REZULTATELE ACTIVITĂŢILOR DE CERCETARE – DEZVOLTARE DESFĂȘURATE ÎN CADRUL TEZEI DE DOCTORAT CU TITLUL

SECURITATEA INFORMAȚIEI FOLOSIND TEHNICI DE BIOCRIPTOGRAFIE

<table>
<tr><td colspan="3">AUTOR
Ing. Marius-Alexandru VELCIU</td><td colspan="3">ÎNDRUMĂTOR
Prof. Univ. Dr. Ing. Victor-Valeriu PATRICIU</td></tr>
<tr><td colspan="6">DOMENIU DE DOCTORAT
CALCULATOARE ŞI TEHNOLOGIA INFORMAȚIEI</td></tr>
<tr><td>Data înmatriculării</td><td>01.10.2013</td><td>Data susținerii publice</td><td>16.09.2016</td><td>Data confirmării</td><td>28.11.2016</td></tr>
<tr><td colspan="6">REZULTATELE ACTIVITĂȚII DE CERCETARE-DEZVOLTARE</td></tr>
<tr><td colspan="2">DENUMIRE REZULTAT</td><td colspan="4"></td></tr>
<tr><td colspan="2">CATEGORIA REZULTATULUI</td><td colspan="2">Rezultat final</td><td colspan="2">DETALIERE CARACTERISTICI ALE REZULTATULUI FINAL</td></tr>
<tr><td colspan="2">documentaţii, studii, lucrări</td><td colspan="2">[X]</td><td colspan="2" rowspan="17">- Conceperea unui framework pentru securizarea conținutului dispozitivelor mobile;
- Accesarea unui mediu de stocare partajat, cu suport pentru criptarea conținutului acestuia;
- Implementarea și evaluarea schemei biocriptografice Fuzzy Vault pentru biometrica voce;
- Evaluarea rezistenței schemei Fuzzy Vault în fața atacurilor statistice prin forță brută;
- Implementarea și evaluarea a două metode de reducere a costului computațional asociat schemei Fuzzy Vault.</td></tr>
<tr><td colspan="2">planuri, scheme</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">tehnologii</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">procedee, metode</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">produse informatice</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">reţete, formule</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">obiecte fizice / produse</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2">brevet invenţie / altele asemenea</td><td colspan="2">[ ]</td></tr>
<tr><td colspan="2" rowspan="5">STADIUL DE DEZVOLTARE</td><td>soluţie / model conceptual</td><td>[ ]</td></tr>
<tr><td>model experimental / funcţional</td><td>[X]</td></tr>
<tr><td>prototip</td><td>[ ]</td></tr>
<tr><td>instalaţie pilot sau echivalent</td><td>[ ]</td></tr>
<tr><td>altele ……</td><td>[ ]</td></tr>
<tr><td colspan="2" rowspan="10">DOMENIUL DE CERCETARE</td><td>tehnologiile societăţii informaţionale</td><td>[X]</td></tr>
<tr><td>energie</td><td>[]</td></tr>
<tr><td>mediu</td><td>[ ]</td></tr>
<tr><td>sănătate</td><td>[ ]</td></tr>
<tr><td>agricultură, securitatea şi siguranţa alimentară</td><td>[ ]</td></tr>
<tr><td>biotehnologii</td><td>[ ]</td></tr>
<tr><td>materiale, procese şi produse inovative</td><td>[ ]</td></tr>
<tr><td>spaţii şi securitate</td><td>[ ]</td></tr>
<tr><td>cercetări socio – economice şi umaniste</td><td>[ ]</td></tr>
<tr><td colspan="2" rowspan="7">CARACTERUL INOVATIV</td><td>produs nou</td><td>[ ]</td><td colspan="2" rowspan="7">DETALIERE CARACTER INOVATIV
- Conceperea unui framework biocriptografic pentru securizarea conținutului dispozitivelor mobile cu senzor de amprentă integrat, ce rulează</td></tr>
<tr><td>produs modernizat</td><td>[ ]</td></tr>
<tr><td>tehnologie nouă</td><td>[X]</td></tr>
<tr><td>serviciu nou</td><td>[ ]</td></tr>
<tr><td>serviciu modernizat</td><td>[ ]</td></tr>
<tr><td>altele…….</td><td>[ ]</td></tr>
</table>

			sistemul de operare Android, cu suport pentru criptarea și decriptarea fișierelor, precum și a directoarelor din sistemul de fișiere; - Dezvoltarea unei aplicații pentru sistemul de operare Android, care implementează funcționalitățile framework-ului descris anterior; - Conceperea și implementarea unui framework biocriptografic pentru accesarea securizată a unui mediu de stocare partajat, cu suport pentru criptarea conținutului acestuia; - Evaluarea rezistenței schemei Fuzzy Vault în fața atacurilor statistice prin forță brută, folosind o arhitectură client-server pentru calcul distribuit proprie; - Propunerea, implementarea și evaluarea unei metode de sporire a nivelului de securitate conferit de schema Fuzzy Vault, folosind hash-uri biometrice cu „salt"; - Implementarea și evaluarea unei metode de reducere a costului computațional asociat etapei de criptare biometrică din cadrul schemei Fuzzy Vault, prin folosirea biocriptogramelor partajate, în scopul eliminării necesității de a utiliza puncte de difuzie; - Implementarea și evaluarea unei metode de reducere a costului computațional asociat reconstrucției polinomiale din cadrul etapei de decriptare biometrică a schemei Fuzzy Vault, prin folosirea codurilor corectoare de erori Reed-Solomon.

INFORMAŢII PRIVIND PROPRIETATEA INTELECTUALĂ	
cerere înregistrare brevet de invenţie	Nr . ..... data.....
brevet de invenţie înregistrat (naţional, european, internaţional)	Nr . ..... data.....
cerere înregistrare modele şi desene industriale protejate	Nr . ..... data.....
modele şi desene industriale protejate înregistrate (naţional, european, internaţional)	Nr . ..... data.....

DOMENII DE APLICABILITATE	**DETALIERE APLICABILITATE**
În domeniul de interes al MApN	- securizarea comunicațiilor între terminalele mobile

	- securizarea conținutului sensibil al terminalelor mobile - control acces la informații clasificate prin autentificare + descriptare biometrică
În alte domenii	- securizarea cheilor criptografice existente - securizarea informațiilor folosind Biometrica "voce" și algoritmi biocriptografici - securizarea informațiilor folosind Biometrica "amprentă" și algoritmi biocriptografici - medicină: accesarea conținutului dosarului medical personal numai în baza unei autentificări biometrice realizate cu success și în urma decriptării biometrice a conținutului acestuia - comunicații VoIP securizate prin criptare biometrică - control acces + suport criptare pentru un mediu de stocare partajat
DISEMINAREA REZULTATELOR CERCETĂRII REALIZATE ÎN CADRUL TEZEI DE DOCTORAT	**DENUMIRE ARTICOL/REVISTĂ/CONFERINȚĂ**
Articole publicate în reviste /Proceedings cotate ISI	1. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu, și Victor-Valeriu Patriciu, "*Bio-cryptographic authentication in cloud storage sharing*", IEEE 9th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2014, ISBN: 978-1-4673-6397-6, DOI: 10.1109/SACI.2014.6840054, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 2. **Marius-Alexandru Velciu**, Victor-Valeriu Patriciu și Mihai Togan, "*An evaluation of the Fuzzy Vault scheme diffusion points order of magnitude*", 14th International Conference on Informatics in Economy (IE), Aprilie 2015, București, ISSN: 2284-7472, indexare: ***ISI*** și ***RePEc*** 3. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu și Victor-Valeriu Patriciu, "*An evaluation of the Reed-Solomon error-correcting codes usage for bio-cryptographic algorithms*", IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2015, ISBN: 978-1-4673-6397-6, DOI: 10.1109/ SACI.2015.7208255, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 4. Alecsandru Pătrașcu, **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Cloud Computing Digital Forensics Framework for Automated Anomalies Detection*", IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2015, ISBN: 978-1-4673-6397-6, DOI: 10.1109/SACI.2015.7208257, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 5. **Marius-Alexandru Velciu**, Victor-Valeriu Patriciu și Ion Bica, "*A Bio-Cryptographic framework for securing mobile devices content*", IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2016, ISBN: 978-1-5090-2379-0, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 6. Mihai-Gabriel Ionita, **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*A Mobile-based Bio-cryptographic Framework for Approving Cyber Warfare Defensive Actions*", International Journal of Computer Science and Information Security (IJCSIS), August 2016 Volume 14, No. 8, ISSN: 1947-5500, indexare: ***ISI***
Articole publicate în reviste /Proceedings cotate BDI	1. **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Methods of reducing bio-cryptographic algorithms computational complexity*", IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Noiembrie 2014, Budapesta, Ungaria, ISBN: 978-1-

	4799-7855-7, DOI: 10.1109/CINTI.2014.7028667, indexare: ***IEEE*** și ***DPLP*** 2. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu și Victor-Valeriu Patriciu, "*Cryptographic Applications of Biometric Methods in Cloud Storage Sharing*", Scientific Bulletin of the Politehnica University of Timisoara, Transactions on Automatic Control and Computer Science, BS-UPT TACCS Volume 59(73) No. 2 / 2014, CNCSIS B+ journal, ISSN: 1224-600X, indexare: **Copernicus** și **VINITI**, factor de impact: 0.9210 3. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu și Victor-Valeriu Patriciu, "*Using Error-correcting Codes to Speed Up the Fuzzy Vault Bo-cryptographic Scheme Biometric Decryption Process*", Scientific Bulletin of the Politehnica University of Timisoara, Transactions on Automatic Control and Computer Science, BS-UPT TACCS Volume 60(74) No. 1 / 2015, CNCSIS B+ journal, ISSN: 1224-600X, indexare: **Copernicus** (factor de impact/2012: 4.86), **Electronics Journal Library**, **Ulrich's**, **Cabell's** și **VINITI**
Articole susținute la conferințe internaționale	1. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu, și Victor-Valeriu Patriciu, "*Bio-cryptographic authentication in cloud storage sharing*", IEEE 9th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2014, ISBN: 978-1-4673-6397-6, DOI: 10.1109/SACI.2014.6840054, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 2. **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Using Shared Vault constructions for bio-cryptographic algorithms*", 7th International Conference on Security for Information Technology and Communications (SECITC), București, Iunie 2014, ISSN: 2285-1798, neindexată 3. **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Methods of reducing bio-cryptographic algorithms computational complexity*", IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Noiembrie 2014, Budapesta, Ungaria, ISBN: 978-1-4799-7855-7, DOI: 10.1109/CINTI.2014.7028667, indexare: ***IEEE*** și ***DPLP*** 4. **Marius-Alexandru Velciu**, Victor-Valeriu Patriciu și Mihai Togan, "*An evaluation of the Fuzzy Vault scheme diffusion points order of magnitude*", 14th International Conference on Informatics in Economy (IE), Aprilie 2015, București, ISSN: 2284-7472, indexare: ***ISI*** și ***RePEc*** 5. **Marius-Alexandru Velciu**, Alecsandru Pătrașcu și Victor-Valeriu Patriciu, "*An evaluation of the Reed-Solomon error-correcting codes usage for bio-cryptographic algorithms*", IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2015, ISBN: 978-1-4673-6397-6, DOI: 10.1109/ SACI.2015.7208255, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 6. Alecsandru Pătrașcu, **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Cloud Computing Digital Forensics Framework for Automated Anomalies Detection*", IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2015, ISBN: 978-1-4673-6397-6, DOI: 10.1109/SACI.2015.7208257, indexare: ***ISI***, ***IEEE***, și ***DPLP*** 7. **Marius-Alexandru Velciu** și Victor-Valeriu Patriciu, "*Enhancing Fuzzy Vault bio-cryptographic scheme security by using genuine points salted hashing*", 8th International Conference on Security for Information Technology and Communications (SECITC), București, Iunie 2015, ISSN: 2285-1798, neindexată 8. **Marius-Alexandru Velciu**, Victor-Valeriu Patriciu și Ion Bica, "*A Bio-Cryptographic framework for securing mobile devices content*", IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Mai 2016, ISBN: 978-1-5090-2379-0,

	indexare: ***ISI***, ***IEEE***, şi ***DPLP*** 9. Mihai-Gabriel Ionita, **Marius-Alexandru Velciu** şi Victor-Valeriu Patriciu, ”*Authorizing cyber warfare countermeasures by using a bio-cryptographic fingerprint authentication method for mobile devices*”, 9th International Conference on Security for Information Technology and Communications (SECITC), Bucureşti, Iunie 2016, ISSN: 2285-1798
Articole susținute la conferințe naționale	1. **Marius-Alexandru Velciu** şi Victor-Valeriu Patriciu, “*Beneficiile utilizării sistemelor biocriptografice în detrimentul sistemelor biometrice tradiționale*”, Conferința Impactul transformărilor socio-economice şi tehnologice la nivel naţional, european şi mondial, nr.8/2015, vol.8, organizată de Institutul de Economie Mondială, București, Iunie 2015, indexare: ***SSRN***

Data *Semnatura*