(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 135009 A2**
(51) **Int.Cl.**
*G16Y 10/05* (2020.01);
*G06Q 50/02* (2012.01);
*H04L 29/02* (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2019 00635**

(22) Data de depozit: **07/11/2019**

(41) Data publicării cererii:
**28/05/2021** BOPI nr. **5/2021**

(71) Solicitant:
• **BEIA CONSULT INTERNATIONAL S.R.L.**,
*STR. POIANA NARCISELOR NR.12, ET.1, AP.3, SECTOR 1, BUCUREŞTI, B, RO*

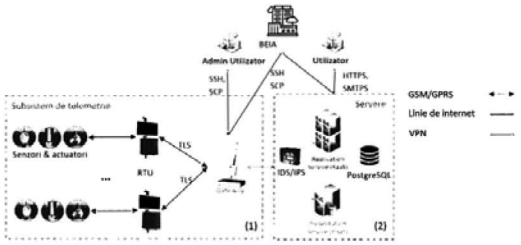
(72) Inventatori:
• **SUCIU GEORGE**,
*STR. POIANA NARCISELOR NR. 12, ET. 1, AP. 3, SECTOR 1, BUCUREŞTI, B, RO;*
• **ISTRATE CRISTIANA IOANA**,
*STR.MIHAIL KOGALNICEANU, NR.14, AP.10, SECTOR 5, BUCUREŞTI, B, RO;*
• **SUCIU GHEORGHE**,
*STR. POIANA NARCISELOR NR. 12, ET. 1, AP. 3, SECTOR 1, BUCUREŞTI, B, RO*

(54) # SISTEM SECURIZAT PENTRU INTERNETUL OBIECTELOR UTILIZÂND IZOLAREA DINAMICĂ

(57) **Rezumat:**

Invenţia se referă la un sistem securizat pentru Internetul obiectelor care se adresează domeniului agro-meteorologic. Sistemul conform invenţiei cuprinde două subsisteme: un subsistem (**1**) de telemetrie care monitorizează culturile utilizând senzori/actuatori pentru colectarea de date, fără fir sau prin cabluri, şi Internetul pentru transportul datelor şi un subsistem (**2**) de servere care procesează datele colectate şi le stochează pentru utilizări ulterioare, în care, în cadrul subsistemului (**1**) de telemetrie, senzorii/actuatorii (**S&A**) comunică cu o unitate (**R**) de telemetrie la distanţă folosind conexiuni prin cablu, unitatea (**R**) de telemetrie la distanţă transmite datele prin GPRS către o poartă (**G**) care face legătura cu serverele, iar înainte de a ajunge la servere, datele trec printr-un sistem de detectare/prevenire a intruziunilor (**IDS/IPS**), la acest subsistem (**1**) având acces doar administratorii, conexiunea efectuându-se printr-un program SCP (Secure File Copy) şi protocolul SSH (Secure Shell) folosind un canal securizat prin VPN (Virtual Private Network), în timp ce la subsistemul (**2**) de servere are acces, prin Internet, orice utilizator înscris, pe baza unor autorizări, conexiunea fiind realizată folosind protocolul SMTPS (Simple Mail Transfer Protocol Secure) şi protocolul HTTPS (Hypertext Transfer Protocol Secure).

Revendicări: 3
Figuri: 1






RO 135009 A2

# 1. DESCRIEREA INVENŢIEI

## 1.1 TITLUL INVENŢIEI

Obiectul invenţiei constă într-un: ***Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică.***

## 1.2 DOMENIUL DE APLICARE AL INVENŢIEI

Invenţia se referă la un ***"Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică"***, dezvoltat în cadrul proiectului European cu titlul „On Demand Secure Isolation" - ODSI (contract subsidiar nr. 63/14.06.2017, al proiectului CELTIC, ID: C2014/2-12).

Soluţia *Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică* se adresează:

- fermierilor;
- agenţiilor guvernamentale: e.g. primării;
- dezvoltatorilor de platforme ce utilizează tehnologia Internetul Obiectelor (Internet of Things – IoT);

## 1.3 STADIUL ACTUAL AL TEHNICII MONDIALE

Diversificarea tehnologiilor de reţea, a mijloacelor informatice, a spectrului aplicaţiilor client dar şi a gamei de ameninţări de securitate, justifică preocupările pentru dezvoltarea şi implementarea unor strategii de securitate moderne şi optimizate. Aceste strategii trebuie să aibă în vedere un context global foarte dinamic în care se dezvoltă aplicaţii de Smart City, IoT, comunicaţii Machine to Machine (M2M), aplicaţii bazate pe virtualizare la nivel de reţea.

Una dintre abordările practice care câştigă un interes sporit este cea de tratare segmentată a funcţiilor de reţea de izolare a zonelor sensibile, în vederea proiectării şi implementării unor mecanisme eficiente de protecţie la intruziuni.

Dintre tehnicile de izolare existente la momentul curent se pot menţiona:

- **Medii de executare de încredere (MEI).** MEI este o zonă securizată a procesorului principal dintr-un telefon inteligent (sau orice dispozitiv conectat la Internet). Se asigură că datele sensibile sunt stocate, procesate şi protejate într-un mediu izolat, sigur. Abilitatea MEI de a oferi o executare sigură, izolată a software-urilor autorizate, cunoscute sub numele de „aplicaţii de încredere", îi permite să furnizeze securitate completă prin impunerea confidenţialităţii, autenticităţii, integrităţii sistemului şi drepturilor de acces la date [1]. Comparativ cu alte medii de securitate, MEI oferă viteze mari de procesare şi o cantitate mare de memorie accesibilă.
- **Medii de executare sigure (MES).** Un mediu de executare în condiţii de siguranţă permite utilizatorilor să „încerce" noi software-uri (sau modificări de configurare ale software-ului existent) fără a fi supuşi riscului de afectare a sistemului, în orice mod. O proprietate importantă a unei MES este aceea că reproduce cu fidelitate comportamentul aplicaţiilor, ca şi cum acestea ar fi funcţionat nativ pe sistemul de operare de bază (gazdă). Acest lucru se realizează printr-o izolare într-o singură direcţie: procesele ce rulează în cadrul MES sunt date cu acces la citire pentru mediul furnizat de sistemul de operare gazdă, însă operaţiunile de scriere sunt împiedicate să scape în afara MES [2]. Ca rezultat, procesele MES nu pot influenţa comportamentul proceselor gazdă ale sistemului de operare sau integritatea datelor pe sistemul de operare gazdă. MES sprijină o gamă largă de sarcini, printre care: studiul codurilor menite să afecteze funcţionarea dispozitivelor, execuţia controlată a software-

ului provenit din surse nesigure, experimentarea cu modificările configurației software, testarea patch-urilor de software.

- **Izolarea Hipervizorului.** Hipervizorul, numit şi monitorul maşinii virtuale, rulează pe sistemul de operare gazdă şi alocă resurse emulate fiecărui sistem găzduit. Când sistemul de operare găzduit face o apelare către sistemul de bază, hipervizorul interceptează acel semnal şi îl traduce într-un apel destinat sistemului de operare gazdă. Hipervizorul controlează accesul fiecărei maşini virtuale la procesor, memorie, dispozitive I/O şi reţea. De asemenea, segmentează resursele fizice în entităţi izolate şi permite fiecărui sistem de operare oaspete să funcţioneze independent. Un atac asupra unei maşini virtuale nu ar trebui să afecteze nici una dintre celelalte maşini virtuale de pe server sau de pe sistemul de operare gazdă. Acest lucru este diferit de un sistem de operare multi-utilizator, în care toţi utilizatorii pot fi afectaţi de un atac. Exemple de astfel de hipervizoare care oferă izolare sunt Qubes OS [3], Xen Management API [4], Libvirt API [5], Red Hat Enterprise Virtualization (RHEV) [6].
- **Izolarea execuţiei.** Izolarea execuţiei este o implementare de referinţă software a conceptului de securitate prin izolare utilizat de Microsoft [7]. Nu este destinat să împiedice pornirea malware-ului sau să evite introducerea acestuia în maşina utilizatorului, ci oferă mai degrabă un mediu limitat în care malware-ul poate funcţiona fără a afecta întregul sistem. Izolarea execuţiei permite manipularea unui grup de astfel de medii „gata de utilizare" pentru a rula aplicaţii necunoscute sau pentru a deschide fişiere sau programe suspecte de la terţi neconfirmaţi. Utilizatorul decide dacă să deschidă un fişier, în funcţie de încrederea pe care o are în originea fişierului. Există o opţiune în care fişierul va fi copiat şi deschis într-un mediu izolat pentru utilizarea acestuia. Toate daunele cauzate de acest fişier, dacă vor exista, vor fi limitate la mediul izolat. Izolarea execuţiei încearcă să profite de tehnologia hardware virtualizabilă disponibilă la momentul curent în majoritatea platformelor şi să o aplice pentru a rezolva unele probleme comune pe care le au utilizatorii în fiecare zi când folosesc computerul.
- **Bază de procesare de încredere (BPI).** Baza de procesare de încredere a unui sistem informatic este setul tuturor componentelor hardware, firmware şi/sau software care sunt critice pentru securitatea sa, în sensul că erorile sau vulnerabilităţile care apar în interiorul BPI ar putea pune în pericol proprietăţile de securitate ale întregului sistem [8]. În acest context dinamic, strategiile de izolare enumerate trebuie implementate împreună cu sisteme de detectare a intruziunilor (IDS - Intrusion Detection Systems) care să fie testate în medii separate, pentru a nu fi compromise datele sensibile.

Una din abordările moderne este cea a dezvoltării unor modele de detecţie bazate pe învăţare maşină. Astfel de modele se utilizează pentru aplicaţii în medii inteligente şi folosesc cele mai avansate dezvoltări de inteligenţă artificială, big data, variate tehnici de modelare şi optimizare şi se pot clasifica după cum urmează:

- Modelele nesupervizate - asigură detecţia anomaliilor în zonele de interes ale reţelelor;
- Modelele supervizate - învaţă să recunoască clase specifice de evenimente la nivelul zonelor de interes ale reţelelor.

În general, aplicarea unor strategii de securizare a reţelelor, indiferent de tehnologiile considerate, necesită, de asemenea, şi considerarea unui cadru metodologic pentru evaluarea riscurilor. Analiza de risc şi analiza vulnerabilităţilor sunt premise esenţiale pentru dezvoltarea unor medii operaţionale sigure şi optimale în raport cu aplicaţiile reale şi cerinţele acestora.

Legat de stadiul actual al cunoaşterii al profilurilor de protecţie (PP), acestea sunt de mai multe tipuri şi axează pe izolarea sigură a proceselor, a stocării, a execuţiilor şi a transferului de informaţii.

## 1. Profil de Protecţie pentru Comutatorul de Partajare Periferică

În contextul acestui PP [9], un comutator de partajare periferic oferă un mecanism pentru a conecta în siguranţă un set comun de periferice (1 la n) la calculatorul ataşat (1 la j) fără a permite partajarea sau transferul de date. Aceasta înseamnă că aceste k periferice pot fi conectate mai întâi la computerul 1 şi apoi comutate de utilizator la calculator 2, iar calculatorul 2 nu va interacţiona cu fluxul de informaţii anterior al calculatorului 1. PSS-ul va urma o acţiune deliberată din partea utilizatorului pentru a permite o interacţiune între perifericele conectate

şi calculatorul selectat. Exemple de tipuri de PSS care ar trebui să pretindă conformitatea cu acest PP includ tastatură, video, mouse, switch-uri (KVM), mouse, switch-uri (KM). Exemple de dispozitive care nu sunt adecvate pentru evaluarea împotriva acestui PP includ Internet Protocol (IP) şi switch-uri ataşate reţelei.

**2. Profil de Protecţie pentru Virtualizarea Serverului**

Virtualizarea Serverului în contextul acestui PP [10] se referă la un sistem de virtualizare care implementează componente hardware virtualizate pe sisteme fizice de tip server. Se creează un mediu hardware virtualizat pentru fiecare instanţă a unui sistem de operare (maşini virtuale sau VM-uri) permiţând acestor medii să execute simultan, menţinând în acelaşi timp aspectul izolării şi controlul exclusiv asupra resurselor de calcul alocate. Fiecare instanţă de maşină virtuală VM acceptă aplicaţii cum ar fi servere de fişiere, servere web, şi servere de email. De asemenea, virtualizarea serverului poate suporta sisteme de operare client într-un mediu virtual desktop sau într-un mediu de tip „thin client".

Componentele unei astfel de Sistem de Virtualizare sunt definite ca instanţe de Maşini Virtuale şi un Manager de Maşini Virtuale, care constă dintr-un Hypervisor, VM, sisteme binare de traducere, şi drivere de dispozitive fizice.

**3. Profil de Protecţie pentru Nuclee de Separare în medii care necesită o robusteţe ridicată**

Spre deosebire de nucleele tradiţionale de securitate care execută toate funcţiile de încredere pentru un sistem de operare securizat, funcţia principală de securitate a nucleului de separare este de a împărţi subiectele şi resursele unui sistem în clase de echivalenţă politică de securitate, şi de a impune regulile pentru fluxurile autorizate de informaţii dintre şi în cadrul partiţiilor. Produsele care respectă acest profil de protecţie [11] susţin controlul fluxului de informaţii, izolarea resurselor, iniţializarea sigură, livrarea sigură, recuperare sigură şi capabilităţi de audit.

**4. Virtualizare Europeană Sigură pentru Aplicaţii de Încredere în Domenii Critice**

Virtualizare Europeană Sigură pentru Aplicaţii de Încredere în Domenii Critice – Niveluri Independente Multiple de Securitate: Sistem de Operare (MILS PP: Operating System). Obiectivul evaluării – Target of Evaluation (TOE) abordat de profilul actual de protecţie [12] este un tip special de sistem de operare, care permite separarea eficientă a diferitelor aplicaţii care rulează pe aceeaşi platformă una de alta. TOE poate găzdui aplicaţii de utilizator, care pot fi, de asemenea, sisteme de operare. TOE asigură că aplicaţiile rău intenţionate, nu afectează nici TOE, nici alte aplicaţii din alte partiţii. TOE este destinat utilizării ca şi componentă (nucleu de separare) în sistemele MILS. Sistemele MILS (Multiple Independent Levels of Security) sunt explicate în [12], [13] şi [14].

TOE controlează utilizarea memoriei, a dispozitivelor, a procesoarelor şi a canalelor de comunicaţii pentru a se asigura separarea completă a aplicaţiilor utilizator şi pentru a preveni interferenţele neaşteptate între aplicaţiile utilizatorilor. TOE impune restricţii privind comunicarea dintre aplicaţiile de utilizator separate specificate de datele de configurare.

**5. Profilul de Protecţie TEE (Trusted Execution Environment)**

Obiectivul evaluării (TOE) în acest tip de profil de protecţie este „Trusted Execution Environment" [15] (TEE) pentru dispozitive de tip embedded care implementează specificaţiile Platformei Globale TEE [16].

TOE este un mediu de execuţie izolat de orice alt mediu de execuţie, inclusiv mediul de tip „Rich Execution Environment" (REE), şi aplicaţiile acestora. TOE găzduieşte un set de „Trusted Applications" (TA) şi le oferă un set cuprinzător de servicii de securitate incluzând: integritatea execuţiei, comunicarea securizată cu „Client Applications" (CA) rulând în REE, stocare de încredere, „key management" şi algoritmi criptografici, management al timpului şi aritmetic API.

**6. Profil de Protecţie pentru Modulul de Securitate al unui „Smart Meter Gateway"**

Acest Profil de Protecţie [16] defineşte obiectivele de securitate şi cerinţele de securitate corespunzătoare pentru un Modul de Securitate care este utilizat de către Gateway pentru sprijin criptografic. De obicei, un Modul de Securitate este realizat sub forma unei cartele inteligente (dar nu este limitat la aceea).

Scopul Evaluării – Target of Evaluation (TOE) care este descris în acest document este o unitate electronică care cuprinde hardware şi software utilizat de către Gateway pentru servicii centrale criptografice şi stocare sigură a cheilor criptografice şi date suplimentare relevante pentru Gateway.

TOE este destinat utilizării de către Gateway pentru funcţionarea sa într-un sistem Smart Metering ca furnizor de servicii criptografice, bazate pe criptografia curbelor eliptice ca generare şi verificare a semnăturilor digitale şi pe acord cheie.

**7. Profil de Protecţie a sistemului de prevenire a intruziunii reţelei**

Acest Profil de Protecţie [17] a fost dezvoltat de Agenţia de securitate a informaţiilor din Coreea (KISA) şi are ca scop definirea cerinţelor funcţionale de securitate cu care trebuie să fie echipat sistemul de prevenire a intruziunii reţelei, şi de cerinţele de asigurare a securităţii pentru a garanta siguranţa cerinţelor funcţionale de securitate.

Sistemul de prevenire a intruziunilor în reţea, dezvoltat în conformitate cu acest profil de protecţie, defineşte cerinţele de bază ale sistemului de prevenire a intruziunilor. Administratorul de reţea trebuie să poată să utilizeze acest profil de protecţie ca referinţă, pentru a propune cerinţe pentru menţinerea în siguranţă a sistemului informatic.

Acest profil de protecţie defineşte cerinţele de securitate ale sistemului de prevenire a intruziunilor în reţea, utilizat ca mijloc de protecţie a reţelei interne de informaţii şi de comunicaţii a unei organizaţii de atacuri de distrugere din Internetul extern. Dezvoltatorul sau autorul Obiectivului de Securitate (ST) poate adăuga cerinţe de securitate la niveluri superioare cerinţelor profilului de protecţie, atunci când se implementează un sistem de prevenire a intruziunilor în reţea. Profilul de protecţie defineşte ameninţările, aşteptările, şi politicile de securitate organizaţională care trebuie abordate în sistemul de prevenire a intruziunilor în reţea, şi descriu obiectivele de securitate, cerinţele funcţionale de securitate şi cerinţele de asigurare a securităţii, independente de mediul de implementare. În cele din urmă, profilul de protecţie oferă raţiune pentru obiectivele de securitate şi cerinţele de securitate.

## 1.4 SCOPUL INVENŢIEI

Sistemul securizat pentru internetul obiectelor utilizând izolarea dinamică este un rezultat al proiectului ODSI (On Demand Secure Isolation), ce propune furnizarea unor noi modele de securitate prezentând caracteristicile şi beneficiile abordărilor hardware şi software. Aceste modele oferă numai caracteristici minime certificate şi validate pentru izolare, cu scopul de a fi utilizate în producţia largă (procesoare având performanţă limitată şi cost redus) în toate abordările ce necesită tehnici de izolare pentru M2M, IoT, partajare infrastructură de reţea, etc.

Soluţiile puse la dispoziţie în acest proiect vor certifica un număr minim de dispozitive software şi hardware cu scopul de a demonstra caracteristica de izolare. Proiectul ODSI furnizează în domeniul industrial:

- Un model de securitate hardware/software;
- Definirea framework-ului de evaluare şi a elementelor necesare pentru certificarea criteriilor comune (de exemplu, modalitatea de protecţie a profilurilor), ce permite asigurarea unui nivel global de securitate a modelelor de izolare disponibile şi a soluţiilor derivate din acestea (soluţii hardware/software);
- Diseminarea modelelor ODSI de nivel înalt, implementarea profilurilor de protecţie şi a studiilor de caz open-source, precum şi standardizarea interfeţelor propuse pentru sectoarele IoT şi M2M.

Referitor la produsele rezultate în urma proiectului, BEIA Consult International a adus îmbunătățiri sistemului său M2M de agro-meteorolgie prin întărirea securității pentru aplicabilitate în scenarii de tip multitenant ale tehnologiilor IoT pentru agricultură inteligentă.

## 1.5 EXPUNEREA INVENȚIEI

Organizația BEIA dispune de un sistem agro-meteorologic, o platformă IoT pentru agricultura de precizie, în special pentru gestionarea bolilor culturilor, folosind alerte și notificări. După cum este prezentat în Figura 1, sistemul colectează date din mediul agricultural și prezintă datele utilizatorilor prin intermediul serviciilor Web.

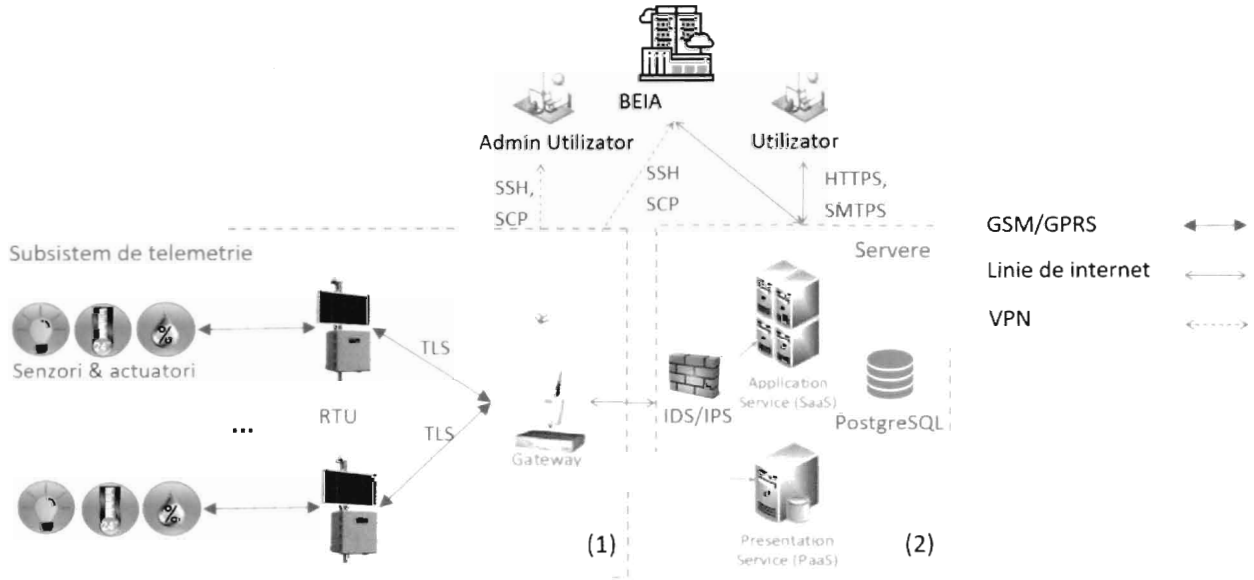



**Figura 1**: Arhitectura funcțională a sistemului agro-meteorologic

Sistemul de agro-meteorologie se împarte în două subsisteme:

- Subsistemul de telemetrie (1): monitorizează culturile utilizând senzori/actuatori prin wireless sau cabluri pentru a colectarea de date și Internetul pentru transportul de date;
- Subsistemul de server (2): procesează datele colectate și le stochează pentru cercetările viitoare.

În cadrul subsistemului de telemetrie, senzorii și actuatorii (**S&A**) comunică cu RTU-ul (Remote Telemetry Unit - Unitate de telemetrie la distanță) **R** folosind conexiuni cablate. RTU-ul transmite datele folosind protocolul TLS (Transport Layer Security) prin GPRS (General Packet Radio Service) către Gateway-ul **G**, un dispozitiv ce face legătura cu serverele. Înainte de a ajunge la serverul SaaS (Software as a Service - Software ca serviciu) sau PaaS (Platform as a Service - Platformă ca serviciu), datele trec printr-un sistem de detectare a intruziunilor/sistem de prevenire a intruziunilor (**IDS/IPS** - Intrusion Detection System/Intrusion Prevention System). Baza de date corespunzătoare este reprezentată de PostgreSQL. La subsistemul de telemetrie, au acces doar administratorii, conexiunea efectuându-se prin programul SCP (Secure File Copy) și protocolul SSH (Secure Shell) folosind un canal securizat prin VPN (Virtual Private Network). La subsistemul de server, are acces, prin Internet, orice utilizator înscris pe baza unor credențiale. Conexiunea se realizează folosind protocolul SMTPS (Simple Mail Transfer Protocol Secure) și HTTPS (Hypertext Transfer Protocol Secure).

Funcționalitatea sistemului de agro-meteorologie poate fi împărțită în 3 funcții de bază:

Tabel 1 Funcţiile de bază

| Funcţia de bază | Descriere |
|---|---|
| Colectare de date | • Citire: Senzorii din culturi colectează periodic informaţii despre temperatură, umiditate, lumina soarelui, etc.;<br>• Acţionare: Dispozitivele de comandă din culturi primesc comenzile de la utilizatori prin intermediul Serverelor şi îndeplinesc acţiunile specificate, de exemplu irigare;<br>• Transmisia datelor: Datele de la senzori şi comenzile de la utilizatori sunt transmise prin senzorii/actuatorii din culturi şi Servere prin Internet. |
| Utilizarea datelor | • Prezentarea datelor: serverul SaaS (Software as a Service - Software ca serviciu) prezintă utilizatorilor informaţiile colectate printr-o interfaţă Web;<br>• Procesarea datelor: serverul PaaS (Platform as a Service - Platformă ca serviciu) prezintă API-uri (Application Programming Interfaces - Interfeţe de programare a aplicaţiilor) pentru utilizatori astfel încât să proceseze datele colectate;<br>• Stocarea datelor: Baza de date stochează datele colectate pentru utilizatori pentru cercetări viitoare. |
| Actualizarea sistemului de la distanţă | • Web service SaaS/PaaS;<br>• RTU - Remote Telemetry Unit (Unitate de telemetrie la distanţă);<br>• Gateway. |

## 1.6 AVANTAJE

Soluţia oferă gestionarea mediilor de lucru într-un mod izolat utilizând containere Docker pe RTU şi servicii Cloud, protecţia împotriva atacurilor Denial of Service (DoS) folosind sisteme de detectare a intruziunilor/sisteme de prevenire a intruziunilor (IDS/IPS), managementul rolurilor şi dispozitivelor folosind canale de comunicare sigure (SSH, SCP, VPN), autentificare şi control al accesului bazate pe mecanismul de verificare al token-urilor (JSON API), comunicare securizată la distanţă folosind criptarea End-to-End (TLS, HTTPS).

# REFERINŢE

[1] Pinto S, Gomes T, Pereira J, Cabral J, Tavares A. IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices. IEEE Internet Computing. 2017 Jan;21(1):40-7
[2] Manès VJ, Jang D, Ryu C, Kang BB. Domain Isolated Kernel: A lightweight sandbox for untrusted kernel extensions. computers & security. 2018 May 1;74:130-43.
[3] Qubes OS https://www.qubes-os.org/doc/mgmt1/
[4] XEN https://docs.citrix.com/content/dam/docs/en-us/xenserver/xenserver-7-0/downloads/xenserver-7-0-management-api-guide.pdf
[5] Libvirt https://libvirt.org/html/index.htm
[6] RHEV https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Virtualization/3.0/html-single/REST_API_Guide/
[7] Mahadev RS, Seshadri A, Rajamani S, Kumar V. Using Trusted Execution Environments to Enable Integrity of Offline Test Taking. InApplications of Cognitive Computing Systems and IBM Watson 2017 (pp. 9-18). Springer, Singapore.
[8] Maene P, Gotzfried J, De Clercq R, Muller T, Freiling F, Verbauwhede I. Hardware-Based Trusted Computing Architectures for Isolation and Attestation. IEEE Transactions on Computers. 2017 Jan 5.
[9] Protection Profile for Peripheral Sharing Switch, NIAP, 3.0, 13 Feb 2015 https://www.niap-ccevs.org/pp/pp_sv_v1.1.pdf
[10] Protection Profile for Server Virtualization, NIAP, 1.1, 14 Sept 2015 https://www.niap-ccevs.org/pp/pp_pss_v3.0.pdf
[11] Protection Profile for Separation Kernels in Environments Requiring High Robustness, IAD, 1.03, 29 June 200 https://www.niap-ccevs.org/pp/pp_skpp_hr_v1.03.pdf

[12] Secure European Virtualization for Trustworthy Applications in Critical Domains – Multiple Independent Levels of Security: Operating System (MILS PP: Operating System), Euro MILS project, 3.1, 12 March 2015 http://www.euromils.eu/downloads/Deliverables/Y2/2015-EURO-MILS-Protection-Profile-White-Paper-V1.2.pdf
[13] MAGERIT https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
[14] Protection Profile PC Client Specific Trusted Platform Module TPM Family, TCG, 1.3, 14 July 2014 http://www.trustedcomputinggroup.org/files/resource_files/296EE64A-1A4B-B294-D0E00F3075CFCD67/PC_Client_TPM_PP_1.3_for_TPM_1.2_Level_2_V116.pdf
[15] Brickell E, inventor; Intel Corp, assignee. Using A Trusted Execution Environment As A Trusted Third Party Providing Privacy For Attestation. United States patent application US 15/475,896. 2018 Oct 4.
[16] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), BSI, 1.03, 11 Dec 2014
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0077V2b_pdf.pdf?__blob=publicationFile&v=1
[17] Network Intrusion Prevention System Protection Profile V1.1, 21 December 2015. https://www.commoncriteriaportal.org/files/ppfiles/CC-20%28IPS%20PP%20V1.1%29.pdf

## 2. REVENDICĂRI

**R1: Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică**, se axează pe cazul de utilizare agro-meteorologic, printr-o platformă „Internetul lucrurilor" (Internet of Things (IoT)) pentru agricultura de precizie.

**R2: Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică**, conform revendicării anterioare **R1**, este caracterizat prin structura acestuia împărţit în două subsisteme: subsistemul de telemetrie şi subsistemul de servere.

**R3: Sistem securizat pentru internetul obiectelor utilizând izolarea dinamică**, conform revendicărilor **R1** şi **R2**, este caracterizat prin aceea că permite colectarea şi transmiterea de date de la senzori, împreună cu transmiterea unor comenzi către actuatori, într-un mod securizat, deoarece orice modul conţine elemente de securitate. Izolarea dinamică reprezintă proprietatea ca orice componentă din cadrul sistemului, dacă este compromisă, nu va afecta securitatea celorlalte componente.

## 3. DESENE

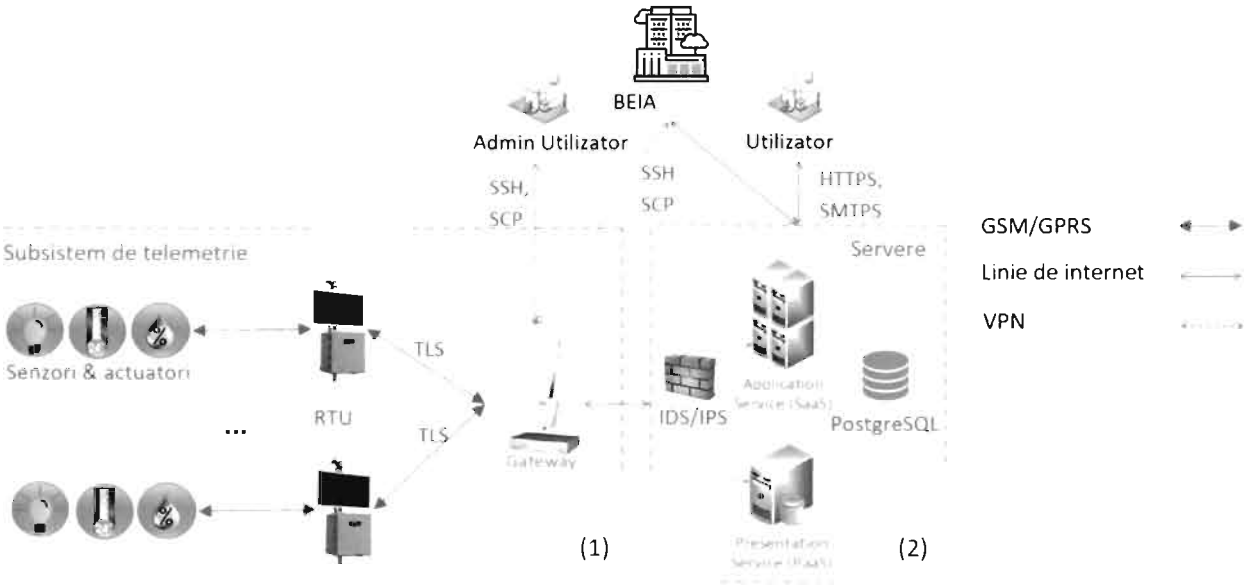



Figura 1: Arhitectura funcțională a sistemului de agro-meteorologie