention could be classified in different ways, and one of them is as follows:

1. application of basic set of rules

2. implementation of EMV standards
3. use of complex security protocols
4. use of smart tools for prevention and detection.

3.1 Comparative analysis of fraud prevention techniques

Table 2. shows evaluation of fraud prevention techniques taking into account general and conceptual features of some techniques such as AVS, CVV2, Manual review, Negative & Positive list, Trusted e-mail, and biometrics (Bogicevic, 2014). These techniques have been compared for following characteristics: are they user friendly, are they easy for implementation, how fast are they, what's their price, is the service being charged, does it require a change in system if implemented, does it secure fraud reduction, and how realistic is to expect this technique to be applied. They came to a conclusion that the most user friendly techniques are AVS, CVV2, Negative&Positive list, authentication, and trusted e-mail. Biometrics, on the other hand, is not easy for implementation, which makes it expensive for realization. Unlike biometrics, AVS and CVV2 are fast and inexpensive techniques that make only slight changes in the system once being implemented. Buyer authentication, trusted e-mail and biometrics are most efficient when it comes to fraud reduction.

Table 2: Evaluation of fraud prevention techniques (Al-Furiah, 2009)

		Evaluation of techniques						
FEATURES		**AVS**	**CVV2**	**Manual Review**	**Negative& Positive list**	**Buyer authentication**	**Trusted e-mail**	**Biometrics**
General	**User friendly**	H	H	M	H	H	H	M
	Simple for implementation	H	H	M	H	H	H	L
	Speed	H	H	L	M	H	H	M
	Price	L	L	M	M	M	L	H
Conceptual	**Service payment**	M	M	NI	NE	H	H	H
	Requires change in the system	L	L	L	M	M	L	H
	Fraud prevention	M	M	L	L	H	H	H
	Real process time	H	H	NE	Hor NE	H	H	H

High -H, Medium -M, Low - L, Not indicated -NI, Not existing –NE

Table 3. displays advantages and disadvantages of following fraud prevention techniques: AVS, CVV2, *Manual review,* Negative&Positive list, Buyer authentication, *trusted e-mail,* Biometrics.

Table 3: Advantages and disadvantages of fraud prevention techniques (Al-Furiah, 2009)

Techniques	**Advantages**	**Disadvantages**
AVS	- simple, fast and easy for implementation - reduces fraud risk - AVS helps merchants to charge the service - there's no additional cost because AVS could be requested as a part of authorization	- In some cases, buyer's valid address differs from the one reported on the occasion of card issuing - It is not a perfect indicator of a fraud - AVS is not effective for *soft* products
CVV2	- Reduces*CNP fraud* - Prevents card counterfeit - No additional costs - Reduces costs induced by fraud	- Not applicable with stolen and lost cards - The hacker can obtain CVV2 values through system breach
Manual Review	- It's most useful when used with other techniques	- Not an effective technique for fraud prevention - Work quality depends on employees' experience and feedback - It's a very expensive and time-consuming method
Negative& Positive list	- It's a basic technique that serves as a starting point for further considerations - User friendly - Negative list is good for fraud reduction	- It cannot prevent the fraud – card number theft - Frequent updating is a must

	- Positive list decreases time needed for checking the valid order	
Buyer authentication	- It's a starting tool that secures protection of merchants from additional fraud-induced costs - Associations provide this technique in order to make buyers use online shopping - Total cost is low - Responsibility for costs is against the buyer	- Only Visa and Master cardholders can use this service - Buyers don't like this technique since it's time-consuming
Trusted e-mail	- It's an effective technique that helps in merchants' protection and cutting costs - Simple for implementation and use - Better than any other method that uses the delivery address or a verification code - Low price - Requires minimum amendments for all participants in e-payment - Doesn't stand in a way of other solutions	- No fault discovered yet
Biometrics	-Very efficient technique for authentication of buyer identity	- Hard for implementation - Expensive - Requires plenty of changes

4. ALGORHITMS FOR DETECTION OF PAYMENT CARDS FRAUD

Hackers use all possible ways to take advantage of some part of the communication chain between the entities, and thus gain data through payment cards use. The only logical solution is prevention and implementation of all the techniques in order to prevent fraud. There are numerous techniques for fraud prevention, and at the same time, those techniques are being enhanced as we speak (Kou, 2004).

Fraud detection is a very complex IT problem, and there's definitely no system that could predict with certainty which type of fraud is going to take place. There are basic rules that could be implemented and applied by Fraud Management Systems (FMS), but sometimes even they are not enough. For that reason, complex algorithms for reviewing and predicting transactions are being used, and they are supposed to tell us whether the transactions are genuine or fraudulent. Those complex algorithms are working on a principle of predicting the possibility of an event, and in this case the event is whether it's a fraud transaction or not. Techniques for prevention and detection are supposed to reduce the number of frauds, and they are a key part of risk management in banking sector, especially when it comes to electronic payment systems. Prevention techniques comprise a series of basic rules, and when that rules fail in preventing a fraud, detection techniques are being applied.

Given that there's a difference between online and offline frauds, we can also distinguish online and offline monitoring in FMS. Different techniques could be used for different kinds of frauds. FMS are to provide next conditions:

1. to detect fraud in early stage and with sharp precision.
2. to provide relevant information to fraud analysts in timely manner.
3. a good system shouldn't detect genuine transaction as a fraudulent transaction.
4. to make this process automatized wherever applicable.
5. to self-adapt to changes in fraud patterns.
6. to self-adapt to changes in consumers' behavior.

Techniques for prevention and detection could be implemented on behalf of the issuer, and also on behalf of the acquirer, but the main difference is that the suspicious transaction is mostly rejected by issuer.

These are the most often used algorithms for detection of card fraud (Zareapoor, 2012):

1. A Hybrid Approach using Dempspter-Shafer Theory and Bayesian Theory
2. Blast-Ssaha Hybridization
3. Hidden Markov Model
4. Neural network

5. Bayesian Network
6. Genetic Algorithm
7. Artificial Immune System
8. K-nearest neighbor algorithm
9. Support Vector Machine
10. Decision Tree
11. Fuzzy Logic Based System
12. Meta Learning Strategy

5. RISK MANAGEMENT

Risk and uncertainty are two key terms when it comes to decision making in any institution whatsoever, and especially in banking institutions that are of special importance for this paper. The probability is the measure of randomly selected uncertainty and statistical models, used to calculate statistical risk. Financial risk could be defined as a measure of uncertainty that the buyer is ready to accept while performing financial transaction. This kind of risk is associated with payment systems and credit options offered to consumers. In the very beginning of e-commerce development, the financial risk mostly referred to those articles that hold lower degree of risk, such as books, music, clothes, and journeys. In general, prices of products are more often viewed in offline shopping mode than in case of online transactions, which carries greater risk for this kind of shopping. Newer researches show that the financial risk depends on the user age, gender, education, and marital status.

For calculating any kind of risk, a math formula, the so-called ratio is being used for creating complex models that calculate more than one ratio and their mutual dependence. Operative risk is dealing with financial transactions and all consequential events. As for the operative risk and frauds in financial transactions, banks in Serbia lack models for that kind of risk, because it is believed that the fraud level is quite low. Therefore, the risk is being regulated by introducing standards, as well as all the methods for prevention and detection of algorithms, which are described in previous chapters of this paper. The most important thing is that all events that cause some kind of fraud are reviewed under operational risk and they are given a certain ponder – it is only important to recognize and define all the events that could happen.

Banks face different types of risks, such as credit risk, market and operational risk (Li, 2013). These risks were originally managed and measured separately. However, this limit moved in time so that in 2007, when the crisis started, it was realized that these risks interact with each other and are inseparable. Banks develop quantitative risk measures that are applicable to all types of risk.

By using different methods, financial analysts create financial data available for operational risk as one of the types of financial risk, and in this way, statistical models could be applicable on operational risk. Many large banks have already started with collecting data on losses and loss measurement through operational risk. Most of them have limited time series, but in spiteof fewer number of data regarding great losses, they represent a mandatory model.

If we are to observe operations of a banking institution, we can see that the credit risk accounts with 60pct, operational risk with 30pct, and the rest goes for market risk – 10pct.

The model of operational risk is a set of functions that represents uncertain future events. The uncertainty could be the occurrence of an event, the time of occurrence, as well as the amount of loss caused by an event (Kim, 2008). The uncertainty could be represented through probability, and therefore, the model of operational risk measurement is actually the probability model.

One of the models of measuring operational risk is the Advanced Measurement Approach-AMA (BIS, 2011).

6. SOLUTION PROPOSAL

Figure 2. shows solution architecture in case when the bank as a card issuer entrusts the service of transaction processing to Processor Company, while checking if the transaction is fraud or not is entrusted to a solution proposed in this paper. The solution proposal is also given for cases when the ATM, POS and Internet transaction (through payment gateway to the bank) are initiated on bank's devices.The cards of bank the issuer could be used on these devices, as well as cards of other bank issuers.

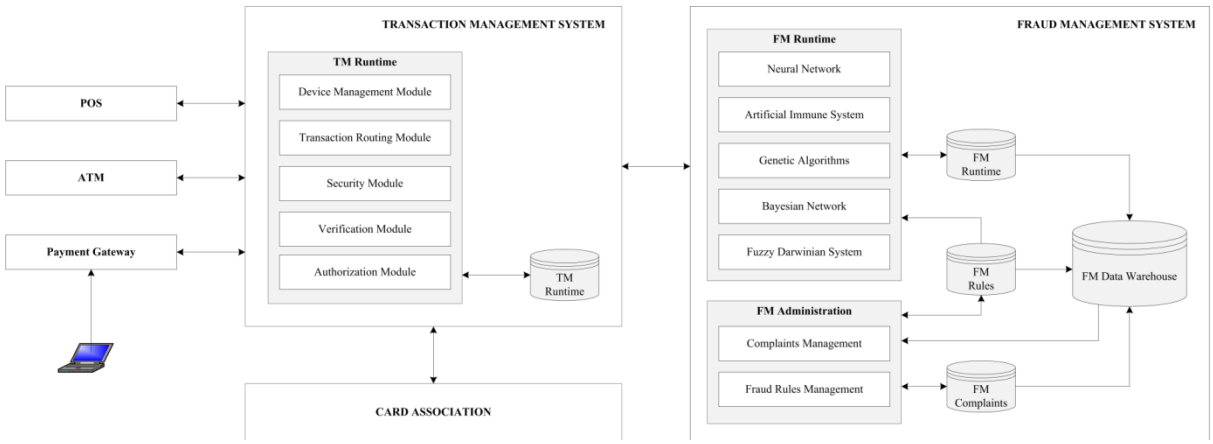


Figure 2: Architecture and software modules of proposed Fraud Management System

System components:

I Transaction Management System – TMS

1. Transaction management Runtime
   - This is a part of TMS that contains several modules that process transaction in real-time mode.
2. Device management module
   - It determines the type of the device on which the transaction is being carried out (ATM / POS/ Internet, i.e. payment gateway) and transcripts it to adequate format required for TMS.
3. Transaction Routing Module
   - Through BIN (Bank Identification Number) it determines to which bank the transaction belongs to,
   - Carries out validation of certain fields, transaction parsing.
4. Security module
   - Runs a check on PIN and decrypts encrypted elements of transaction message
5. Verification module
   - Validation of card validity, among other things, checking card expiration date
6. Authorization module
   - Checking if there's enough money on the account and authorizes the transaction
7. TM Runtime Database
   - All transaction that take place, either fraud or genuine ones, are stored in this base
   - Transactions that have been rejected in some of the modules TM Runtime are also stored.

II Fraud Management System

1. FM Runtime module
   - This module defines algorithms for detection of frauds, including Bayesian Network, Neural Network, Artificial Immune Systems, Genetic Algorithm, and Fuzzy-Darvin algorithm. These algorithms detect whether the transaction is fraud or not, because they implement defined rules within DB rules.
2. Fraud management runtime database
   - This is operating data base used by FM RT module, and which contains all data concerning the transactions that took place.
3. Fraud management data warehouse database
   - This is a DW database that helps in making decisions and serves for displaying statistical data and more detailed consideration of card owner behavior, which eventually leads to making a decision on whether the transaction is fraud or not.
4. Fraud management administration
   - This GUI can change parameters and introduce new rules in FM rules, or make new decisions on transactions based on information obtained by FM Complaints.
5. FM Rules database

- This base holds all the rules defined for fraud prevention, and in case of non-compliance with those rules the transaction is considered to be illegitimate, and this raises the alarm level. The values of parameters for those rules are defined in here.
- Visa's rules are adjusted to bank's needs
- General rules:
    - Tied to transaction location
    - If it's an Internet transaction, attention is paid to IP address
    - What's the time scope between two transactions
    - Type of account being used

- Control rules:
    - What's the BIN
    - What's the amount of transaction
    - Values for AVS, CVV – for cards with magnetic stripe, CVV2, PAN
    - User's limits
- Rules for operational risk measurement where we can monitor:
    - Risk given the territory of transaction initiation
    - Risk for merchants' activities
    - Risk given the financial effect.

6. FM Complaints database
    - In case some transaction left the system as being valid, and it turns out that there was a system error, i.e. it's a fraudulent transaction not recognized by the system, it is necessary to enter corrections into FM DW.

III Card Association

1. These are card organizations, which, in a solution presented in this paper, receive transactions from TMS, initiated by a payment card which is not issued by a bank that is in ownership of one of those devices (ATM, POS), and process them.
2. Card organizations are as follows:
    - VISA
    - MasterCard
    - Diners.

Steps with transaction processing:

1. Transaction is initiated by a device (ATM, POS, Internet transaction)
2. DMM determines the origin of the device and transcripts it to adequate TMS format.
3. After that, TRM determines the bank in question based on BIN, and if it's on-us (transaction from the card issued by a bank – issuer for which the processing activities are being done), it sends the transaction in FMS to check if it's genuine or fraudulent. In opposite, if the transaction is done with a card that belongs to a bank whose processing activities are not carried out by our processor, the transaction is sent out to Card organization for further check.
4. Once the transaction reached FMS, based on rules defined in FM Rules, FM Runtime processes a transaction by using an algorithm for fraud detection, and places executed transactions into FM Runtime operational base.
5. Upon the executed transaction, FM Data Warehouse is being loaded in real time, and updated with information from FM Complaints.
6. Based on all input streams, including reading rules from FM Rules, data Warehouse provides different types of reports which helps FM administration to change users' and system rules, and at the same time solves the problem of suspicious transactions in FM Complaints.
7. After the transaction is processed, FMS provides either positive or negative reply.
8. In case the replay was positive, the transaction is being sent for further processing to SM, together with all the necessary fields.
9. After that it is being forwarded to VM.
10. AM authorizes the transaction, or to be more precise, it checks whether there's enough money on user's account and then sends the response back to user in the form of successfully or unsuccessfully processed transaction. At the same time, it is updating TM Runtime database.

7. CONCLUSION

Over the years, we were the witnesses of greater use of electronic payment systems, but also of the attached risks. Just the same, payment cards are more and more used for shopping, while cash is used less, and the reason for this is to be found in a fact that people grow trust in the safety of these systems. Fraud systems and thefts are developing, but security measures for protection against fraud are getting better and up-to-date.

One of the directions of future research is the selection of complex algorithms that are best to be applied for modeling Fraud Management System that will be grounded on several algorithms. This FMS will apply positive features of every respective algorithm, and at the same time, it will try to eliminate their faults. On the other hand, back in the past biometrics was almost in the field of science fiction when it comes to e-commerce, while today this is something that is real and widely spread. Today, finger scanning is the most commonly used technique for determining the user identity. However, iris scanning is the future of electronic payment systems, with an aim to reduce frauds and financial losses, thus increasing the level of security.

ACKNOWLEDGMENTS

This paper is part of the project 'Multimodal biometry in Identity Management', funded by the Ministry of Science and Technological Development of Serbia, number of contract TR-32013.

REFERENCE

Aite Group (2012). Card Fraud in the United States: The Case for Encryption.

Al-Furiah, S., & Al-Braheem, L. (2009). Comprehensive study on methods of fraud prevention in credit card e-payement system, Procedings of iiWAS.

Benson, C. (2013). Russian hackers charged in biggest data breach case, 160mn credit card numbers stolen, Reuters, preuzeto sa http://rt.com/news/us-hacking-ring-charged-587/

BIS (2011). Bank for International Settlement, Basel Committee on Banking Supervision Operational Risk-Supervisory Guidelines for the Advanced Measurement Approaches, preuzeto sa http://www.bis.org/publ/bcbs196.pdf

Bogicevic, M., Milenkovic, I., & Simic, D. (2014). "Identity Management – A Survey", Palgrave Macmillan, Innovative Management and Firm Performance - An Interdisciplinary Approach, ISBN 9781137402226.

Economist (2014).The Economist, Skimming Off the Top: Why America has such a high rate of payment-card fraud, preuzeto sa http://www.businessinsider.com/why-america-has-such-a-high-rate-of-payment-card-fraud-2014-2

Godin, D. (2009). TJX suspect indicted in Heartland, Hannafors breaches, preuzeto sa http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/.

Jones, D., & Finkle, J.F. (2013). Largest Case Launched After Credit Card Info Stolen From J.C.Penney, Visa Licensee, preuzeto sa http://www.huffingtonpost.com/2013/07/25/credit-card-stolen-visa_n_3653274.html.

Kim, Y., Savoldi, A., Lee, H.,Yun, S., Lee, S., & Lim, J. (2008). Design and Implementation of a Tool to Detect Accounting Frauds, IEEE Computer Society, DOI 10.1109/IIH-MSP.2008.257.

Kou, Y., Lu, C., Sinvongwattana, S., & Huang, Y. (2004). Survey of Fraud Detection Techniques, Proceedinges of the 2004, IEEE, International Conference on Networking, Sensing and Control.

Li, J., Zhu, X., Lee, C.F., Wu, D., Feng, J., & Shi, Y. (2013). On the aggregation of credit, market and operational risks, Springer, DOI 10.1007/s11156-013-0426-0.

Lindsay (2014). America leading the world in credit card fraud, preuzeto sa http://www.nerdwallet.com/blog/current-events/america-leads-world-credit-card-fraud/

Riley, B. (2012). Card Fraud Management Systems, CEB TowerGroup , preuzeto sa http://www.fico.com/en/wp-content/secure_upload/Card_Fraud_FICO_CEB_TowerGroup.pdf

Wagenseil, P. (2014). Neiman Marcus Data Breach FAQ: What to Do Now, Tom's guide, preuzeto sa http://www.tomsguide.com/us/target-neiman-marcus-data-breach-faq,news-18199.html.

Zareapoor, M., Seeja, K.R., & Alam, M.A. (2012) Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria, International Journal of Computer Applications, volume 52, issue 3.

CASH, HASH OR TRASH - HASH FUNCTION IMPACT ON SYSTEM SECURITY

Milos Zivadinovic[1], Ivan Milenkovic[1], Dejan Simic[1]
[1]Faculty of Organizational Sciences, Belgrade, Serbia
mzdv@outlook.com, ivan.milenkovic@fon.bg.ac.rs, dsimic@fon.bg.ac.rs

Abstract: *Authentication methods present an important part of every secure system. Traditional, but still dominant authentication method is the authentication by password. In order to be evaluated, passwords have to be stored on the system. Usually, stored passphrases are protected by the use of the hash functions. The goal of this paper was to test vulnerability of commonly used hashing algorithms to password recovery attacks. Hashcat and oclHashcat utilities were used to generate password hashes. The experiment results are given, and reveal potential weaknesses in some of the algorithms.*

Keywords*: hash functions, authentication, password security*

1. INTRODUCTION

A chain is as strong as its weakest link, says the proverb. Data security presents one of the cornerstones of modern business. As the amount of data generated and consumed by a business exceeds all expectations, our processes applied to securing it must become more resilient. Identity management within an organization must be organized utmost care. An important part of the identity management process is the activity of authentication (Milenkovic, Sosevic and Simic, 2012). As passwords are still a common authentication method used today, there is a need for their secure storage. Application of hashing functions to the domain of data security becomes more of a reality due to the increase of computation power, but it comes with a cost: users have to be more aware of the authentication tokens they are using.

With that in mind, users are quickly becoming the weakest link due to the fact that they are predictable and follow specific patterns in their lives, both conscious and subconscious. This allows us to easily “break the chain” and become one step closer to accessing unauthorized data by generating a large number of hashed words and then comparing them with the actual hashed data containing user authentication tokens (e.g. passwords).

This paper tests two popular password recovery tools on a real world scenario. A standard laptop with an Intel I5 processor and a dedicated graphic card is used for the experiment. Tested algorithms were MD5, SHA 512 and BCrypt. Section 2 of paper describes the problem statement in more details. In section 3 hash functions analyzed are described in more details. Password recovery solutions used are described in Section 4. Experiment results are given in Section 5, and they are followed by conclusions in Section 6.

2. PROBLEM STATEMENT

A hash function is a function that maps an arbitrary length input to a fixed sized length message (Andreeva, Mennink and Preneel, 2015). Ideally, the mapping of data from the original set to the data from the hashed set should be bijective - one element from the original set should correspond to one element in the hashed set. According to that definition, authentication of users becomes simpler since we do not need to handle the original access token, just its hashed representation which is then compared to the stored value.

With the improvement of technology and processing power, most prominently in the GPGPU and ASIC components, previous hash functions that were deemed secure in terms of collision, become compromised. Furthermore, the usage of processing power allows us to generate large amounts of hashes in a relatively short time, thus creating our comparison set upon which we can deduce the original authentication token. This process allows us to easily discover unsafe authentication passwords, such as short passwords or passwords without a large number of possible characters (e.g. plain numeric passwords such as dates of birth) even with continuous auditing with tools such as Seraphim (Zivadinovic, Milenkovic and Simic (2014)).

What is the best way to secure our data, our identities and our means of authentication in this highly competitive environment? There are two paths that provide answers to this question. One of them is to

rapidly improve and implement new kinds of hashing functions or to improve the ones that currently exist. This can become troublesome and problematic due to the nature of hash functions and mathematical foundations which is out of this paper's scope. The other path presents the possibility of improving hash function performance in securing our identities and data by increasing the entropy of available characters used for the creation of our authentication tokens which are then hashed for comparison. Furthermore, this process allows us to drastically improve our system's security with zero infrastructure changes and minimal interventions from the users of the system, thus reducing costs both in training and infrastructure and in technical debt.

3. HASH FUNCTIONS

In general, the output of a hash function can be considered as a data "fingerprint". An important definition concerning hash functions is the definition of an "ideal" hash function. An ideal hash function maps inputs of arbitrary length to outputs of finite length, where the distribution of the outputs is uniform over a given range space (Maurer, Renner, Holenstein, 2004). The mapping should follow the principle of a random oracle, as the mapping function is perceived as a black box. The definition of an ideal hash function is mainly important because real world examples are evaluated on their differences from the ideal case.

In practice, each hash function is characterized by following attributes: collision, preimage security and second preimage (Merkle, 1979). Collisions describe situation where two different inputs produce a same output value. Preimage security is connected to the following scenario, how hard is for a potential attacker to guess which input was used to generate a known output. In second preimage attack, we have a known input. The attacker goal is to find another input which gives the identical hash value as the known input.

MD5 is a cryptographic hash function which creates a 128 bit hash value. It was introduced in 1992 by Ron Rivest as a replacement for MD4 algorithm (Rivest, 1991). Today, MD5 is not considered a very secure algorithm, as it has several deficiencies. As first, MD5 is prone to collision attacks. In (Dobbertin, 1996), H. Dobbertin provided an example of pseudo collision for MD5. (Stevens, et al) presented construction of two public certificates. Although certificates had different public keys, the MD5 hash value was the same. In (Xie and Feng, 2010) first single block MD5 collision was published.

All of the attacks described above exploit either the collision or second preimage. As a consequence, a password hashes created with MD5 should be secure against a first preimage attack. Unfortunately, MD5 algorithm is very fast, and does not require a great amount of memory space for execution. Therefore, brute force and dictionary attacks can be a threat for MD5 password hashes. These treats are relevant, as it is still possible to find MD5 used in different applications (Silent Signal Techblog, 2015).

SHA-512 and SHA-256 (*Secure Hash Algorithm*) belong to family of SHA-2 algorithms, designed by National Security Agency (NSA). Difference between SHA-256 and SHA-512 is in the size of blocks used. SHA-512 uses 64 bit words, while SHA - 256 uses 32-bit words.SHA-512 is in literature considered cryptographically secure, as best attempts at breaking preimage resistance have succeeded at 57 out of 80 rounds of SHA-2 algorithm (Khovratovich, Rechberger, Savelieva, 2012).

BCrypt is hash function based on Blowfish cipher (Provos, Mazieres, 1999). It can be adapted in order to increase computational complexity, so it has an increased resistance against brute force attacks. BCrypt is used for hashing user passwords in BSD and SUSE Linux.

4. PASSWORD RECOVERY SOLUTIONS - HASHCAT, OCLHASHCAT, JOHN THE RIPPER

Hashcat is a popular CPU based password recovery utility. It is available on *Linux/Unix*, *Windows* and *OS X* operating systems. *Hashcat* works with more than 150 algorithms and focuses on high performance. Command line is used as a control interface. Support for multiple cores is included, and *Hashcat* also allows distributed cracking. *Hashcat* allows creating different types of rules to combine dictionary and brute force attacks, needed to defeat highly iterated modern hashes. Although it was closed source for most of its history, the author of *Hashcat* has recently moved the source code to open domain.

oclHashcat uses GPU for password recovery computations. Currently, it is fastest publicly available password cracker. It supports the use of up to 128 GPUs simultaneously. As for the hardware support, all CUDA and Stream enabled cards should be compatible with oclHashcat. Simple dictionary attacks are supported (such as combinator attack), together with brute force and mask attacks. A major feature of oclHashcat is the GPU based rule engine (oclHashcat, 2016). Sometimes, copying the wordlist for dictionary

attacks can have a significant impact on performance. Using GPU rule engine, it is possible to copy a relatively small wordlist to the GPU memory and then increase it size.

Hashcat, together with *oclHashcat* was used by team *Hashcat* for several victories in row on CMIYC (*Crack Me If You Can*) contests (Korelogic Security, 2016). For example, some of the competition themes were the ability to create wordlists based on certain categories, passphrases, creating custom rules based on cracks and cracking passphrase which use non standard character encodings.

John the ripper is an another popular password cracker. It is available on several different platforms, such as *Linux, BSD, Solaris, Windows*, etc. Basic version is somewhat limited in number of supported algorithms, but community enhanced version gives access to a wider array of available algorithms, such as raw MD5 and salted SHA-512. *John the Ripper* offers some GPU support, but when compared to *oclHashcat* it is more of an experimental feature. It has some advantages over CPU based *Hashcat*, such as preprocessor, which generates multiple rules for a single source line. However, superior speed and functionalities of *oclHashcat* make this tool somewhat lacking.

5. EXPERIMENT

Experiment consisted of performing twelve iterations of brute-force attacks on above hashing algorithms, with the final goal of determining if the GPU provides advantages in figuring out very strong passwords and how the algorithms above perform when they are applied in the creation of a very large number of hashes. The passwords chosen as an example during the experiment, where every password was regenerated for the next iteration, consisted of eight alphanumeric characters, including upper and lower case letters. This was determined to be the best-practice password pattern advised by security experts due to the amount of entropy generated by the number of possible characters and the password length.

The experiment was performed under the *Ubuntu 14.04* GNU/Linux operating system, running on a *Lenovo Y500* laptop, equipped with *Intel i5 3230* CPU and *Nvidia GT750m* graphics card. Software used for performing the experiment was *hashcat* and *oclHashcat*.

Following results present mean values of all twelve iterations both on *hashcat* and *oclHashcat*. These results may and will vary according to different CPU and GPU configurations, due to the fact that the experiment was performed on previous generation hardware laptop that was considered to be average in terms of consumer usage. The metric "*Number of hashes per second*" represents the generation and comparison of hashes to the hash we are trying to collide with.

Table 1: Comparison of algorithms and their performance on different hardware

Algorithm	CPU/GPU	Number of hashes per second (lower is better)	Estimated time
MD5	CPU	37 million	250-300 days
Bcrypt	CPU	75	Over 10 years
SHA-512	CPU	690	Over 10 years
MD5	GPU	847 million	90 days
Bcrypt	GPU	68	Could not estimate
SHA-512	GPU	23.315 million	9 years 1 month

We can see from the above table that, in general, MD5 performed the worst in both CPU and GPU tests, where the GPU brute force attack provided more than twenty times better performance. This confirms that MD5, as a legacy algorithm, should be avoided at all costs.

One more interesting thing is the performance of the BCrypt algorithm experiment which was ten percent worse in number of hashes when performed on the GPU. Main reason for this anomaly is hidden in the fact that BCrypt requires a lot of memory accesses, which must be pipelined through the CPU when the brute force attack is being performed on the GPU, thus increasing the number of intermediate steps in generating the hash that is being used for comparison.

SHA-512 gives us drastic improvements when it is being attacked using the GPU, which, in turn, opens questions of its ability to provide a secure mechanism of hashing in modern business.

6. CONCLUSION

Even though the experiment performed is highly reliant on underlying hardware, we can safely conclude several things. One of them is that BCrypt presents significant advantages over SHA-512 and MD5 hashing algorithms. According to that, BCrypt should be used in place of SHA-512 and MD5 algorithms, where it is possible. SHA-512 can potentially provide better performance than BCrypt, but this statement requires more data to be either proved or disproved.

Next, we can safely conclude that eight character passwords which contain alphanumeric characters are a safe bet against brute force attacks, and in some way, adequate protection against dictionary attacks (due to the ability that dictionaries do not contain numbers paired with words, while implementing checks for numbers transforms the dictionary attack into a brute force attack). Additional improvements to the safety of algorithms can be added by implementing password salts, adding an additional layer of security to the hash by transforming it according to random data which is used later, in a reverse process, to reconstruct the hash.

It would be interested to note the performance of these algorithms on machines with much more performant hardware, including CPU and GPU clusters augmented by high frequency RAM. Also, extending the experiment to cover the winner of PHC (Password Hashing Competition) - Argon2 (“Password Hashing Competition”, 2016) and to include other PHC finalists, due to their novel design and possible improvements over BCrypt.

REFERENCES

Andreeva, E., Mennink, B., Preneel, B. (2015). Open problems in hash function security. Designs, *Codes and Cryptography, 77(2), 611-631*, http://dx.doi.org/10.1007/s10623-015-0096-0

Dobbertin, H. (1996). The status of MD5 after a recent attack. *CryptoBytes,2(2).*

Khovratovich, D., Rechberger, C., & Savelieva, A. (2012, March). Bicliques for preimages: attacks on Skein-512 and the SHA-2 family. *In Fast Software Encryption, 244-263*. Springer Berlin Heidelberg.

KoreLogic Security. Crack me if you can, offical web page. *Retrieved from http://contest.korelogic.com/. Last visited 04/15/2016*

Maurer, U., Renner, R., & Holenstein, C. (2004). Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. *In Theory of cryptography, 21-39*. Springer Berlin Heidelberg.

Merkle R.C (1979). Secrecy, Authentication and Public Key Systems. *Ph.D. thesis, UMI Research Press*, Italy

Milenković, I., Šošević, U., & Simić, D. (2012). Architectures of comprehensive identity and access management. *Presented at Electronic International Interdisciplinary Conference, Proceedings of the EIIC,*

ISSN:1338-7871, ISBN 978-80-554-0551-3.

oclHashcat. Official project wiki. *Retrieved from https://hashcat.net/wiki/doku.php?id=oclhashcat, Last visited 04/15/2016*

Password Hashing Competition. (n.d.). *Retrieved from https://password-hashing.net/, Last visited 04/15/2016*

Provos, N., & Mazieres, D. (1999, June). A Future-Adaptable Password Scheme. In *USENIX Annual Technical Conference, FREENIX Track, 81-91*.

Silent Signal Techblog. (2015). Poisonous MD5 - Wolves Among the Sheep. *Retrieved from https://blog.silentsignal.eu/2015/06/10/poisonous-md5-wolves-among-the-sheep/*

Stevens, M., Karpman, P., Peyrin, T. (2015). Freestart collision for full SHA-1. *Retrieved from https://eprint.iacr.org/2015/967.pdf, Last visited 04/15/2016*

Rivest, R.L. (1991). The MD4 message digest algorithm, *Advances in Cryptology, Crypto’90, Springer-Verlag, 303-311.*

Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A., & De Weger, B. (2009). Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. *In Advances in Cryptology-CRYPTO 2009 (pp. 55-69). Springer Berlin Heidelberg.*

Xie, T., & Feng, D. (2010). Construct MD5 Collisions Using Just A Single Block Of Message. *IACR Cryptology ePrint Archive, 2010, 643.*

Zivadinovic, M., Milenkovic, I., Simic, D., Seraphim: Linux kernel module for resource management and command execution. *Presented at Symorg 2014, Zlatibor, Serbia*

GIS IN BUSINESS MANAGEMENT

Mirjana Kranjac*[1], Uroš Sikimić[2], Srđan Tomić[3]
[1]University of Novi Sad, Faculty of technical sciences, Novi Sad,
[2] Singapore management university, Institute of Innovation and Entrepreneurship, Singapore
[3]University Nikola Tesla, Faculty for engineering management, Belgrade, Serbia
*Corresponding author, e-mail:mirjana.kranjac@uns.ac.rs

Abstract: *Nowadays, fast and effective decisions are the main request for the management staff in order to achieve company's sustainable development. Geographic information systems (GIS) are suitable ICT tool for management. GIS offers possibility to visualize spatial data and to make decisions faster. The authors are dealing with the problem how to improve internal communication within company. They are proposing application of GIS within company's communication what will bring benefit to the management teams in sense of more effective governing of their companies within the turbulent, changeable time. Their research, elaborated within a production company, proved that GIS contributes to better understanding between teams within company and to more effective decision making process when used for internal communication.*

Keywords*: GIS, business management, meter spatial information system, spatial data, visualization*

1. INTRODUCTION

Geographic information systems are a group of software useful to solve problems within many sectors of human activities. They are used in all areas which are dealing with spatial, georeferenced data. First implementation of GIS was by geographers and surveyors. They were designing different sorts of maps.
The scientists are conducting researches of various topics with GIS (Goodchild, 2010). They are presenting data into the maps, placed to their locations according to their coordinates, and separated into the more layers for doing investigations. Business subjects are implementing GIS with the goal to increase their profit. With GIS they do the following (Cheng, Li & Yu, 2007):

- Market research by:
- ✓ looking for the optimum locations of the headquarters, offices, distribution centers, selling points,
- ✓ analyzing trading possibilities, finding right empty niches for their products and services, (Moon, Lee, Ryu & Oh, 2014) and

- Marketing of products and services by:
- ✓ Presenting spatial distribution of consumers, distribution of customer's groups by their age, frequency of cooperation with the company, type of purchased products/services, results of surveys on customers' satisfaction etc. (Li, Kong, Pang, Shi, &. Yu, 2003), (Heywood, Cornelius & Carver, 2006).

Public utilities visualize utility infrastructure, maintenance centers, and malefactions locations, do project designs, prepare maps for the maintaining staff and doing new investments (Esri report, 2008).

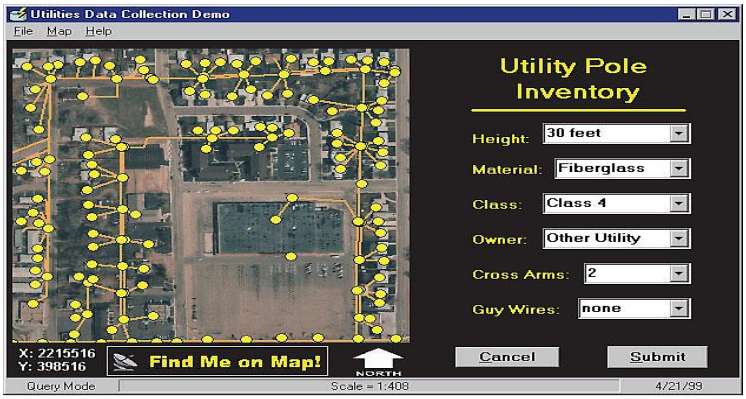


Figure 1: GIS in utility company. Source: http://www.esri.com/what-is-gis/who-uses-gis#utilities_panel

Prerequisite to utilize GIS software is to have data with geographic coordinates what enables their location on the maps. GIS maps consist of layers (Perry, Hakimpour, Sheth, 2006) which can be seen at the same time such enabling cross cutting of various data and watching them at the same time. Much less companies use GIS for solving management problems of companies and for decision making process. In some USA companies there are departments specialized in using GIS:

- for the problems solving (Esri in industry, 2015).

Utilization of GIS in such activities demands logical analyzing of problems and their decomposition into the spatial segments which are layers in GIS application. This process requests good experts knowing problems and their logical flows, as well as good experts of GIS presentation and if needed, experts for WEB surroundings. GIS enables viewing of decomposed layers and their overlapping which gives good platform to follow data influences, observe some significant inter-effects and to decide about problems' solutions (Kumar, 2013). Even, when problems are solved, new data are put into the layers and new effects can be again visualized and analyzed. This enables timely reactions and following the data changes through the time (Fu & Sun, 2010), (Kranjac, Sikimić, Dupljanin & Tomić, 2015).

The sector which is not covered by the use of GIS is business process management (BPM). Namely, BPM is a management discipline which integrates strategy and goals of a company with expectations and needs of customers in the way that "end to end" process is in focus. BPM includes policies, goals, culture, structure, IT to analyze, design, implement, permanently improves and compose good governing within "end to end" process in a company (Benedickt, Bilodeau, Vitkus & Powell, 2013). GIS is underestimated as ICT tool for visualization of existing business processes with their bottlenecks and milestones. GIS could enhance decision making process to company's management. GIS could be effectively involved as an ICT tool in:

- Meetings which should bring quick decisions
- Clear presentation of different business scenarios to the management
- Convincing the management into proposed solution
- Presentation to employees the situation
- Inform employees to know different scenarios of future development
- Proving what were good or bad solutions from the past (Burger, 2006).

These all should be done by GIS visualization much quicker than with other tools, because "an image is much more worth than thousand words".

The authors of the paper tackle the problem how to improve communication within actors of production process: management team and workers, by using geographic information systems. They are analyzing problem of workers' productivity by introducing spatial factors. Namely, spatial factors explain reasons of different productivity at the same type of machines within production plant. Reasons for differences can be discovered only when internal communication between management and workers runs smoothly. Spatial visualization created with GIS facilitates this good understanding (Kranjac, Sikimić, Vučinić &Trubint, 2015).

The authors want to prove that involvement of GIS applications into the dialogue between management and workers will bring better short-term outputs and long-term results of the companies and to prove the hypothesis that GIS can improve effects of the dialogues inside the company what brings total improvement of decision making process and better integral indicators of company's success.

2. LITERATURE OVERVIEW

Gaining competitive advantage is the main goal of the companies' management which will make company sustainable at the regional, national or international market or all of them. Growing number of corporations are looking for the ICT solutions which will enhance their functioning. The very important segment within companies is the way of communication between various groups: board members, management staff, employees in different departments, workers and the external world. External world are as the most important: costumers of products and services, distribution centers, dealers, financial institutions, logistic support points, marketing companies etc. Fast and clear communication without artifacts', confusions and conflicts makes company faster growth, easy functioning and spreading. Visualized data bring much more information into the communication process than any other type of data. This is even more important when one takes into account that companies' owners are not always experts from the area of organization activities and they need simple and exact explanations enough well presented to bring easy and right decisions.

GIS and data visualization as analytical and decision support packages are recognized as powerful tool in

corporations. When dealing with big data, what is usually the case, GIS contributes to the intuitive comprehension of big data. This enables bringing fast solutions. The experts who are preparing GIS presentations must identify crucial variables. Than GIS will help them in analyzing relationships between the significant factors. In some cases, when applications are user friendly and/or in put in web platform they enable end users investigations which they do by themselves (http://fargeo.com/blog/gis-and-big-data-visualization/). Sometimes, maps or layers made with GIS are too complicated, in too many colors what could make them incomprehensible for users who they are prepared for. This is a risk which new technology brings, that with desire to use it with more power, it could be turned into its opposite. Risks of GIS could appear during customization and integration. Sometimes layers could be visually overwhelmed what brings unclear vision to the users and even can confuse them. Deep analyzing process, careful approach and serious studding are inevitable when using GIS (Gioules, Hannmann Jodi-Lee& Evan Sullivan, 2010).
Some authors present a comprehensive approach for computing of navigation for an indoor space. They focus on a single floor, but the work is easily extensible to multi-level spaces. This is a small example of using GIS to solve some organizational problems. They use a formal model and combine map with geometric and semantic information. The program takes as input the building plans with geometric structure of the floors and semantics of the building and connects with GIS mapping (Yang and Worboys, 2015).
In some cases GIS is a mean for the interchange of information between departments what is shown in some papers. Such use is fostering horizontal connections between departments and it enables better understanding of “the whole picture of the comapany“. Use of GIS when analayzing efficiency of a company, a postal enterprise, is described in paper of Kranjac, Sikimić & Vujaković, 2015. The authors explain some maps which reflects efficiency and productivity data within the postal department in JP PTT „Srbija“.

3. CASE STUDY: GIS WITHIN COMMUNICATION PROCESS IN ENTREPRISES

Authors of the paper wanted to find GIS solutions which would enhance dialogue between:

- management staff and workers.

The goal was to improve companies' results. For this reason they explored a production company with 10 employees, 7 working on machines, in the production plant. They researched two problems:

1. problem of machines’ productivity and
2. problem of employees’ productivity.

They did following calculations:

Machine productivity = number of produced parts per machine per hour
Employee productivity = number of produced parts per employee per hour

These calculations are usual measures of production effectiveness. To better analyze and understand the situation, authors included the geographic position, actually locations of machines, as an important factor to analyze input elements of production’s productivity. Data are presented in GIS layers what enables better understanding of problems.
The maps made in GIS can show different aspects of the quality and work’s results and assist management to present this to workers on a visualized way, more understandable to workers.
The following example explains GIS maps which were used for the discussion between management team and workers about productivity of production process and reasons of the differences between workers/machines’ results.
First example shows visualized data about productivity. The second example implements new factors which explain differences of production productivity elements, which workers pointed out and which are coming from their experience and explanations. These new spatial factors are described as bottlenecks in the process of taking input material for the machines. By simple actions they could be reduced or completely canceled and thus total productivity could be increased.

Example 1.

Figure 2. presents placement of machines in one manufacturing plant of the company. There are 7 machines in it and they are marked with labels: A, B, C, D, E, F and G.

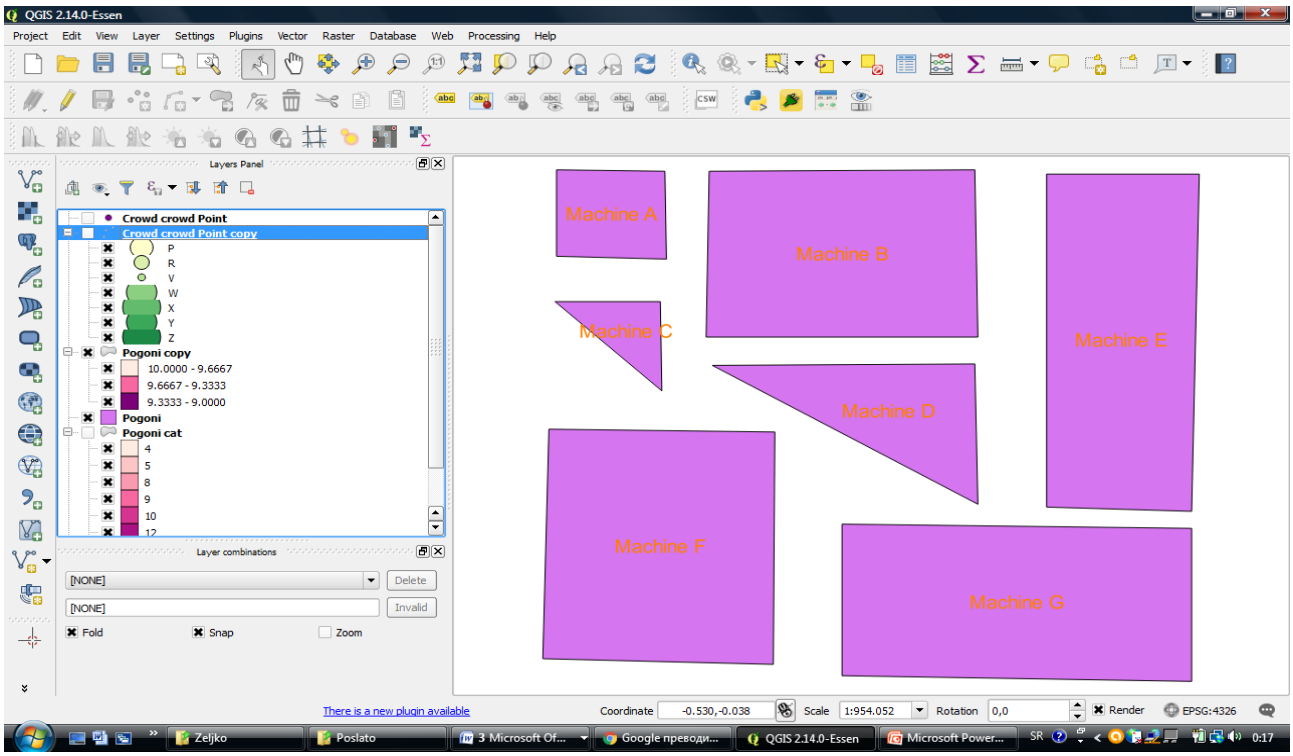


Figure 2: Plan of the machines in a manufacturing plant. Source: authors

In next Figure 3. are shown machines in different colors in such way that colors are sorted to the value of machine's productivity per one hour. The darker color, the more productive of the machine. The most productive is machine marked with A, with 12 produced pieces per hour and the least productive machine is labeled G, with 4 produced pieces per hour.

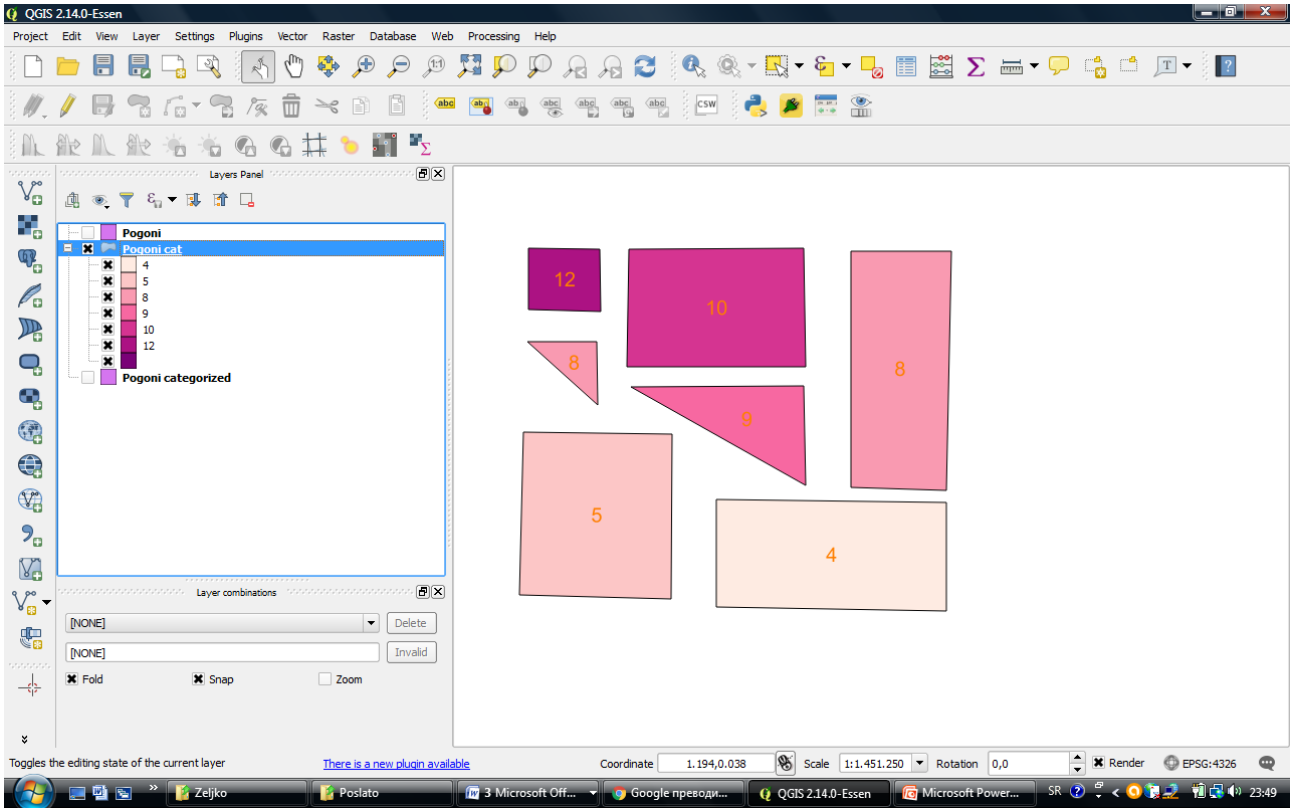


Figure 3: Colors ranged according to the machine productivity. Source: authors

Example 2.

This example shows the new factor which influences workers during their work on machines. Use of GIS map, in this case, is a tool for workers to explain their problem to the management. The circle's size presents

the bottlenecks for the movement of workers when they are taking input material for production. The spatial plan of machines or location of input materials, should be changed. GIS map is the best way to make the problem understandable to the management, by visualizing it. Namely, at Figure 4, the size of the circles and their color present the intensity of the problem which the workers have when they are moving through the production plant. If the color is darker and the circle's size is bigger, the problem is more expressive.

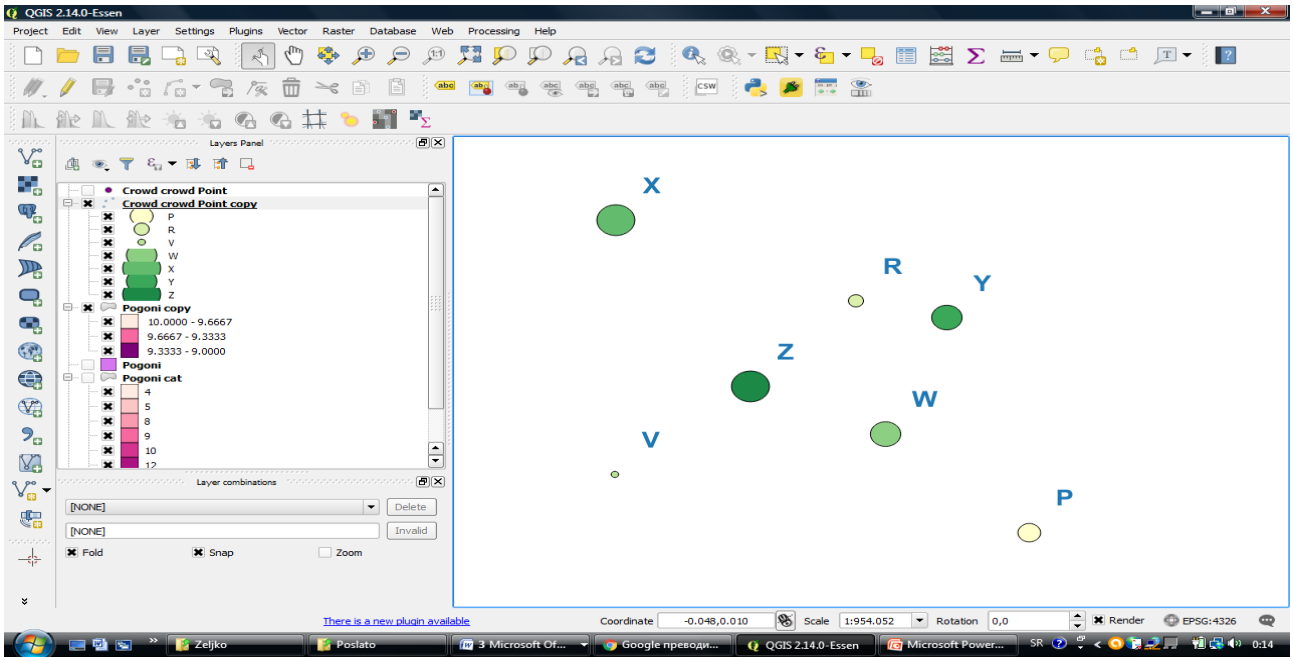


Figure 4: Bottlenecks in the manufacturing plant of the researched company, visualized by size and color. Source: authors

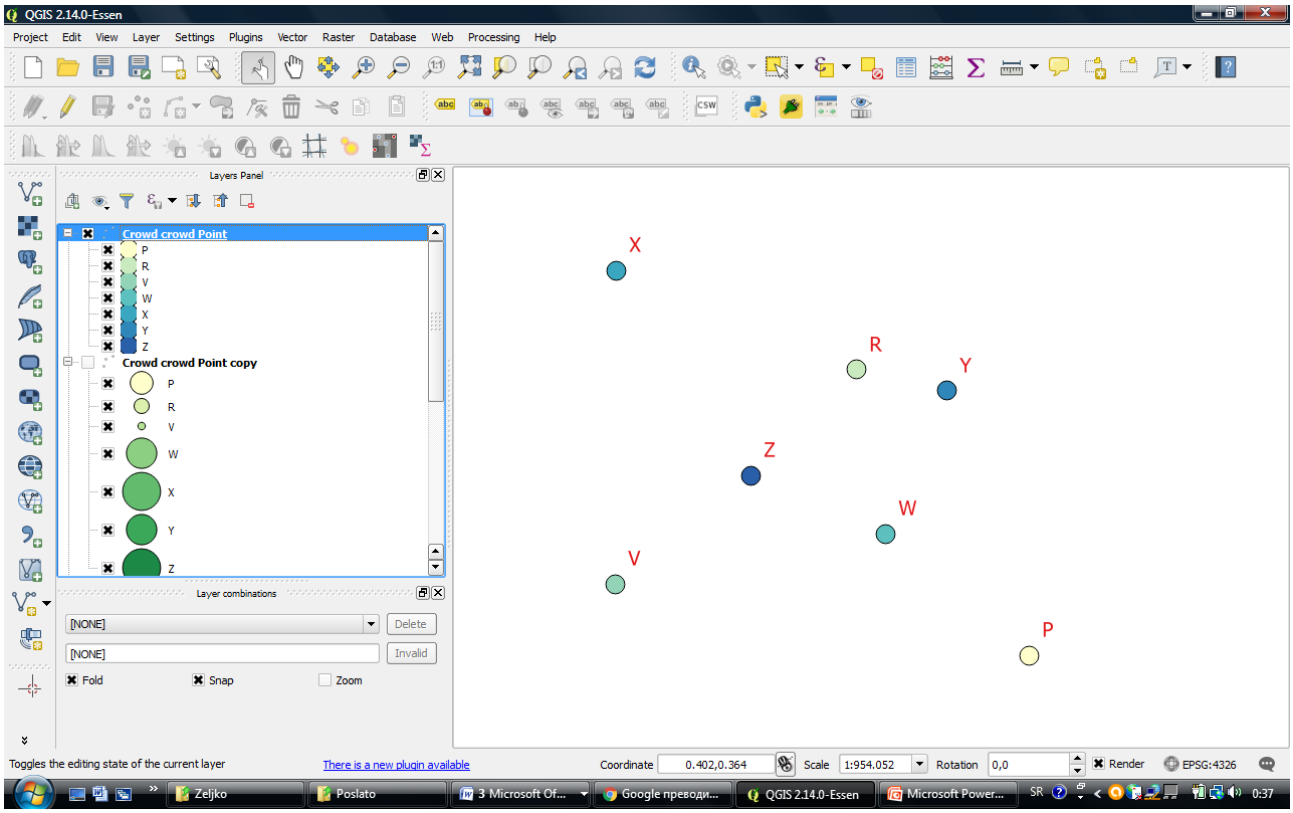


Figure 5: Bottlenecks in the drive of the researched company visualized by color. Source: authors

Figure 5 is less expressive; it presents the information only by color, and not by size of the circle.
Both examples show contribution of GIS in the process of communication within groups which are participants in the processes within companies.

4. TESTING RESULTS OF THE CASE STUDY

The maps described in examples 1 and 2 are results of authors' research. Maps are results of discussion between authors' team and two groups from the explored company: workers and staff members. Problems presented in examples were problems which these two groups from the company wanted to clarified and solve.

GIS maps were elaborated according to their demands. After the GIS maps were done, authors wanted to measure the effects of their use to the groups and made a survey. The results of survey made for workers are presented in Figure 6. The question was: "How do you assess the contribution of GIS maps to better communication between workers and management?"

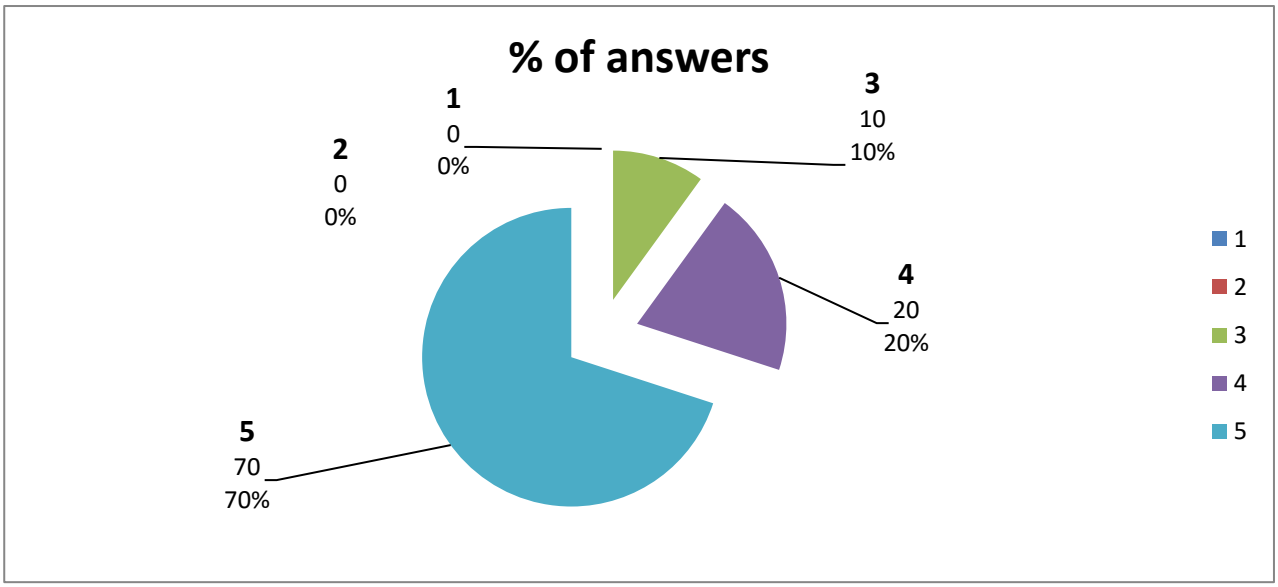


Figure 6: Assesment of workers (1 is the worse, 5 is the best). Source: authors

The results of survey made for management staff are shown in Figure 7.

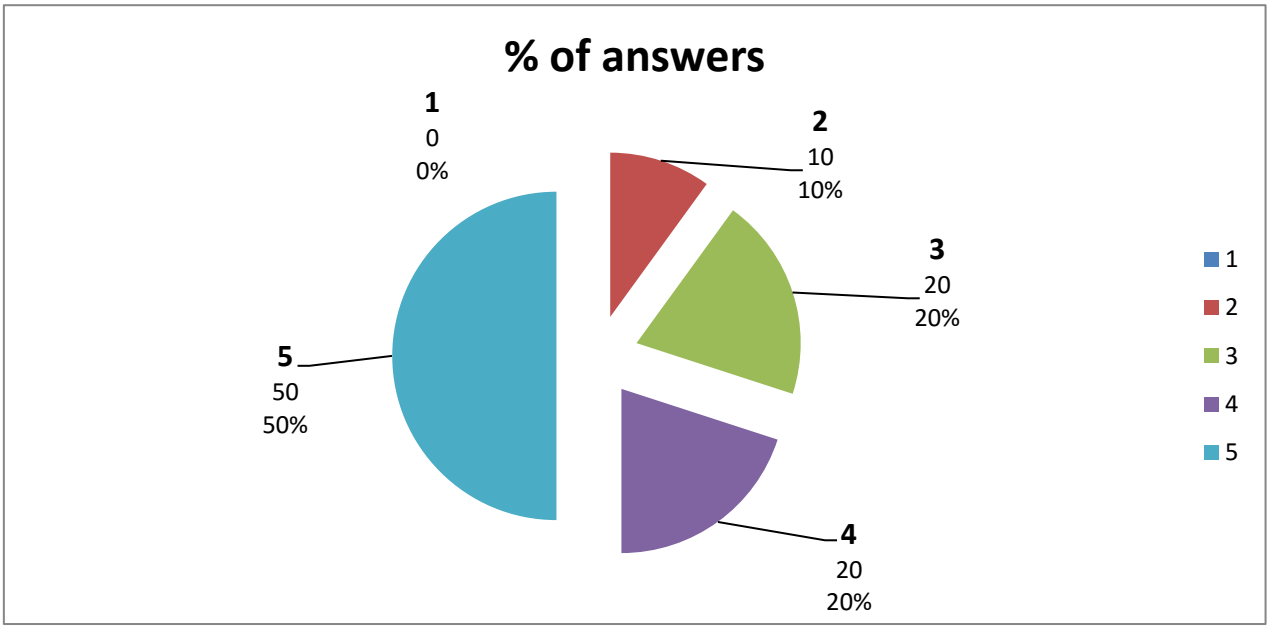


Figure 7: Assesment of management staff (1 is the worse, 5 is the best). Source: authors

The results show that management staff was less satisfied by the use of GIS maps, than workers. They had more doubt and have to be more trained about GIS and convinced of its usefulness.

5. CONCLUSION

The paper presents preparation for the meetings between management and workers enhanced by the use of GIS. GIS shortens their duration and improves the dialogue atmosphere. Authors' case study and survey prove the proposed hypothesis that GIS can improve effects of the dialogue inside the company and improve communication effects and business results.

The authors' scientific contribution is implementation of spatial information into the productivity problems that were subject of the internal communication. Spatial information is the digital connection between location, people and activities.

They presented use of an ICT tool, GIS software, in business management. Besides geographic information system which use is for larger spaces, authors introduce a sub GIS dimensions (defined by the accuracy of GPS), which are used in smaller spaces, like: production plants, logistic centers, laboratories,... This leads to the nano spatial management system which is dealing with nano dimensions.

Research should be continued and diversified to other factors of business management process with spatial components which were not analyzed before and which can bring improvement of business results.

REFERENCES

Benedickt, T., Bilodeau, N., Vitkus, P., Powell, E. (2013). BPM CBOK Version 3.0: Guide to the Business Process Management Common Body Of Knowledge, ABPMB, ISBN-13: 978-1490516592

Burger, A. (2006). GIS, Part 3: Making the Most of Your Enterprise Data", *E commerce Times*. http://www.ecommercetimes.com/story/53544.html

Cheng, E., Li, H. & .Yu, L. (2007). A GIS approach to shopping mall location selection, Building and Environment, 42 (2), 884-892.

ESRI Report, 2008, Retrieved from http://www.esri.com/news/arcnews/summer08articles/usps-fights-crime-with.html

Esri in industry (2015). Available: http://www.esri.in/industries/government/egovernance

Fu, P. & Sun, J. (2010). *Web GIS: Principles and applications*, ISBN:158948245X 9781589482456, Esri Press, New York, 25-28.

Garnett, R, Kanaroglou, P. (2016) *Transactions in GIS*, Volume 20, Issue 1, 1–159, John Wiley & Sons Ltd, New York

Gioules , M., Hannmann Jodi-Lee, L. & Evan Sullivan, S. (2010) Sustainable transportation mapping, Worcester Polytechnic Institute

Goodchild., M. (2010). Twenty years of progress: GIS science in 2010, *Journal of Spatial Information Science*, 12-13.

Heywood, I., Cornelius, S. & Carver, S. (2006). *An Introduction to Geographical Information Systems*, (3rd ed.), Essex, England: Prentice Hall, 230-232, 2006.

Kranjac, M., Sikimić, U., Dupljanin,Dj. & Tomić, S. (2015). Use of Geographic information systems in analysis of telecommunication market, *Proceeding ICIST 2015*, Kopaonik, 303-308.

Kranjac, M., Sikimić, U and M. Vujaković, Model for calculation of post service efficiency by using GIS", *Proceeding Mipro 2015*, Opatija, ISBN 978-953-233-083-0, 353-359.

Kranjac, M., Sikimić, U, Vučinić, M. & Trubint, N. (2015). The use of GIS in the model of implementation of the light train transport in Novi Sad, *Conference Towards a human city*, Novi Sad, FTN, ISBN 978-86-7892-541-2, 124-130.

Kumar, A. (2013). Participatory GIS for e-governance and local planning: A case study in different environments on its applicability, *Proceeding of Centre for Study of Regional Development*, New Delhi, India.

Li, H., Kong, C., Pang, Y, Shi, W. &. Yu, L. (2003). Internet-Based Geographical Information Systems System for E-Commerce Application in Construction Material Procurement, *Journal of Construction Engineering and Management,* Vol. 129, No. 6, 689-697.

using 3D GIS Information, *International Journal of Information Technology & Computer Science*, Volume 14 Issue No 1, 25-33.

Perry, M., Hakimpour, F. & Sheth, A. (2006). Analyzing theme, space and time: An ontology-based approach, *Proceeding: ACM International symposium on Geographic information systems* , 147–154.

Yang, L., Worboys, M. (2015). Generation of navigation graphs for indoor space, *International Journal of Geographical Information Science*, Volume 29, Issue 10, 1737-1756, Taylor&Francis, New York

Retrieved from http://www.esri.com/what-is-gis/who-uses-gis#utilities_panel

http://fargeo.com/blog/gis-and-big-data-visualization/ Retrieved: 2nd. March 2016

PROSPECTS AND TRENDS IN THE DEVELOPMENT OF TELEMEDICINE

Marina Jovanovic Milenkovic[1]*, Dejan Milenkovic[2], Slobodan Ristic[1]
[1]Faculty of Organizational Sciences, University of Belgrade
[2] Serbian Armed Forces General Staff
*Corresponding author, e-mail: marinaj@fon.bg.ac.rs

Abstract: *The telemedicine has emerged middle of the last century but its implementation has just begun with introduction of the information - communication technologies. Information-communication technologies led to the fact that telemedicine is applied effectively, efficiently and with better quality. In European countries, telemedicine has developed with a different tempo. The paper describes the development of telemedicine trends during 2016, such as: Expanding Reimbursement, International connectivity and Arrangements, Continued Momentum at the State Level, The increase in telemedicine services in hospitals, Using Technology to improve care and reduce costs. The paper provides an overview of the application of telemedicine services in Europe and in Serbia, also the prospects of further development.*

Keywords*: health system, information - communication technologies, telemedicine, trends in development, telecardiology*

1. INTRODUCTION

The health system is one of the most complex systems of any country. The goal of health care system is a healthy population. In order to achieve the objective, the health system has experienced many changes. These changes relate to the introduction of the informational and communication technologies (ICT). ICT have led to the development of telemedicine services (Jovanović Milenković, Jeremić, Martić, 2014). Telemedicine aims to provide advice and support, and to reduce the chances of illness or injury. This paper gives an overview of trends in the application of telemedicine during 2016.

2. TELEMEDICINE

The primary goal of any health care services for the population is security, health and longer living. Prevention often reduces the need for treatment. Telemedicine therefore seeks to provide advice and support, and to reduce the chances of illness or injury. Historically, technology has evolved over the centuries to give the population a better future. That is why greater interest is to improve medical and health technology and to provide more efficient and accessible services to as many people as possible.

Medical and health technology is being used by everyone: patients, doctors, health care workers, end-users, engineers, clinicians and hospitals, etc. Health services are no longer restricted to be provided in certain locations such as clinics and hospitals, but communication technologies are transferred to users who are on the move or at home. Caring for the community is to assist people with disabilities, taking care of children and the elderly, treating sick or injured, as well as support to vulnerable individuals.

Telemedicine is a combination of information and communication technology, multimedia and computer networks for the transfer of medical data. The word telemedicine is composed of the Greek words *tele* which means distance and the word *medicine*, which means the medicine at a distance.

Today in the world there are following definition of telemedicine:

- In the journal The Telemedicine Information Exchange (Brown, 1996) defines telemedicine as the use of electronic services for the transfer of medical data from one side to the other through the Internet, phones, computers, satellites or video conferences in order to provide health care services.
- Author Reid (1996) defines telemedicine as a use of complex technology for the exchange of information of health and health service delivery, where there are geographical, temporal, social or cultural constraints. Telemedicine involves the use of informational and communication technologies, and two-way interactive audio/video connection and a computer. This allows the provision of health services to distant patients. This facilitates the exchange of information between primary care physicians and specialists who are far from each other.

- Telemedicine is extending health services to remote and exchange medical information using the information-communication technologies. Its meaning is broad and includes activities such as prevention and disease diagnosis, treatment, medical education of users, research and evaluation in medicine. The application of telemedicine beyond the physical, temporal, social, and cultural barriers. It reduces the potential time and cost of transportation of the patient to the doctor, or the doctor to the patient. The emphasis in telemedicine is the transmission of information between doctors and health care users.

Among these variations of the definition, there are several things that are common. First, the definition of the term was created in the 1990s. Secondly, it has been providing different kinds of medical services from a distance using information and communication technologies. The most important aspect of telemedicine is quality, because the diagnostic and therapeutic quality improves. It also allows early detection of adverse effects of the applied therapy.

In recent years, with the introduction of internet technologies, telemedicine is more developed. In the health system, telemedicine has experienced growth in all branches of medicine. On the global market, every country has done a lot on infrastructure development (Kamsu-Foguem, Tiako, Fotso, Foguem, 2015).

3. TRENDS IN THE DEVELOPMENT OF TELEMEDICINE

3.1. Development factors of telemedicine

Services of telemedicine are experiencing big growth in health systems both in developed countries than in developing countries (Ekeland, Bowes, Flottorp, 2012). But it has not being developed in all countries equally. Diversity emerged depending on the level of development of the country (Boubacar Traore, Kamsu-Foguem, Tangara, 2016). In developed countries, the country is faced with the following problems:
- An increase in the elderly population;
- Increased costs of technologies that provide medical services
- Patient expectations are higher
- Economic and social changes.

Their problems have led to disparities in the provision of health services. State governments have tried to solve this problem in two ways: through tax increases and increased costs of providing health services. Given the complexity and sensitivity of the problem, the only solution that arises is through a variety of telemedicine services, reduction of costs.

The key factors that have helped the development of telemedicine (Norris, 2001):
- Expanded access to health services;
- Health care for the population who is constantly traveling;
- Military applications;
- Tele-home care;
- Reduction of costs;
- Market Development;
- Health Policy and Strategy

Expanded access to health services
Expanded access to health services includes access to health services of individuals who live at a great distance from large urban centers. They are motivated to use telemedicine services. Some parts of Australia and America are examples where residents do not have proper medical specialists in the environment of life and apply these services. Also, these services are intended for the handicapped, the elderly and people who have mental difficulties.

Health care for the population who is constantly traveling
Telemedicine is an important factor in the health insurance department. Some examples can be sailors, who spend their life time at sea. In these circumstances, radio connections play a big role to provide medical advice for many years. Transfer of ECG, X-ray images and video conferencing can greatly help a patient who at that time seeks medical assistance. Similar problems may happen to astronauts or passengers while being on flights.

Military applications
Military insured person who is in the inaccessible terrain may seek medical care supported by applications. Video conferencing is the best way to communicate with the military insured.

The US military applied system *Primetime I11*, which provides an opportunity for health care, regardless of geographic location. This approach has been used by the troops who took part in the NATO operation in Bosnia and Herzegovina.

Tele-Home Care
Tele-Home Care is designed to provide medical care for the elderly. In 1998, there were 380 million people who have had more than 65 years. That number is growing all over. Two thirds of the population older than 65 years are living in developed countries.

Increasing the number of older population also leads to changes in diseases. The application of tele home care, leads to every patient and care of his health, but at the same time reducing the costs of hospitalization, which is very expensive and the arrival of a doctor on a home visit. Home visits are replaced with tele-visit.

Costs reduction
The application of telemedicine put an influence on reducing some of the costs in the health system. The costs include costs of arrival and departure physician home visits, reduce medical and economic costs that can occur when a specialist works in the rural areas.

Market development
A few years ago the world has been using only analog signals during data transfer. Today, digital signals are applied in telemedicine.

Health policy and strategy
Each country should adopt a health policy and future strategy of applying telemedicine in its country. Adequate strategy makes it possible to do the infrastructure required for the provision of such services.

3.2. Trends in telemedicine during 2016

The global telemedicine market will become larger at a compound annual growth rate of 14.3 percent through 2020. It is anticipated to reach $ 36.2 billion. During 2014 there was a $ 14.3 billion (Lacktman, 2015). According to some authors, these five trends will drive telemedicine's continued growth and transformation of health care delivery in 2016:

- Expanding Reimbursement
- International connectivity and Arrangements
- Continued Momentum at the State Level
- The increase in telemedical services in hospitals
- Using Technology to improve care and cut costs

1. Expanding Reimbursement
Private and state institutions continue to develop telemedicine services. This will lead to better service delivery and will lower the cost. The main obstacle in providing health services were cost. But changes in the law will lead to a reduction of these costs.

2. International connectivity and Arrangements
In 2016, hospitals and health services will have to establish ties overseas medical institutions. In this way, knowledge of health care expands abroad. This cross-border partnership will allow access to a larger number of patients, to generate additional income. According to the American Telemedicine Association, more than 200 academic medical centers in the US already offer video-based consulting in other parts of the world. While many of these are pilot programs, 2016 will come to the commercialization of the majority of those treaties. The increase of a purchase power happened in the middle class population in countries such as China, and also the opportunities for growth is in Western medical centers.

3. Continued Momentum at the State Level
State authorities are working on the implementation of telemedicine services. Many states have passed laws that provide health care services via telemedicine, during 2015.

4. The increase in telemedical services in hospitals
A recent study found that more than 35 percent of employers with onsite health facilities offer telemedicine services, and another 12 percent plans to add these services in the next two years. Other studies suggest that nearly 70 percent of employers will offer telemedicine services as an employee benefit by 2017 (Lacktman, 2015).
Additionally, consumers are increasingly willing to visit retail medical clinics and pay out-of-pocket for the convenience and multiple benefits of telemedicine services when telemedicine is not covered by their insurance plans.

5. Using Technology to improve care and cut costs
Using technology and Internet, 2016 will be the year of telemedicine. In that way, the costs will be so the patients would take the best health services.

4. PROSPECTS OF TELEMEDICINE SERVICES

4.1. Prospects of telemedicine services in Europe

Telemedicine applications are constantly growing. The following figure 1, according to research, is done for Europe (Somsainathan, 2011). It was noted that telemedicine in Europe is mostly applied in the UK. The second place is Germany, and then Scandinavian countries. Teleradiology is used 66% in the UK and Scandinavian countries, while services in Telecardiology are highest in the UK with 6%.

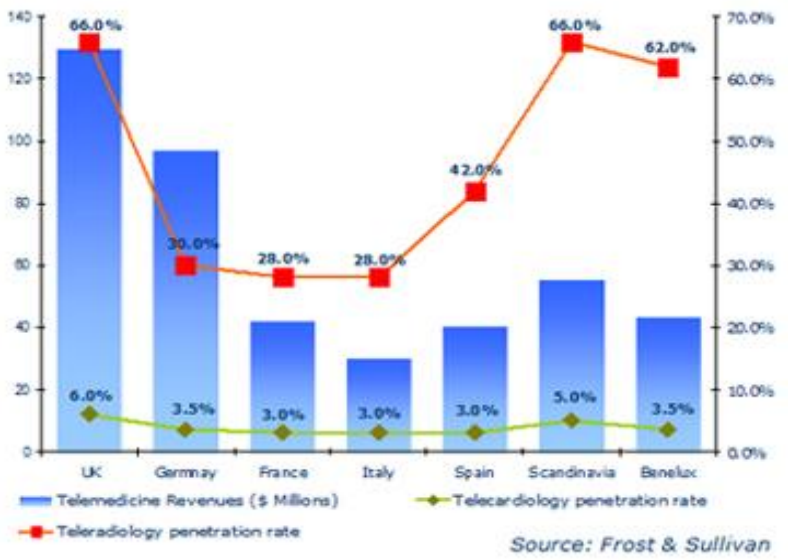


Figure 1. Application of telemedicine in European countries (Somsainathan, 2011)

According to a survey done in 2013, it is considered that the use of telemedicine and its services is increasing every year (UCLA, 2013). The study referred to the consideration of the parameters that affect the application of telemedicine. The period of time is perceived from 2005 to 2013. On that basis, forecasting is done of the application in telemedicine is to be in year 2030. This is seen in the graph Figure 2, which shows that the use of telemedicine increases, ie. that an increasing number of doctors applying telemedicine and its services and providing health care services over the years.

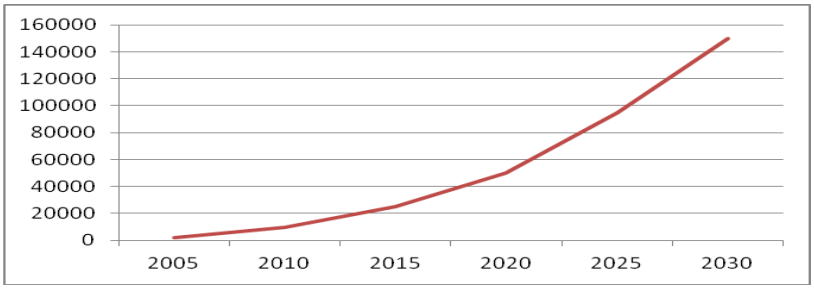


Figure 2. The application of telemedicine in the future (adapted from UCLA, 2013)

4.2. Prospects of telemedicine services in Serbia

In Serbia, telemedicine was developed in the 1990s. The first project was launched in the context of the Telemedicine Center in Belgrade, the Military Medical Academy (MMA), the Institute of Pathology and Forensic Medicine. When this project began, digitized libraries of classic glass started to slide. Telepathological established a permanent link between the Military Hospital and the Institute of Pathology, Faculty of Medicine and the Military Medical Academy in Belgrade, 1997. (Milosavljević, Spasic, et al 1997). The project was launched in the application of telemedicine services that related to sampling during surgery in Nis, and sent to Belgrade to determine the diagnosis. Although there was a modest technology, the telemedicine connection is proved safe. Since then it has functioned permanent connection to Nis, where the MMA has made several experimental relationship with other medical centers in Podgorica, Sremska Kamenica, KBC Bežanijska Kosa, where it carried out the transfer of radiological images, in addition to digitized microscopic images.

In recent years, Serbia was working on the introduction of electronic health records and electronic cards (Jovanović Milenković, Milenkovic, Jeremić, 2014). The hospitals are mainly used teleconsultation with doctors who are on other geographical localities. In most cases applied in cardiology.

In Emergency service vehicles are installed equipment that allows data transfer to the hospital. In Belgrade, Emergency service vehicles are equipped with modern apparatus for the transmission of ECG signals. These devices make it possible to record the ECG transmitted directly to the central Emergency Department regardless of whether the record was made in the apartment of a patient, in a public place or in the ambulance. The record is transmitted through GSM (Global System for Mobile Communications) on the server, where it is available for review and analysis by more doctors. In this way, by teleconsultation, doctors may indicate the doctor who is next to the patient so which is the best way to administer first aid to the patient. This ensures a higher quality of services and more accurate diagnosis. In addition, a team of doctors who are in the hospital can quickly and adequately provide further medical assistance (Reljin, Gavrovska, 2013).

In April 2016, MMA organized online course entitled "ENT surgery live - online". Speakers talked about education via the Internet as the most modern method of distant learning. Thanks to ICT technology, consumers had the opportunity to watch a live webcast of four operations in the field of otolaryngology, supported by the *Big Blue Button* software for distance learning, with a *Medapp Moodle* educational platform. The physicians performed in the operating room at the MMA. In addition to involvement in the educational platform of audio or video link, users had the possibility of direct communication with the operator. They were able to ask questions via the audio link or messages in real time, and the possibility of mutual communication and communication with the moderators of the course. The moderator has joined the course in Basel. Doctors for otolaryngology responded to the message. Clinic of ENT has organized such a course in which for the first time in the region otolaryngology surgery transmitted live via the Internet, certainly made a pioneering endeavor and set a new standard in the field of education (The Military Medical Academy, 2016).

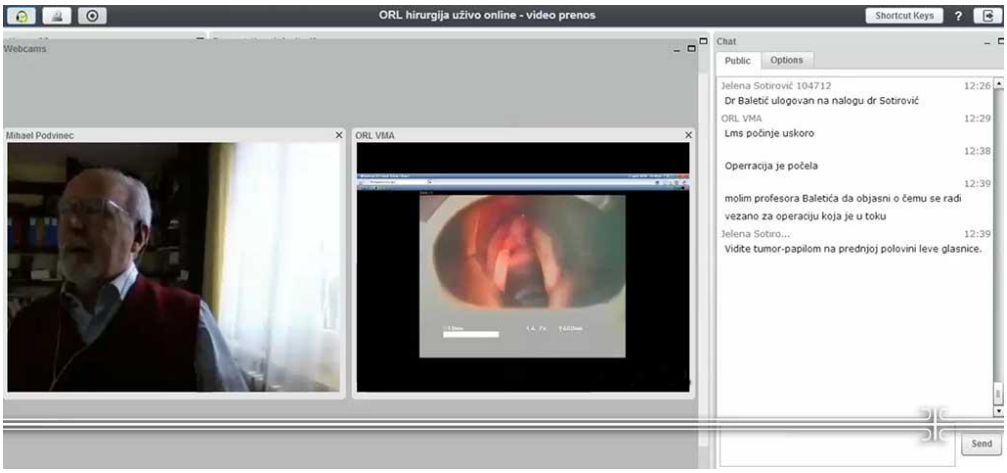


Figure 3. ENT surgery live – online (The Military Medical Academy, 2016).

At the global level, it is necessary to support the development of adequate infrastructure for the development of telemedicine services.

4. CONCLUSION

The health sector has undergone various changes in recent years. These changes were related to the introduction of information and communication technologies. This was reflected in telemedicine. But telemedicine is characterized by various factors that makes it more efficient. These include: Expanded access to health services; Health care for the population who is constantly traveling; Military applications; Tele-home care; Reduction of costs; Market Development; Health Policy and Strategy.

Pursuant to these factors, the paper describes the trends that are crucial for the further development of telemedicine in the course of 2016. These are: Expanding Reimbursement, International connectivity and Arrangements, Continued Momentum at the State Level, The increase in telemedical services in hospitals, Using Technology to improve care and cut costs.

Analyzing trends can be observed on directions of development of telemedicine in Europe. The paper is an overview and future projections described providing telemedicine services in Europe. Telemedicine in Europe mostly applied in the UK. The second place is Germany, and then Scandinavian countries. Teleradiology is used 66% in the UK and Scandinavian countries, while telecardiology services are highest in the UK 6%. In Serbia, it is shown to be the intensive use of new technology in telemedicine. Devices are introduced into the ambulance, which will help in monitoring the health status of the patient remotely. In April 2016, the MMA did the first online operation in the field of otolaryngology. More specifically, doctors were able to follow four operations online in the field of otolaryngology, supported by the Big Blue Button software for distance learning, with a Medapp Moodle educational platform.

At the end, we can conclude that telemedicine is a sector that every day is more and more developed with the aim of better medical care of patients. Telemedicine influence to provide quality health services. The paper shows that hospitals in Serbia following the development and to provide of telemedicine services. This concept should be expanded to all hospitals in Serbia to the entire population had adequate health care. Constant development and growth in use of telemedicine in the future is inevitable.

REFERENCES

Boubacar Traore B., Kamsu-Foguem B. & Tangara F., (2016), Integrating MDA and SOA for improving telemedicine services, *Telematics and Informatics 33*, 733-741

Brown, N. (1996). Telemedicine Coming of Age. Telemedicine Information Exchange. Retrieved from http://tie.telemed.org/articles/article.asp?path=telemed101&article=tmcoming nb tie96.xml

Ekeland A.G., Bowes A. & Flottorp S., (2012). Methodologies for assessing telemedicine: a systematic review of reviews. *International Journal of Medical Informatics 81 (1),* 1–11.

Jovanović Milenković M., Jeremić V. & Martić M., (2014). Sustainable Development in the e-Health Sector of the European Union. *Journal of environmental protection and ecology. 15(1*), 248-256

Jovanović Milenković M., Milenković D. & Jeremić V., (2014). *Introduction and Implementation of Electronic Health Card.* In Maja Levi Jaksic, Sladjana Barjaktarovic, Milan Martic (Eds) Innovative Management and Firm Performance- An Interdisciplinary Approach and Cases. 444-464, ISBN 978-1-137-40220-2

Kamsu-Foguem B., Tiako F.P., Fotso P. L. & Foguem C. (2015), Modeling for effective collaboration in telemedicine, *Telematics and Informatics 32*, 776-786

Lacktman M. N., (2015), Five Telemedicine Trends Transforming Health Care in 2016, Retrieved from https://www.foley.com/five-telemedicine-trends-transforming-health-care-in-2016/

Milosavljević I., Spasić P., et al. (1997). Centar za telemikroskopsku dijagnostiku u Zavodu za patologiju i sudsku medicinu VMA. *Acta Medica Medianae XXXVI. 1*. 5-12

Norris A.C., (2001). Essentials of telemedicine and telecare. John Wiley & Sons. New York. ISBN 0-471-53151-0

Reid, J. (1996). A Telemedicine Primer: Understanding the Issues. Innovative Medical Communications. ISBN: 0965304507.

Reljin I. & Gavrovska A., (2013). Telemedicina. Akademska misao. Beograd. ISBN 978-86-7466-458-2

Somsainathan. C.K., (2011). Telemedicine: The Inevitable Component of Modern Healthcare, Medical devices, Frost & Sullivan. 4(2)

The Military Medical Academy, (2016), First ENT Surgery Live via the Internet Held at MMA, Retrieved from http://www.vma.mod.gov.rs/eng/

UCLA (2013). Pilot program study finds pediatric obesity patients like telehealth services. Los Angeles. University of California.

MODEL-DRIVEN APPROACH TO THE IMPLEMENTATION OF WEB SERVICE INTERFACES FOR 4GL SYSTEM

Slavimir Vesić*[1], Nenad Aničić[1], Slađan Babarogić[1]
[1]University of Belgrade, Faculty of Organizational Sciences
*Corresponding author, e-mail: vesic.slavimir@gmail.com

Abstract: *Interoperability becomes one of the most important demands for IT function in company. 4GL-based information systems are present a few decades in IT industry and because of their inflexibility they make big problems in the design, implementation and maintenance of software for modern business. Large number of these systems are faced with the inability to meet the demands of design in a way that they does not support business processes or the inability to use the latest technologies and solutions. Because of that they are actually legacy system. Solution that exposes 4GL procedures of legacy system as Web services is not effective in a situation where we have a large number of changes in the legacy system and high dependencies between procedures. So, if we design executable specification of the existing 4GL procedures and execute it as runtime model we can achieve interoperability. In first phase we specified transformation of Web service model to 4GL procedures model and as result we have annotated model. In second phase we designed algorithm that performs interpretation of annotated model and runs existing 4GL procedures in legacy system. To achieve this we used MDA approach and UML profiles. Proposed solution is explained in the example of execution of the distributed workflow between public utility companies in Belgrade.*

Keywords: *interoperability, MDA, 4GL, legacy system*

1. INTRODUCTION

Fourth generation of programming languages, briefly 4GL, was created in the period from 1970 to 1990 with initial idea to reduce time, efforts and resources which are invested in programming and learning conventional programming languages of third generation, briefly 3GL, as Pascal, Cobol and C. The need in the industry at that time was to reduce the dependence of professional programmers and to shift the focus on the user, which led to the idea that the development environment will be opened to the general population and programming will be more simplified. 4GLs are designed for specific problem domain, e.g. development of business software. In comparison to the generation of programming language before them, they are one level of abstraction away from the machine, which means that they are closer to the problem domain. Depending on the application, they can be classified into several categories: table-driven programming languages, report-generator programming languages, forms generators and data management 4GLs. 4GLs can be procedural languages or not or they can combine both concepts. Examples some of these programming languages are: Clipper, FoxPro, PowerBuilder, SQL, Informix 4GL, Ingres 4GL, Progress 4GL, Oracle Reports, ABAP, Clarion etc.

Legacy systems are old information systems which are still in use in the organization because they support fundamental business processes and the organization cannot or does not want to replace them or to redesign them. Legacy systems developed in the past, usually used older or obsolete technology. These systems are consist not only of hardware and software but also they include legacy procedures and processes – old way of doing things that are difficult to change because they rely on legacy software (Somerville, 2010). On one hand, enterprises see legacy systems as barriers to implementing new business processes because they are hard to adapt to new business requirements. On the other hand, they contain priceless knowledge about business and business operations. Because of these facts, enterprises are in dilemma what to do with them. Van den Heuvel (2009) explains that this business knowledge is constructed not only by explicit knowledge about business processes, policies and data, but also by tacit knowledge, which is very important in daily business operations.

Interoperability viewed as the ability of two or more systems to exchange information and services and to use the information that has been exchanged, with no access restrictions, or implementing, becoming one of the most important demands for enterprise. If we look at the EU's initiative for the integration of European public administration, proposed as part of the European Interoperability Framework - EIF 2.0, interoperability between public companies is one of the common goals that information systems of those companies should provide (ISA, 2010).

This paper presents the preliminary design and the procedure for enabling interoperability of a legacy 4GL system. The basic idea is to enable interoperability between public utility companies in Belgrade by exchanging models between them, transformation and execution of models. Complete procedure is illustrated in the case of complaint. In example both enterprises are involved. Basic research questions are:

- mapping between models of Web service and model of legacy 4GL system

- transformation of this mapping in execution model and calling existing Progress 4GL procedures from legacy system

The procedure is performed using a UML profile, as well as annotating Web services model in the 4GL model and then use this annotated models in the execution. For description of the Web service we used SoaML, OMG standard.The paper is organized as follows. The next section briefly presents related works from the research field. Section 3 describes the problem scenario to be analyzed. Section 4 describes the proposed solution. Following this conclusion is presented together with reference material.

2. RELATED WORK

Martin and McClure (1983) display a large list of characteristics of 4GL languages, whereby it should be noted that some of the works challenged the future, were outlined Grub and Takang (2003). Some of the benefits of these languages in the context of software maintenance are: reduction of development cost, easy understanding, automatic documentation and reduction in workload. On the other hand Grub and Takang (2003) presented a list of weaknesses of 4GL languages. *Application-Specific* - 4GLs are hard to use in a different domain compared to the one for which they were originally designed. Proprietary - 4GL environments are proprietary and incompatible with other environments and the organization cannot simply get rid of them and move on to other or similar systems. It directly affects the long-term evolution of the system. *Hyped Ease of Use* - It's adopted that the 4GL languages are very simple and that the 4GL languages designed for non-professional developers. What had once been pointed out as the main advantage, may prove to be a major weakness. This attitude leads to a big risk that the program code is unsustainable, and the system poorly designed and implemented, due to the fact that the systems will be developed by people without expertise. In this way, existing investments in 4GL systems will fail. Linthicum (1994) emphasizes that 4GL tools bind companies to software vendor, which is not standard and 4GL languages do not have sufficient flexibility, which OO languages offer and therefore they may represent the best alternative.

Interoperability has been an important area for research for years. Numerous researches and organizations propose different definitions, concepts, approaches, levels, frameworks and maturity models (ISA 2010; Berre et al 2007; Chen and Daclin 2007, Winters et al 2006, Vernadat 2010). Panetto (2007) analyzed different approaches to interoperability and classified them in relation to applications, models and standards.

Davidson et al (2001) design 4GL applications through UML models via tool VG UML Modeler. The aforementioned tool enables connection between procedural 4GL language and OO software development, with the appropriate mapping UML class in 4GL parts. The model supports the three-tier Model-View-Controller architecture.

In the context of model-driven engineering (MDE), and their motto "models are all" models can be used for transformation between models. The transformation is usually carried out in two phases. First phase defines the mapping between the elements of one model in the other. Second phase is automating the generation of the actual transformation rules. System receives two model definitions, uses rule and produces transformation (Brambilla et al., 2012). Janković et al (2012) propose approach of formal modelling cross-organizational business processes (CBP) using UML profiles.

For modelling purpose we use OMG standard for modelling Web services, SoaML. Gebhart and Bouras (2013) describe mapping rules and transformation from specification to implementation artifacts, which we use in our solution in a way that we generate additional files which describe model implementation.

Mottupalli et al (2009) design approach to SOA for Informix 4GL system, with deploying of 4GL function as Web services. W4GL tool automatically generates required skeletons, headers and wrapper files that are required. Specification of Web service is provided through configuration file. In relation to the above approach, our proposed solution is distinguished by the fact that we can combine several 4GL procedures in common communication and exchange data between them.

3. PROBLEM DEFINITION

In Belgrade, there are two public utility companies, briefly PUC. PUC "Belgrade Waterworks and Sewerage", briefly PUC BWS, specializes in production, distribution, selling and payment of consumed water and sewage services. PUC "Infostan" performs payment service for many PUC in town. We analyze the non-automated operation between companies – raise a complaint. When customer raises a complaint about the invoice and submits it to execution manually in PUC "Infostan", PUC "Infostan" archives document and forwards complaint to the PUC BWS. PUC BWS solves the complaint and informs the customer. This situation is presented in Figure 1.

Operation between two companies, raising a complaint, should be executed automatically through the Web portal of "Infostan". When customer submits a complaint on Web portal, complaint should be transferred to PUC BWS and inserted into information system of PUC BWS. This practically means that it is

necessary to enable interoperability between information systems of two PUC. We have to consider that PUC BWS use legacy 4GL IS, designed and implemented in Progress 4GL. Also, there is no possibility to switch to a new environment, it is necessary to enable executions of Progress 4GL procedures.

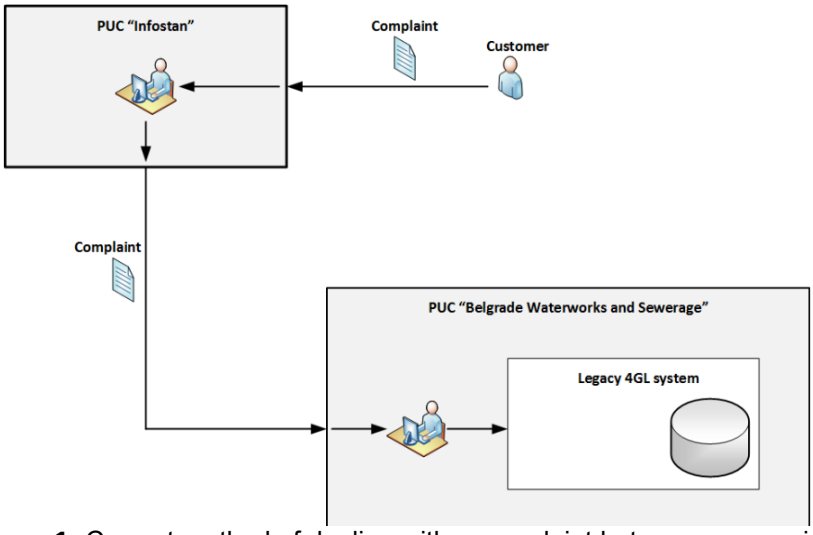


Figure 1: Current method of dealing with a complaint between companies

4GL procedure of legacy system can be exposed as set of Web services. To provide that, it is necessary to use a special tool to package and expose existing 4GL procedures, also with server which has to run existing procedures. Also, there is a need to achieve a higher degree of interoperability and exchange information between companies, and the above mentioned method can be proven as inefficient in situations which consider constant changes of existing 4GL procedures and changes in communication between Web services of two companies. It is also risky, changing existing procedures manually or programming the new ones, can prevent the legacy system from working. Such a procedure, in which we have frequently-changing ways of doing business, would require changing 4GL procedures, packaging 4GL procedures into Web services manually and the possible change in the sequence of communication between the Web services of companies.

4. SOLUTION

The proposed solution consists of several components, which are described in Figure 2.

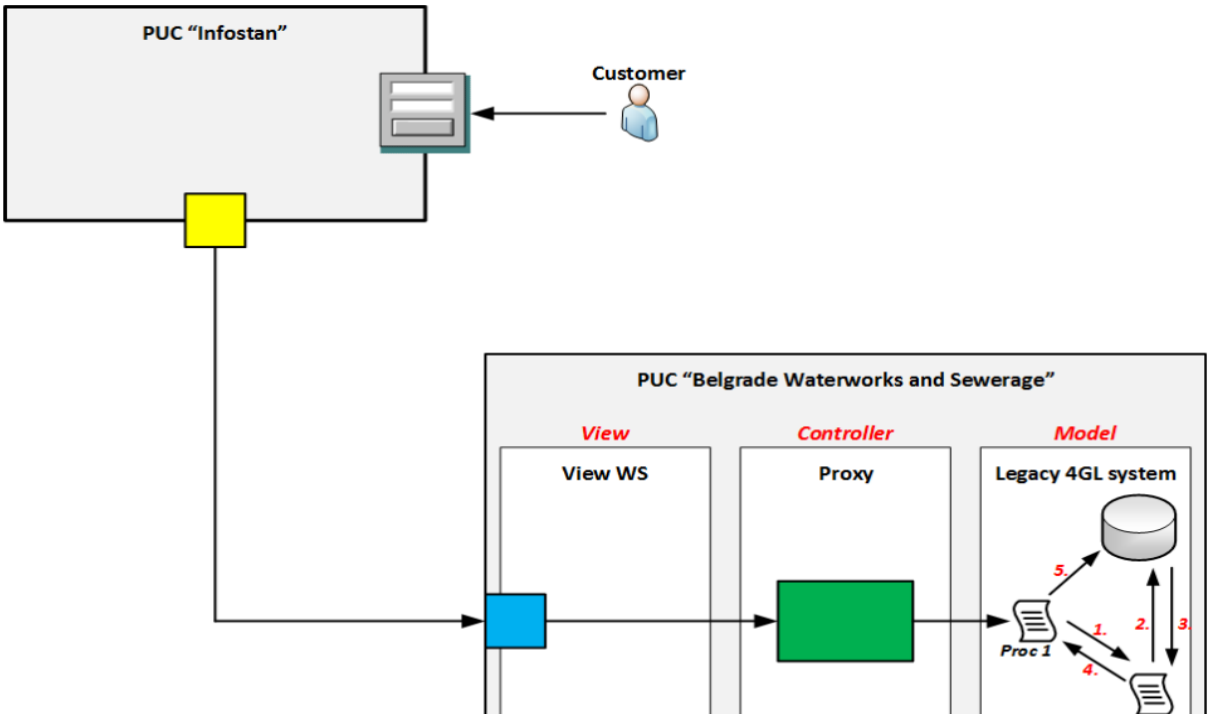


Figure 2: Proposed solution

Web service interfaces for legacy 4GL system consists of several components: ViewWS, Proxy and Legacy 4GL, which are organized according to the Model, View and Controller layers in architectural pattern Model-View-Controller, MVC. ViewWS is encapsulated functionality of legacy 4GL system, exposed to other systems as a Web service. When “Infostan” Web service forwards information about the complaint it calls ViewWS within the PUC BWS through SOAP message. In the context of MVC this component has the role of View, or the interface. Proxy is a component that accepts SOAP message from ViewWS, then make the annotation of model of Web service into 4GL and after that execute that specification from Web services into 4GL. Proxy component is the essence of the proposed project solution and the central theme of this work. Below we describe the component in a detail. In the context of MVC, this component has the role of controller.
Legacy 4GL system is existing legacy 4GL system that executes 4GL procedure. In contexts of MVC, this component has a role of Model.

Proxy Component has a role to implement the specification of annotated model Web services in 4GL model and then to execute 4GL procedures and that will way to execute business function of legacy systems. Running T2M transformation of existing 4GL procedures we can get M1 model of 4GL. M1 models of 4GL’s are stored in the section Proxy component called the 4GL model Registry and it contains M1 model every 4GL procedures required for the execution of certain business functions of information system. M1 model of Web service is described by SoaML. Transformation Editor is part of Proxy component which specifies how annotation model of Web service conforms to 4GL model. After specification whole specification is memorized in WS model register component. Transformation Executor is part of Proxy component which executes specification and as result of execution procedures of Legacy 4GL systems are executed. Architecture of proposed solution is presented in Figure 3.

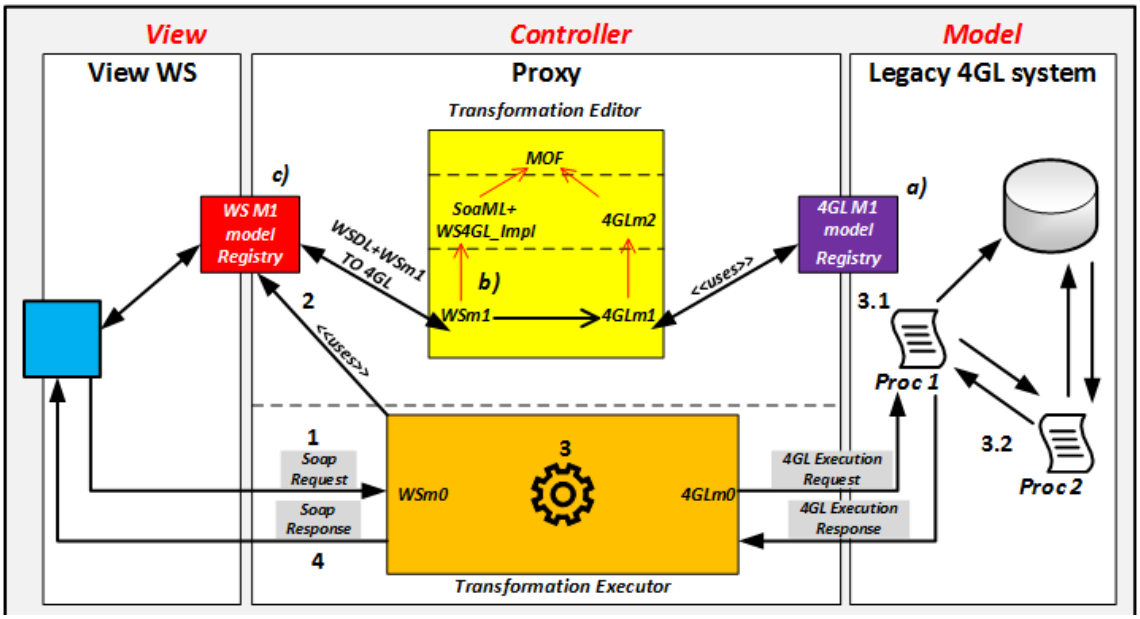


Figure 3: Architecture of proposed solution

Steps that are being carried out to build Web service interfaces for legacy 4GL system are:

1. *Service specification* – it consists of 3 steps, presented in Figure 3. and indicated as a), b) and c)

   a) *Description of 4GL procedures of legacy system and their registering into 4GL model Registry*

UML profiles used to extend the basic concepts of UML. UML profiles for 4GL are presented in Table 1.
Figure 4 displays models of two procedures from legacy 4GL system with the names CheckRegister and CreateComplaint and their attributes. Logic of 4GL procedures CheckRegister is to check whether the appropriate condition is satisfied, and if so, to call a procedure that raises a complaint - CreateComplaint and passes its parameters. CreateComplaint procedure stores Complaint into the table in Progress 4GL database of legacy 4GL system.

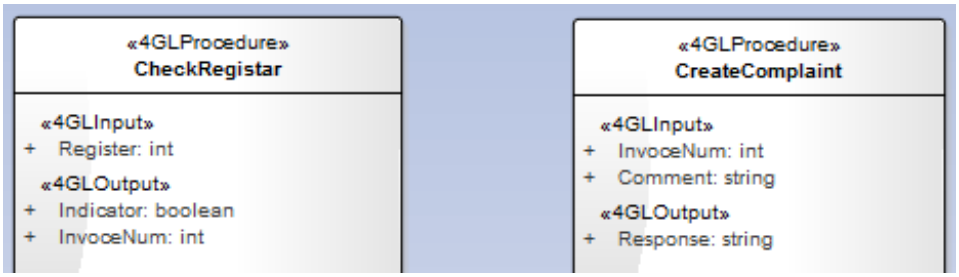
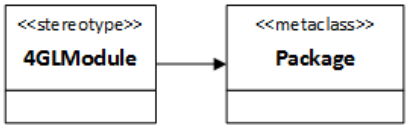
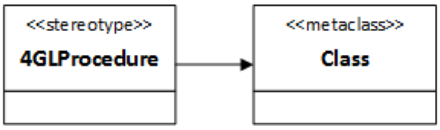
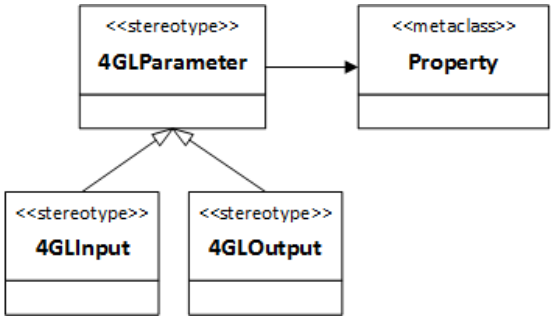


Figure 4: 4GL Procedures model

Procedures are stored in the 4GL model Registry in an automated way through T2M transformation.

Table 1: UML 4GL Profile

Stereotype	Description
	**a) stereotype: 4GLModule** Describes package which contained a set of 4GL procedures for some domains.
	**b) stereotype: 4GLProcedure** Allows to present 4GL procedure as a class. Performs a single business operation such as raising a complaint. Thus, the existing procedures are viewed as legacy systems functionality to be performed in the correct order
	**c) stereotype: 4GLParametar** Each 4GL procedure contains input and output parameters. Input parameters of one procedure can be output parameters to other procedures. Using this method, procedures are linked together.

b) the design of the implementation of Web services operations through 4GL procedure

In this part we will describe specification of Web services new part of system that needs to accept SOAP message and after that to execute functionality of legacy system, and after that to return the response to the consumer. OMG specifies UML profile for SOA to define SOA concepts inside existing UML concepts. Specification of Web services through SoaML is presented in Figure 5.

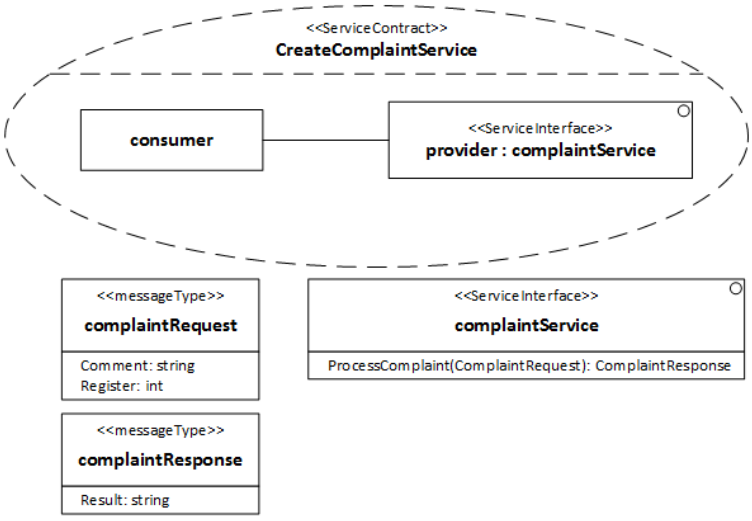
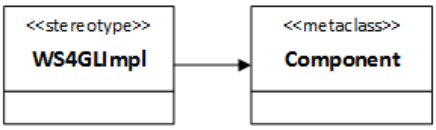
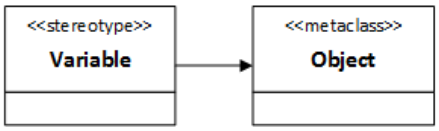
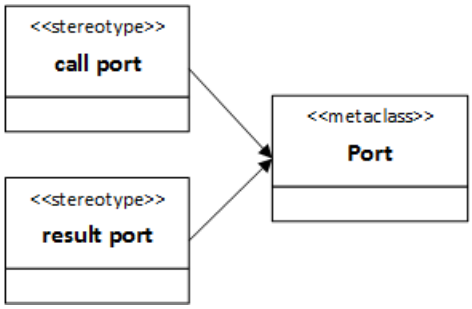
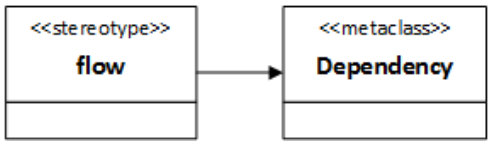


Figure 5: Specification of Web services

ServiceContract defines the conditions under which the participants in interaction must agree. Figure 5 shows that this interaction is simple and defines ServiceContract for CreateComplaintServis. In contract a consumer of Web service commits that will interact with provider, in this case complaintService. In general interaction can be more complex and include choreography, as defined in SoaML standard. MessageType describes the exchange of information between the consumer and the service. Provider calls CompliantService and send complaintRequest, which contains Comment and Register as data and as response it gets complaintResponse which contains Result. For each Web service operation it defines separate 4GL module i.e. component which presents control flow of execution registrated 4GL procedures. This description of service implementation is provided through WS4GLImp profile. WS4GLImpl profile is presented in Table 2.

Table 2: WS4GLImpl profile

Stereotype	Description
	**a) stereotype: WS4GLImpl** Indicates the component that performs 4GL procedures from the legacy system.
	**b) stereotype: Variable** Specifies the variables that will be filled with results of execution each 4GL procedures. Variables will be used for the exchange of values between procedures.
	**c) stereotype: call port** Specifies input port WS4GLImpl component. ComplaintService send message on these port. **d) stereotype: result port** Specify the output port component WS4GLImpl, which will display the result of execution flow of 4GL procedures.
	**e) stereotype: flow** Connects classes and defines execution flow of set of procedures.

Defined rules and constraints throught UML profile WS4GLImpl, which are not included in the table, allows valid specification of implementation of service with application general algorithm explained in step 2. of part *Service Execution*. Described model implementation of component which uses WS4GLImpl profile is shown in Figure 6. Diagram is created in Enterprise Architect tool. Specification implementation from Figure 6. describes how Web service ComplaintService, through operation ProcessComplaint initiates call of ProcessComplaint_Impl component and throught call port forwards complaintRequest message.

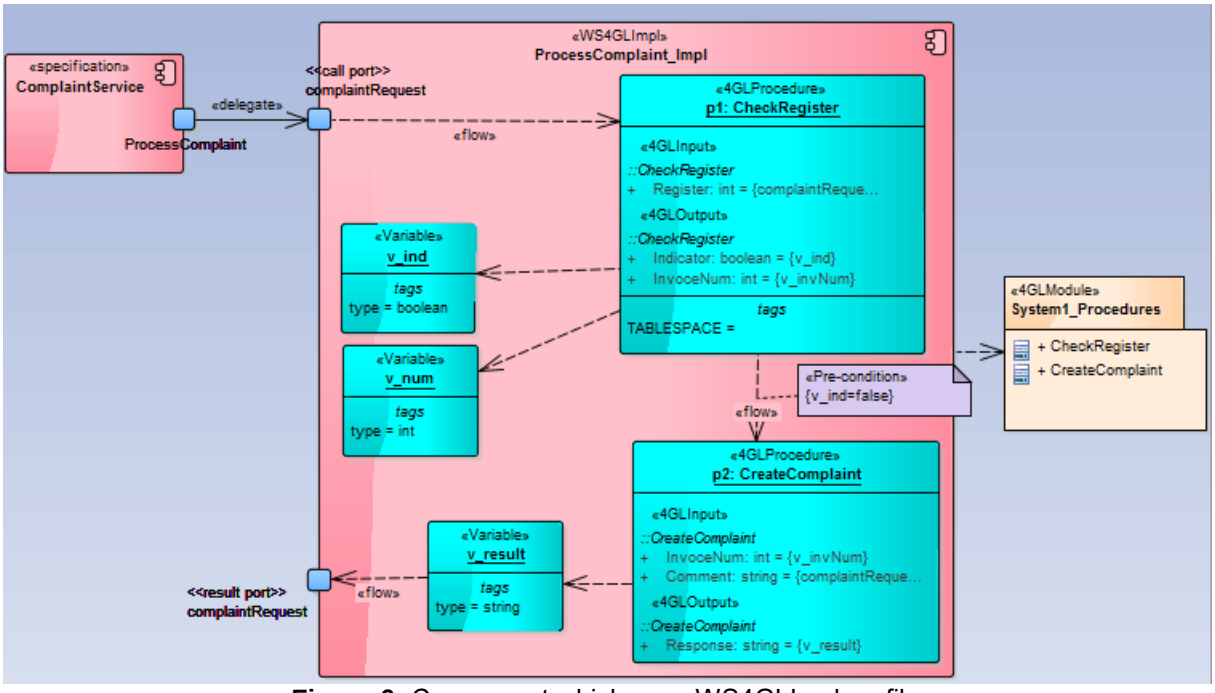


Figure 6: Component which uses WS4GLImpl profile

ProcessComplaint_Impl component takes the message, annotates the value from the message into the parameters of 4GL procedures and calls the object p1 of class CheckRegistar. The result of execution is stored in variables v_ind and v_num, in a way that object p2 of class CreateComplaint can use them. The result is memorized in the variable v_result. Web Service ComplaintServis through resultPort returns result of execution ProcessComplaint operations.

c) *check of designed model of Web services and their publishing into WS model Register*

In this step, constraints are checked with the values of input/output parameters in profiles and model is saved into WS model Register. This step is performed because model is exposed through WSDL and it is input for component which interprets that model in a runtime.

2. *Service execution* - it consists of few steps

    1. *When SOAP message arrives, there is recognition of annotated model which will be used*

    2. *Intepretation of annotated model, which is described in step b in first part Service specification, and executing actions which are described through algorithm in activity diagram presented on Figure 7.*

Interpretation of annotated models starts by finding corresponding component that executes 4GL Module, in this case WS4GLImpl. After that, the component WS4GLImpl finds the first procedure, which should call and evaluate parameters obtained from the annotated models. After that, algorithm prepares parameters, calls the procedure, accepts the result of execution and writes values into variables. Then algorithm checks is there further control flow of execution and if it exists, checks constrints, which can be defined before calling the procedure and relates to the value of the variable, which was set by previously performed procedure. If the constraint is satisified, algorithm calls next procedure. The process takes as long as procedures exists in control flow of execution. After that, algorithm is continued and prepares the response and sends it.

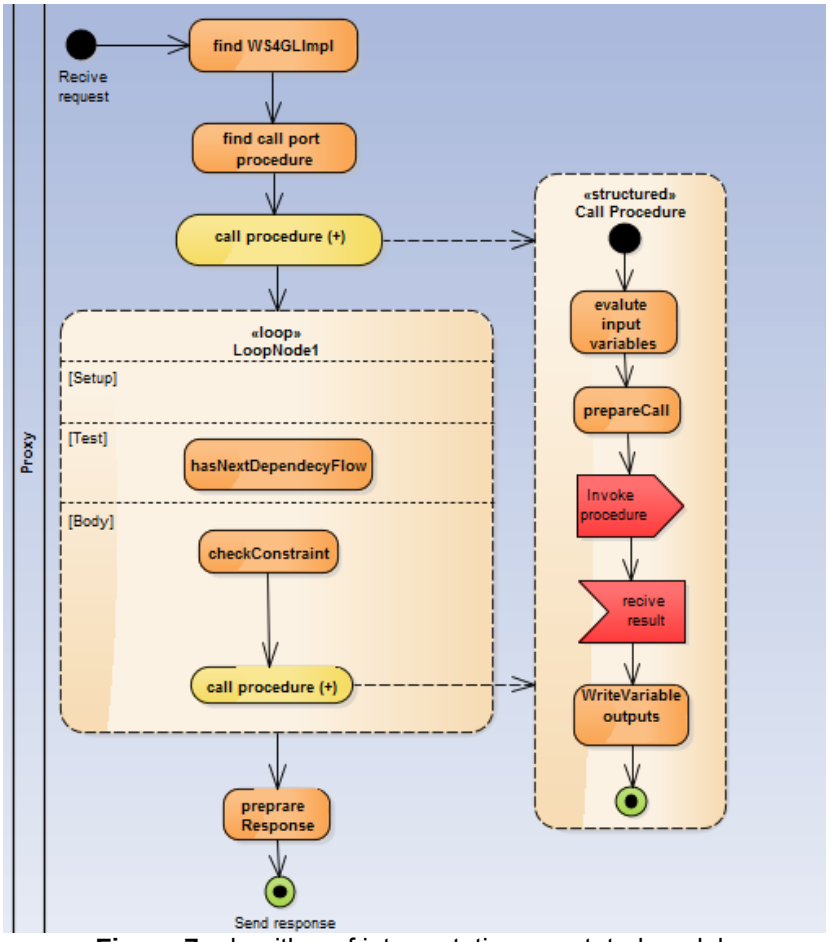


Figure 7: algorithm of interpretation annotated model

3. *component that preforms interpretation forwards response to the component which inovkes it*

Algorithm described in step 2 of Service execution is presented on an abstract level without technical implementation details of platform on which it is implemented. The task of the last activity in the algorithm is to prepare and validates the response message in accordance to specifications.

5. CONCLUSION

This paper addresses two major topics. First, it presents an approach to design Web service interface for legacy 4GL system which operates as runtime model and as such eliminates need for large number of changes in that system and also prevents potential malfunctions because of high dependencies between existing 4GL procedures. Second, it describes steps for the implementation of such an interface.

The key contributions of this paper are:

- the definition UML profile for 4GL, as specification mechanism of existing 4GL procedures
- the definition of specification Web services which calls 4GL module of legacy system, based on annotated model
- the definition of algorithm for executing that specification and calling 4GL procedures without additional changes of existing legacy system

We believe that our proposed approach is good in a situation where we want to expose modules of legacy 4GL system through proper operation of Web services, in a way that module can achieve interoperability with other system, without changing the way that existing legacy 4GL system operates. We are currently working on developing a framework to support this approach and we are experimenting with .NET development environment.

REFERENCES

Berre, A., Elvesæter, B., Figay, N., Guglielmina, C., Johnsen, S., Karlsen, D., Knothe, T., & Lippe, S. (2007). The ATHENA interoperability framework, In R. J. Gonçalves, J. P. Müller, K. Mertins, & M. Zelm (Eds.), *Enterprise Interoperability II*, 569-580. London: Springer-Verlag London Limited. doi:10.1007/978-1-84628-858-6_62

Brambilla, M., Cabot, J., & Wimmer, M. (2012). *Model-Driven Software Engineering in Practice.* Publisher: Morgan & Claypool Publishers. DOI: 10.2200/S00441ED1V01Y201208SWE001

Chen, D., & Daclin, N. (2007). Barriers Driven Methodology for Enterprise Interoperability, In L. Camarinha-Matos, H. Afsarmanesh, P. Novais, & C. Analide (Eds.), *Establishing the Foundation of Collaborative Networks*, 243, 453-460. IFIP, NY: Springer.

Davidson, S., Keren, M., Porat, S., & Zodik, G. (2001). Designing Procedural 4GL Applications through UML Modeling. In *Workshop of the pUML-Group held together with the «UML»2001 on Practical UML-Based Rigorous Development Methods - Countering or Integrating the eXtremists*, 69-85.

Grubb, P., Takang, A. (2003). *Software Maintenance: Concepts and Practice* (2nd ed.). Singapore: World Scientific Publishing Co Pte Ltd

Gebhart, M., Bouras, J. (2013). Derivation of Web Service Implementation Artifacts from Service Designs Based on SoaML, In *International Journal on Advances in Software*, *6*, 170-180.

Interoperability solutions for European public administrations. (2010). *European Interoperability Framework (EIF) for European public services - Annex 2*, Retrieved from: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Janković, M., Ljubičić, M., Aničić, N., & Marjanović, Z. (2014). Enhancing BPMN 2.0 Informational Perspective to Support Interoperability for Cross-Organizational Business Processes. Paper presented at the *4th International Conference on Information Society and Technology (ICIST 2014)*.

Linthicum, D. (1994). 4GLs: No easy answers*. Object Magazine 4(5)* 38-42.

Martin, J., & McClure, C. (1983). *Software Maintenance – The Problem and Its Solutions*. New Jersey: Prentice Hall

Mottupalli, S., Maheshwari, G., & Mahadevaiah, T. (2009) *Deploy 4GL functions as Web services*. Retrieved from: http://www.ibm.com/developerworks/data/library/techarticle/dm-0902mottupalli/dm-0902mottupalli-pdf.pdf

Panetto, H. (2007). Towards a Classification Framework for Interoperability of Enterprise Applications. In *International Journal of Computer Integrated Manufacturing, 20(8)*, 727-740. PA: Taylor & Francis

Sommerville, I. (2008). *Supplementary material with book Software Engineering.* Retrieved from: http://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Web/LegacySys/index.html

van den Heuvel, W. (2009). *Aligning Modern Business Processes and Legacy Systems: A Component-Based Perspective*. MA: The MIT Press.

Vernadat, F. (2010). Technical, semantic and organizational issues of enterprise interoperability and networking, In *Annual Reviews in Control*, *34*(1), 139-144.

Winters, L., Gorman, M., & Tolk, A. (2006). Next Generation Data Interoperability: It's all About the Metadata. Paper presented at the *Proceedings of Fall Simulation Interoperability Workshop*.

OMG (2012). *SoaML*. Retrieved from http://www.omg.org/spec/SoaML/1.0.1/PDF/