A Multimodal Biometric System Based on an Active Database Paradigm

Kornelije Rabuzin, Mirko Maleković, Miroslav Bača

Faculty of Organization and Informatics, Pavlinska 2, 42000 Varaždin, Croatia
{kornelije.rabuzin, mirko.malekovic, miroslav.baca}@foi.hr

Today, on many occasions and in many different places, one must be authorised in order to use certain services or applications or to access protected data. A user (person) can be authorised in three different ways or combinations of ways: it is either information that the user knows, something that the user possesses or a measurement of some physical or psychological characteristics unique to that user, i.e. biometric characteristics. In this paper we emphasize this third possibility. When talking about biometrics we can distinguish two basic types of systems: unimodal and multimodal. The main difference is that the unimodal biometric system is based solely on a single biometric feature, while multimodal biometric systems combine several features. We intend to show how active databases could be used in order to implement a multimodal (unimodal) biometric system and reduce the time needed for authorisation (identification or verification). Specifically, the concept of reactivity upon which active databases rely could be the core of a multimodal biometric system, as will be shown in the paper. We will especially consider the use of complex events used in active databases for authorisation purposes.

Key words: ADBMS, active database, complex events, biometrics, biometric system

Dandanes se velikokrat dogodi, da ljudje, ki hočejo koristiti določene storitve ali aplikacije ali želijo dobiti pristop do zaščitenih podatkov itd., potrebujejo avtorizacijo. Uporabnik se lahko avtorizira na tri različne načine oziroma s kombinacijo teh treh načinov: s pomočjo nečesa, kar uporabnik pozna, s pomočjo nečesa, kar uporabnik poseduje, ali s pomočjo merjenja določenih fizičnih ali psihičnih značilnosti, ki so lastne in enkratne vsaki osebi, tj. tako imenovanih biometričnih značilnosti. V tem prispevku bo poudarek na tem zadnjem, tretjem načinu. Ko govorimo o biometriki, lahko razlikujemo med dvema osnovnima tipoma biometričnih sistemov - enomodalnim in večmodalnim biometričnim sistemom. Glavna razlika med njima je v tem, da enomodalni biometrični sistem temelji le na eni biometrični značilnosti, medtem ko večmodalni biometrični sistem za avtoriziranje posameznika kombinira več biometričnih značilnosti. V tem prispevku bomo pokazali, kako se lahko pri vgradnji večmodalnega (enomodalnega) biometričnega sistema uporabijo aktivne baze podatkov, s čimer se skrajša čas, ki je potreben za avtorizacijo (identifikacijo ali verifikacijo). Med drugim bomo pokazali, da je koncept reaktivnosti, na katerem temeljijo aktivne baze podatkov, lahko jedro večmodalnih biometričnih sistemov. Posebno pozornost bomo posvetili kompleksnim dogodkom za avtorizacijske namene, ki se v glavnem uporabljajo v aktivnih bazah podatkov.

Ključne besede: ADBMS, aktivna baza podatkov, kompleksni dogodki, biometrika, biometrični sistem

1 Introduction

An organization may be defined as a set of people gathered together to accomplish a common goal or goals which are of great importance for the organization itself (Žugaj, Šehanović and Cingula, 2004). In order to accomplish these goals, people must use certain resources (data, information, etc.). Some resources are not intended to be *public*, but rather to be known or accessed only by a small number of authorised individuals. For example, if one wants to use e-mail, one must have an account (a login name and password). Today, people often possess several different accounts in order to use certain services, applications or to access protected data.

Generally speaking, a user can be authorised in three different ways: either through information the user knows (passwords), something the user possesses (different cards) or by measuring physical or psychological characteristics which are unique to the user, i.e. biometric characteristics. With respect to passwords, people usually choose passwords which are easy, intuitive and generally not complex enough to afford secure authorization. Registration numbers or birth dates are used as well as names, and users usually write them down somewhere. On the other hand, smart cards can be stolen, which is not good either. For personal recognition, biometrics rely on who you are or what you do, as opposed to what you know (a password) or what you have (some card). Biometric features are intrinsic to every human and are therefore a suitable means to authorize users. Biometric-based identification is preferred over traditional methods because a biometric cannot be forgotten or lost (Prabhakar and Jain, 2002).

Although the relational data model has been used for over 30 years, the development and use of new technologies, object-oriented programming, real time systems, etc. have resulted in the emergence of different kinds of database systems, among which are also Active Database Management Systems (ADBMS). ADBMS is a conventional database system capable of reacting to events of interest which occur within the database or outside it (Andler and Hansson, 1998; Paton 1998). To understand how this works in practice, the basic concept on which an ADBMS relies, the concept of ECA or active rules, needs to be considered (ECA stands for Event-Condition-Action). When certain events occur (ON EVENT) and certain conditions are fulfilled (IF CONDITION), specified actions are performed automatically (THEN ACTION). These actions are performed without any need for user intervention. At the conceptual level people often talk about ECA rules, but these rules are mostly implemented using triggers in specific ADBMS. More on ECA rules can be found in (Andler and Hansson, 1998; Montesi and Torlone, 2002; Dittrich et al., 2003; Rabuzin and Maleković, 2005).

Databases nowadays are often used for biometric purposes. Due to the capability that huge amounts of data can be stored, updated and extracted efficiently, large quantities of *biometric data* (pictures, video clips, etc.) can be stored in databases.

According to Paton (1998), most database applications are still passive, i.e. they do not use active features even though the underlying DBMS (Database Management System) may offer them. As will be shown later, sample processing and decision making in a biometric system are performed outside of the database; the module responsible for comparison is usually placed outside of the database and the biometric system operates as a passive application. This means that data must be polled from the database and data processing as well as decision making are performed outside of the database. We will try to convert a (multimodal) biometric system into an active application. In that way the decision-making module will be placed within the database with the result that the time needed for authorisation can be significantly reduced. The functionality of multimodal biometric systems can be expressed (borrowing terms used in active database theory) as *real-time complex event detection*. The basic idea is that we define a complex event consisting of several (n) simple events, and each simple event represents a fact that the user was identified by means of one biometric features that comprise the multimodal biometric system . This paper will show how this was done and present some preliminary results.

The rest of the paper is organized as follows: Section 2 deals with biometrics, Section 3 discusses unimodal and multimodal biometric systems, Section 4 briefly presents active database theory, Section 5 describes how we have modelled the identification problem using complex events, Section 6 presents preliminary results and, finally, Section 7 summarizes the findings of the paper.

2 Biometrics

Biometrics are automated methods of identifying a person or verifying the identity of a person based on physiological or behavioural characteristics (Podio and Dunn, 2001). Biometrics is a method using the physiological or behavioural features of a person for automated detection and verification of their identity (Bača and Rabuzin, 2005).

A dozen or so biometric features are in use today, the most applicable of which are the fingerprint and the facial image (Bača and Rabuzin, 2005). Both of these features are used daily in personal identification and verification, ranging from police lineups to police files, which explains why end users also find them quite acceptable. Regarding all currently known biometric features, two main types can be distinguished, i.e. contact and contactless features (Bača and Rabuzin, 2005). This distinction is a result of observing the user's condition during the process of singling out a biometric feature.

Authors have formulated the biometric verification problem as follows (Prabhakar and Jain, 2002): "Let the stored biometric signal (template) of a person be represented

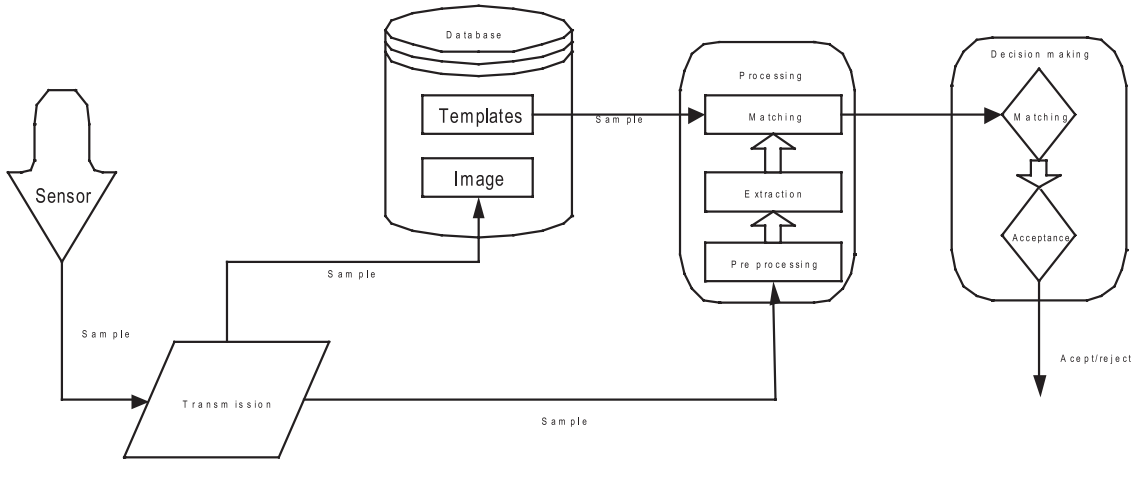

Figure 1. The main modules of a biometric system (Bača and Rabuzin, 2005)

as ***S*** and the acquired signal (input) for authentication be represented by ***I***. Then the null and alternate hypotheses are:

H0: $I \neq S$, input fingerprint does not come from the same finger as the template,

H1: $I = S$, input fingerprint comes from the same finger as the template.

The associated decisions are as follows:

D0: person is an imposter,

D1: person is genuine.

The verification involves matching ***S*** and ***I*** using a similarity measure. If the matching score is less than a defined decision threshold ***T***, then decide ***D0***, else decide ***D1***."

Most currently known and applied biometric features contain a flaw which makes them impossible to be considered ideal. Most commonly, biometric features must meet the following requirements (Frischholz and Dieckmann, 2000): universality, uniqueness, permanence, collectibility, accuracy and acceptability, as well as the likelihood of circumvention involved. Consequently, the ideal biometric feature has to meet the following criteria (Jain, Bolle and Pankanti, 1999): it has to be permanent and inalterable in terms of time, the procedure of gathering personal features has to be inconspicuous and conducted by means of devices involving minimal or no contact, it has to enable total automation of the system, the system has to be highly accurate and its operating speed such that it enables real-time operation.

As can be seen in *Figure 1*, each biometric system contains four main modules: the sensor module responsible for singling out features from raw data, the feature extraction module responsible for extracting a set of features best representing the features of the raw data, the feature-matching module which ensures the classification and matching of the set of features extracted with templates usually stored in the database, and the decision-making module responsible for accepting or rejecting the user (Bača and Rabuzin, 2005).

Considering that none of the biometric features is sufficiently reliable, combining single features in one of two possible ways – by means of unimodal or multimodal systems – arises as an immediate solution. Each of the two approaches has its advantages and disadvantages, so they should be used in strict accordance with the policy of the system they are intended to secure. We can end this section with the following statement (Prabhakar, Pankanti and Jain, 2003): biometrics cannot be lost or forgotten.... they are difficult for attackers to forge and for users to repudiate.

3 Unimodal vs. multimodal biometric system

A unimodal biometric system uses a single biometric feature for personal identification. It is typical that this (one) feature is singled out by means of several technologically distinct methods and systems (Bača and Rabuzin, 2005). Multimodal biometric systems use several biometric features and technologies simultaneously. Although this approach may seem far more effective at first glance than unimodal systems, it is necessary to examine the implied limitations. These limitations are related to applicability within a certain domain, due to unacceptable performance, as well as an inability to function over a large number of users (Bača and Rabuzin, 2005). According to (Brunelli and Falavigna, 1995), the question arises as to the chief purpose the multimodal biometric system is to be used for, how it operates, biometric features to be integrated, as well as how many biometric features are needed in total.

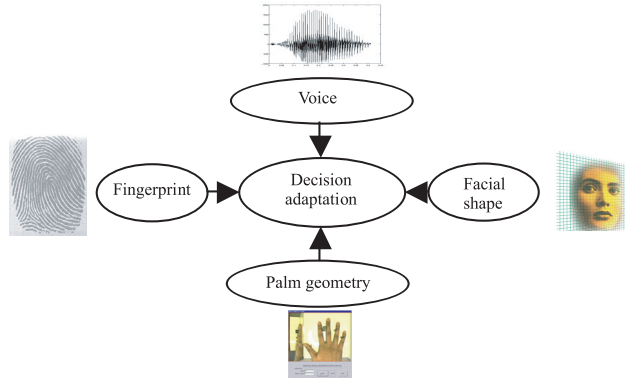

Figure 2. Multimodal biometric system (Bača and Rabuzin, 2005)

The strength of a multimodal system relies exclusively on the characteristics of individual biometric features to be included in the system itself (Brunelli and Falavigna, 1995). These characteristics, similar to those in a unimodal biometric system, refer to accuracy and speed. The accuracy indicates the extent to which a multimodal biometric system is reliable and confidential when distinguishing a legitimate user from an imposter; the speed of a multimodal biometric system indicates the time needed by the system to perform the personal identification (Bača and Rabuzin, 2005). It is only through appropriate and relatively fast integration of biometric features that the overall speed of a multimodal biometric system can be increased. A multimodal system combining fingerprints, facial shape, voice and palm geometry is illustrated in *Figure* 2:

Initially, the question arises as to the chief purpose of the multimodal biometric system, how it operates, biometric features to be integrated, as well as how many biometric features are needed (Jain, Bolle and Pankanti, 1999; Frischholz and Dieckmann, 2000). Further on, the obstacle to be dealt with is the adequate selection of biometric features to constitute such a system (Brunelli and Falavigna, 1995). The selection of biometric features to be used in both unimodal and multimodal biometric systems is fairly complex, and there is no ideal biometric feature; we have previously given a brief review of features according to their usage and requirements, and addressed the question of proper biometric features selection in (Bača and Rabuzin, 2005; Rabuzin, Bača and Sajko, 2006). Unimodal biometric systems can be applied for a single given degree of security, depending on whether they use a strong (iris pattern, DNA), medium (fingerprint) or soft (voice) feature. Unlike these, multimodal systems cover a wide range of different

degrees of security, which makes them considerably more acceptable in daily use.

4 Active database management system

It has already been mentioned that active database management systems have the capability of reacting automatically to certain events which occur within a database or outside it. An event can be defined as a state change of interest which requires intervention (Rabuzin and Maleković, 2005). These events can be divided into two categories: simple and complex. Simple events are basic database operations like *INSERT*, *UPDATE* or *DELETE*, or time events which can be subdivided into absolute, periodic and relative time events. Transaction events (for example, the beginning or the end of a transaction), method events (used in active object-oriented DBMSs) and abstract events are also treated as simple events. Complex events consist of one or more simple events connected with logical operators (if you have simple events *E1* and *E2*, then $E1 \wedge E2$ or $E1 \vee E2$ represents a complex event), but there are also special kinds of complex events such as *REPEAT*, *SEQUENCE* or *NEGATION* which take one or more simple events as parameters. More on different kinds of events can be found in (Koschel and Lockemann, 1998; Paton 1998; Tan and Goh, 1999; Xiaoou, Marín and Chapa, 2002).

The event component of an abstract active rule determines when the rule should be considered, the condition component determines whether the action part of the rule should be executed, and the action component of the rule represents the actions to be executed. An active rule is triggered when the event specified in the event component of that rule occurs. The triggered rule does not have to be executed; this depends on condition evaluation. Each ADBMS has a language which is used for trigger specification (definition) and possesses an execution model which determines how the rules are going to be executed. Active databases are used in many different areas (Paton 1998). Due to the increasing awareness about what active rules can do, interesting papers concerning their use are (Bailey, Poulovassilis and Wood, 2002; Thalhammer, Schrefl and Mohania, 2001; Casati, Fugini and Mirbel, 1999). We would add biometric systems as well.

There are several arguments justifying the use of ADBMSs. First of all, it is cheaper to build such an application and its performance is better, at least when a small number of triggers is involved (Paton 1998). All constraints are written in one place, making it possible for calculations and queries to be grouped into units which could be executed on the server. In that way the client/server communication is reduced and performance is better (less time is needed). Secondly, such an application is smaller and easier to maintain (Paton 1998). Active rules can be added or deleted independently of other rules (if they have to be changed). Thirdly, they represent a declarative approach, and according to Date (2000), "the trend has clearly always been away from procedural and toward declarative – that is, from how to what". Active databases are very useful, but in certain cases they exhibit unpredictable behaviour due to complex rule processing. This happens only in cases when certain relationships (interdependencies) between rules exist, and this must be kept in mind.

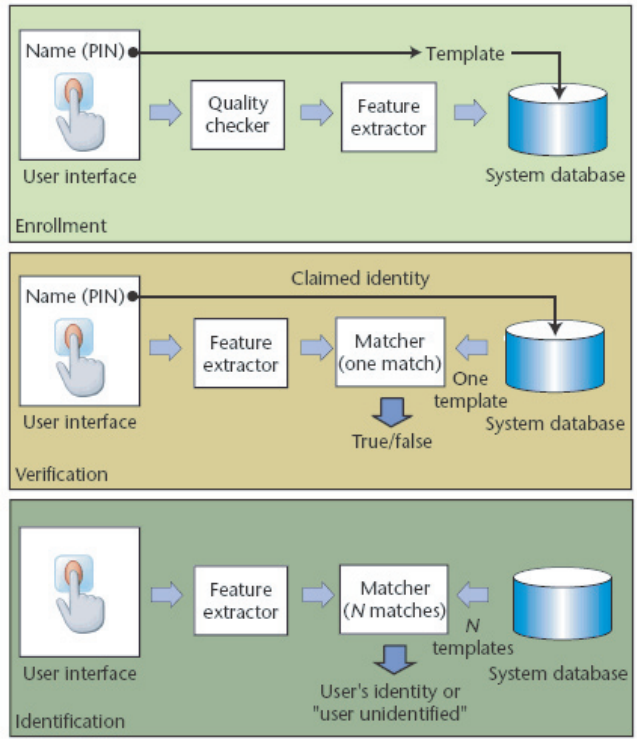

Figure 3. Block diagrams of enrolment, verification and identification tasks (Prabhakar, Pankanti and Jain, 2003)

5 Complex events used within multimodal biometric systems

Databases are used for biometric purposes to a great extent. Due to the huge capability for storage of data, updated and extracted efficiently, a large quantity of *biometric data* can thus be stored within databases.

Enrolment creates an association between an identity and its biometric characteristics: in a verification task, an enrolled user claims an identity and the system verifies the authenticity of the claim based on his/her biometric features, whereas an identification system identifies the enrolled user based on his/her biometric characteristics without the user having to claim an identity, as can be seen in *Figure 3.* (Prabhakar, Pankanti and Jain, 2003). Another point of view is delineated in *Figure 4*:

According to Podio and Dunn (2001), biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during login); identification is a much harder problem than verification because an identification system must perform a larger number of comparisons.

As can be seen in *Figures 1, 3* and *4,* sample processing and decision making in a multimodal system are performed

outside of the database; the module responsible for comparison is placed outside of the database and the system operates as a passive application. This means that data must be polled from the database and that data processing (as well as the decision-making process) is performed outside of the database (for multimodal biometric systems, even more data has to be extracted).

According to Paton (1998) most database applications are still passive, i.e. they do not use any active features even though the underlying DBMS may offer them; active applications use these capabilities. In *Figures 1, 3 and 4*, we can see that biometric systems are treated as passive applications too. Since we have already mentioned that active databases (triggers) have certain advantages when compared to application solutions (the execution time of triggers is very small and can be even neglected, servers usually possess better performance, etc.), we think that active databases represent a much better solution when building a biometric system – namely, the decision-making module can reside within the database and thus the performance of the biometric system can be significantly improved. The functionality of a multimodal biometric system can be considered as real-time complex event detection. The basic idea is that we define a complex event consisting of several (n) simple events, and each simple event represents a fact that a user was identified by a single biometric feature within the multimodal biometric system. Since a multimodal biometric system uses several biometric features in order to authorise a person (n features), the complex event *User_authorization* could consist of n simple events and could be written as follows:

$$User\_authorization = Biometric\_feature_1 \wedge Biometric\_feature_2 \wedge \ldots \wedge Biometric\_feature_n$$

or more concretely, as in *Figure 2:*

$$User\_authorization = Fingerprint \wedge Facial\_shape \wedge Palm\_geometry \wedge Voice$$

There are certain cases where user authorization must be performed within a given time interval t (Jain, Bolle and Pankanti, 1999); in that case we can use the complex event constructor *within* which denotes that an event (simple or complex) must occur within time interval t. The idea of a complex event *within* was presented in *Rock and Roll*

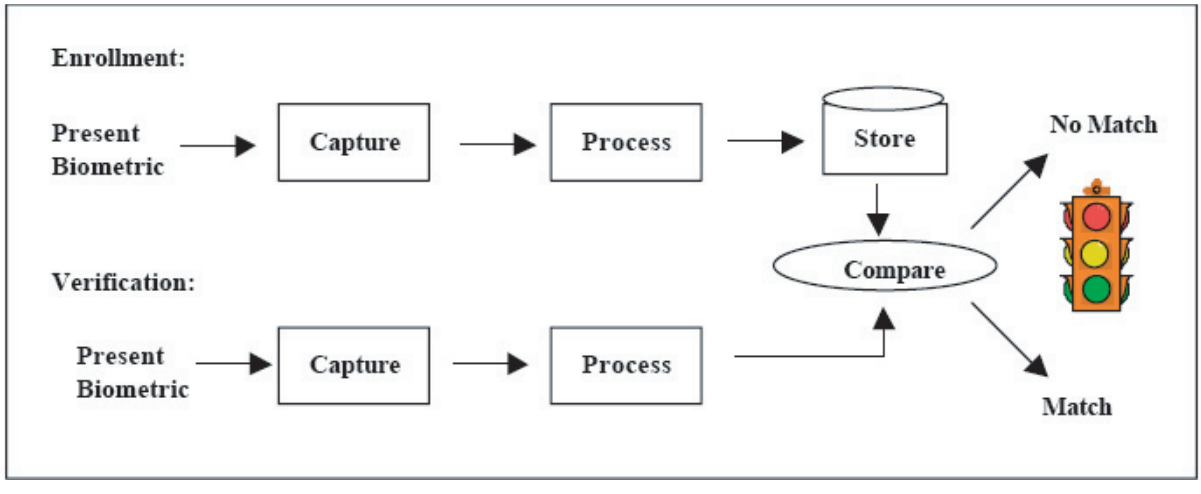

Figure 4. Enrolment and verification (Podio and Dunn, 2001)

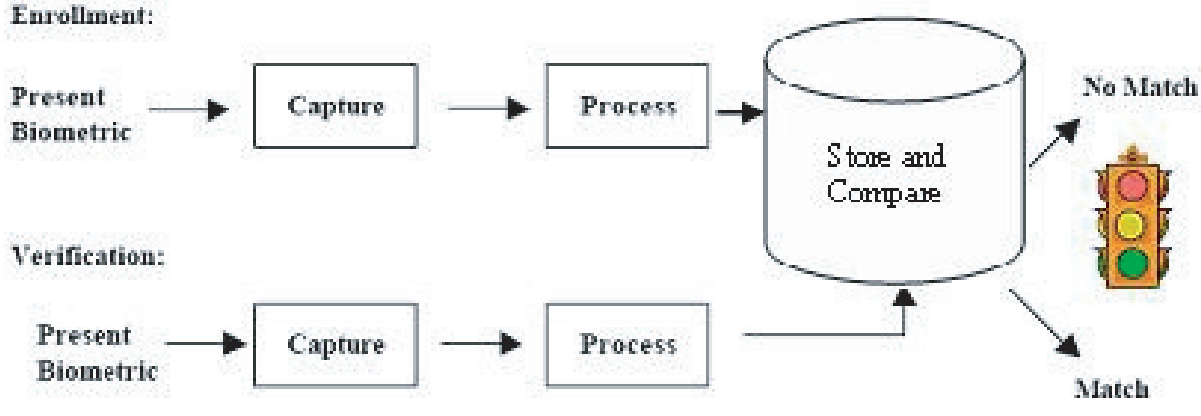

Figure 5. Enrolment and verification – the new approach

ADBMS in (Bassiliades and Vlahavas, 1997). So, complex event ***C*** could be written as:

C = *User_authorization* **within** *t*

where the event *User_authorization* is already defined. The meaning of complex event ***C*** is as follows: if a user's fingerprint matches a fingerprint already stored in the database and the user's facial shape and palm geometry together with voice match already stored templates in the database, and all four features have been checked (verified) within time interval *t*, the user is authorised.

If a user tries to log into the system and authorization has to be performed within time interval *t*, this situation can be modelled using the constructor *within*. Of course, when a user attempts to log into the system, proper data is stored within the database. Since time is a very important component of a biometric system, and given that it has been shown that an active databases need less time, then complex events and active databases could provide a better (faster) solution; comparison is performed within the database, making the authorisation process much quicker (*Figure 5)*.

6 Preliminary results

We have already used active databases in order to test the benefits of their usage when implementing different kinds of business rules (Rabuzin and Maleković, 2005); we have especially emphasized how to write business rules in active databases and what the problems are during this process. We have come to the conclusion that it is easier to implement certain types of business rules in active databases (code is smaller, network traffic is reduced, performance is improved, etc.) than in some programming language. Based upon these results we have expected to achieve and provide certain improvements when building multimodal biometric systems using triggers as well.

We had to build two solutions (application- and trigger-based) to test the proposed model. We started with a WEB application which stores biometric traits in the database and tries to authorise (identify) the user and implemented triggers (and procedures) based on complex events and the constructor *within*, which behave as already described. The constructor *within* was not supported (we used PostgreSQL) so we had to implement it. When a feature (trait) is extracted, it is stored in the database. After the storage process, the WEB application poses a query to the database and tries to authorise the user (if it is possible); the time required is measured as well. When a biometric trait is stored in the database, triggers are triggered and they also try to authorise (identify) the user. The database only contains a small number of traits for now; this affects the results but does not represent a problem because the proposed solution is general and can be used within databases which contain much more data. The time, which was measured for both solutions, represents how long the decision-making process (identification) lasted.

Preliminary results show that our proposed model requires about one-tenth of the time (about 0.5–0.6 ms) compared to the WEB-based application (about 6–7 ms); the measured time represents how long the authorisation process took, per person, using two biometric features. What needs to be done is to test a multimodal biometric system consisting of more than two features and including different architecture (2-tiered or 3-tiered). This will be done in the next paper, but the idea seems very promising and preliminary results have confirmed our assumptions.

7 Conclusion

We have presented how a multimodal biometric system and its performance could be improved using the active databases and complex events presented in active database theory. Instead of having many different modules responsible for different biometric features, when using active databases (semantic) constraints are collected and written in just one place. Since triggers are placed and executed on the server and the server usually has better performance, trigger execution time is small and the system can react almost immediately to registered events, which, in our case, reduces the time needed for authorization. In that way the authorisation process is much faster and is performed automatically as a reaction to specified events. The rules which constitute such a biometric system are easy to manage (change, delete) and the authorisation process is executed without any intervention. Preliminary results have shown that the proposed solution is about ten times faster when authorising a person than an application doing the same work. The results achieved are encouraging, and we will continue to develop our idea; we will include a probability model and time management regarding complex events in the model as well.

References

Andler, S. F. & Hansson, J. (1998). *Active, Rea-Time and Temporal Database Systems*, Springer Verlag, Berlin.

Bača, M. & Rabuzin, K. (2005). Biometrics in Network Security, *Proceedings of the XXVIII International Convention MIPRO 2005*, Edited by Baranović, M., Sandri, R., Čišić, D. & Hutinski, Ž. Opatija 30 May – 3 June, 2005. Rijeka : MIPRO.

Bailey, J., Poulovassilis, A. & Wood, P. T. (2002). Analysis and optimisation of event-condition-action rules on XML, *Computer Networks*, **39**(3): 239 - 259.

Bassiliades, N. & Vlahavas, I. (1997). DEVICE: Compiling production rules into event-driven rules using complex events, *Information and Software Technology*, **39**(5): 331 - 342.

Brunelli, R. & Falavigna, D. (1995). Personal identification using multiple cues, *Pattern Analysis and Machine Intelligence*, **17**(10): 955 - 966.

Casati, F., Fugini, M. & Mirbel, I. (1999). An environment for designing exceptions in workflows, *Information Systems*, **24**(3): 255 - 273.

Date, C. J. (2000). *What Not How: The Business Rules Approach to Application Development*, Addison Wesley, Reading.

Dittrich, K. R., Fritschi, H., Gatziu, S., Geppert, A. & Vaduva, A. (2003). SAMOS in hindsight: experiences in building an active object-oriented DBMS, *Information Systems*, **28**(5): 369 - 392.

Frischholz, R.W. & Dieckmann, U. (2000). Bioid: A multimodal biometric identification system, *IEEE Computer*, **33**(2): 64 - 68.

Jain, A., Bolle, R. & Pankanti, S. (1999). *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, Norwell Massachusetts.

Koschel, A. & Lockemann, P. C. (1998). Distributed events in active database systems: Letting the genie out of the bottle, *Data & Knowledge Engineering*, **25**(1-2): 11-28.

Montesi, D. & Torlone, R. (2002). Analysis and optimization of active databases, *Data & Knowledge Engineering*, **40**(3): 241 - 271.

Paton, N. W. (1998). *Active Rules in Database Systems*, Springer, New York.

Podio, F. L. & Dunn, J. S. (2001). Biometric Authentication Technology: From the Movies to Your Desktop, Available from http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf (Accessed 20. April 2006).

Prabhakar, S. & Jain, A. K. (2002). Decision-level fusion in fingerprint verification, *Pattern Recognition*, **35**(4): 861 - 874.

Prabhakar, S., Pankanti, S. & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns, *Biometrics*, Mar/Apr 2003: 33 - 42.

Rabuzin, K., Bača, M. & Sajko, M. (2006). E-learning: Biometrics as a Security Factor, *Proceedings of the International Multi-Conference on Computing in Global Information Technology ICCGI*, Edited by Dini, P., Poporviciu, C., Dini, C., Velde, G. V. & Borcoci, E. Bucharest 1-3 aug. 2006. Bucharest : IEEE Computer Society Press.

Rabuzin, K. & Maleković, M. (2005). Implementing business rules in active databases, *Proceedings of 15th International Conference on Information and Intelligent Systems*, Edited by Aurer, B. & Bača, M. Varaždin 21-23 sep. 2005. Varaždin : Faculty of Organization and Informatics Varaždin.

Tan, C.-W. & Goh, A. (1999). Composite event support in an active database, *Computers & Industrial Engineering*, **37**(4): 731 - 744.

Thalhammer, T., Schrefl, M. & Mohania, M. (2001). Active data warehouses: complementing OLAP with analysis rules, *Data & Knowledge Engineering*, **39**(3): 241 - 269.

Xiaoou L., Marín, J. M. & Chapa, S. V. (2002). A Structural Model of ECA Rules in Active Database, *MICAI 2002: Second Mexican International Conference on Artificial Intelligence Merida*, Edited by Coello, C. A. C., Albornoz, A., Sucar, L. E. & Battistutti, O.C. Yucatan 22-26 apr. 2002. Berlin : Springer Verlag.

Žugaj, M., Šehanović, J. & Cingula, M. (2004). *Organizacija*, Tiva tiskara, Varaždin.

Kornelije Rabuzin studied at Faculty of Organization and Informatics in Varaždin, University of Zagreb, where he graduated in 2001 as the best student in his class. During his study, he was awarded twice as one of the best students. After graduation, he was employed at the Faculty of Organization and Informatics, where he works as an assistant. Currently he is holding classes in Databases and Programming I. In 2003, he received an award as the best young assistant at the Faculty. He received an MSc. degree in 2004. He has published more than 20 scientific and professional papers. His fields of interests include (active) databases, biometrics and agent systems. He has worked on several projects concerning e-learning, biometrics and multiagent systems, and was a member of the organizing committees of IIS and INES conferences. He is a member of the editorial board of JIOS (Journal of Information and Organizational Sciences).

Mirko Maleković is Professor of Information Science at the University of Zagreb, Faculty of Organization and Informatics, Varaždin. Key responsibilities: Head of the Department of the Theoretical and Applied Foundations of Information Science. Professor of Databases (undergraduate), Relational Databases, Object Databases, and Deductive Databases (postgraduate). He serves as a member of the Steering Committee of INES (Inte rnational Conference on Intelligent Engineering Systems, IEEE). He is also a member of the Program Committee of the following international conferences: ICEIS (International Conference on Enterprise Information Systems) and IIS (International Conference on Intelligent Information Systems). He serves as an editor of JIOS (Journal of Information and Organizational Sciences) and a member Editorial Board of ComSIS (Computer Science and Information Systems). Research interests include databases, knowledge bases, semantic modelling, reasoning about knowledge and multi-agent systems.

Miroslav Bača received his MSc. degree in Information Science in 1999 and a PhD. degree in 2003, both from the University of Zagreb, Faculty of Organization and Informatics at Varaždin. His fields of interests include biometrics, security systems and computer crime. He is currently an assistant professor at the University of Zagreb, Faculty of Organization and Informatics. He has completed several courses regarding computer system management, database searching and e-learning. He is currently a member of the Program and Organizing Committee of the international POWA conference, and Organizing Committee chairman of the international conference on Information and Intelligent Systems (IIS). He has published two books: Police and Security (in Croatian) and Introduction to Computer Security.

discussed. On this basis, an alternative conceptual model separating strategic direction from the key organizational leverages of market orientation is proposed, which better suits the addressed challenges.

Key words: Market orientation, Marketing concept, Services marketing, Strategic management

Kornelije Rabuzin, Mirko Maleković, Miroslav Bača

A Multimodal Biometric System Based upon the Active Database Paradigm

Today, on many occasions and in many different places, one must be authorised in order to use certain services or applications or to access protected data. A user (person) can be authorised in three different ways or combinations of ways: it is either information that the user knows, something that the user possesses or a measurement of some physical or psychological characteristics unique to that user, i.e. biometric characteristics. In this paper we emphasize this third possibility. When talking about biometrics we can distinguish two basic types of systems: unimodal and multimodal. The main difference is that the unimodal biometric system is based solely on a single biometric feature, while multimodal biometric systems combine several features. We intend to show how active databases could be used in order to implement a multimodal (unimodal) biometric system and reduce the time needed for authorisation (identification or verification). Specifically, the concept of reactivity upon which active databases rely could be the core of a multimodal biometric system, as will be shown in the paper. We will especially consider the use of complex events used in active databases for authorisation purposes.

Key words: ADBMS, active database, complex events, biometrics, biometric system

Aleksandar Kešeljević

Understanding of Knowledge as a Cognitive Process within the Framework of Economic Theory of Organization

The paper looks into the (deficiency in) understanding of knowledge as a cognitive process within the economic theory of organization. The author's analysis is based on rationality. By employing the concept of rationality as the least common denominator in the economic organization theory, a new understanding of economic organization theory's evolution is presented, as well as a new way of surpassing the numerous divisions in the scientific community.

Key words: cognitive process, rationality, economic theory of organization.

Živa Čeh

How to Teach English for Specific Purposes to Improve Human Resources Efficiency

The paper deals with the language for specific purpose which has undoubtedly become a key factor in efficiency of company's human resources. First, characteristics of the language for specific purpose are dealt with. The author addresses the process of teaching language for specific purpose and points out the importance of vocabulary and development of language skills. Finally, the paper focuses on programmes, the process of collecting and writing material and concludes with the evaluation of such programmes.

Key words: language for specific purposes, teaching language for specific purposes, language for specific purpose programmes.

Bojan Beškovnik

Changes in Organization of Goods Supply in Supply Logistics

This theoretically conceived paper discusses about significant changes in supply logistics. The arguments are based primary on the presentation of new trends in organization of goods supply, because changes in international economy and transport market have pushed factories to change their market strategy.

The results of the paper point out the basic changes in supply logistics, where supply management must take advantages of »just in time« and »door to door« concepts, by reducing cost and necessary delivery time. With appearance of globalization the maritime transport and containerization strengthen their role, due to the competitive advantages against other types and technologies of transport. Their advantages are shown in reliability, security and lower transport costs (up to 80%). The price of transport is the key element in supply logistics, but companies should take into consideration also speed and regularity of the service.

Supply management must consider that the concepts of transportation-logistics services are changing, and transportation processes and traffic technologies of individual traffic branches are constantly modernizing. Therefore, new approaches have to be adopted, where timely information is a prerequisite instrument to coordinate and organize the activities in production process. For companies that are forming a supply chain the setting up of the effective information system is becoming more and more important, in order to obtain important information on time.

Key words: supply logistics, supply chain, new transport technologies, information support