(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 130798 A0
(51) Int.Cl.
G06F 21/50 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2015 00347**

(22) Data de depozit: **19/05/2015**

(41) Data publicării cererii:
30/12/2015 BOPI nr. **12/2015**

(71) Solicitant:
• **MUŞAT BOGDAN**, *STR. BRIZEI NR. 18, BL. FD7, SC. D, ET. 7, AP. 95, CONSTANŢA, CT, RO*

(72) Inventatori:
• **MUŞAT BOGDAN**, *STR. BRIZEI NR. 18, BL. FD7, SC. D, ET. 7, AP. 95, CONSTANŢA, CT, RO*

(54) # PLATFORMĂ HARDWARE ŞI SOFTWARE PENTRU PREVENŢIA ŞI DETECŢIA ATACURILOR CIBERNETICE

(57) **Rezumat:**

Invenţia se referă la o platformă hardware şi software pentru prevenirea şi detectarea atacurilor cibernetice asupra reţelelor de calculatoare. Platforma conform invenţiei cuprinde: un sistem (**1**) de detectare a intruziunilor, alcătuit dintr-un modul (**1a**) de decodare a pachetelor, responsabil cu decodarea diferitelor formate de pachete preluate din reţea, dintr-un modul (**1b**) de preprocesare, responsabil cu reconstrucţia unui flux de comunicaţie în baza pachetelor primite, şi dintr-un modul (**1c**) responsabil cu executarea regulilor de identificare a atacurilor asupra pachetelor de date primite din reţea, un sistem (**2**) de agregare a informaţiilor, alcătuit dintr-un modul (**2b**) care distribuie informaţiile extrase în urma prelucrării regulilor, către diferite sisteme interne sau externe, dintr-un modul (**2a**) care transmite alerte şi notificări către terţe sisteme, şi dintr-un modul (**2c**) de stocare a informaţiilor despre fluxurile din reţea, şi a informaţiilor parţiale sau totale obţinute în urma aplicării regulilor, şi un sistem (**3**) expert de management al reţelei, alcătuit dintr-un modul (**3b**) responsabil cu agregarea diferitelor informaţii din modul (**2c**), şi trecerea lor printr-o serie de transformări şi corelări; rezultatele obţinute sunt adăugate la o bază de cunoştinţe (**3c**), fie prin adăugare, fie prin corectarea unor informaţii deja existente, cu privire la tendinţe şi activităţi înregistrate şi învăţate de către sistem, dintr-un sistem (**3a**) expert care poate fi declanşat de informaţii primite de la un modul (**2b**) şi care, folosind informaţii din baza de cunoştinţe (**3c**), poate declanşa una sau mai multe acţiuni corective, în reţea, pentru a stopa sau limita un atac cibernetic, şi dintr-un modul (**3d**) care primeşte comenzi de la sistemul (**3**) expert şi poate reconfigura echipamentele de reţea pentru stoparea şi/sau limitarea atacurilor cibernetice.

Revendicări: 7
Figuri: 3

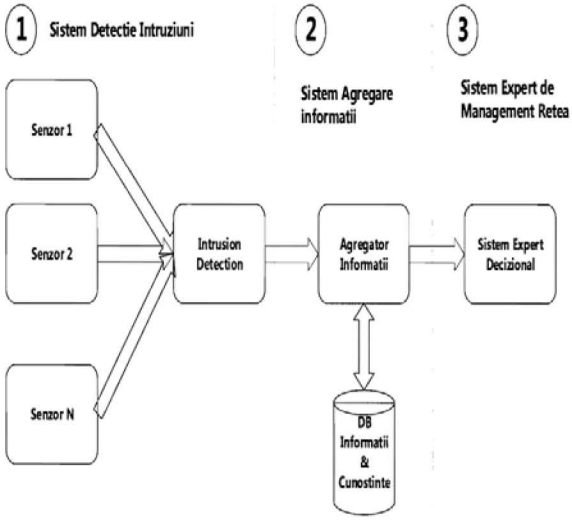

Fig. 1

RO 130798 A0

PLATFORMĂ HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE

Inventia se refera la o platformă hardware și software pentru prevenția și detecția atacurilor cibernetice, a rețelelor de calculatoare prin folosirea de tehnici avansate de calcul paralel în identificarea tiparelor de atac și metode avansate de statistică a clusterelor pentru modelarea vectorilor de atac precum și a atacurilor distribuite cu identificarea celor mai bune măsuri de apărare prin reconfigurarea dinamică a echipamentelor de rețea., destinat special pentru prevenția și detecția atacurilor cibernetice asupra rețelelor de calculatoare .

Sunt cunoscute mai multe sisteme de prevenție și detecție a atacurilor cibernetice, sisteme software, dar și sisteme dedicate pre-configurate pe o platformă hardware. În aproape fiecare rețea se găsește un astfel de sistem, cel mai adesea se regăsesc sub denumirea de IDS (Intrusion Detection Systems) și IPS (Intrusion Prevention Systems), care alături de sistemele de tip Firewall și Antivirus formează principalele componente ale sistemului defensiv într-o rețea de calculatoare.

Cele mai cunoscute și utilizate sisteme de prevenție și detecție a atacurilor cibernetice sunt:

- SNORT http://www.snort.org un sistem OpenSource, unele dintre cele mai folosite sisteme de tip IDS/IPS. Are suportul unei mari comunități care contribuie la dezvoltarea sa. Acest sistem a fost preluat de anumite companii și în regim comercial, prin adăugarea de cunoștințe proprii în regulile de detectare a tiparelor de atac. Sistemul permite în baza unor reguli să identifice tipuri de atacuri cibernetice sau anomalii în funcționarea rețelei doar dacă au fost definite apriori, astfel de reguli. Sistemul de procesare al regulilor este proiectat în regim- single-thread, din acest motiv nu beneficiază de capacitățile de multiprocesare și execuție paralelă a sistemelor de tip server moderne.

- OSSIEM – Open Source SIEM http://www.alienvault.com, atât versiunea open source cât și versiunea comercială AlienVault, folosesc sisteme de tip IDS/IPS proprietare sau externe cum ar fi SNORT, dar merg mai departe decât simpla detecție și declanșare a unei alarme, oferă un

sistem de integrarea a informațiilor într-o baza de date unica și generarează anumite rapoarte cu privire la funcționarea rețelei din punct de vedere al securității IT.

- Suricata – http://www.suricata-ids.org, este un sistem OpenSource de tip IDS/IPS, principalul concurent pentru SNORT. Are sprijinul comunității pentru definirea de reguli necesare motorului de identificare a atacurilor. Avantajul oferit față de SNORT este ca are suport pentru multi-threading beneficiind astfel de avantajele noilor modele de procesoare

- McAfee Network Security Platform http://www.mcafee.com una dintre cele mai sofisticate platforme de Securitate ce integrează alături de servicii de tip IDS/IPS și servicii de tip Firewall și servicii de protecție desktop – Antivirus. Sistemul de IDS/IPS este bazat tot pe semnături – reguli predefinite, incluse în motorul de filtrare pachete, reguli ce pot identifica atacurile cibernetice știute.

- Cisco http://www.cisco.com, comercializează o gama mare de sistem de tip IDS/IPS, ca extensii la echipamentele de tip Firewall în care compania are un istoric relevant. Sistemele de tip IDS/IPS se bazează tot pe reguli predefinite, și actualizate periodic pentru identificarea atacurilor cunoscute.

Sistemele prezentate au urmatoarele dezavantaje :

- Detectarea atacurilor se face prin filtrarea pachetelor de date din rețea folosind un set de reguli. Procesarea acestor reguli este foarte consumatoare de resurse de tip procesor, datorită volumului mare de pachete de date. Astfel limitarea de banda a unui sistem de IDS/IPS este dată de capacitatea de procesare și analiză a pachetelor din rețea. Procesarea se face folosind procesoarele convenționale CPU (Central Processing Unit), proiectate pentru calcule secvențiale complexe și mai puțin pentru procesarea paralelă a unui volum mare de date.

- Aceste sisteme asigură detecția vectorilor de atac la nivelul unui segment de rețea, majoritatea atacurilor sunt de tip distribuit având mai mulți vectori de atac simultan. Fără o abordare integrată de corelare a informațiilor de la toate segmentele de rețea este imposibil detectarea atacurilor complexe distribuite.

- Sistemele se bazează pe procesarea unor reguli în identificarea unui atac. Regulile știu să identifice atacurile cunoscute, nefiind eficiente pentru atacurile noi, pentru care nu a fost definit un set de reguli.

- Pentru atacurile noi, unde nu a fost definită încă o regula, se folosesc reguli generale definite în baza unor algoritmi euristici, specifici fiecărei categorii de vectori de atac. Aceste reguli nu asigură un nivel satisfăcător de eficiență și nu pot identifica modele noi de vectori de atac.

- Sistemele prezentate nu includ un sistem automat de răspuns la atacuri. Aceste sisteme declanșează alarme care să fie primite de către operatorii echipamentelor de rețea, urmând ca aceștia să ia anumite măsuri de prevenție. Automatizarea răspunsului este limitat, datorită naturii foarte variate a atacurilor cibernetice.

Un obiectiv al inventiei este existența unui modul – **Sistem Detecție Intruziuni** (1), sistem ce folosește ca în modelul clasic reguli, dar procesarea acestora se face prin metode de calcul paralel de înaltă performanță puse la dispoziție de către procesoarele grafice aflate pe plăcile grafice/video. În acest caz procesorul central CPU va fi degrevat de sarcina procesării regulilor, putând desfășura alte tipuri de activități. Procesorul grafic (GPU) preia fluxul de procesare al regulilor. La nivelul actual tehnologic, un procesor central CPU deține și 8 nuclee (core), dacă se activează opțiunea de hyperthreading, atunci un procesor (un chip), poate rula maxim 16 fire de execuție. Un procesor grafic de la NVIDIA de exemplu, conține pe un chip și 16 procesoare fiecare capabil să ruleze 1600 fire de execuție. Mutând efortul de procesare a regulilor de filtrare pe procesorul sau procesoarele grafice, avem la dispoziție o putere de calcul paralel dată de peste 24.000 de fire de execuție, iar procesorul central CPU putând efectua alte activități în sistem., **un alt obiectiv** este existența unui modul - **Sistem Agregare Informații (2)**, ce permite colectarea și agregarea informațiilor primite de la mai multe module de tip Detecția Intruziuni (1), aflată în mai multe segmente de rețea. Astfel avem un singur loc în care sunt stocate toate informațiile si pe aceste informații se pot face corelări de evenimente și alte transformări ce pot duce la identificarea de informații cu privire la întreaga rețea informatică, **un alt obiectiv** este existenta unui modul – **Sistem Expert de Management Rețea (3),** ce conține metode avansate de procesare a informațiilor colectate. Acest modul conține algoritmi de procesare statistică a datelor, algoritmi de analiza a clusterelor și algoritmi de detectare a anomaliilor, precum și algoritmi pentru identificarea evenimentelor rare. În baza acestor metode statistice, sistemul va fi capabil să se

autoadapteze și să identifice tipuri de atacuri cibernetice noi, pentru care nu exista reguli predefinite pentru identificare. Acest modul include o bază de cunoștințe segmentată pe principalele elemente de atacuri cibernetice și poate lua decizii de contracarare a atacurilor. Sistemul decizional este bazat pe un motor de învățare și algoritmi de tip teoria jocurilor adaptați pentru fiecare fragment specific de atac. Decizia poate fi luată automat sau asistată de către un operator, în acest caz modulul având rolul de suport și sistem expert. Măsurile de răspuns pot fi comenzi de (re)configurare a echipamentelor de rețea.

Problema pe care o rezolva inventia este asigurarea creșterii performanței cu privire la procesarea regulilor de identificare a atacurilor cu pa la 40x prin mutarea efortului de procesare pe GPU.

O alta problema pe care o rezolva inventia este agregarea tuturor informațiilor într-o bază unică, ca suport pentru procesări și identificare de informații noi cu privire la atacurile distribuite.

O alta problema pe care o rezolva inventia este analiza datelor din punct de vedere statistic, pe modele de cluster și detectare de anomalii, permițând identificarea tipologiilor noi de atacuri.

O alta problema pe care o rezolva inventia este ca metodele statistice pot identifica atacurile distribuite.

O alta problema pe care o rezolva inventia este ca include un sistem expert ca suport decizional ca răspuns la atacurile cibernetice.

PLATFORMĂ HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE este alcatuita din:

- **Modulul - Sistem Detecție Intruziuni** (1) ,care este alcătuit din următoarele sub-module:
- Modul Decodare Pachete (1a), responsabil cu decodarea diferitelor formate de pachete preluate din rețea
- Modul Preprocesare (1b), responsabil cu reconstrucția unui flux de comunicație în baza pachetelor primite, se lucrează la nivel de protocoale de rețea.
- Motor Detecție (1c), responsabil cu execuția regulilor de identificare a atacurilor asupra pachetelor de date primite din rețea. Acesta este compus din:

- Modul Scanare Conținut (1d), responsabil cu transferul dintre memoria internă către și dinspre memoria grafică, și organizarea informațiilor în blocuri, pregătite pentru procesarea paralela.
- Modul Procesare GPU (1e), responsabil cu procesarea paralelă de capacitate mare la nivelul procesorului grafic
- Modul Filtru Pattern Matching (1f), responsabil cu filtrarea informațiilor obținute în urma aplicării regulilor de identificare a atacurilor.

Sunt cunoscute mai multe sisteme de detectia intruziunilor cum ar fi: SNORT http://www.snort.org, Suricata http://www.suricata-ids.org , Cisco http://www.cisco.com . Majoritatea sisemelor de detectia intrusiunilor sunt similar in arhitectura, fie ca sunt de tip open source sau cu cod proprietar. Unele solutii sunt funizate ca si appliance (preinstalate pe un echipament dedicate) fie ca Solutia software ce poate fi instalata si configurata pe unul din echipamentele utilizatorului.

Sistemele existente au dezavantajul de a fi limitate in capacitatea de executie, in volumul de trafic de retea care poate sa-l inspecteze. Aceste solutii capteaza toate pachetele de date ce trec prin segemntul de retea in care sunt prezente si pleand de la un set de reguli de validare, testeaza fiecare pachet pentru a depista elemente de trafic iin retea neautorizate. Aceste limitari sunt datorate capacitatii de procesare a procesorului diposnibil pe echipamentul de calcul folosit. Datorita faptului ca numarul atacurilor si tipologia atacurilor cibernetice este din ce in ce mai variata, numarul regulilor de valiadre prin care trebuie sa treaca fieare pachet de retea, creste exponential, mult mai repede decat evolutia in viteza de procesare a echipamentelor hardware.

Obiectivul aplicatiei informatice, este de a introduce noi algoritmi care sa oferere o crestere semnificativa a capacitatii de filtrare a pachetelor, prin folosirea unor gramatici de reguli ce folosesc din plin calculul paralele, iar acesti algoritmi vor fi executati pe procesoare specializate in calcul paralele cum sunt procesoarele grafice.

Avantajele Degreveaza procesorul central de efectuarea analizei traficului din retea prin reguli seriale, si mutarea efortului de procesare in algoritmi paraleli pe procesul/procesaorele grafice, specializate pentru astfel de operatii. Priin acesta schimabre se obtine o crestere semnificativa a performantelor, de oridinul zecilor de ori. Echipamentele hardware pe care se instaleaza acest modul, va avea unul sau mai multe sub-module hardware, care nu sunt altceva decat placi grafice ce contin procesaore grafice GPU. In acest fel procesorul crentral este degrevat de activitatile de filtrare putand si directionat catre activitati de coordonare si management de resurse interne.

- **Modului – Sistem Agregare Informații (2),** este alcătuit din următoarele sub-module:

Modul Log Alert System (2b), sistem care distribuie informațiile extrase în urma procesării regulilor către diferite alte sisteme interne sau externe.

- Modul Sisteme Alertare Terțe (2a), sistem de trimitere alerte și notificări către sisteme terțe (modul opțional)

- Modul DB Loguri (2c) un sistem de stocare a informațiilor despre fluxurile din rețea a informațiilor parțiale sau totale obținute în urma regulilor, datorită activităților desfășurate în rețea.

Sunt cunoscute mai multe sisteme de tip detectie a intruziunilor care asigura mecanisme de agregare a informatiilor, cum ar fi ¨ **SNORT http://www.snort.org, Suricata** http://www.suricata-ids.org , Cisco http://www.cisco.com, **OSSIEM** http://www.alienvault.com si altele

Sistemele existente au dezavantajul de a face agregare totala a informatiilor primmite. Majoritatea sistemelor exitente au fost concepute pentru a lucre in mod individual, inspectand un singur segment de retea cel in care sunt instalate. Pentru arhitecturi de retea mai complexe care necesita mai multe astfel de sisteme, atunci fie prin capacitate proprie fie prin scripturi scrise de catre administratori se colecteaza toate informatiile primite de la fiecare sistem individual si stocate intr-o baza de date unica. Volumul de date astfel colectat poate fi foarte mare si de cele mai multe ori nu este relevant. De exemplu se pot colecta evenimente dintr-un segment de retea care nu are nici o influenta sau nu prezinta nici un risc pentru arhitectura generala a retelei.

Obiectivul aplicatiei informatice de a implementa un mecanisme de politici distribuite de colectarea informatiior de la aceste sisteme distribuite in diferite segmente de retea. acest set de politici este decis de printr-o interfata unica la nivel central dupa care este distribuit in fiecare nod al retelei, astfel incat colectarea informatiilor sa se face doar pentru informatiile necesare, iar informatiile colecatte sa fie intr-o forma prelucrate, nu in stare bruta (capture de trafic de retea). Astfel in baza de date central, vor fi captate informatii sintetizate si relevante pentru analiza la nivel central a intruziunilor a securitatii de retea in general.

Avantajele solutiei propuse consta in structurarea si selectarea informatiilor ce urmeaza a fi colectate din diferite segment de retea. acesta structurare se face dupa o procesare locala a datelor, in baza unui set de politici central, care tine cont de modelul de riscuri in reteaua informatica implementat. Astfel resursele IT implicate vor colecat un numar mai mic de de nformatii dar mult mai relevant. De exemplu, in mod normal pentru a identifica volumul de trafic catre o anumita destinatie, atunci trebuie contorizate toate pachetele spre acea destinatie captate de catre toate dispozitivile instalate in retea. Modulul nostrum poate distribuii un set de politici de colectare a datelor astfel incat sistemel din retea sa trimita doar informatii sintezitate – contori analitici cu privire la traficul catre destinatia respective, urmand ca la nivel central acesti contori sa fie sumarizati. Avand la nivel central o baza de date de dimensiuni mai mici si care contine date mult mai sintetizate, va avea avantajul oferiri de rapoarte complexe intr-un timp mult mai scurt.

- **Modulul – Sistem Expert de Management Retea (3),** este alcătuit din următoarele sub-module:

- Modul Data Mining & Correlation (3b), responsabil cu agregarea diferitelor informații din DB Loguri (2c), și trecerea lor printr-o serie de transformări și corelări. Aceste transformării le pute grupa în următoarele tipuri de algoritmi:
    - Cluster Analysis (K-means clustering, Expectation-Maximization Algoritm, Hierarchical clustering, single-linkage clustering, DBSCAN, OPTICS, SUBCLU, Canopy clustering,...)

- Anomaly detection (LOF – Local Outline Factor, OPTICS-OF, Distance Based Outliners, Local Correlation Integral, Local Distance-Based Outlier Factor).

- Baza de Cunoștințe (3c), rezultatul prcesării din modulul Data Mining (3b), este adăugat la acestă bază de cunoștințe fie prin adăugare fie prin corectarea unor informații deja existente, cu privire la trenduri și activități înregistrate și învățate de către sistem.
- Sistem Expert (3a), care poate fi declanșat de către informații primite de la modulul Log Alert System (2b), și folosind informații din Baza de Cunoștințe (3c), poate declanșa una sau mai multe acțiuni corective, în rețea pentru a stopa sau limita un atac cibernetic.
- Configuration Management (3d), primește comenzi din partea sistemului expert (3a), și poate reconfigura echipamentele de rețea (4) pentru stoparea și/sau limitarea atacurilor cibernetice.

Sunt cunoscute mai multe sisteme de tip detective si preventia a intruziunilor care pun la dispozitie mecanisme de automatizare a raspunsurilor, doar prin rapuns automat la o serie de evenimente ce au loc in retea, sau sunt specializate in procesarea si prezentare de rapoarte similare cu sistemele de tip business intelligence. Sisteme cur ar fi: McAfee Network Security Platform http://www.mcafee.com sau OSSIEM – Open Source SIEM http://www.alienvault.com

Sistemele existente au dezavantajul de a analiza la nivel de sensor – segment de retea iinformatiile cu privire la un atac cybernetic. Analiza distribuita a informatiilor colectatea din intreaga retea si corelarea acesteia pentru a identifica analomalii de comportament nu sunt facuta in astfel de sisteme specializate in detectia intruziunilor. Un atac cIbernetic poate fi foarte distribuit si variat in forma, din acest motiv este necesara implementarea unor algoritimi ce au la baza metode statistice de detectarea anlomaliilor in functionarea unei retele informatice. In prezent sisteme de detectie a intruziunilor folosesc doar mecanisme de colecatrea a informatiilor in vederea identificarii atacurilor cunoscute, pe baza de semnatura sau variatii in traficul de retea cu probabilitate mare de a fi trafic specific unui atac cIbernetic pe baza unor semnaturi comportamentale.

Obiectivul aplicatiei informatice de a implementa algoritmi specifici de detectarea anomaliilor, anomalii ce pot trece neobservate in fata sistemelor ce merg pe o baza de semnaturi si tipologii. Un atac cIbernetic poat fi distribuit si desfasurat pe o perioada mare de timp. Acest modul isi propune sa identifice anomaliile din retea, care pot identifica astfel de atacauri folosind principia de teoria clusterilor din matematica statistica precum modelarea evenimentelor rare, folosite cu success in alte domenii cum ar fi cel al preventiei dezastrelor. Modulul pune la dispozitie si un sistem expert cu autoinvatare pentru support decisional placand de la informatiilor colectate correlate cu istoricul de eveniment si actiuni din trecut.

Avantajele modulului sunt de a depista atacurile cibernetice incluziv cele sophisticate si complexe, cum sunt cele distribuite si de lunga durata, prin coleralarea de informatii si identificarea de anomalii, precum si oferirea suportului decisional pe baza de cunostinte si algoritmi specifici teoriei jocurilor, pentru activarea masurilor corecte de preventive si contracarare. Modulul foloseste algoritimi matamatici cunoscuri folositi cu success in alte domenii, asigurand o continutate intre detectia anamaliilor si a

evenimentelor rare cu actiuni de preventive ajustate dynamic in baza unor reguli specifice algoritmilor de optimizare conform teoriei jocurilor.

Se da in continuare un <u>model de realizare a inventiei</u> in legatura cu **figurile 1-3, care reprezinta:**

Fig.1 - Un modul - Sistem Detecție intruziuni (1);

Fig.2 – Un modul – Sistem Agregare Informații (2);

Fig.3 – Un modul – Sistem Expert de Management Rețea (3).

Se da in continuare un model de realizare a inventiei.

In figura 1. este prezentata Schema Macro privind modul de utilizare al **PLATFORMEI HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE** in raport cu fluxurile de date specifice primite si cu care sistemul interactioneaza,precum si legatuar intre cele trei module la nivel de flux informational si decisional pt intreaga platforma. Conform reprezentarii in reteaua informatia pot fi mai multe componente ce include modulul - **Sistem Detecție Intruziuni(1)**, pe face procesari si oclectari de informatii din diferite segmente de retea., informatii care sunt trimise intr-o locatie central, acestea fiind captate de atre modulul - **Sistem Agregare Informații (2)**, iar acest modul alimenteaza cu informatii modulul - **Sistem Expert de Management Retea (3)**, ce face procesari avansate de detectie a anomaliilor si ia decizii de executie a masurilor preventive prin schimabri de configuratie a echipamentelor din retea.

In figura 2. este prezentat Schema **Fluxului de date si Componente Sistem** ce urmeaza a fi transmise si procesate de **PLATFORMA HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE**, care se ocupa de colectarea si procesare informatiilor colectatea din retea. la nivelul fiecarui modul se pot identifica sub-componentele principale. De exemplu petru modulul - **Sistem Detecție Intruziuni(1)** avem o component responsabila cu decodarea formatului pachetelor(1a) de retea, o component responsabila cu preprocesarea pachetelor(1b) de retea cum ar fi

ordonarea lor pentru anumite tiprui de trafic, si component motorului de detectie(1c) ce foloseste calcul paralel executat pe procesoarele grafice avute la dispozitie. Modulul - **Sistem Agregare Informații (2)**, are o component de distribuire a informatiilor (2b), o component de alertare a sistemelor terte (2a), si o componenta de stocare a informatiilor primite (2c). Modulul - **Sistem Expert de Management Retea (3)**, are o component de Data mining & Corellation (3b), ce foloseste algoritimi de tip clustering si evenimente rare pentru a extrage informatii sintetizate cu care este aprovizioata o alta componenat baza de cunostinte (3c), precum si declansarea unor evenimente in sistemul expert (3a), care cu algoritmi de optimizare si tip teoria jocurlir, poate lua in mod automat prin reconfigurarea unro echipamente de retea (4), prin intermediul componentei specializate in acest sens (3d).

In figura 3. este prezentata **un Exemplu de retea functionala cu sistem de detectare a intruziunilor bazat pe PLATFORMA HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE, este un exemplu tipic de arhitectura de reta in care se poate vedea segmentele de retea importante unde se poate instala un sistem de detective si preventia a intruziunilor (IDS/IPS)**, astfel incact sa asigure o captare si analiza inteligenta a traficului relevant din retea.

a-2015--00347-
19-05-2015

42

REVENDICARI

PLATFORMĂ HARDWARE ŞI SOFTWARE PENTRU PREVENŢIA ŞI DETECŢIA ATACURILOR CIBERNETICE, caracterizata prin aceea ca este compusa din :

- **Modulul - Sistem Detecţie Intruziuni (1) este alcătuit din următoarele sub-module:**

- Modul Decodare Pachete (1a), responsabil cu decodarea diferitelor formate de pachete preluate din reţea
- Modul Preprocesare (1b), responsabil cu reconstrucţia unui flux de comunicaţie în baza pachetelor primite, se lucrează la nivel de protocoale de reţea.
- Motor Detecţie (1c), responsabil cu execuţia regulilor de identificare a atacurilor asupra pachetelor de date primite din reţea. Acesta este compus din:
    - Modul Scanare Conţinut (1d), responsabil cu transferul dintre memoria internă către şi dinspre memoria grafică, şi organizarea informaţiilor în blocuri, pregătite pentru procesarea paralela.
    - Modul Procesare PGU (1e), responsabil cu procesarea paralelă de capacitate mare la nivelul procesorului grafic
    - Modul Filtru Pattern Matching (1f), responsabil cu filtrarea informaţiilor obţinute în urma aplicării regulilor de identificare a atacurilor.

- **Modului – Sistem Agregare Informaţii (2), este alcătuit din următoarele sub-module**:

- Modul Log Alert System (2b), sistem care distribuie informaţiile extrase în urma procesării regulilor către diferite alte sisteme interne sau externe.

- Modul Sisteme Alertare Terţe (2a), sistem de trimitere alerte şi notificări către sisteme terţe (modul opţional)
- Modul DB Loguri (2c) un sistem de stocare a informaţiilor despre fluxurile din reţea a informaţiilor parţiale sau totale obţinute în urma regulilor, datorită activităţilor desfăşurate în reţea.

- **Modulul – Sistem Expert de Management Retea (3), este alcătuit din următoarele sub-module:**

- Modul Data Mining & Correlation (3b), responsabil cu agregarea diferitelor informații din DB Loguri (2c), și trecerea lor printr-o serie de transformări și corelări. Aceste transformării le pute grupa în următoarele tipuri de algoritmi:
    - Cluster Analysis (K-means clustering, Expectation-Maximization Algoritm, Hierarchical clustering, single-linkage clustering, DBSCAN, OPTICS, SUBCLU, Canopy clustering,...)
    - Anomaly detection (LOF – Local Outline Factor, OPTICS-OF, Distance Based Outliners, Local Correlation Integral, Local Distance-Based Outlier Factor).
- Baza de Cunoștințe (3c), rezultatul prcesării din modulul Data Mining (3b), este adăugat la acestă bază de cunoștințe fie prin adăugare fie prin corectarea unor informații deja existente, cu privire la trenduri și activități înregistrate și învățate de către sistem.
- Sistem Expert (3a), care poate fi declanșat de către informații primite de la modulul Log Alert System (2b), și folosind informații din Baza de Cunoștințe (3c), poate declanșa una sau mai multe acțiuni corective, în rețea pentru a stopa sau limita un atac cibernetic.
- Configuration Management (3d), primește comenzi din partea sistemului expert (3a), și poate reconfigura echipamentele de rețea (4) pentru stoparea și/sau limitarea atacurilor cibernetice.

PLATFORMĂ HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE, caracterizată prin aceea că este compusă dintr-un motor de detecție (1c), bazat pe reguli ce folosește procesorul grafic GPU, prin calcul paralel conform arhitecturilor specifice GPU, degrevând procesorul principal CPU de activitatea de procesare a regulilor de filtrare pachete de date din rețea.

PLATFORMĂ HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE, caracterizată prin aceea că este compusă dintr-un modul de Data Mining si Correlation (3b) ce permite identificare clusterelor de evenimente din rețea identificate și stocate în baza centralizată (2c). Permite identificarea clusterelor și urmărește dinamica acestor clustere pe axa timpului, măsurând gradienții de transformare in timp.

PLATFORMĂ HARDWARE ȘI SOFTWARE PENTRU PREVENȚIA ȘI DETECȚIA ATACURILOR CIBERNETICE, caracterizată prin aceea că modulul de Data Mining & Correlation (3b) include algoritmi de detectare a anomaliilor datorate activităților desfășurate în rețea ca urmarea a unor atacuri cibernetice.

PLATFORMĂ HARDWARE ŞI SOFTWARE PENTRU PREVENŢIA ŞI DETECŢIA ATACURILOR CIBERNETICE, caracterizată prin aceea că modulul de Data Mining & Correlation (3b) include algoritmi de detectare a evenimentelor rare datorate activităţilor desfăşurate în reţea ca urmarea a unor atacuri cibernetice.

PLATFORMĂ HARDWARE ŞI SOFTWARE PENTRU PREVENŢIA ŞI DETECŢIA ATACURILOR CIBERNETICE, caracterizată prin aceea că sistemul conţine un modul Sistem Expert (3a) ce poate lua decizii pe baza de cunoştinţe generate din modelari de tip cluster, detectare anomalii si evenimente rare.

PLATFORMĂ HARDWARE ŞI SOFTWARE PENTRU PREVENŢIA ŞI DETECŢIA ATACURILOR CIBERNETICE, caracterizată prin aceea că modulul sistemul Sistem Expert (3a) include algoritmi bazaţi pe teoria jocurilor, algoritmi derivaţi şi specifici fiecărui tip de atac cibernetic.

DESENE

Figura1.-Schema SISTEM MACRO

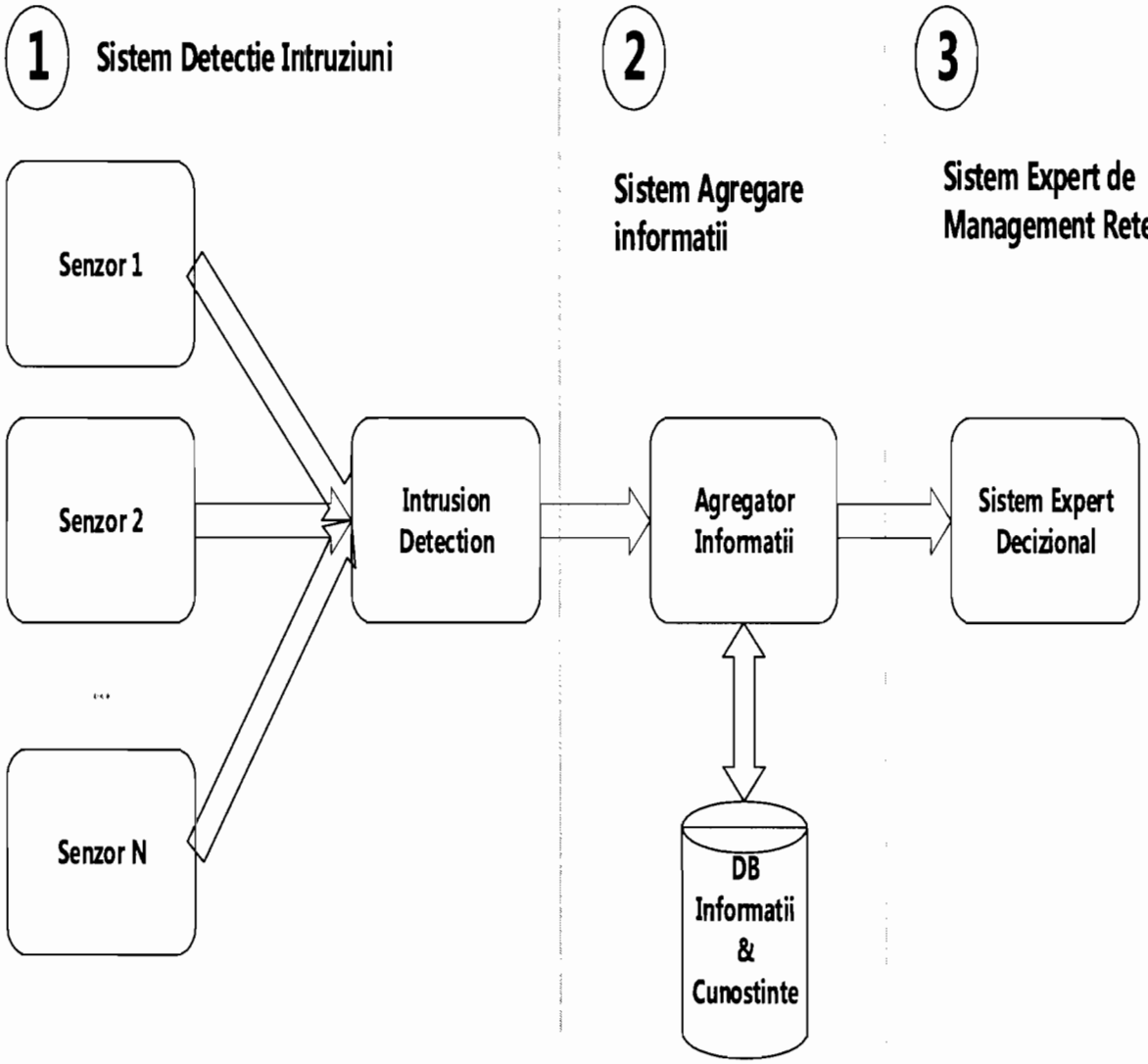

Figura 2. SCHEMA FLUX INFORMATII si COMPONENTE SISTEM

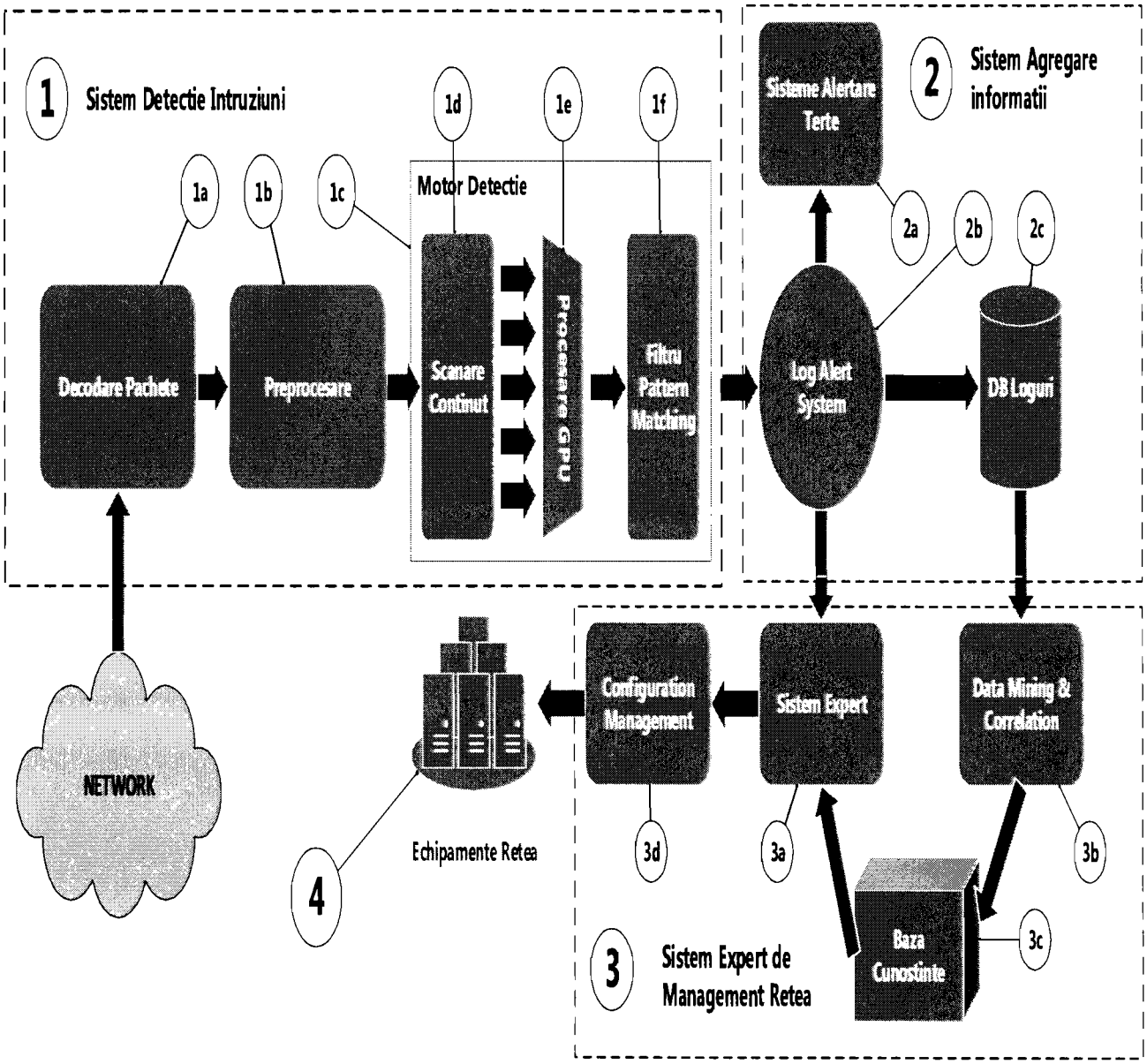

Figura 3. - EXEMPLU RETEA CU SISTEM DE DETECTAREA A INTRUZIUNILOR