Securizarea accesului la sisteme de comunicații prin metode de identificare biometrică

Drd. ing. Sorin SOVIANY, Drd. ing. Gheorghiță PESCARU*,*
*Ing. Mihaela TACHE**

Rezumat. *Tehnologiile biometrice se bazează pe o abordare inovatoare pentru securizarea accesului fizic sau logic la resurse critice din punct de vedere al securității. Aceasta este mai avantajoasă deoarece nu mai obligă o persoană să memoreze o parolă sau să păstreze o cheie sau un card magnetic de acces, dar ridică totuşi unele probleme legate de precizia recunoaşterii şi de erori interente în procesul de capturare a datelor biometrice primare. Utilizarea metodelor biometrice de identificare pentru securizarea accesului la sisteme de comunicații prezintă avantaje dar şi puncte slabe, care pot fi abordare prin combinarea mai multor metode de autentificare.*

Cuvinte cheie: *metode biometrice, şablon, potrivire biometrică.*

Abstract. *The biometric technologies are relying on emergent approach for physical or logic access to resources that are critical from security. This is more convenient because it does not require for password or access token special protection, but there are still challenges concerning recognition precision and also errors that are inherent for the primary biometric data acquisition. Using biometric identification methods for communications systems access securing has advantages but also drawbacks and these could be approached by combining more authentication methods.*

Key words: *biometric methods, template, biometric matching.*

1. Introducere

Biometria *reprezintă studiul metodelor pentru recunoaşterea unică a persoanelor pe baza uneia sau mai multor caracteristici fizice sau comportamentale intrinseci.

Tehnologiile biometrice includ acele tehnologii care susțin utilizarea caracteristicilor fiziologice sau comportamentale umane pentru determinarea sau verificarea identității. O formulare mai riguroasă ar trebui să includă expresia *utilizare asistată automat*, deoarece în multe cazuri sistemele de autentificare/identificare bazate pe metode biometrice implică un grad de corelație cu decizii umane finale, în scopul stabilirii sau verificării unei identități.

Un **sistem biometric** include **toate componentele hardware, software şi cele de rețea necesare pentru a realiza activități de identificare şi autentificare folosind metode biometrice** (deci exploatând caracteristici fiziologice şi comportamentale specifice indivizilor pentru care se doreşte verificarea identității).

Tehnologiile biometrice sunt utilizate pentru recuoaşterea identității pe baza unui eşantion de intrare,

* I.N.S.C.C.– Institutul Național de Studii şi Cercetări pentru Comunicații.

care se compară cu un model de referință. Practic, metodele biometrice urmăresc identificarea unor persoane prin anumite caracteristici specifice ale acestora.

Caracteristicile biometrice pot fi grupate în 2 mari clase:

- **fiziologice –** legate de componente anatomice ale corpului uman. Cea mai cunoscută dintre acestea este amprenta, utilizată de mai mult de 100 de ani în aplicațiile din domeniul judiciar-criminalistic. Alte metode biometrice bazate pe caracteristici fizice (statice) sunt cele bazate pe caracteristici faciale, geometria mâinii şi modelul irisului;
- **comportamentale –** legate de comportamentul unei persoane. Cea mai cunoscută metodă biometrică din această categorie este dinamica semnăturii. Alte abordări se bazează pe dinamica tastării şi recunoaşterea vocii. Strict vorbind, vocea este, de asemenea, şi o trăsătură fiziologică, deoarece pentru fiecare persoană se pot evidenția caracteristici vocale specifice. Sistemele de recunoaştere a vocii se bazează pe extragerea de caracteristici acustice care reflectă atât particularități anatomice ale persoanei, dar şi aspecte dinamice.

Autentificarea biometrică se poate utiliza atât în aplicații de control al accesului fizic în incinte sau camere cu destinații speciale, cât şi pentru securizarea accesului logic la resurse informatice cum ar fi baze de date (figura 1).

2. Structura de principiu a unui sistem de control al accesului bazat pe metode biometrice. Modul de funcționare al unui sistem de identificare bazat pe metode biometrice

Diagrama din figura 2 prezintă schema-bloc simplificată (generică) a unui sistem biometric.

Principalele operații pe care sistemul biometric le poate efectua sunt *înregistrarea (înscrierea)* şi *testarea (compararea pentru identificare sau pentru verificare).* În timpul fazei de înregistrare, informațiile biometrice ale unui individ sunt stocate. În timpul fazei de testare, datele biometrice sunt detectate şi comparate cu informațiile stocate anterior. De notat că este crucial ca acțiunile de stocare şi de regăsire a informațiilor, în cadrul acestor sisteme, să fie securizate, pentru ca sistemele biometrice să se dovedească robuste.

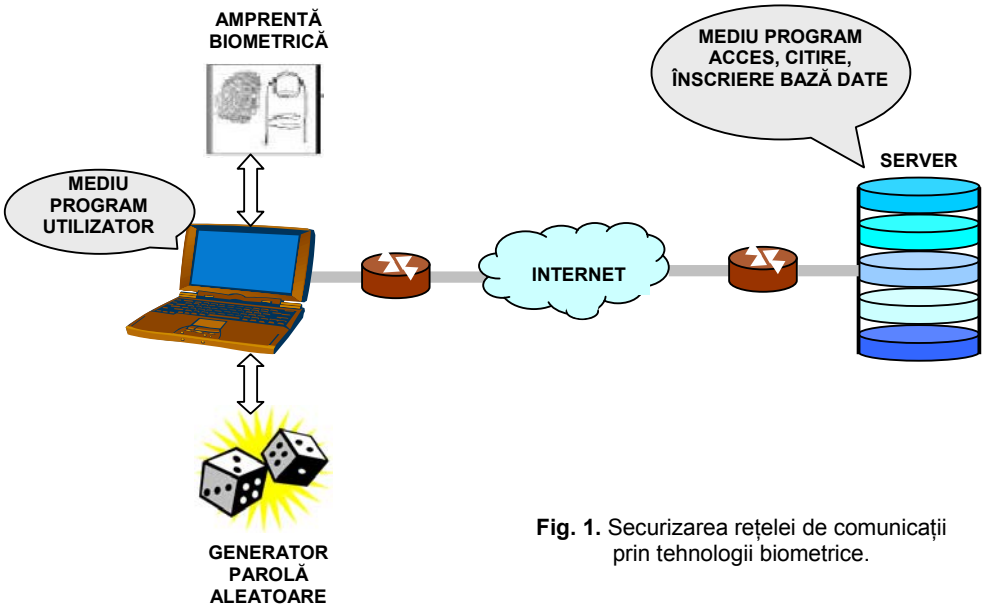

Fig. 1. Securizarea rețelei de comunicații prin tehnologii biometrice.

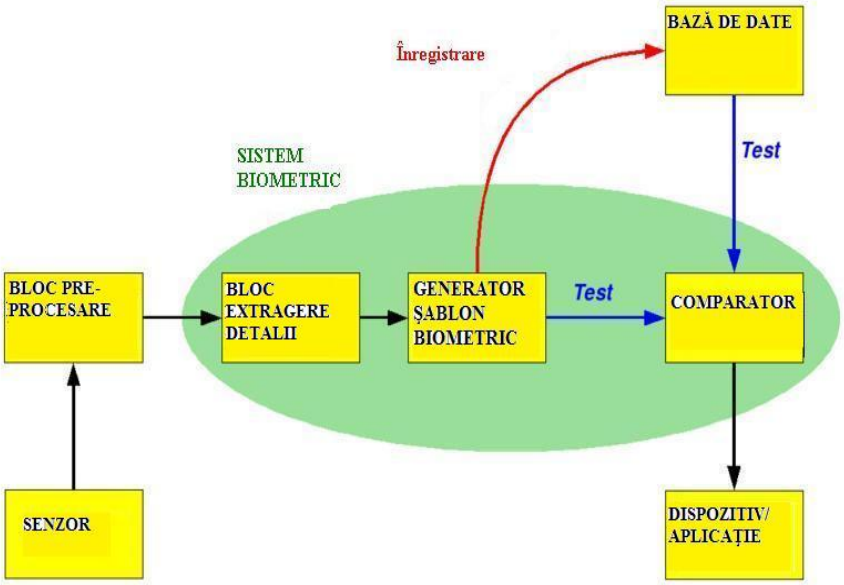

Fig. 2. Schema bloc de bază a unui sistem biometric.

Primul bloc (senzorul) reprezintă interfața între lumea reală şi sistemul biometric; el trebuie să asigure obținerea tuturor datelor necesare. În majoritatea cazurilor, acest bloc este un sistem de achiziție de imagini, dar el poate varia de la caz la caz, în funcție de natura caracteristicilor dorite. Al doilea bloc execută toate operațiile necesare de pre-procesare ; astfel, el elimină elementele redundante din informațiile primare obținute de blocul senzor, reducând dimensiunea datelor folosite ulterior în procesul de recunoaştere. În cadrul celui de-al treilea bloc, caracteristicile necesare (şi relevante) sunt extrase. Extragerea detaliilor relevante se realizează prin aplicarea algoritmilor de detecție a contururilor în imagini, precum şi a tehnicilor de segmentare folosite în prelucrarea imaginilor. În cazul amprentelor, detaliile relevante constau în şanțuri, ridicături şi terminații sau bifurcații. Un vector cu valori numerice sau o imagine cu proprietăți particulare se poate utiliza pentru a se crea un *şablon*. Un ***şablon*** este **o sinteză a tuturor caracteristicilor extrase din informațiile sursă, la o dimensiune optimă pentru a permite o identificare adecvată**.

În cursul fazei de *înregistrare*, şablonul biometric este stocat pe un suport care poate fi un smartcard sau o bază de date centralizată. În faza de *potrivire*, şablonul obținut de la utilizatorul curent se transferă către blocul funcțional care execută comparația cu şabloane deja existente, estimând diferențele dintre şablonul biometric al persoanei care se autentifică şi unul sau mai multe dintre şabloanele preînregistrate, prin utilizarea unui algoritm specific (de exemplu, prin calcularea distanței Hamming). Rezultatul acestei comparații se utilizează ca bază pentru decizia de acceptare sau de respingere a accesului fizic sau logic; securizarea accesului fizic se referă la permiterea sau respingerea accesului în incinte sau locații fizice cu destinații speciale, în timp ce securizarea accesului logic vizează protecția resurselor informatice şi de date dintr-o rețea sau chiar de la nivelul unui sistem de calcul.

Un sistem biometric îndeplineşte următoarele 2 funcții:

- **Verificare.** Este procesul de autentificare a utilizatorilor legitimi, proces efectuat în conjuncție cu un smartcard, username sau număr special de iden-

tificare (ID number). Şablonul biometric capturat este comparat cu cel stocat anterior (fie pe un smartcard, fie într-o bază de date);

- **Identificare.** Este procesul prin care se realizează autentificarea utilizatorilor, dar fără să apeleze la forme de stocare pre-înregistrată a unor date biometrice (smartcarduri, nume de utilizatori sau coduri numerice personale). Şablonul biometric curent este comparat cu toate înregistrările din baza de date, şi este returnat scorul care indică cea mai strânsă potrivire. Cea mai strânsă potrivire care satisface pragul minim de securitate determină autentificarea şi acceptarea utilizatorului în sistem.

3. Precizia şi performanța sistemelor biometrice

Una dintre problemele care se pun în cazul sistemelor biometrice este aceea a construirii şi implementării unui sistem care să asigure, teoretic, o potrivire 100% la fiecare comparare între datele biometrice curente şi informațiile de referință stocate în baza de date. În realitate, un astfel de sistem ar fi lipsit de utilitate practică, deoarece foarte puțini utilizatori l-ar putea folosi (sau chiar nici unul). Majoritatea utilizatorilor care ar solicita accesul la resursele protejate prin autentificare biometrică ar fi respinşi practic tot timpul, deoarece rezultatele măsurărilor parametrilor obținuți din procesarea datelor biometrice nu ar fi niciodată aceleaşi la fiecare proces de comparație (*variabilitate*).

În mod real, se permite o *variabilitate* a datelor biometrice (o gamă admisă a acestei variabilități fiind de 0,1-1%), pentru a nu fi respinşi foarte mulți dintre utilizatorii legitimi. Această variabilitate este totuşi limitată de nivelul de securitate dorit. Cu cât variabilitatea permisă este mai mare, cu atât mai ridicată este şi probabilitatea ca un impostor cu date biometrice „asemănătoare" datelor de referință să fie acceptat în sistem, ca utilizator legitim (autorizat). În mod uzual, această variabilitate permisă pentru datele biometrice este calificată drept prag sau nivel de securitate. Când variabilitatea permisă este mică, atunci pragul sau nivelul de securitate este *ridicat*, iar dacă se permite o variabilitate mai mare, atunci pragul sau nivelul de securitate este *scăzut*.

Cei 3 parametri de performanță sunt: *rata falselor acceptări sau a potrivirilor false* (FAR – false acceptance rate -sau FMR – false match rate), *rata falselor respingeri sau a nepotrivirilor false* (FRR – false rejection rate sau FNMR – false nonmatch rate), precum şi *rata erorilor la înregistrare* (FTER-failure to enroll rate).

O **potrivire falsă** apare atunci când sistemul potriveşte o identitate în mod incorect, iar FMR (sau FAR, rata falselor acceptări) reprezintă probabilitatea ca indivizii să fie acceptați în urma unei potriviri false. În sistemele de verificare şi de identificare pozitivă, persoane neautorizate pot obține acces la facilități sau resurse ca urmare a domeniului de toleranță larg. Într-un sistem de identificare negativă, rezultatul unei false potriviri poate fi respingerea falsă a accesului unui utilizator legitim, dacă domeniul de toleranță este foarte îngust. **Rata falselor acceptări** se defineşte prin probabilitatea ca sistemul să declare o potrivire reuşită între şablonul de intrare şi un şablon din baza de date, şablon care, în realitate, nu se potriveşte cu cel curent prezentat sistemului biometric. Acest parametru exprimă procentul potrivirilor nevalide. Astfel de sisteme sunt critice, deoarece ele sunt utilizate, în mod comun, pentru a interzice anumite acțiuni pentru persoane neautorizate.

O **nepotrivire falsă** apare atunci când un sistem respinge o identitate validă, iar FNMR (sau FRR, rata respingerilor false) este probabilitatea ca un utilizator valid să nu fie potrivit, în mod eronat. În sistemele de identificare pozitivă şi în cele de

verificare, utilizatorilor legitimi li se poate respinge accesul la facilități şi resurse ca urmare a eşecului sistemului în a realiza o potrivire corectă. În sistemele de identificare negativă, rezultatul unei nepotriviri greşite (false) poate fi acela că o persoană ar obține acces la resurse pentru care, de fapt, nu este autorizat, şi deci pentru care ar fi trebuit să i se respingă accesul. **Rata falselor respingeri** se defineşte prin probabilitatea ca sistemul să declare, în mod incorect, eşecul unei potriviri între şablonul biometric de intrare şi şablonul pre-înregistrat în baza de date. Acest parametru redă procentajul intrărilor valide care sunt rejectate în mod eronat.

Potrivirile false (greşite), şi, în consecință, acceptările false, apar din cauză că există un grad ridicat de similaritate între caracteristicile a 2 indivizi. Nepotrivirile false (şi, deci, şi respingerile false) apar atunci când nu există similarități suficient de mari între datele de referință înregistrate ale utilizatorilor şi şabloanele provenite din datele biometrice prezentate în mod curent la solicitarea accesului la resursele securizate; acest lucru se poate datora unor diverse condiții, obiective şi subiective. De exemplu, caracteristicile biometrice ale unui individ se pot modifica ca rezultat al vârstei sau al unor condiții fiziologice sau patologice particulare. Dacă sistemul biometric ar fi perfect, ambele rate de eroare ar trebui să fie nule. Totuşi, deoarece sistemele biometrice nu pot identifica indivizii cu o acuratețe de 100%, trebuie luat în considerare un compromis între cele 2 rate de eroare.

Ratele de potrivire falsă şi, respectiv, de nepotrivire falsă sunt invers corelate; prin urmare, ele trebuie evaluate în tandem, şi nivele acceptabile de risc trebuie puse în balanță cu dezavantajele inconvenienței. De exemplu, pentru o aplicație de control al accesului, un nivel perfect de securitate ar necesita respingerea accesului pentru oricine. Invers, acordarea accesului pentru oricine ar însemna că nu se respinge nimănui accesul. În mod evident, nici una dintre cele 2 situații extreme nu este rezonabilă, iar sistemele biometrice trebuie să opereze, de fapt, între cele 2 limite.

Producătorii de dispozitive biometrice specifică şi un alt parametru, *rata erorilor egale* (EER –equal error rate). Aceasta reprezintă un parametru suplimentar derivat din FMR şi FNMR, care se utilizează pentru a descrie precizia sistemelor biometrice. EER se referă la punctul în care rata potrivirilor false egalează rata nepotrivirilor false. **Rata erorilor egale** reprezintă acel procentaj de eroare la care ambele tipuri de rate de eroare, de falsă acceptare, respectiv falsă respingere, sunt egale. Atunci când este necesară compararea rapidă a performanțelor a două sisteme, se utilizează EER. Cu cât rata erorilor egale EER este mai scăzută, cu atât sistemul este considerat mai precis. Setarea pragului de securitate al sistemului la nivelul specificat de EER va însemna că probabilitatea ca o persoană să fie potrivită în mod fals egalează probabilitatea ca persoana să fie nepotrivită în mod eronat. Totuşi, această abordare statistică tinde să suprasimplifice echilibrul dintre FMR şi FNMR, deoarece în aplicațiile practice (reale) în care se foloseşte biometria, se urmăreşte asigurarea unui nivel de securitate care să corespundă cerințelor specifice aplicațiilor, precum şi convenienței utilizatorilor finali.

Graficele din figurile 3 şi 4 vizează problemele prezentate anterior, respectiv evoluția ratelor de eroare, precum şi modul de definire a parametrului *rata de erori egale.*

Astfel, graficul din figura 3 ilustrează relația dintre **rata potrivirilor false** şi **rata nepotrivirilor false**. Referitor la aceste rate de erori, trebuie făcută o observație importantă. Rata FMR coincide cu rata acceptărilor false (FAR) în cazul sistemelor de

verificare şi al sistemelor de identificare folosite pentru identificare pozitivă. Rata FNMR coincide, de fapt, cu rata respingerilor false (FRR) în cazul sistemelor de verificare şi de identificare pozitivă.

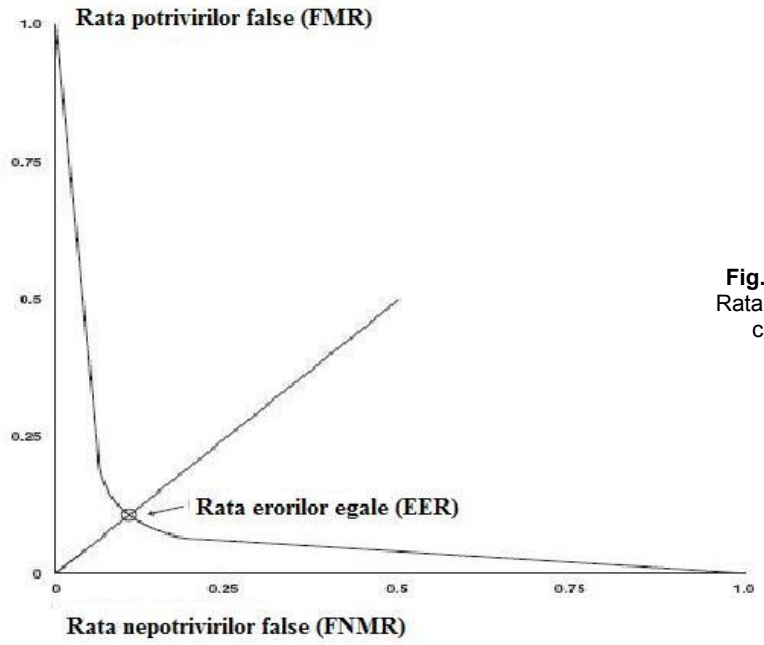

Fig. 3. Relația generală dintre FMR şi FNMR. Rata erorilor egale (EER) se obține în punctul în care rata FMR este egală cu rata FNMR.

Dacă se reprezintă grafic evoluțiile ratelor falselor acceptări (FAR), respectiv ale ratelor respingerilor false (FRR) în funcție de nivelul sau pragul de securitate stabilit pentru sistemul care trebuie protejat, se obține graficul din figura 4.

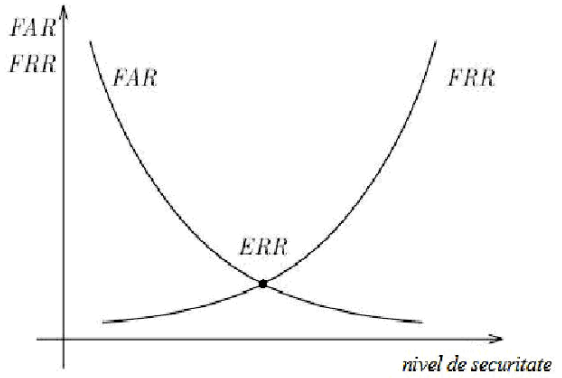

Fig. 4. Reprezentare grafică pentru ratele erorilor FAR şi FRR ca funcții de nivelul de securitate.

Curbele reprezentând evoluțiile FAR şi FRR se intersectează într-un punct în care cele două rate, de false acceptări şi, respectiv, false respingeri, sunt egale. Valoarea care corespunde acestui punct reprezintă *rata de erori egale (EER)* sau *precizia sistemului*. În principiu, această valoare nu are o utilitate practică evidentă (în condițiile în care foarte rar se doreşte ca FAR şi FRR să fie identice), dar reprezintă un indicator pentru cât de precis este dispozitivul. Dacă avem 2 dispozitive pentru care ratele de erori egale sunt de 1%, respectiv 10%, atunci se poate stabili că primul dispozitiv este mai precis (deoarece produce mai puține erori) decât celălalt. Totuşi, astfel de comparații nu sunt, întotdeauna, foarte relevante (concludente) pentru ceea ce se întâmplă în cazul sistemelor biometrice reale. În primul rând, orice valori ale ratelor de eroare, furnizate de către producătorii dispozitivelor, nu sunt comparabile deoarece producătorii nu publică informații despre condițiile exacte în care au realizat testările dispozitivelor lor. În al doilea rând, chiar dacă există o supervizare obiectivă a testărilor,

rezultatele încercărilor efectuate sunt dependente foarte mult de comportamentul utilizatorilor, precum şi de alte influențe externe.

Din analiza reprezentărilor grafice redate în figurile 3 şi 4, şi cu deosebire din cea care redă evoluția ratelor de acceptări false şi de respingeri false în funcție de nivelul de securitate, se pot face mai multe observații legate de precizia sistemelor de identificare biometrică. Într-un sistem biometric ideal, nu ar trebui să existe nici respingeri false şi nici acceptări false. Într-un sistem biometric real, există un anumit număr de erori (respingeri false şi, respectiv, acceptări false), şi acest număr depinde de nivelul sau pragul de securitate ales sau fixat pentru respectivul sistem. Cu cât **pragul/nivelul de securitate** este mai *ridicat*, cu atât există *mai multe respingeri false* şi mai *puține acceptări false*. Cu cât **pragul/nivelul de securitate** este mai *scăzut*, cu atât sunt *mai puține respingeri false* şi *mai multe acceptări false*. **Numărul de respingeri false** şi **numărul de acceptări false** sunt invers proporționale. Decizia privind **nivelul de securitate** ales depinde, în principal, de scopul pentru care se foloseşte sistemul biometric, în esență de cerințele specifice impuse de natura aplicației şi a datelor generate, stocate şi transmise. De regulă, se recurge la un *compromis* între securitatea şi utilizabilitatea sistemului.

4. Beneficii ale utilizării sistemelor biometrice pentru securizarea accesului la sisteme de comunicații

Metodele biometrice de autentificare au avantajul general, față de metodele bazate pe date cunoscute, că ***datele biometrice nu pot fi transmise altei persoane*** (intenționat sau neintenționat). O parolă poate fi comunicată altei persoane, care poate să o folosească în acelaşi mod ca şi proprietarul legitim, în timp ce o **caracteristică biometrică poate fi folosită în mod natural doar de către proprietar**. Astfel, ***o caracteristică biometrică este legată de o persoană şi numai de ea.*** Aceste argumente sunt valabile atât pentru caracteristicile biometrice statice, cât şi pentru cele dinamice. În plus, caracteristicile biometrice statice au avantajul că nu pot fi pierdute sau uitate. Oricând se poate pierde o cheie sau se poate uita o parolă, dar o caracteristică biometrică statică va fi mereu prezentă la o persoană. Acest argument nu mai este, însă, valabil pentru caracteristicile biometrice dinamice, care presupun efectuarea unei acțiuni.

Un alt avantaj al sistemelor de identificare biometrică este acela că, prin modul de colectare, **datele biometrice nu sunt secrete**, spre deosebire de parole sau coduri PIN, care trebuie protejate prin mecanisme uneori sofisticate şi costisitoare (de regulă prin metode criptografice). Din acest motiv, *securitatea unui sistem de autentificare biometrică poate să nu depindă de ținerea secretă a datelor de verificat*. Mai important este ca datele care trebuie verificate de un senzor să fie autentice, de exemplu, procesul să fie capabil să recunoască dacă datele colectate de senzorul biometric sunt prelevate direct de la posesorul acestora.

Pe de altă parte, metodele biometrice de identificare pot fi folosite combinat cu metodele de autentificare tradiționale bazate pe date cunoscute, conducând astfel la **creşterea nivelului de securitate** pe care acestea îl pot asigura, pe partea de control al accesului la sisteme de comunicații folosite ca suport pentru diferite aplicații.

Tehnologiile biometrice reprezintă o **abordare inovatoare** în domeniul soluțiilor de securitate, iar

utilizarea de sisteme biometrice, combinate cu alte categorii de soluții de securitate susține dezvoltarea de noi aplicații software, în vederea cărora se susține crearea de noi locuri de muncă în domenii precum informatica, electronica şi comunicațiile.

Nu în ultimul rând, utilizarea de tehnologii biometrice conduce şi la **reduceri de costuri** în implementarea de soluții de securitate pentru protecția resurselor sistemelor de comunicații. Multe tipuri de date biometrice pot fi colectate în moduri ieftine, comod de folosit de către utilizatori obişnuiți, şi aceste elemente sunt premise pentru o utilizabilitate largă a acestora.

Bibliografie

[1] Patriciu Victor, Ene-Pietroşanu M., Bica I, Priescu J. *„Semnături electronice şi securitate informatică. Aspecte criptografice, tehnice, juridice şi de standardizare”*, Editura BIC ALL, 2006

[2] *** *INFORMATION SECURITY. Technologies to Secure Federal Systems*, United States General Accounting Office, Report to Congressional Requesters, March 2004, *http://www.gao.gov/new.items/d04467.pdf*

[3] Riha Z., Matyas V. *Biometric Authentication Systems*, Faculty of Informatics Masaryk University, FI MU Report Series, FIMU-RS-2008-08, Nov. 2000, *http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf*

[4] *** *BORDER SECURITY. Challenges in Implementing Border Technology*, United States General Accounting Office, Report to Congressional Requesters, 2003, *http://www.gao.gov/new.items/d03546t.pdf*