REZULTATELE ACTIVITĂŢILOR DE CERCETARE–DEZVOLTARE DESFĂȘURATE ÎNCADRUL TEZEI DE DOCTORAT CU TITLUL

Soluții inovative folosind mecanisme criptografice pentru a asigura securitatea datelor în cloud

<table>
<tr><td colspan="3">AUTOR
CristianLUPAȘCU</td><td colspan="3">ÎNDRUMĂTOR
Prof.univ.dr.ing.Victor-ValeriuPATRICIU</td></tr>
<tr><td colspan="6">DOMENIUDEDOCTORAT</td></tr>
<tr><td>Data înmatriculării</td><td>02.10.2017</td><td>Data susțineriip ublice</td><td>04.06.2021</td><td>Data confirmării</td><td></td></tr>
<tr><td colspan="6">REZULTATELEACTIVITĂȚIIDECERCETARE-DEZVOLTARE</td></tr>
<tr><td colspan="2">DENUMIREREZULTAT</td><td colspan="4"></td></tr>
<tr><td colspan="2">CATEGORIAREZULTATULUI</td><td colspan="2">Rezultat final</td><td colspan="2" rowspan="2">DETALIERECARACTERISTICI ALEREZULTATULUIFINAL</td></tr>
<tr><td colspan="2">documentaţii,studii,lucrări</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">planuri,scheme</td><td colspan="2">[X]</td><td colspan="2" rowspan="17">Obiectivul dominant al acestei teze este acela de a propune soluții inovative folosind mecanisme criptografice pentru a asigura securitatea datelor în cloud, în special cu focus pe datele în folosință, având ca fundament concluziile și rezultatele analizei amănunțite cu privire la tehnologiile emergente, eficiența acestora precum și utilitatea practică a lor. Ca obiectiv secundar, lucrarea prezentă are scopul de a studia și inventaria mecanismele prezente prin care să se poată garanta securitatea datelor la un nivel foarte ridicat. Alături de acest obiectiv auxiliar, teza își propune să facă și o analiză din punctul de vedere al vulnerabilităților și al amenințărilor fiecărui tip de tehnologie potrivită în asigurarea protecției datelor.</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">produseinformatice</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">reţete,formule</td><td colspan="2">[X]</td></tr>
<tr><td colspan="2">obiectefizice/produse</td><td colspan="2">[]</td></tr>
<tr><td colspan="2">brevetinvenţie/alteleasemenea</td><td colspan="2">[]</td></tr>
<tr><td rowspan="5">STADIULDEDEZVOLTARE</td><td>soluţie/modelconceptual</td><td>[X]</td></tr>
<tr><td>modelexperimental/ funcţional</td><td>[X]</td></tr>
<tr><td>prototip</td><td>[]</td></tr>
<tr><td>instalaţiepilotsauechivalent</td><td>[]</td></tr>
<tr><td>altele……</td><td>[]</td></tr>
<tr><td rowspan="10">DOMENIULDECERCETARE</td><td>tehnologiilesocietăţii 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,securitateaşi siguranţaalimentară</td><td>[]</td></tr>
<tr><td>biotehnologii</td><td>[]</td></tr>
<tr><td>materiale,proceseşiproduse inovative</td><td>[]</td></tr>
<tr><td>spaţiişisecuritate</td><td>[X]</td></tr>
<tr><td>cercetări socio – economice şiumaniste</td><td>[]</td></tr>
</table>

			Deși fundamentele matematice necesare acestor tehnologii de protejare a datelor în timpul execuției există de multă vreme, o parte din propunerile actuale nu au ajuns încă la maturitatea utilizării pe scară largă iar alte soluții au deja implementări comerciale de succes. Portofoliul disponibil pentru rezolvarea neajunsurilor în materie de securitatea informației este unul vast cu numeroase abordări dar și cu un potențial enorm de inovare și perfecționare a metodelor existente. Soluții precum criptarea homomorfică sau computațiile sigure multi-participant au capacitatea procesării datelor într-o formă indescifrabilă fără să compromită caracterul confidențial al informațiilor, iar altele asigură doar un mediu de încredere pentru execuție. Alte tehnologii sunt capabile să asigure anonimitatea procesului sau să descentralizeze computațiile la marginea rețelei fără sacrificiul securității.

CARACTERULINOVATIV	**produsnou**	[]	**DETALIERE CARACTERINOVATIV** - Cel mai eficient circuit de adunare a numerelor întregi în spațiul Zn folosind operațiilehomomorfice din schemele FHE bazate pe erori. Costul asociat unei astfel de funcții estelog2 n. - O nouă schemă de criptare homomorfică ce nu se bazează pe problema învățării cu erori șiimplementarea aferentă, plecând de un cadru general brevetat și criptosistemul GM. - O abordare multi-GPU pentru accelerarea hardware a unei biblioteci software de criptarehomomorfică bazată pe LWE. - O schemă teoretică de prelucrare a datelor confidențiale și non-senzitive prin care suntcriptate homomorfic doar cele secrete, legătura între acestea realizându-se prin circuite deegalitate evaluate homomorfic. - Aplicabilitatea unei scheme de criptare homomorfică fără erori asupra operațiilormorfologice pe imagini digitale binare prin: eroziune, dilatare respectiv compunereaacestora și comparația cu alte scheme RLWE.
	produsmodernizat	[]	
	tehnologienouă	[**X**]	
	serviciunou	[**X**]	
	serviciumodernizat	[**X**]	
	altele…….	[]	

			- Utilizarea criptării homomorfice pentru a proteja confidențialitatea datelor într-o aplicațiede urmărire a contactelor în contextul pandemiei Covid-19. - Propunerea unor metode de trecere dintr-o schemă de criptare homomorfică non-LWE încele RLWE fără decriptarea intermediară, denumite bridge-uri. - Un sistem de autentificare complet descentralizat a senzorilor din zona industrială IoT,utilizând un registru distribuit și protocoale de SMPC pentru eliminarea punctelor centralece pot fi ținta unui atac cibernetic. - Un modul de securitate software asemănător unui HSM, ce utilizează setul de instrucțiuniIntel SGX pentru execuția operațiilor criptografice într-un mediu sigur (TEE).

INFORMAŢIIPRIVINDPROPRIETATEAINTELECTUALĂ	
cerereînregistrarebrevetdeinvenţie	Nr.....data.....
brevetdeinvenţieînregistrat(naţional,european, internaţional)	Nr.....data.....
cerereînregistraremodeleşideseneindustrialeprotejate	Nr.....data.....
modele şi desene industriale protejate înregistrate(naţional,european,internaţional)	Nr.....data.....

DOMENII DEAPLICABILITATE	**DETALIEREAPLICABILITATE**
ÎndomeniuldeinteresalMApNșif lotedenavecomerciale	- Procesareadocumentelorstocate criptatînoricefeldemediu.ex:cloudprivat militar,fărăaafecta securitatea acestora; - Indicarea comportamentul maliționsprin analiza datelor criptate din rețea - Detectarea documentelor cu caracter sensibil transmise într-o rețeasecurizată; - Soluțiideanalizăadatelorcolectatedintr-orețea, fără a le decripta,cuscopuldeasusțineactivitatea ofițeruluide securitate;
În alte domenii: medical,financiar-bancar,audit,etc.	- Toate soluțiile propuse în această lucrare suntcompatibilecumaimultedomeniicareutilizeaz ădispozitiveelectronice. - Soluțiiledeprotecțiea datelor utilizateîndomeniulmedicalșifinanciar-bancar sunt o necesitate întrucât conțin datesensibile; - În contextul actual Covid-19 regăsim propus un sistem de detecție a contactelor - Soluțiile de detectare a comportamentului malițios într-oinstituție publică sau privată sunt necesare pentrusecurizareacompanie, fără însă a pune în pericol caracterul confidențialitatea acestora.
DISEMINAREAREZULTATE LORCERCETĂRII REALIZATE ÎNCADRULTEZEI DE DOCTORAT	**DENUMIREARTICOL/REVISTĂ/CONFERINȚĂ**
Articolepublicateînreviste /ProceedingscotateISI	1. **Cristian Lupașcu**, Alexandru Lupașcu, Ion Bica, "DLT basedauthenticationframework for IndustrialIoTdevices", Sensors, MDPI, Vol. 20, Issue 9, pp 2621, 2020, https://doi.org/10.3390/s20092621

Articolepublicateînreviste /ProceedingscotateBDI	1. Adrian Matei, **Cristian Lupașcu**, Ion Bica, "On GPU Implementations of EncryptionAlgorithms", Journal of Military Technology, MilitaryTechnical Academy"Ferdinand I" PublishingHouse, Vol. 2, No. 2, Dec., 2019
Articolesusținutelaconferinței nternaționale	1. Alexandru Lupașcu, Mihai Togan, **Cristian Lupașcu**, "SGX-Based Cloud SecurityModule withUser's Sole Control", International Conference onCommunications (COMM), IEEE, pp. 413-416, 2018 2. **Cristian Lupașcu**, M. Togan, Victor-Valeriu Patriciu, "AccelerationTechniques forFully-HomomorphicEncryptionSchemes", International Conferenceon Control Systemsand Computer Science (CSCS), IEEE, pp. 118-122,2019 3. **Cristian Lupașcu**, CezarPlește, Mihai Togan, "PrivacyPreservingMorphologicalOperations for Digital Images", International Conference onCommunications (COMM), IEEE, pp. 183-188, 2020
Articolesusținutelaconferințe naționale	-

Data *Semnatura*
11.05.2021