UNIVERSITATEA "POLITEHNICA" DIN TIMIŞOARA
FACULTATEA DE AUTOMATICĂ ŞI CALCULATOARE

TEZĂ DE DOCTORAT

REZUMAT

SECURITY SOLUTIONS FOR CLOUD COMPUTING
SOLUŢII DE SECURITATE PENTRU CLOUD COMPUTING

Conducători ştiintifici: prof. dr.ing. Octavian PROŞTEAN
prof. Huaglory TIANFIELD, PhD

Doctorandă: ing. Alina Mădălina LONEA

2012

Cuprins

Evoluţia sistemelor de tip Cloud Computing constituie îmbunătăţirea tehnologiei informaţiei (IT), deoarece serviciile cloud devin o utilitate de calcul care facilitează viaţa noastră de zi cu zi. Cu toate acestea, chiar dacă avantajele oferite de această tehnologie îndeamnă companiile să îşi mute datele în serviciile cloud, întreprinderile sunt îngrijorate de riscurile de securitate implicate de procesul externalizării resurselor în mediul cloud computing.

Una dintre principalele probleme întâlnite în cazul migrării întreprinderilor la serviciile cloud este aceea a integrării identităţii utilizatorilor în mai multe servicii cloud folosind o legătură securizată. În plus, soluţiile actuale de autentificare în serviciile cloud constă din autentificarea bazată pe text a utilizatorului (nume de utilizator şi parolă), precum şi certificatele X.509. Problemele cu autentificarea bazată pe text sunt dificultatea de reamintire a şirurilor de caractere sigure folosite pentru parole, împreună cu dezavantajul parolelor construite din coduri nesigure de a fi vulnerabile la un număr crescut de atacuri. Astfel, o nouă soluţie de autentificare în serviciile cloud trebuie să crească securitatea, să rezolve problema dificultăţii de reamintire şi să întâlnească cerinţa de utilizare. Mai mult decât atât, indispensabilitatea securizării informaţiei în cloud computing este dovedită de întreruperile produse the atacurile Denial of Service (DoS) şi Distributed Denial of Service (DDoS) în serviciile cloud ale furnizorilor. Astfel, disponibilitatea serviciilor cloud a fost compromisă pe durata mai multor ore (întreruperi în Amazon Web Services, AppEngine şi Gmail). Astfel de întreruperi de acces ale utilizatorilor la serviciile cloud înregistrează costuri ridicate pentru toate organizaţiile, iar contramăsurile pentru protejarea serviciilor cloud împotriva atacurilor DoS şi DDoS sunt sistemele de detectare a intruziunilor (IDS). Din păcate, aceste sisteme IDS au dezavantajul că generează un număr mare de alerte şi produc o rată ridicată de fals pozitiv şi o rată mare de rezultate de tip fals negativ, fiind o povară de a analiza fişierele de logare generate de senzorii IDS.

Prin urmare, în această teză sunt propuse soluţii noi de securitate pentru cloud computing în vederea rezolvării problemelor mai sus menţionate. Teza este structurată pe 7 capitole, iar rezultatele de cercetare se referă la îmbunătăţirea securizării identităţii utilizatorilor, a informaţiei şi a infrastructurii.

Capitolul 1 intitulat ***"Introduction"*** a început cu prezentarea teoretică a noţiunilor despre cloud computing, care a inclus compararea cloud computing-ului cu mai multe tehnologii conexe, descrierea serviciilor cloud furnizate, descrierea modelelor de dezvoltare şi a caracteristicilor cloud computing, urmată de prezentarea procesului propus pentru întreprinderile care doresc să îşi migreze resursele spre serviciile cloud. Astfel, capitolul 1 prezintă un studiu comparativ dintre Cloud Computing şi tehnologiile conexe (virtualizarea, grid computing, cluster computing, arhitecturi orientate spre servicii). După prezentarea comparaţiei dintre Cloud Computing şi tehnologiile conexe, capitolul 1 defineşte conceptul de cloud computing prin cinci caracteristici esenţiale, prin trei tipuri de servicii şi prin patru modele de implementare. De asemenea, a fost conceput procesul de administrare al migrării resurselor întreprinderilor mici şi mijlocii (SMEs) spre serviciile Infrastructura ca şi Serviciu (IaaS). Procesul propus a fost realizat într-o succesiune justificată de activităţi interdependente. Activităţile descrise în acest proces sunt împărţite în patru paşi: analizarea datelor, luarea deciziilor, migrarea şi administrarea. Pasul iniţial este realizat prin analizarea datelor şi include: analizarea oportunităţilor de migrare spre serviciile cloud, studiul riscurilor întâlnite şi examinarea infrastructurii curente folosită de întreprindere. Apoi, un alt obiectiv este luarea deciziilor care include următoarele decizii: ce informaţie trebuie mutată în cloud şi cine va accesa acea informaţie, luarea deciziei în privinţa definirii cerinţelor pentru serviiciile cloud, ce furnizor de serviciu (Cloud Service Provider CSP) va alege organizaţia şi cum organizaţia va realiza administrarea serviciilor cloud. În continuare, mutarea efectivă a întreprinderilor la serviciile cloud este realizată prin pasul de migrare, care cuprinde două activităţi: dezvoltarea contractului Service Level Agreement (SLA) şi dezvoltarea modelului cloud folosind capabilităţile furnizorului de servicii cloud, precum şi cerinţele serviciilor definte în pasul 2. Pasul final al procesului propus prezintă activitatea de administrare a serviciilor cloud, prin două funcţii de management: funcţia business şi funcţia operaţională. Acest proces a fost conceput pentru a analiza provocările cu care se confruntă întreprinderile, printre care pentru problemele de securitate această teză a furnizat soluţii inovative.

De asemenea, capitolul 1 a abordat motivaţia tezei, obiectivele de cercetare investigate, precum şi structura acestei teze cu subiectele discutate în fiecare capitol.

În continuare, în **capitolul 2** intitulat ***"Cloud Computing Security"*** s-a prezentat un studiu al securităţii în cloud computing, prin analiza managementului securităţii, împreună cu

problemele şi soluţiile de securitate. Managementul securităţii implică conformarea la reguli şi audit, crearea planurilor de asigurare a continuităţii afacerilor şi de refacere după dezastru, precum şi investigarea şi monitorizarea electronică a datelor în serviciile cloud. În ceea ce privesc problemele de securitate abordate în acest capitol, studiul efectuat prezintă propunerea unei clasificări a acestora prin împărţirea lor în două categorii: probleme de securitate ale aplicaţiilor şi probleme de securitate ale virtualizării, punând în evidenţă tehnicile de diminuare ale fiecărei ameninţări de securitate corespunzătoare fiecărei categorii în parte. Astfel, problemele de securitate ale aplicaţiilor s-au referit la atacurile wrapping şi la problemele de securitate ale browser-ului (de exemplu: account Hijaking şi spoofing), în conformitate cu tehnicile de diminuare care au fost identificate. De asemenea, problemele de securitate ale virtualizării au fost evaluate împreună cu strategiile de diminuare corespunzătoare. Astfel, problemele de securitate ale virtualizării discutate sunt următoarele: atacurile flooding, atacuri la adresa maşinilor virtuale, respectiv atacuri side-channel. Din listele sugerate a tehnicilor de diminuare pentru fiecare ameninţare a securităţii în cloud computing am observat predominenţa următoarelor soluţii: o autentificare puternică, tehnici de filtrare, sisteme de detectare a intruziunilor, izolarea datelor şi soluţii de monitorizare, care sunt întâlnite ca şi soluţii pentru securizarea componentelor din cloud computing.

În plus faţă de managementul securităţii şi ameninţările de securitate care au fost prezentate, în capitolul 2 o atenţie specială a fost îndreptată către soluţiile de securitate din cloud computing şi anume: securizarea identităţii, securizarea informaţiei şi securizarea infrastructurii, care reprezintă soluţiile de securitate în cloud computing, în ceea ce priveşte evitarea riscurilor de securitate şi eliminarea ameninţărilor. Astel, principalele preocupări legate de securizarea identităţii sunt îndeplinirea următoarelor cerinţe de securitate: autentificare puternică, furnizarea identităţii, federarea identităţii şi autorizare granulară. În ceea ce priveşte securizarea informaţiei, au fost descrise mecanismele de protejare a confidenţialităţii şi integrităţii datelor stocate, datelor în transmisie şi a datelor în utilizare, precum şi mecanisme de asigurare a disponibilităţii datelor. Măsurile discutate de protejare a datelor în condiţiile menţionate sunt: izolarea datelor, administrarea măsurilor de protejare împotriva atacurilor (intrusion management), precum şi criptarea datelor şi stabilirea unui management al cheilor criptate. În continuare, au fost discutate măsurile pentru securizarea infrastructurii în mediul cloud: controlul securităţii infrastructurii fizice, control securităţii mediului, controlul securităţii virtualizării şi realizarea securităţii de reţea.

Pe baza analizei securităţii în mediul cloud computing prezentate în capitolul 2, au fost dezvoltate îmbunătăţirile propuse în capitolele 3, 4 şi 6.

Astfel, **capitolul 3** denumit ***"Architectural Solution of Security for Cloud Computing"*** vizează ca şi obiectiv principal securizarea identităţii în cloud computing, urmată de atribuirea controlului securităţii la nivel de reţea, precum şi de izolarea datelor clienţilor, ceea ce punctează aplicarea măsurilor de securitate precum şi pentru informaţie şi infrastructură. Aceste considerente de securitate au fost folosite pentru proiectarea unei soluţii arhitecturale de securitate pentru cloud computing, soluţie construită prin descompunerea gradată pe nivele (Nivel 1-4) (Figura 1).

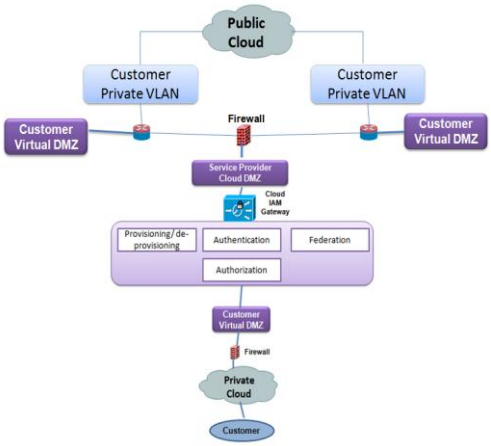

Figura 1 Layer 4 of the Architectural Security Solution in Cloud Computing

Prin urmare, unul dintre elementele principale ale acestei soluţii arhitecturale de securitate este definit în nivelul 1 şi este reprezentat de componenta denumită poarta de acces cloud a managementului identităţii şi accesului (Cloud IAM gateway), de asemenea denumit şi Managementul Identităţii şi Accesului ca şi Serviciu (IAMaaS). Acest prim element al soluţiei arhitecturale a fost conturat în urma stabilirii cerinţelor de securitate pentru Managementul Identităţii şi Accesului (IAM) şi în urma analizei sintetizate a soluţiilor curente ale Managementului Identităţii şi Accesului, care au determinat selectarea soluţiei Cloud IAM gateway. Această preferinţă s-a datorat faptului că soluţia IAM aleasă, contribuie la creşterea securităţii clienţilor şi întăreşte capabilitatea întreprinderilor de a coopera cu furnizorii de servicii cloud, spre deosebire de celelalte două metode: IAM dezvoltat de către întreprindere într-un cloud privat şi IAM dezvoltat de către furnizorii de servicii cloud. Ultimele 3 niveluri ale soluţiei arhitecturale prezentate au fost concentrate pe securizarea informaţiei şi infrastructurii, prin aplicarea controlului de securitate la nivel de reţea şi prin izolarea datelor clienţilor.

În continuare, mai multe protocoale au fost analizate pentru cerinţele de securitate ale componentei cloud IAM gateway, prin sinteza unei analize comparative. Standardele analizate pentru furnizarea identităţilor sunt: SPML (Service Provisioning Markup Language) şi SCIM (Simple Cloud Identity Management). Totodată, în contextul federării identităţilor, protocolul SAML (Security Assertions Markup Language) este preferat în producţie datorită caracteristicilor sale: securitate, scalabilitate şi dependabilitate. În acelaşi timp au fost discutate şi soluţii pentru realizarea autentificării într-un mod securizat. De asemenea, evaluarea s-a realizat şi pentru cerinţa de autorizare, care a fost prezentată pentru două modele: centrată pe utilizator (user-centric) şi centrată pe întreprindere (enterprise-centric).

În **capitolul 4** intitulat ***"An Hybrid Text-Image based Authentication for Cloud Services"*** este continuată abordarea securizării identităţii prin definirea, proiectarea şi analiza unei soluţii propuse de autentificare hibridă pentru cloud computing. Soluţia propusă de autentificare combină soluţia existentă de autentificare cu tehnica propusă de autentificare hibridă text-imagine. Pornind de la analiza tehnicilor de autentificare bazate pe cunoaştere, tehnica de autentificare hibridă este identificată ca şi soluţie viabilă în comparaţie cu celelalte două metode: autentificare bazată pe parolă şi autentificare bazată pe imagine, lucru ce este dovedit de impactul soluţiei hibride în contextul creşterii securităţii şi a creşterii capacităţii de reamintire a parolei de către utilizatori. Definirea soluţiei propuse de autentificare în cloud computing este prezentată prin abordarea pe trei niveluri de securitate ce o alcătuiesc, aducând îmbunătăţirea folosirii tehnicii propuse hidride text-imagine la soluţia curentă de autentificare în cloud computing, care este reprezentată de autentificarea bazată pe parolă şi pe certificatele X.509 pentru accesarea serviciilor cloud (Figura 2).

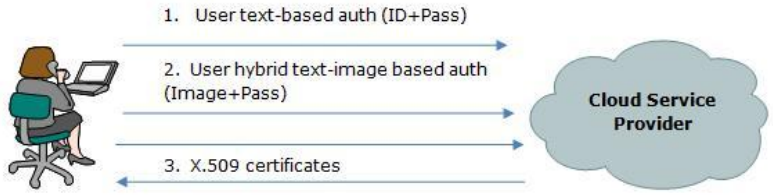

Figura 2 Proposed Cloud Computing Authentication Solution

Mai mult decat atât, tehnica hibridă propusă a fost concepută să combine trei imagini aleatoare din setul de imagini individual cu setul de parole individual, unde setul de imagini individual constă din trei imagini care au fost alese de utilizator la procesul de înregistrare din trei seturi de imagini ("flori", "animale" si "fructe") şi setul de parole individual consistă din parole pe care utilizatorul le-a alocat la procesul de înregistrare pentru fiecare imagine din setul de imagini individual (Figura 3).

Figura 3 Individual Image Set and Password Image Set

Astfel, nivelul de securitate propus a fost proiectat pentru a reduce compromisul dintre cerinţele de securitate şi utilizare, avantajele acestei tehnici fiind analizate la sfârşitul acestui capitol, prin următorii factori: soluţii pentru posibile atacuri, timpul necesar pentru înregistrare şi autentificare, precum şi uşurinţa în utilizarea sistemului.

În continuare, în **capitolul 5** intitulat ***"Private Cloud Set Up using Eucalyptus"*** s-a prezentat dezvoltarea platformei private cloud folosind Eucalyptus open-source. Eucalyptus a fost ales pentru implementarea cloud-ului privat, datorită avantajelor sale de a furniza interfeţe compatibile cu Amazon Web Services (AWS), chiar dacă robusteţea acestui soft este influenţată de faptul că Eucalyptus este open-source în dezvoltare, lucru care se poate observa prin problemele întâlnite în dezvoltarea, gestionarea şi executarea platformei private Infrastructură ca şi Serviciu (IaaS). Scopul acestei părţi experimentale a fost de a dezvolta o platformă de cloud privat, în vederea utilizării acesteia pentru implementarea topologiei cloud propuse pentru sistemele de detectare a intruziunilor din capitolul 6. În prima parte, capitolul a început prin descrierea celor cinci componente care formează arhitectura Eucalyptus: cloud controller, walrus, cluster controller, storage controller şi node controller. În plus, capitolul 5 a detaliat implementarea cloud-ului privat şi următoarele informaţii au fost raportate: versiunea softului folosit, topologia, infrastructura fizică şi hypervisor-ul folosit (Figura 4).

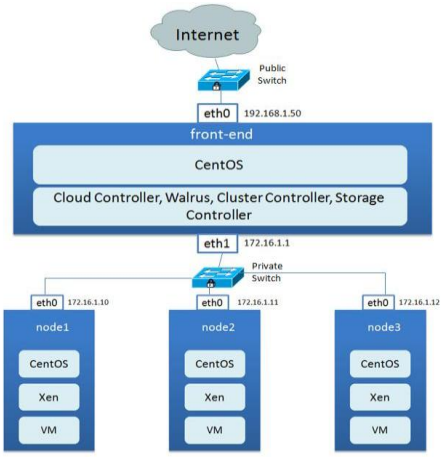

Figura 4 Private Cloud Configuration

Mai mult decat atât, o evaluare a instrumentelor de gestionare a Eucalyptus-ului a fost introdusă. Interfeţele de management discutate sunt: interfata web-based şi instrumentele de client (interfaţa linie de comandă, clientul API, interfeţe utilizator grafice şi instrumente de gestionare a treia parte). De asemenea, capitolul a explicat principalele operaţii care pot fi realizate folosind interfata linie de comandă euca2ools, care au fost urmate de prezentarea problemelor întâlnite şi rezolvate în cadrul platformei private cloud.

În **capitolul 6** denumit ***"Experimental Results and Evaluation on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud"*** s-a propus o topologie cloud de sisteme de detectare a intruziunilor pentru situaţiile de incertitudine în mediul cloud (Figura 5), care a fost implementată pe platforma privată cloud prezentată în capitolul 5. Topologia propusă include două părti: partea de detectare a atacurilor care se realizează în cadrul maşinilor virtuale configurate cu sistemul de detectare a intruziunilor (IDS) Snort, denumite maşini virtuale bazate pe IDS (VM-based IDS) şi partea de analiză a acestor atacuri, care se realizează în unitatea cloud de fuziune (Cloud Fusion Unit).

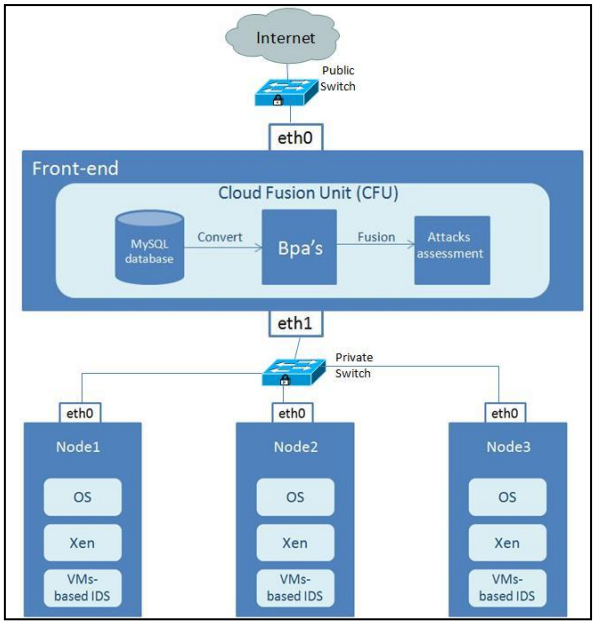

Figura 5 IDS Cloud Topology

Utilizând sistemele IDS în cadrul maşinilor virtuale se evită problemele de supraîncarcare şi se reduce impactul generat de posibilele atacuri.

În vederea analizării evenimentelor primite de la fiecare maşină virtuală bazată pe IDS, s-a utilizat teoria Dempster-Shafer în 3 valori logice împreună cu analiza bazată pe arborele de defectare (Fault-Tree Analysis FTAs). Conform teoriei Dempster-Shafer (DST) au fost analizate şi situaţiile de incertitudine, în cazul în care nu a fost cunoscută exact starea evenimentului, reducând în acest fel rata mare de alarme false generate de sistemele IDS. Prin urmare, elementul (Adevarat, Fals) a fost introdus pentru descrierea impreciziei, şi se referă la faptul că evenimentul poate fi sau Adevarat sau Fals, dar nu amândouă variantele.

Astfel, pentru fiecare maşină virtuală bazată pe IDS s-a calculat funcţia de masă (m - mass function) pentru toate cele 3 stări: Adevărat, Fals şi (Adevărat, Fals):

$$\begin{cases} m_x(\textit{Adevarat}), \textit{atacul DDoS a avut loc} \\ m_x(\textit{Fals}), \textit{atacul DDoS nu a avut loc} \\ m_x(\textit{Adevarat, Fals}), \textit{nu se cunoaşte dacă s-a întamplat sau nu, un atac DDoS} \end{cases}$$

unde x $\in$ {TCP, UDP, ICMP} atacuri flooding în platforma privată cloud
şi considerând următoarea relaţie DST:

$$m(\text{Adevarat})+m(\text{Fals})+m(\text{Adevarat, Fals})=1.$$

Apoi, evidenţele obţinute de la senzori au fost analizate folosind analiza prin arbore de defectare (Fault Tree Analysis FTA) (Figura 6), urmată de combinarea acestor evidenţe folosind regula Dempster.

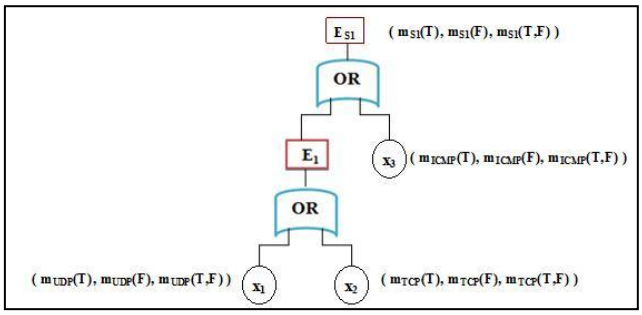

Figura 6 Bpa's calculation

În urma analizei efectuate cu arborele de defectare (FTA) s-a evidenţiat o rată de detectare ridicată şi o rată scăzută de alarme false. Ulterior, deoarece conflictul generat de maşinile virtuale bazate pe IDS a fost irelevant, regula de combinare Dempster a produs maximizarea ratei de detectare şi minimizarea ratei de alarme false, rezultate care au fost evaluate cu metricile: precizie şi rata de eroare.

Pentru a rezuma, prin folosirea teoriei DST soluţia propusă are următoarele avantaje: să acomodeze starea de incertitudine, să reducă ratele de alarme false, să crească rata de detectare, să rezolve conflictele generate de combinarea informaţiilor furnizate de senzori multipli şi să atenueze munca administratorilor de cloud.

În finalul acestei teze, în **capitolul 7** au fost prezentate concluziile împreună cu contribuţiile aduse şi au fost evidenţiate posibilele direcţii de dezvoltare.

Astfel, contribuţiile revendicate sunt următoarele:

- S-a realizat un studiu comparativ între Cloud Computing şi tehnologiile conexe, evidenţiind asemănările şi deosebirile.

- S-a conceput procesul de administrare al migrării aplicaţiilor întreprinderilor spre serviciile cloud computing. Procesul propus a fost realizat într-o succesiune justificată de activităţi interdependente.

- S-a efectuat un studiu cu scopul de a clasifica problemele de securitate pentru cloud computing (probleme de securitate ale aplicaţiilor, probleme de securitate ale virtualizării). Pentru fiecare problema de securitate, a fost creat un tabel evaluativ cu ameninţările si tehnicile de diminuare ale acestora.

- S-a realizat sinteza unei analize a soluţiilor curente ale Managementului Identităţii si Accesului (IAM- Identity Access Management), evidenţiind preferinţa utilizării soluţiei Cloud IAM gateway, datorită avantajelor sale în comparaţie cu IAM dezvoltat într-un cloud privat şi IAM dezvoltat de către furnizorul de servicii cloud (Cloud Service Provider).

- S-a realizat proiectarea unei soluţii arhitecturale de securitate pentru cloud computing, propunându-se o structură bazată pe o descompunere multi-nivel (Nivel 1-4). Primul nivel include poarta de acces cloud a managementului identităţii şi accesului (Cloud IAM gateway), cu scopul de a îndeplini cerinţele IAM definite, în timp ce ultimele 3 niveluri asigură securitatea infrastructurii şi informaţiei în mediul cloud, prin aplicarea controlului de securitate de reţea şi prin izolarea datelor clientilor.

- S-a realizat sinteza unei analize comparative a mai multor protocoale pentru componenta Cloud IAM gateway.

- S-a definit, proiectat şi analizat o soluţie nouă de autentificare pentru cloud computing, care combină tehnica propusă de autentificare hibridă text-imagine cu soluţia existentă de autentificare. Soluţia de autentificare hibridă text-imagine propusă a fost prezentată în comparaţie cu tehnicile existente de autentificare imagine-text şi partea de analiză demonstrează performanţa îmbunătăţirii propuse sistemului iniţial de autentificare din cloud computing în contextul securităţii şi utilizării.

- S-a efectuat implementarea cloud-ului privat folosind softul Eucalyptus şi realizarea unei analize comparative a instrumentelor de gestionare ale acestuia.

- S-a proiectat, implementat, testat şi validat o topologie cloud de sisteme de detectare a intruziunilor (IDS Cloud Topology), având ca obiectiv detectarea şi analiza atacurilor Distributed Denial of Service (DDoS) în aplicaţiile cloud computing. O atenţie deosebită a fost acordată cerinţelor de eficienţă (de exemplu, rata de detecţie și timpul de calcul), precum și cerinţei de utilizare, care au fost îndeplinite.