Design of Fuzzy Expert System for Evaluation of Contemporary User Authentication Methods Intended for Mobile Devices

Dragan Korać, Dejan Simić

University of Belgrade, Faculty of Organizational Sciences, 11000-Belgrade, Serbia
E-mail: korac@teol.net, simić.dejan@fon.bg.ac.rs

Abstract: In this paper, the Fuzzy Expert System (FES) for evaluating contemporary user authentication methods intended for mobile devices is designed and applied. The parameters used as input for this FES are user's priorities such as security, usability, accessibility, pricing, complexity and privacy (SUAPCP) and the output parameter is evaluation (grade) of mobile solutions. The results obtained from developed fuzzy expert system indicate that proposed system can be effectively used for evaluation of contemporary user authentication methods intended for mobile devices. The strength of presented FES is assignment of a concrete numeric value to a specific mobile authentication solution. This FES should have profound positive impact not only on the better quantification of mobile authentication solutions but also on aspect of filling gaps in the current researches such as creating strong mobile authentication in regard to user's priorities. Finally, it is necessary to be noted that the designed FES would not be limited only to mobile context but could be applied to all authentication methods.

Keywords: Expert system, fuzzy logic, fuzzy rules, mobile solutions, user authentication.

1. INTRODUCTION

Over the past few years, the rapid development of different mobile technologies is creating new challenges with regards to mobile authentication process. This phenomenon has the growing importance because new authentication solutions are being developed by applying different technologies. With the growing number of different authentication solutions a question that arises is their best selection and evaluation. For development of any authentication solution the vital user parameters are security, usability, accessibility, pricing, complexity and privacy (SUAPCP). Undoubtedly, security is the most important user's factor in authentication process. Today, aimed at creating a better security mobile authentication uses multifactor authentication methods. These terms are used to describe any authentication solutions where more than one factor is required to authenticate a user. There are three universally recognized authentication factors: what you know (e.g. passwords), what you have (e.g. mobile phone, or tokens), and what you are (e.g. fingerprints, face, iris, etc.). However, the criteria differ from application to application. For example, one wants to have security as a priority (e-banking), the other one doesn't (application for displaying a bus route). This happens when security factor can prevent or limit regular applying of other factors where for example one wants to have pricing as a priority. An example for this is the registration of employee.

Nowadays, a value of mobile authentication solutions is descriptively presented in literature expressed with different linguistic terms such as strong, stronger, weak, low, medium, high, etc. The terms are descriptively used to indicate to which extent a certain authentication method meets a specific set of user's criteria. However, the used terms represent an obstacle in creating "the most suitable" mobile solution for mobile authentication. Term "the most suitable" presents notion that is for many users sufficiently good mobile solutions. Otherwise, "The most suitable" solution is one of the main challenges faced currently in the Information Society. When choosing the most suitable mobile solutions the basic problem is the impossibility of determining its numeric value.

Due to the lack of numerical evaluation of mobile authentication solution, the choice of the most suitable mobile solution is pervaded with fuzziness and uncertainty. In the light of all these considerations, problem of the mobile solutions evaluation cannot be generalized or analyzed using the binary logic that has only two truth values, true - 0 or false – 1. It requires the use of fuzzy systems. Since the fuzzy set was proposed by (Zadeh, 1965), they are widely used for solving problems in variety of domains that are very complex and cannot be modeled precisely even under various assumptions and approximations. Domains of application are law, agriculture, tourism, military operations and many more (Bellman et al., 1990; Pedrycz et al., 2008; Zadeh, 1975).

Undoubtedly, mobile authentication solutions are complex of the system where conventional mathematical models cannot give satisfactory results. In spite of being highly complex and uncertain, fuzzy systems can give a multivalued logic similar to human thinking and interpretation. The main reason of choosing fuzzy systems lies in the fact that fuzziness, described as the vagueness in the value of mobile solutions, is generally found wherever human decisions, judgment, or evaluation plays an important role. The main feature of fuzzy systems is based on Fuzzy logic that has the ability of merging human heuristics into computer-assisted decision-

making. Just that fact singles out these systems as one of the most successful today's technology which is used in many applications (Nezam et al., 2002; Cărbureanu, 2014; Kramar et al., 2015; Wallam et al., 2014; Feng 2006; Precup et al., 2011; Linda et al., 2011; Vaščák et al., 2012; Dumitrache et al., 2006;). Taking into consideration the fact that fuzzy logic describes imprecise human perception as an appropriate mathematical tool, this methodology can be used in solving very complex problems that are presented in mobile authentication domain. The main task of this methodology is the pursuit of crisp value of mobile solutions.

Contribution of this paper: A new methodology of the approach that is introduced enables evaluation of mobile authentication solutions with quantative data instead of descriptive. With an insight into available literature, proposed methodology is not found. Therefore, it is necessary to highlight here, that this is the first time that this innovative methodology is proposed for selection of the most suitable mobile authentication method in a given context. The purpose of FES is to provide a tool to help decision makers in enterprises and organizations to choose the most suitable mobile solutions for their usage scenario. This paper differs from other papers because it gives a concrete numeric value to mobile solutions taking into account predefined prioritized user's parameters. Also, other contribution of this paper is a possibility to change users priority and according to the priority to get numeric value for the chosen mobile solutions. Finally, unlike previous papers this paper consider holistically wider set of contemporary user authentication methods intended for mobile devices as well as comparison factors with a wider set of classified entries.

The remaining of this paper is structured as follows. Section two gives results of previous research. Section three gives methodology of FES. Section four gives design of fuzzy expert system. Section five gives results and discussion. Finally, section six concludes the paper.

2. PREVIOUS PAPERS

From available different papers are provided data that point out that there is no paper on fuzzy logic for evaluation of mobile authentication solutions. There are papers like (Arakala et al., 2009; Jeffers et al., 2006; Nandakumar et al., 2007) that are used the Fuzzy Vault for secure comparison of minutiae-based fingerprint templates. Contrary to that, literature provides the approach in which the evaluation value of the mobile authentication solutions is descriptively expressed.

In that context, it is necessary to highlight that (O'Gorman, 2003) was one of the first who compared authentication methods passwords, tokens and biometrics based on the main comparison factors such as security, convenience and cost. Also, in previous paper (Helkala et al., 2008) cover different areas of authentication and dealt with issues such as security, cost and usability. (The Electronic Authentication Guideline from NIST, 2008) covers different areas of remote authentication based on secrets and discusses security requirements as well as only the user factor. On the other hand, there are more papers that cover comparisons within categories. An example is (Pond et al., 2000) that covers within the 'something you know' - category, (Abott, 2003 and Husemann, 1999) within the 'something you have' – category, while (Maio et al., 2002; Phillips et al., 2000; Mansfield et al., 2002; Maltoni et al., 2003) within the 'something you are' - category. Also, in previous researches (Maltoni et al., 2009) as well as (Karovaliya et al., 2015) are dealt with comparison of commonly used biometric traits where descriptive values are classified into three levels (high, medium, low).

3. METHODOLOGY OF THE FUZZY EXPERT SYSTEM DEVELOPMENT

In this section, an innovative methodology approach of FES development for evaluating mobile solutions is introduced. The essence of the proposed methodology is that certain imprecision and indeterminacy presented as linguistic expression in mobile authentication methods can be changed with fuzzy number. The objective of this methodology is that by means of suitable inference rules manages and explores the knowledge in specific mobile authentication domain throughout reasoning value of authentication methods. This methodology is oriented towards numerical processing. In figure 1, the methodology of the fuzzy expert system design is given by means of the generic structure.

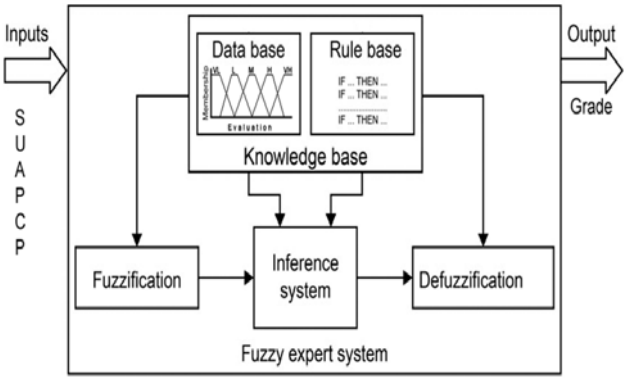

Fig. 1. The generic structure of fuzzy expert system for evaluation of mobile solutions.

This system can be divided into several functional blocks such as rule base, database, fuzzy inference system, fuzzification and defuzzification. The rule base contains the fuzzy rules while a database defines the membership functions (MFs) of the fuzzy sets used in the fuzzy rules. MF refers to the degree of truth i.e., in which extent the value of a particular parameter belongs to the defined set. Fuzzy inference system is an essential part of every expert system that lies at the core of the hybrid structure. This system performs the inference operations through the fuzzy rules defined in the knowledge base. In other words, fuzzy inference system enables the mapping from a given input to an output using fuzzy logic variables also denoted as linguistic variables. These variables have fuzzy value in range [0,1] that is assigned for each category of the input parameter. The objective of fuzzy logic is to define the situations of uncertainties via giving appropriate membership functions (MFs) for the input and output variables as well as

estimating the parameters of the system. The MF associates a weighting of the input, defines functional overlap between them, and ultimately determines an output response. Determining the number of input variables is based on the expert knowledge. This methodology approach of development of FES uses Mamdani-type (see Mamdani et al., 1975) because of its relatively simple structure as well interpretable nature of the rule base. This type develops the rules in the form of if–then methods, given by, if antecedent, then consequent. The common form of the fuzzy rule base system with multiple inputs and one output can be described as:

Rule 1: If A_1 is x_1 and A_2 is y_1 and . . . and A_n is z_1, then B is w_1:
Rule 2: If A_1 is x_2 and A_2 is y_2 and . . . and A_n is z_2, then B is w_2:
.....
Rule n: If A_1 is x_n and A_2 is y_n and . . . and A_n is z_n, then B is w_n,

where A_i (i=1,2,...,n), ($\forall$ n$\in$N) are input variables that describe the users priority; B is the output variable; and x_i, y_i, . . . , w_i are the linguistic terms used for the output variables.

Using these rules, the result of mobile solutions in term of percentage (%) can be computed. The fuzzification is a process of converting the numerical input variables into fuzzy variables with linguistic marks. The defuzzification is a process of converting the fuzzy results of the knowledge base in combination with the results of the fuzzy inference system into a crisp output value. The system uses a centroid method to aggregate the inference of fuzzy expert system (see Mamdani et al., 1975). The proposed fuzzy expert system for evaluation of mobile solutions value, has been implemented and tested by using MATLAB, by exploiting the fuzzy descriptions and processing made available by the Fuzzy System Toolbox.

4. DESIGN OF FUZZY EXPERT SYSTEM

As the above in prior section, when designing of the Fuzzy expert system the first process is a determination of the Fuzzy rule. In literature, this process is described as the most difficult process, one of the greatest difficulties. In paper the authors (Mount et al., 2001) are cited that "there is no all-encompassing, unified theory of how to acquire knowledge, and probably never will be". In this paper, the acquisition of knowledge is derived from human expert as well as from data found in available literature. The results from previous research are used as an important source for creating Table 1. Table 1 is defined as sublimate all acquired results from previous research. This table covers all authentication domains and brings all SUAPCP factors together in a single pattern. It implies that the contemporary mobile authentication methods and users' priorities are not separately viewed but only as a whole. Therefore, the contemporary user authentication methods intended for mobile devices include following methods PIN, Password, A one-time password-OTP, OTP using SMS, Mobile certificate, Fingerprint, Face, Iris, Voice/Speech, Keystroke Dynamics and Gait Recognition as well as Near field communication technology. The user's priorities used for forming Table 1 are security, usability, accessibility, pricing, complexity and privacy. These factors have been taken into consideration due to importance they have when selecting desired authentication.

Table 1. Comparison of various mobile authentication methods based on the perception of the authors.

Features	S	U	A	P	C	P
PIN	VL	VH	VH	VL	VL	VH
Password	VL	VH	VH	VL	VL	VH
A one-time password-OTP	L	H	H	M	M	H
OTP using SMS	M	H	H	M	M	H
Mobile certificate	M	L	M	M	M	M
Near field communication	M	L	M	M	M	M
Fingerprint	H	L	L	H	H	VL
Face	VH	VL	VL	VH	VH	VL
Iris	VH	VL	VL	VH	VH	VL
Voice/Speech	H	M	M	L	L	VL
Keystroke Dynamics	H	M	L	M	L	L
Gait Recognition	H	M	L	H	M	L

To design this FES the security is taken as the essential criterion. Hence, the optimal rule base is based on security. Descriptive values of particular authentication methods for concrete user's parameters are differentiated on the basis of available literature and given in comparison of the Table 1. Entries in the Table 1are based on the perception of the authors. Very High, High, Medium, Low and Very Low are denoted by VH, H, M, L and VL, respectively. These value mobile methods present quantification input that is a crucial step in the evaluation of mobile solutions. Hence, Table 1

gives comparison of various mobile authentication methods based on the main comparison factors such as SUAPCP.

The first step in the design of a fuzzy logic system is definition of fuzzy variables and selection of appropriate MFs, i.e., determination of input and output variables. Membership function shows in which extent a certain user's priority matches with the degree of membership. The design of this FES consists of six inputs and 1 output. The input variables consist of user's priorities that are presented as SUAPCP factors while the output variables present the value of mobile solutions. It is necessary to highlight that MF is the same for all users' priorities and because of that MF is presented with SUAPCP factors. The membership functions of SUAPCP factors with their linguistic variables are given in Figure 2. For input variables, a curve Gauss shape of a MF is employed to describe the fuzzy sets. It is very important to stress that the process of testing is made and for other function such as triangular, trapezoid and bell shaped but the best results are acquired for Gaussian MFs. This function is provided the slightest error on the output of this FES. Because of that, this function is used in this paper. The linguistic variables are classified into five categories i.e., five fuzzy sets such as very low, low, medium, high and very high. Linguistically, it implies that these variables are represented with five Gaussian membership functions. The importance of Gauss function is that approximate descriptive values of authentication methods can be specified as fuzzy numbers which represent quantitative input variable defined in the range from 0 to 1. In the other words, the Gaussian membership functions allow to determine rule table for fuzzy input as fuzzy interval for each of linguistic variable.

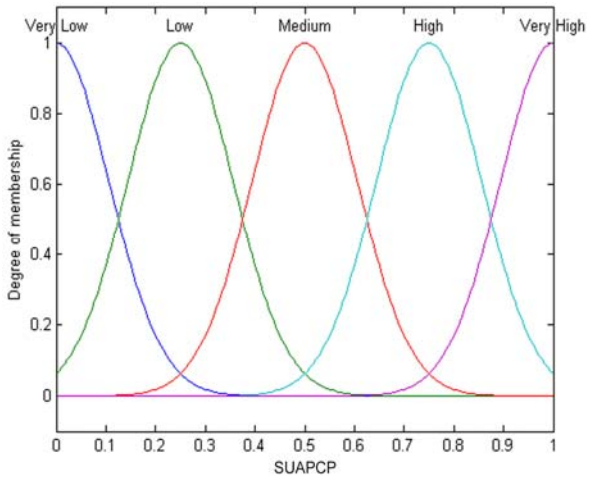

Fig. 2. Membership functions for SUAPCP factors.

Based on Figure 2, descriptive values of contemporary user authentication methods intended for mobile devices are changed with fuzzy number. The values of fuzzy numbers are assigned by authors and presented in Table 2. It is necessary to highlight that the assigning values for particular technology is made on the basis of comparison Table 1 whose base were also based on the earlier comparison approaches such as (Pond et al., 2000; Maio et al., 2002; Maltoni et al., 2009; Karovaliya et al., 2015).

Table 2. Assigned values for contemporary user mobile authentication methods.

Features	S	U	A	P	C	P
PIN	0.05	0.9	0.9	0	0.05	0.95
Password	0.1	0.95	0.95	0	0.1	0.95
A one-time password-OTP	0.25	0.85	0.85	0.4	0.4	0.85
OTP using SMS	0.4	0.75	0.75	0.5	0.5	0.75
Mobile certificate	0.6	0.2	0.2	0.6	0.6	0.4
Near field communication	0.5	0.3	0.3	0.4	0.4	0.5
Fingerprint	0.8	0.25	0.25	0.75	0.75	0.05
Face	0.9	0.1	0.1	0.9	0.9	0.05
Iris	0.95	0.05	0.05	0.95	0.95	0.05
Voice/Speech	0.65	0.5	0.5	0.2	0.2	0.1
Keystroke Dynamics	0.7	0.45	0.35	0.55	0.35	0.15
Gait Recognition	0.75	0.55	0.25	0.75	0.55	0.15

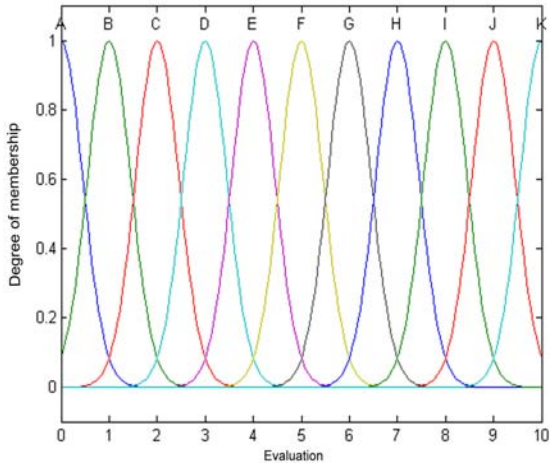

Fig. 3. Membership functions for evaluation of mobile solutions.

In this fuzzy expert system, the proposed fuzzy inference system is based on the defuzzification module, where output is represented in the range [0, 10]. The output of the system, which is the evaluation of mobile solutions, has eleven MFs with eleven grades. Also, a curve Gauss shape of a MF is employed to describe the fuzzy sets for output variables. The grades are classified from A-K on based of expert's knowledge, where the grade A is presented at lower value while the grade K at the utmost value. MFs and the grades for evaluation of mobile solutions as the output parameter are given in Figure 3.

In the next step, fuzzy rules are formulated to establish the relationship between the input and the output in a fuzzy system. A fuzzy rule based model is developed from the expert knowledge. The number of fuzzy rules is related to the number of fuzzy sets for each input variable. Hence, taking into consideration the six input and five linguistic variable, the maximum number of rules for this system is 15 625. When the number of fuzzy rules is too large, there are twofold limited factors for the work system. First, system may require more time to produce output because of the large number of computational steps. Second, to function this system needs large memory space. Thus, if it is possible to determine the approximate output of the fuzzy expert system without increasing the rules, then the overall system architecture is simplified, and reduces computational steps as well as the memory space. Therefore, only 100 of 15 625 possible rules are selected for constructing the rule base. On the basis of the authors expert knowledge a choice reduction of the primary rules base is made for every grade. This reduction doesn't affect the accuracy of the results. Once all of the fuzzy rules are defined, it is possible to examine performance of the fuzzy expert system.

5. DISCUSSION

After the setup of the fuzzy inference system and its implementation, the system is applied for the contemporary user mobile authentication methods. In Table 3, the results are given and indicated that the proposed FES is effective in getting numeric value of mobile authentication methods. The results are acquired on the basis of the assigned quantification value of mobile authentication methods. From the results acquired, it is evident that the fuzzy logic technique is a good tool for handling of ambiguous and imprecise information that are presented in mobile authentication domain within the range of input parameters under consideration.

Based on the comparison of acquired results it can be clearly concluded that technology based on "something you are", where security factor is priority, provides the utmost grade, while technology based on "something you know" provides the lowest grade. With the given inputs, the results are shown as "GRADE" for each of mobile authentication method. The results obtained from the system reveal that biometric method substantial provides the utmost level of security in mobile authentication. According to results acquired from Table 3, for security factor as priority, Iris authentication methods have utmost grade 7.7921 while PIN is mobile authentication method with the lowest value of grade 2.024.

Table 3. The Grade of value for contemporary user mobile authentication methods based on assigned values of expert knowledge.

Authentications method	Grade
PIN	**2.024**
Password	**2.0261**
A one-time password-OTP	**2.8907**
OTP using SMS	**3.605**
Mobile certificate	**5.5290**
Near field communication	**5.0246**
Fingerprint	**6.9992**
Face	**7.6079**
Iris	**7.7921**
Voice/Speech	**6.1772**
Keystroke Dynamics	**6.5894**
Gait Recognition	**6.7361**

However, for all the other user priorities PIN methods provides the best results. Just that fact explains why is PIN the most suitable methods for using in multifactor authentication approaches. The advantage of the designed FES is a possibility to change user's priority and form crisp value of a mobile solution. In that case, when evaluating mobile authentication methods neglects the factor of security i.e. it assigns zero value for the security factor. Also, for multifactor mobile solutions it is necessary to determine the arithmetic mean of authentication methods which represents the solution, in order to obtain a unique crisp value. To present the validity and effectiveness applied in the proposed FES towards multifactor authentication solutions, some examples from practice are taken and tested. The results of grade are given in Table 4. From the results acquired in Table 4, it can be concluded that in the authentication approach, the process of multifactor authentication accomplishes synergistic approach. When integrating different factors through multifactor authentication, the individual factors keep their own original form while adding a new level of security. Hence, biometric methods such as Iris or Face can be recommended as a fundamental technology of weapon in the fight to achieving better security factor. Table 4 shows that this FES is a very efficient and accurate method to calculate the value of multifactor authentication methods.

The variation of authentication methods with different combinations of users parameters are studied using the fuzzy response for evaluation of mobile solutions. The output evaluation of the fuzzy inference system enables analyzing the effects and trends of the user's parameter with the variation of evaluation of mobile solutions. Figure 4(a), (b),

(c) and (d) show only some examples of relationships. In the context of paper subject, the relevance of these Figures is to show how is possible to find the maximum of function for all presented user's parameters in order to achieve the highest grade of mobile solutions. In Figure 4(a) is given the influence of the user's parameters security and usability on evaluation mobile solutions. As it can be observed from the diagram, the maximum of function covers diagram's upper surface where security has a high value, while the usability is in ranges from the minimal to maximum value.

Table 4. The results of grade for multifactor authentication solutions.

Authentication solution – (source)	Grade
Face + OTP (Karovaliya et al., 2015)	5.2493
Password + keystroke dynamic (Monrose et al., 2001)	4.3078
Password + OTP (Gunson et al., 2011)	2.4584
Fingerprint + Password (Go et al., 2014)	4.5126
OTP + Fingerprint (Cha et al., 2013)	4.9449

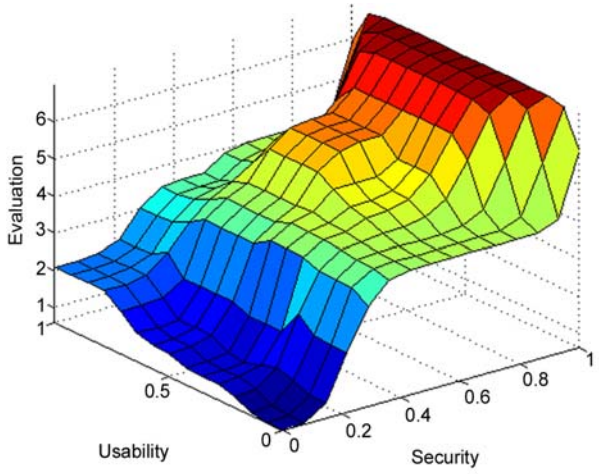

Fig. 4(a). Surface plot for the user's parameters, namely, usability and security.

In Figure 4(b) is given the influence of the users parameters security and accessibility on evaluation mobile solutions. As it can be clearly observed from the diagram, the maximum of function covers the diagram's upper layer surface where the security is in range from the middle to maximum value. Also, this diagram point out that there is resemblance between these factors. Actually, this fact indicates a close relation between these factors. Based on the similar characteristics of this and previous diagram, it can be concluded why authors like Thatcher et al. [37] cite the accessibility factor as a subset of usability.

In Figure 4(c) is given the influence of user's parameters, privacy and security on the evaluation of mobile solutions. As shown in the Figure 4(c), the maximum of function covers the diagram's upper layer surface, where the security is in range from the middle to maximum value, while the privacy is in range from the minimal to middle value.

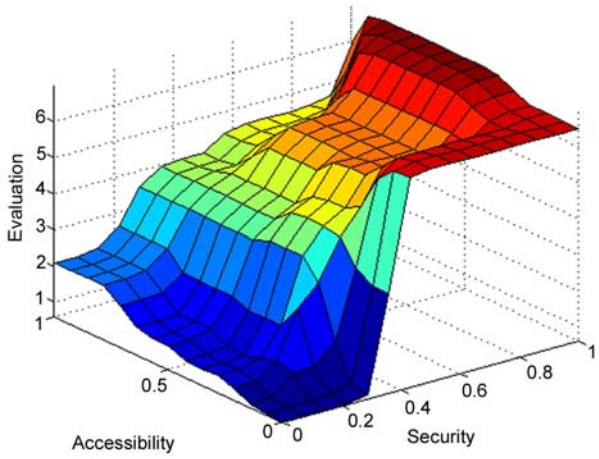

Fig. 4(b). Surface plot for the user's parameters, namely, accessibility and security.

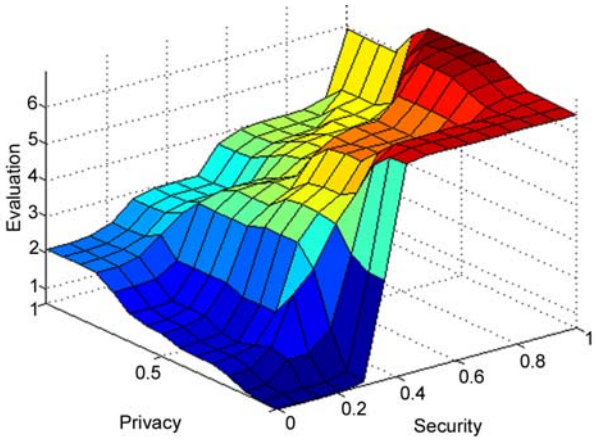

Fig. 4(c). Surface plot for the user's parameters, privacy and security.

Finally, the variation of security and pricing on the evaluation of mobile solutions is given in Figure 4(d). As shown in the Figure 4(d), the maximum of function covers the diagram's upper layer surface, where the security has a maximum value, while the pricing is in range from the minimal to middle value.

In this paper, all these presented facts confirm that SUAPCP factors are closely related as well as that each SUAPCP factor plays an important role in contemporary mobile authentication domain. On the basis of the results presented in this paper, regarding to the experts and taking the users priority SUAPCP as a criteria into considerations, it is possible to give recommendation to the following rule;

IF security is very high AND usability is very high AND accessibility is very high AND pricing is very low AND complexity is very low AND privacy is very high THEN grade is utmost – K.

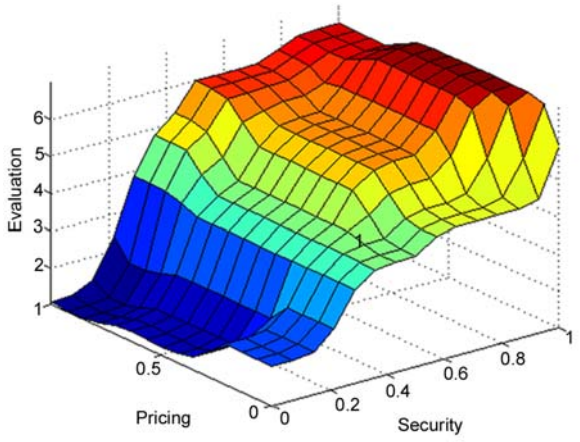

Fig. 4(d). Surface plot for the user's parameters, namely, pricing and security.

The recommended rule presents a template that should be strived to create the most suitable authentication solution. Importance of the FES development is based on facts that this system provides crisp value of mobile solutions. In that way, with numeric measurement value of mobile solutions, it is possible to design new improved multifactor authentication solutions. In comparison to pertinence of fuzzy logic in IT this concept is still new in the field of mobile authentication methods. This is clearly highlighted from the fact that the contribution to the literature based on fuzzy logic is much less from IT compared to other science fields such as medicine, economics, etc. Unlike other science fields, such as the field of economy, determination of quantification issue is relatively complex in this domain. The complexity refers to defining metric approach that is very complex issue for all user priorities, except pricing. Taking into account that metric approach is still in development in information technologies, it presents certain limitations to quantification issue in mobile authentication domain. With more precise determination of quantification inputs the results of mobile solutions assessments will be even more precise. However, the utility of fuzzy logic and other techniques as such in various domain of IT can attain popularity in the near future.

6. CONCLUSIONS

In this paper, the fuzzy expert system for evaluation of mobile authentication solutions is developed and discussed. This paper shows how fuzzy system could be used successfully for evaluation of mobile authentication solutions. Six input variables SUAPCP are used for the fuzzification method while output variable, namely, grade in range [0, 10] is used. A set of 100 rules is defined on the basis of using the database as well as the expert knowledge in the mobile authentication domain. Based on acquired results, a recommended rule can be given in regards to creating the most suitable mobile authentication solution. If the security factor should be used as priority then biometric methods such as, for example Iris or Face, need to be included in mobile solutions.

One of the major advantages of the developed system is that it can deal with inaccurate or imperfect information in approaches to mobile authentication. This system offers better quantification of mobile authentication solutions, the assignment of a concrete numeric value to a specific mobile authentication solution and simplified decision-making process for selection of authentication method. Furthermore, this method is very practical. In addition to this advantage of developed system has flexibility and easy of modifications because FES can be used when new authentication solutions are being designed. The changes require only adding some other variables (mobile authentication methods or user priority) or rules without additional development. Importance of the designed FES is a possibility to be applied for any information system. Moreover, further improvement of the FES is possible by introducing a wider set of authentication methods as well as users priority with a larger number of linguistic variables, and a wider range of output crisp grade. This FES has for a goal to fill the gap in the current research and to help developers to create the best mix of mobile authentication. The major drawback of this system is within quantification where gathering data and extracting important numeric values are often complicated because of unavailability of statistical information. Therefore, as a direction for future research, one could highlight determination of the quantification issue in mobile authentication domain, i.e. defining metric approach.

ACKNOWLEDGEMENTS

This paper 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

Abott, J. (2003), Smart cards: How secure are they?, www.sans.org/reading_room/whitepapers/authentication/131.php, (Accessed 18.07.2015).

Arakala, A. Jeffers J., and Horadam K.J, (2009), Fuzzy extractors for minutiae- based fingerprint authentication. In:Lee,S.W., *Li, S.(eds.) Proceedings of the Second International Conference in Biometrics*, Springer, Seoul, South Korea, 760–769.

Bellman R., and Zadeh, L.A. (1990). Decision making in a fuzzy environment, *Manage. Sci.* 17, 141–164.

Burr, W.E., Dodson, D.F., and Polk, W.T. (2008). Electronic authentication guideline. Technical Report 800-63, National Institute of Standards and Technology, 2008.http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. (Accessed 10 May 2015).

Cărbureanu, M. (2014). The Development of a Neuro-Fuzzy Expert System for Wastewater pH Control. *Journal of Control Engineering and applied Informatics*, 16(4), 30-41.

Cha, B.R., Kim, Y.I. and Kim, J.W. (2013). Design of new P2P-enabled Mobile-OTP system using fingerprint features. *Telecommunication Systems*, 52(4), 2221-2236.

Dumitrache, I., and Dragoicea, M. (2006). Some Problems Of Advanced Mobile Robot Control. *Journal of Control Engineering and applied Informatics*, 7(4), 11-30.

Feng, G., (2006). A survey on analysis and design of model-based fuzzy control systems, *IEEE Transactions on Fuzzy Systems,* 14(5), 676–697.

Go, W., Lee, K., and Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal of Intelligent Manufacturing,* 25, 217–230.

Gunson, N., Marshall, D., Morton, H., and Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*. 30 (4), 208–220.

Helkala K., and Snekkenes, E. (2008). A Method for Ranking Authentication Products. *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008).*

Husemann, D. (1999), The smart card: don't leave home without it", *IEEE Concurrency,* 7, 24-27.

Jeffers, J., and Arakala, A.(2006). Minutiae-based Structures for a Fuzzy Vault, *Proceedings of the Biometrics Consortium Conference, Biometrics Symposium, 1–6*. IEEE Press, Baltimore, Maryland, USA, (2006).

Karovaliya, M., Karedia, S., Oza, S., and Kalbande D.R. (2015). Enhanced security for ATM machine with OTP and Facial recognition features. *Procedia Computer Science,* 45, 390 – 396.

Kramar, D. Cica, D. Sredanovic, B., and Kopac, J. (2015). Design of fuzzy expert system for predicting of surface roughness in high-pressure jet assisted turning using bioinspired algorithms. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing,* Available on CJO 2015 doi:10.1017/S0890060415000189

Linda, O. and Manic, M. (2011). Uncertainty-robust design of interval type-2 fuzzy logic controller for delta parallel robot, *IEEE Transactions on Industrial Informatics*, 7(4), 661–670.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J., and Jain, A. (2002). FVC2000: Fingerprint Verification Competition, *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 24(3), 402-412.

Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*, Springer, ISBN: 0387954317.

Maltoni, D., Maio, D., Jain, A.K., and Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Second Edition, Springer-Verlag London Limited.

Mamdani, E., and Assilian, S. (1975). An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller, *International Journal of Man-Machine Studies,* 7(1), 1-13.

Mansfield, A., and Wayman, J. (2002). Best practices in Testing and Reporting Performance of Biometric Devices. *NPL Report CMSC 14/02, Version 2.01.*

Monrose, F., Reiter, M.K., and Wetzel, S, (2001). Password hardening based on keystroke dynamics. International Journal of Information Security, Springer, Heidelberg 1, 69–83.

Mount, C., and Liao, T.W. (2001). Prototype of an intelligent failure analysis system, in *Proceedings of the 4th International Conference on Case-Based Reasoning (ICCBR '01)*, Vancouver, BC, Canada, 716– 731.

Nandakumar, K., Jain, A.K., and Pankanti, S. (2007) Fingerprint-based Fuzzy vault: implementation and performance. *Information Forensics and Security, IEEE Transactions on*, 2(4), 744–757.

Nezam, N., and Dumitrache, I. **(**2002). Mamdani, Sugeno fuzzy systems and control the output flow of an equalization basin. *Journal of Control Engineering and applied Informatics*, 4(1), 27-32.

O'Gorman, L. (2003), Comparing passwords, Tokens, and Biometric for User Authentication, In *Proc. of IEEE,* 91, 2019-2040.

Pedrycz, W. Park, B.J., and Oh, S.K. (2008). The design of granular classifiers: a study in the synergy of interval calculus and fuzzy sets in pattern recognition, *Pattern Recognation,* 41, 3720–3735.

Phillips, P. J., Moon, H., Rizvi, S. A., and Rauss, P. J. (2000). The FERET Evaluation Methodology for Face-Recognition algorithms, *Pattern Analysis and Machine Intelligence*, IEEE Transactions on*,* 22(10), 1090-1104.

Pond, R., Podd, J., Bunnell, J., and Henderson, R. (2000). Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates, *Computers & Security,* 19, 645-656.

Precup, R.E., and Hellendoorn, H. (2011). A survey on industrial applications of fuzzy control, *Computers in Industry*, 62(3), 213–226.

Thatcher, J., Waddell, C.D., Henry, S.L., Swierenga, S. Urban, M.D., Burks, M. Regan, B. and Bohman P. (2003). Constructing Accessible Web Sites. Glasshaus, San Francisco.

Vaščák, J., and Paľa M., (2012). Adaptation of fuzzy cognitive maps for navigation purposes by migration algorithms, *International Journal of Artificial Intelligence*, 8 (12), 20–37.

Wallam, F., and Abbasi, A.R. (2014). Evaluating the Transient Handling Capability of a Fuzzy Logic Controller for a Pressurized Heavy Water Reactor. *Journal of Control Engineering and applied Informatics*, 16(2), 40-48.

Zadeh, L. A. (1965). Fuzzy Sets, *Information and Control*, 8(3), 338-353.

Zadeh, L.A. (1975). Fuzzy logic and approximate reasoning, *Synthese,* 30(3), 407–428.