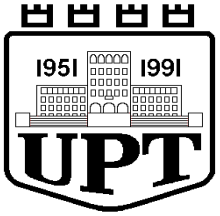

UNIVERSITETI POLITEKNIK I TIRANËS

FAKULTETI I TEKNOLOGJISË SË INFORMACIONIT

DEPARTAMENTI I ELEKTRONIKËS DHE TELEKOMUNIKACIONIT

ERGEST ALITE

PËR MARRJEN E GRADËS

"DOKTOR"

NË "TEKNOLOGJITË E INFORMACIONIT DHE KOMUNIKIMIT"

DREJTIMI "TELEKOMUNIKACION DHE INXHINIERI INFORMACIONI"

DISERTACION

PROJEKTIMI I NJË SISTEMI SIGURIE PIKË-MË-PIKË DHE KRIJIMI I NJË MEKANIZMI VET-MBROJTËS NË CLOUD COMPUTING

TIRANË, 2021

Udhëheqës Shkencor

Prof. Asoc. OLIMPJON SHURDI

PROJEKTIMI I NJË SISTEMI SIGURIE PIKË-MË-PIKË DHE KRIJIMI I NJË MEKANIZMI VET-MBROJTËS NË CLOUD COMPUTING

Disertacioni

I paraqitur në Universitetin Politeknik të Tiranës

për marrjen e gradës

"Doktor"

në

"Teknologjitë e Informacionit dhe Komunikimit"

Drejtimi Telekomunikacion dhe Inxhinieri Informacioni

nga

z. Ergest Alite

2021

JURIA PËR VLERËSIMIN E DISERTACIONIT PËR FITIMIN E GRADËS SHKENCORE “DOKTOR”

Miratuar

Me vendimin e Këshillit të Profesorëve të FTI-së Nr_____, datë_____.

Kryetari i Jurisë: Prof. Dr. Vladi Koliçi

Anëtar i Jurisë: Prof. Asoc. Indrit Enesi

Anëtar i Jurisë: Prof. Asoc. Evjola Spaho

Anëtar i Jurisë: Prof. Dr. Kozeta Sevrani

Anëtar i Jurisë: Prof. Asoc. Nevila Baci

Dekani i Fakultetit të Teknologjisë së Informacionit

Prof. Dr. Elinda Kajo Meçe

.....To My Father

Though you never got to see this

You're in every page

ABSTRACT

For several years now the virtualization of IT infrastructures and as a consequence utilization of Cloud Computing platforms and services is becoming one of the major research challenges. This is highlighted more during the outbreak of the pandemic situation, caused by the Covid-19 virus. These virtual and remote IT platforms are providing important and vital services nowadays. Such importance and utilization are becoming a real attraction to hackers and cybercriminals who are trying to benefit monetary values or perform industrial espionage. In this regard, this research is bringing a new protection technique equipped with self-protection capability and automatic interaction against cyber-attacks that cloud computing platforms might experience. The new technique is called SECURE+

SECURE+

The self-protection feature is of high interest in cloud computing platforms because of the high and unpredictable malicious activities happing every day on different cloud platforms. Faced with such threats and heterogonous cloud platforms the automatic interaction proposes, simpler, stronger, and more efficient security approach. Previous techniques, yet are facing some limitations like high utilization of computing resources, low percentage overdetection of attacks, higher levels of false-positive rate and a non-wide technique.

This paper is presenting SECURE+, self-protection, and automatic interaction technique which is overcoming such limitations. SECURE+ is compounded by integration of an open-source Intrusion Detection System (IDS) called SNORT and a machine learning, decision tree algorithm called eXtreme Gradient Boost (XGBoost). Such a technique is a signature-based one and is enforcing security across network level. SNORT is used to detect known attacks meanwhile XGBoost is detecting unknown attacks. Coordination between them is enforcing a broad spectrum of security protection and reaction.

Such architecture is enabling simple integration with existing cloud computing platforms offering them a higher guaranty to be untouched by malicious net activities and attacks. Performed lab experiments have shown that applicable design is effective and flexible self-protection technique for cloud private and public cloud infrastructures.

Conclusion

SECURE+ is a generic, flexible and open architecture technique enhancing cloud computing platforms' security. This technique is offering protection against DoS, DDoS (including UDP Flooding and NTP amplification), Probing, U2R, and R2L attacks. Through experimental results, it has shown that it has a higher Intrusion Detection Rate (IDR), a lower False Positive Rate (FPR) and lower computing resource utilization compared with other solutions. Analysis and the evaluation of such technique have shown that security on cloud public and private platforms can be enhanced.

ABSTRAKT

Prej disa vitesh tashmë, virtualizimi i infrastrukturave të IT dhe si pasojë përdorimi i platformave dhe shërbimeve Cloud Computing po bëhet një nga sfidat kryesore të kërkimeve shkencore. Kjo theksohet më shumë gjatë shpërthimit të situatës pandemike, të shkaktuar nga virusi Covid-19, ku këto platforma virtuale dhe në distancë të IT-së, po ofrojnë shërbime të rëndësishme dhe jetësore për të gjithë ne. Një rëndësi dhe përdorim i tillë po bëhet një tërheqje e madhe për hakerat dhe kriminelët kibernetikë të cilët po përpiqen të përfitojnë vlera monetare ose të kryejnë spiunazh industrial. Në këtë drejtim, ky dizertacion po sjell një teknikë të re mbrojtjeje të pajisur me aftësi të vetëmbrojtjes dhe ndërveprimit automatik ndaj sulmeve kibernetike që mund të përjetojnë platformat cloud computing. Teknika e re quhet SECURE+.

SECURE+

Karakteristika me vetëmbrojtje është me interes të madh në platformat cloud computing për shkak të aktiviteteve të mëdha, të dëmshme dhe të paparashikueshme që përjetojnë çdo ditë platformat e ndryshme cloud. Përballë kërcënimeve të tilla dhe platformave të shumëllojshme cloud, ndërveprimi automatik propozon, një qasje më të thjeshtë, më të fortë dhe më efikase të sigurisë. Megjithatë, vlen të theksohet se teknikat e mëparshme paraqesin disa kufizime si, shfrytëzimi i lartë i burimeve informatike, përqindja e ulët mbi zbulimin e sulmeve, nivele më të larta të normës false pozitive dhe faktin që janë teknika jo gjithë-përfshirëse.

Ky punim paraqet teknikën SECURE+, një teknikë me vetëmbrojtje dhe ndërveprim automatik, e cila i tejkalon kufizimet e tilla. SECURE + përbëhet nga integrimi i një sistemi të zbulimit të ndërhyrjeve (IDS) me burim të hapur të quajtur SNORT dhe një algoritmi me vendim pemë i quajtur eXtreme Gradient Boost (XGBoost). Një teknikë e tillë është e bazuar mbi nënshkrimin dhe zbaton sigurinë në të gjithë nivelin e rrjetit. SNORT përdoret për të zbuluar sulme të njohura ndërkohë XGBoost zbulon sulme të panjohura. Koordinimi midis tyre zbaton një spektër të gjerë të mbrojtjes dhe reagimit të sigurisë.

Një arkitekturë e tillë mundëson një integrim të thjeshtë me platformat ekzistuese cloud computing duke u ofruar atyre një garanci më të lartë për të mos u prekur nga aktivitetet dhe sulmet e dëmshme të rrjetit. Eksperimentet e kryera laboratorike treguan se teknika e zbatuar është teknikë efektive dhe fleksibël, me vetëmbrojtje për infrastrukturat cloud computing private dhe publike.

Përfundim

SECURE + është një teknikë e përgjithshme, me arkitekturë fleksibël dhe e hapur që rrit sigurinë e platformave cloud computing. Kjo teknikë ofron mbrojtje ndaj sulmeve DoS, DDoS (gjithashtu UDP Flooding dhe NTP), Sondë, U2R dhe R2L. Përmes rezultateve eksperimentale është treguar se ajo ka një shkallë më të lartë të zbulimit të ndërhyrjeve (IDR), një shkallë më të ulët false pozitive (FPR) dhe përdorim më të ulët të burimeve informatike krahasuar me zgjidhjet e tjera. Analiza dhe vlerësimi i një teknike të tillë ka treguar që siguria në platformat cloud computing publike dhe private mund të rritet.

MIRËNJOHJE

Dëshiroj të shpreh falenderimet e mia të përzemërta për të gjithë ata që në një mënyrë apo një tjetër dhanë ndihmesën e tyre për ta bërë punën time me doktoraturën më të lehtë dhe më të këndshme. Fillimisht dëshiroj t'i drejtoj falenderimet e mia të sinqerta udhëheqësit tim shkencor Prof. Asoc. Olimpjon Shurdi, për ndihmën dhe mbështetjen e tij të pakushtëzuar dhe tek i cili kam gjetur gjithmonë sugjerime me vlerë, mbështetje dhe orientimin shkencor, duke më nxitur gjithmonë drejt kërkimeve dhe ideve të reja në lidhje me punimin e dizertacionit.

Dua të shpreh mirënjohjen time për drejtuesit e Departamentit të Elektronikës dhe Telekomunikacionit në Universitetin Politeknik të Tiranës, të cilët më dhanë mundësinë të vazhdoj studimet e doktoraturës për thellimin e studimeve në fushën e sigurisë të platformave cloud computing. Njëkohësisht, mirënjohja ime shkon për të gjithë pedagogët e Departamentit të Elektronikës dhe Telekomunikacionit për rekomandimet e tyre të vlefshme dhe të pakursyera sa herë që kam pasur nevojë.

Së fundmi, një falenderim i veçantë i shkon familjes sime, e cila ka qenë motivimi dhe shtysa kryesore gjatë gjithë përpjekjeve të mia për përfundimin me sukses të punimit të doktoraturës.

PËRMBAJTJE

Përmbajtje 1

Lista e tabelave 4

Lista e figurave 5

Akronime 8

1 Hyrje 12

1.1 Motivimi 14

1.2 Qëllimi i punës dhe metodologjia e kërkimit 14

1.3 Teknologjia Cloud Computing, Konceptet Themelore 16

1.3.1 Modelet e Shërbimit të Përdorura në Teknologjinë Cloud Computing 17

1.4 Teknologjia Cloud Computing në Shqipëri 17

1.4.1 Rregulloret për Mbrojtjen e të Dhënave Personale 18

1.4.2 Legjislacioni Shqiptar 18

1.5 Konceptet bazë të sigurisë në Cloud Computing 19

1.6 Punime të Ngjashme 23

2 Siguria kompjuterike në Cloud Computing 38

2.1 Dobësitë dhe sulmet 39

2.1.1 Shtresa e Aplikimit 39

2.1.2 Shtresa e Sistemit të Operimit 40

2.1.3 Hipervizori, Storage, Hardware dhe Rrjeti 42

2.2 Mekanizmat e sigurisë në cloud 42

2.2.1 Siguria e të dhënave 43

2.2.2 Nënshkrimi dixhital 43

2.2.3 Hashing 45

2.2.4 Siguria e virtualizimit 45

2.3 Privatësia dhe siguria në shërbimet cloud storage 46

2.3.1 Modelet e mbrojtjes së të dhënave në Cloud 47
2.3.2 Zbatimi i rregullave të kontrollit të aksesit në Cloud 49
2.4 Shkaqe të tjera të Rrjedhjes së Të Dhënave në Cloud 50
2.5 Makina e Vektorit Mbështetës (SVM) 51
2.5.1 SVM për klasifikim 52
2.5.2 SVM për regres 52
2.5.3 Aplikime të SVM-së 53
2.5.4 Avantazhe dhe disavantazhe të përdorimit të SVM 53
2.6 Algoritmi MAPE-K 54
2.6.1 Arkitektura MAPE-K për vetë-adaptimin 54
2.7 Algoritmi i Përmirësimit Ekstrem të Gradientit (XGBoost) 55
2.8 Mbrojtja e Duhur e Informacionit të të Dhënave 57
2.9 Aspektet e Sigurisë së Rrjeteve Cloud 59
2.10 Kontrollet e Sigurisë në Infrastrukturën Fizike 61
3 Klasifikimi i Sulmeve në Cloud Computing dhe prezantimi i teknikave vet-mbrojtëse të zhvilluara ndaj këtyre sulmeve 64
3.1 Kategoria e parë e sulmeve – Mohimi i Shërbimit (ang. Denial of Service - DoS) 64
3.1.1 Mekanizmat e sulmit të përmbytjes 65
3.1.2 Mekanizmat e sulmit logjik 66
3.2 Klasa e dytë e sulmeve – Mohimi i Shpërndarë i Shërbimit (ang. Distributed Denial of Service - DDoS) 67
3.2.1 Sulmet nga përmbytja HTTP 68
3.2.2 Sulmet e Ditës Zero 70
3.3 Klasa e dytë e sulmeve – Kompromisit 71
3.3.1 Sulmet nga Distanca në Ambientin Lokal (R2L) 71
3.3.2 Sulmet nga Përdoruesi në Ambientin Rrënjë (U2R) 71
3.4 Klasa e dytë e sulmeve – SONDË (ang. Probing) 72
3.5 Prezantimi i teknikave vet-mbrojtëse të zhvilluara ndaj këtyre sulmeve 72
4 Teknika SECURE dhe përmirësimi i kësaj teknike duke përfshirë edhe mbrojtjen nga sulmet UDP Flood dhe NTP Amplification 75
4.1 Prezantimi i teknikave vet-mbrojtëse të zhvilluara ndaj këtyre sulmeve 75

4.1.1 Mekanizmi vet-mbrojtës – pseudo_kodi. 77

4.2 Vlerësimi i Performancës 78

4.3 Zgjerimi i Teknikës SECURE për Mbrojtjen Nga Sulmet e Tjera DDoS (UDP Flood dhe NTP Amplification) 83

5 Teknika e Mbrojtjes SECURE+ Në Platformat Cloud Computing 84

5.1 Blloqet funksionale të Teknikës SECURE+ 85

5.1.1 Sistemi i Dedektimit të Sulmeve të Njohura nëpërmjet SNORT 87

5.1.2 Sistemi Autonom i Dedektimit të Sulmeve të Panjohura nëpërmjet Teknikës me mësim automatik (ML) 89

5.1.3 Menaxhimi i Burimeve Kompjuterike 90

5.2 Metrikët bazë të teknikës SECURE+ 91

5.3 Funksionimi i Teknikës SECURE+ 92

5.3.1 Konfigurimet SNORT 93

5.3.2 Konfigurimet dhe Algoritmet e përdorur në teknikën SGBoost 95

5.4 Përshkrimi i Metodologjisë së Kërkimit 100

5.5 Ambjenti Eksperimental 101

5.6 Kryerja e eksperimenteve dhe Analiza përkatëse 102

6 Konkluzione, puna në të ardhmen 116

6.1 Punët në të ardhmen 118

7 Referencat 119

8 SHTOJCA _A 130

8.1 Algoritmet e Përdorur 130

8.1.1 Algoritmi 1 Funksioni pikë-më-pikë 130

8.1.2 Algoritmi 1 - Kodi Burim (Python) 131

8.1.3 Algoritmi 2 Krijimi i Karakteristikave 132

8.1.4 Algoritmi 2 - Kodi Burim (Python) 133

8.1.5 Algoritmi 3 Përllogaritja e Karakteristikave dhe Statistikave të Përbashkëta 134

8.1.6 Algoritmi 3 - Kodi Burim (Python) 135

9 SHTOJCA _B 137

9.1 Rezultatet e Përfituara nga Eksperimentet në Formë Tabelare 137

LISTA E TABELAVE

Tabela 3-1 Krahasimi i Teknikës SECURE me Teknikat Ekzistuese 73

Tabela 5-1 Përshkrimi i karakteristikave të rrjedhës 100

Tabela 5-2 Specifikimet teknike të ambjentit eksperimental..... 104

Tabela 9-1 Përdorimi i CPUs në (%) për teknikat SECURE+ dhe SECURE për shpejtësi të ndryshme të trafikut 137

Tabela 9-2 Përdorimi i memorjes në (Gbps) në të dy teknikat SECURE+ dhe SECURE për shpejtësi trafiku të ndryshme 139

Tabela 9-3 Shpejtësia e procesimit të paketave për sekondë në të dy teknikat SECURE+ dhe SECURE për kohë të ndryshme..... 140

Tabela 9-4 Rrëzimi mesatar i paketave (në përqindje) në shpejtësi të ndryshme rrjeti për të dy teknikat SECURE+ dhe SECURE 141

Tabela 9-5 Norma Fals Pozitive për llojet e sulmeve (në përqindje) për të dy teknikat 142

Tabela 9-6 Norma Fals Negative për llojet e sulmeve (në përqindje) për të dy teknikat 143

Tabella 9-7 Norma e dedektimit të ndërhyrjes në varësi të kohës (në përqindje) për të dy teknikat..... 144

LISTA E FIGURAVE

Figura 1-1 Mesazhi i lëshuar nga konsumatori i cloud për shërbimin cloud konsiderohet konfidencial vetëm nëse nuk arrihet ose lexohet nga një palë e paautorizuar 19

Figura 1-2 Mesazhi i lëshuar nga konsumatori i cloud për shërbimin cloud konsiderohet të ketë integritet nëse nuk është ndryshuar 19

Figura 1-3 Niveli i kontrollit të konsumatorit 22

Figura 2-1 Dobësitë e sigurisë në Cloud Computing 39

Figura 2-2 Dobësitë e injektimit SQL 40

Figura 2-3 Dobësitë e TOCTTOU 42

Figura 2-4 Shembull i autentikimit të sigurtë me SSL 44

Figura 2-5 Shërbimi zinxhir në Cloud 47

Figura 2-6 Modeli i mbrojtjes së të dhënave cloud 48

Figura 2-7 Procesi i JARs (i brendshëm dhe i jashtëm) 49

Figura 2-8 Arkitektura e algoritmit MAPE-K 55

Figura 2-9 Vizualizimi i algoritmit XGBoost 56

Figura 2-10 Arkitektura referuese për cloud publike 58

Figura 2-11 Projektimi logjik i rrjetit të Cloud provider 60

Figura 2-12 Segmentimi i rrjetit të data center-it 61

Figura 2-13 Zgjerimi i data center-it të një cloudi publik 62

Figura 3-1 Klasifikimi i Sulmeve DDoS 68

Figura 3-2 Sulmet nga përmbytja HTTP 69

Figura 4-1 Arkitektura e Teknikës SECURE 76

Figura 4-2 Hapat e sistemit Autonom si p.sh. monitorimi, analizimi dhe planifikimi, dhe ekzekutimi 77

Figura 4-3 Procesi i gjenerimit të nënshkrimit 78

Figura 4-4 Konfigurimi Eksperimental i Teknikës SECURE 79

Figura 4-5 Shpejtësia Fals Pozitve përkundrejt Kohës 80

Figura 4-6 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Sulmeve 81

Figura 4-7 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Kohës 81

Figura 4-8 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Sulmeve 82

Figura 4-9 Shpejtësia e Gjenerimit të Nënshkrimit (SGR) përkundrejt Sulmeve. 82

Figura 5-1 Shembull Vendimi Pemë për Përmirësimin e Gradientit gjatë Detyrës së Dedektimit të Ndërhyrjes së Rrjetit 85

Figura 5-2 Arkitektura e teknikës SECURE+ 86

Figura 5-3 Ndërveprimi i nën-njësive të sistemit autonom 89

Figura 5-4 Caktimi i Burimeve në platformat Cloud 90

Figura 5-5 Bllok-skema e funksionit pikë-më-pikë 96

Figura 5-6 Bllok-skema e funksionit të krijimit të Karakteristikave 97

Figura 5-7 Bllok-skema e funksionit të përllogaritjes së karakteristikave dhe statistikave të përbashkëta 98

Figura 5-8 Ambjenti Eksperimental 102

Figura 5-9 Paraqitja e rrjetit të ambjentit eksperimental 103

Figura 5-10 Mesatarja e përdorimi të CPUs. 105

Figura 5-11 Mesatarja e përdorimi të memorjes RAM. 106

Figura 5-12 Mesatarja e shpejtësisë së procesimit (numri i paketave në njësinë e kohës) për të dy teknikat. 107

Figura 5-13 Shpejtësia mesatare e rrëzimit të paketave UDP 108

Figura 5-14 Shpejtësia mesatare e rrëzimit të paketave TCP 108

Figura 5-15 Shpejtësia mesatare e rrëzimit të paketave ICMP 109

Figura 5-16 Norma Fals Pozitive për llojet e sulmit e Mohimit të Shërbimit (DoS) ... 110

Figura 5-17 Norma Fals Pozitive për llojet e sulmit nga Ambjenti Lokal në Bërthamë (L2R) 111

Figura 5-18 Norma Fals Pozitive për llojet e sulmit nga Distanca në Ambjentin Lokal (R2L) 111

Figura 5-19 Norma Fals Pozitive për llojet e sulmit Sondë (Probing) 112

Figura 5-20 Norma Fals Pozitive për llojet e sulmit Mohimi i Shpërndarë i Shërbimit (DDoS) 112

Figura 5-21 Norma Fals Negative për llojet e sulmit të Mohimit të Shërbimit (DoS) . 113

Figura 5-22 Norma Fals Negative për llojet e sulmit nga Ambjenti Lokal në Bërthamë (L2R) 113

Figura 5-23 Norma Fals Negative për llojet e sulmit nga Distanca në Mbjentin Lokal (R2L)..... 114

Figura 5-24 Norma Fals Negative për llojet e sulmit Sondë (Probing)..... 114

Figura 5-25 Norma Fals Negative për llojet e sulmit Mohimi i Shpërndarë i Shërbimit (DDoS)..... 114

Figura 5-26 Norma e dedektimit të ndërhyrjes për 8 orët e para (në përqindje) për të dy teknikat..... 115

Figura 5-27 Norma e dedektimit të ndërhyrjes për 40 orët e fundit (në përqindje) për të dy teknikat..... 115

AKRONIME

AAA	- Authentication, Authorization, and Accounting
ABE	- Attribute Base Encription
ACK	- Acknowledgement
AKSHI	- Agjensia Kombëtare e Shoqërisë së Informacionit
Amazon EC2	- Amazon Elastic Compute Cloud
Amazon S3	- Amazon Simple Storage Service
AMI	- Amazon Machine Images
API	- Application Programming Interface
APT	- Automatically Programmed Tool
ARP	- Address Resolution Protocol
AWS	- Amazon Web Services
BGP	- Border Gateway Protocol
BSD	- Berkeley Software Distribution
CA	- Certificate Authority
CART	- Classification And Regression Trees for Machine Learning
CCE	- Cloud Computing Environment
CCS	- Cloud Computing and Services
CMS	- Content Management System
CPCS	- Self-Protecting Cloud Service
CIA	- Confidentiality, Integrity and Availability
CIO	- Chief Information Officer
CSA	- Cloud Service Alliance
CSP	- Cloud Service Provider
CTMS	- Cloud based Trust Management System

CVE	- Common Vulnerability dhe Exposures
CVSS	- Common Vulnerability Scoring System
DB	- Data Base
DDoS	- Distributed Denial of Service
DMZ	- Demilitarized Zone
DNS	- Domain Name System
DoS	- Denial of Service
DNN	- Deep Neural Network
EDoS	- Economic Denial of Service
e-mail	- electronic –mail
FPR	- False Positive Rating
FTP	- File Transfer Protocol
GDPR	- Genaral Data Protection Regulation
HTML	- Hyper Text Markup Language
HTTP	- Hypertext Transfer Protocol
HTTPS	- Hypertext Transfer Protocol Secure
Hy –IDS	- Hybrid – Intrusion Detection System
IaaS	- Infrastructure as a Service
IAM	- Identity and Access Management
ICMP	- Internet Control Message Protocol
IDC	- International Data Corporation
IDR	- Intrusion Detection Rate
IDS	- Intrusion Detection System
IGMP	- Internet Group Management Protocol
IMAP	- Internet Message Access Protocol
IoT	- Internet of Things
IP	- Internet Protocol
IPS	- Intrusion Prevention System
IPsec	- Internet Protocol Security
ISO	- International Organization for Standartization
IT	- Information Technology

JAR	- Java ARchive
JPEG	- Joint Photographic Experts Group
KNN	- K Nearest Neighbor
MAC	- Media Access Control
MICSP	- Malware Inspired Cloud Self-Protection
ML	- Machine Learning
NANOG	- North American Network Operator'S Group
NDA	- Non Disclosure Agreement
NetBIOS	- Network Basic Input/Output System
NMAP	- Network Mapper
NIST	- National Institute of Standards and Technology
NS	- Name Server
NTP	- Network Time Protocol
OS	- Operating System
PaaS	- Platform as a Service
PC	- Personal Computer
PHP	- Hypertext Preprocessor
PNG	- Portable Network Graphics
PVLAN	- Private Virtual Local Area Network
QoS	- Quality of Service
R2L	- Remote to Local
SaaS	- Software as a Service
SADM	- Self-Adaptive Data Management
SAML	- Security Assertion Markup Language
SAT	- Secure Autonomic Technique
SDLC	- Software Development Life Cycle
SECURE	- Self-protEction approaCh in cloUd Resource management
SLA	- Service Level Agreement
SMB	- Small Medium Business
SMVR	- Secure Management technique for Virtualized Resources
SPDS	- Self-Protection DataScheme

SPI	- Serial Peripheral Interface
SQL	- Structured Query Language
SSH	- Secure Shell
SSL	- Secure Sockets Layer
SSO	- Single Sign On
SVM	- Support Vector Machine
TCP	- Transmission Control Protocol
TCP/IP	- Transmission Control Protocol / Internet Protocol
TCCP	- Trusted Cloud Computing Platform
TOCTTOU	- Time to Check To Time of Use
TLS	- Transport Layer Security
TPM	- Trusted Platform Module
U2R	- User to Root
UDP	- User Datagram Protocol
UTM	- Unified Thread Management
VESPA	- Virtual Environment based Self-Protecting Architecture
VM	- Virtual Machine
VLAN	- Virtual Local Area Network
VPN	- Virtual Private Network
XGBoost	- eXtreme Gradient Boosting
XML	- Extensible Markup Language
XSS	- Cross Site Scripting

1 HYRJE

Në ditët e sotme, të gjithë janë të lidhur me botën ekzistuese dixhitale, në një ose në një mënyrë tjetër dhe kjo është arsyeja kryesore mbrapa rritjes së teknologjisë së informacionit. Faktori kryesor i lidhur me këtë rritje është mjedisi miqësor për përdoruesit, i cili është i arritshëm nga kudo dhe në çdo kohë.

Interneti ofron mundësi për grupe të ndryshme njerëzish (si biznesmenë, studiues, student, etj.) për të përfunduar punët dhe duke u dhënë mundësi për të përmbushur qëllimet e tyre. Shumë përdorues lidhen me internetin dhe përdorin infrastrukturën e IT për të kompletuar kërkesat e tyre të përditshme.

Ndërsa kërkesa për internet po rritet, shërbimi i ofruar si Softuerët, Platformat, Shërbimet e Bazave të të Dhënave (DB), Shërbimet Storage etj përmes internetit gjithashtu rritet. Në këtë rast ekziston termi i rëndësishëm Cloud Computing, i cili ofron një sasi të madhe shërbimesh të ndryshme për përdoruesit e tij përmes internetit. Gjithashtu me anë të mundësisë së marrjes së shërbimit "Paguaj sipas Përdorimit", përdoruesi bazë mund të marrë përfitime maksimale duke përdorur këtë shërbim me kosto më të ulët.

Duke parë teknologjinë Cloud Computing të zhvilluar në 15 vitet e fundit sëbashku me aplikacionet përkatëse, duket pothuajse sikur këto janë krijuar për të trajtuar tronditjen e kërkesës globale të shkaktuar nga pandemia e Covid-19. Jo vetëm që pandemia shndërroi miliona punonjës zyre në punonjës nga shtëpia dhe në punonjës që punojnë në largësi brenda natës, por gjithashtu ndryshoi mënyrën se si funksionon çdo departament IT dhe njësive të biznesit. Pa aplikacionet cloud në internet, prezencën e njësive tregtare në internet, mjeteve dhe infrastrukturës të disponueshme për çdo biznes dhe konsumator sipas kërkesës, imagjinoni se sa ndryshe (dhe e çorientuar) do të kishte qenë përgjigjia ndaj pandemisë. Në vitin 2020, teknologjia Cloud Computing provoi se, në të vërtetë, nuk duhet lejuar kurrë që një krizë e rëndë të shkojë dëm.

Duke marë në konsideratë shpërthimin e Pandemisë, COVID-19 të shkaktuar nga korona virusi, kompanitë dhe institucionet i kanë udhëzuar punonjësit e tyre të punojnë nga shtëpia si një masë paraprake për të zvogëluar rrezikun e infektimit. Megjithatë, punonjësit kanë qenë të ekspozuar ndaj rreziqeve të ndryshme të sigurisë për shkak të punës në shtëpi. Për më tepër, përhapja e shpejtë globale e COVID-19 ka rritur vëllimin e të dhënave të gjeneruara nga burime të ndryshme. Puna nga shtëpia varet kryesisht nga aplikacionet e bazuara në teknologjinë Cloud Computing, të cilat kanë ndihmuar

punonjësit të përmbushin me efikasitet detyrat e tyre. Mjedisi Cloud Computing është një hero i heshtur në këtë krizë pandemike. Ky mjedis përfshin praktika të shpejta për shërbimet që pasqyrojnë trendin e aplikacioneve të vendosura me shpejtësi për mirëmbajtjen e të dhënave. Përkundër rritjes së përdorimit të aplikacioneve Cloud Computing, ekziston një sfidë e vazhdueshme kërkimore në fushat që kanë lidhje me të dhënat, garantimin e sigurisë dhe disponueshmërinë e aplikacioneve në platformat Cloud Computing [1].

– Organizimi i kapitujve

Ky punim doktorature do të përmbajë kapitujt të cilët kanë paraqitje si më poshtë:

Kapitulli 1 – Në kapitullin e parë shqyrtohen koncepte themelore të punimit duke përfshirë hyrjen, qëllimet e punës dhe metodologjinë e kërkimit, motivimin si dhe teorinë themelore të sigurisë për teknologjinë Cloud Computing. Gjithashtu paraqiten modelet e shërbimit të përdorura në këtë teknologji si dhe përdorimin e kësaj teknologjie në Shqipëri. Për shkak të rëndësisë që ka aspekti rregullator, ky kapitull pasqyron rregulloret për mbrojtjen e të dhënave në Shqipëri si dhe legjislacionin Shqiptar për këtë fushë. Në fund paraqiten punime të ngjashme të realizuara për fushën e studimit të këtij punimi shkencor.

Kapitulli 2 – Në kapitullin e dytë, do të trajtohen konceptet që lidhen me kërcënimet, sfidat dhe udhëzimet e shoqëruara me sigurimin e infrastrukturës bazë të Teknologjisë së Informacionit të një organizate në nivelet e rrjetit, serverit ku hostohet dhe aplikacionit.

Kapitulli 3 – Kapitulli i tretë pasqyron një analizë për klasat kryesore të sulmeve të kryera mbi Infrastrukturat Cloud. Përveç kësaj prezantohen teknikat e zhvilluara nga kërkues shkencor të ndryshëm gjatë këtij dhjetë vjeçari për të bërë të mundur, dedektimin, parandalimin dhe mbrojtjen e Infrastrukturave Cloud nga këto sulme dhe nga ndikimet që mund të kenë këto sulme mbi përdoruesit e këtyre rrjeteve dhe ofruesve të tyre.

Kapitulli 4 - Kapitulli i katërt jep një punim që lidhet me teknikën e cila trajton sulmet e sigurisë ajo quhet SECURE, Teknika me Vet-Mbrojtje në Manaxhimin e Burimeve Cloud (ang. Self-protEction approaCh in cloUd Resource management). Si përfundim pasqyrohen konkluzionet rreth kësaj teknike.

Kapitulli 5 - Kapitulli i pestë pasqyron teknikën vet-mbrojtëse dhe automatike të propozuar të sigurisë ndaj ndërhyrjeve të paautorizuara në platformat cloud computing, e quajtur SECURE+. Jepet ambienti i testimit, i cili është një platformë virtuale dhe i ngjashëm më një platformë cloud, duke imituar një ambient real me burime kompjuterike të njëjta. Ky ambient testimi shërben për të llogaritur me saktësi dhe efikasitet performancën e teknikës së propozuar. Gjithashtu jepen edhe algoritmet e implementimit të kësaj teknike. Më pas pasqyrohen metrikët e studiuar të kësaj teknike dhe rëndësia e tyre në efikasitetin e saj. Paraqiten informacionet mbi eksperimentet e realizuara për këtë teknikë dhe krahasimi i tyre në lidhje me teknikën SECURE. Në fund jepen rezultatet e

përfituara nga eksperimentet e realizuara si dhe pasqyrohet analiza e këtyre rezultateve sipas simulimeve përkatëse.

Kapitulli 6 - Kapitulli i gjashtë lidhet me dhënien e konkluzioneve rreth kësaj teknike në bazë të simulimeve të realizuara në këtë punim doktorature, si edhe paraqiten disa sugjerime për punët në vazhdim.

1.1 Motivimi

Punimi i kësaj teze përveç sfidës ka qenë edhe një kënaqësi për të kontribuar në një fushë e cila sot po gjen një përdorim të zgjeruar dhe kryesor në fushën e Teknologjisë së Informacionit, si dhe për të më ndihmuar dhe përditësuar në lidhje me problematikat dhe çështjet e hasura në fushën time të studimit dhe si rrjedhojë edhe asaj të punësimit.

Kërkimet për këtë temë lidhen me përdorimin e një kombinimi mekanizmash ku një pjesë e të cilave përdoren nga Operatorët Ndërkombëtarë të Shërbimeve Cloud dhe një pjesë tjetër janë akoma në faza eksperimentale, për të ofruar një nivel sigurie më të lartë në platformat Cloud Computing. Studimi do të bazohet ekskluzivisht mbi platformat cloud computing komerciale duke i konsideruar ato platforma të synuara nga grupet dashakeqe dhe për të parandaluar tentativat e tyre të dëmshme. Gjithashtu do të preket edhe aspekti rregullator Europian dhe Shqiptar duke pasqyruar të mirat dhe ndërhyrjet që duhet te ushtrojnë këto rregullore për të garantuar një qasje të sigurtë për të gjithë klientët Shqiptarë.

Po kështu lidhur me këtë temë do te jepet edhe aspekti financiar që ndikon drejtpërsëdrejti mbi abonentët dhe ofruesit e shërbimeve Clould Computing. Në mënyrë të veçantë do të studiohen kompanitë Shqiptare (ndonëse këto shërbime nuk janë në nivelet ndërkombëtare) të cilat kanë tentuar të ofrojnë shërbimet Cloud Computing duke pasqyruar ndikimet e drejtpërdrejta nga cënimet e sigurisë mbi këto platforma si dhe mbi të dhënat të cilat ato mbartin.

1.2 QËLLIMI I PUNËS DHE METODOLOGJIA E KËRKIMIT

Në këtë studim do të përdorim teknikën me vet-mbrojtje e quajtur SECURE, si një nga teknikat më efektive në krahasim me teknikat e tjera të studiuara deri më sot nga studiues të ndryshëm, në termat e shpejtësisë së dedektimit të ndërhyrjes, kohës së përgjigjes dhe të shpejtësisë false pozitive. Studimin tonë do ta bazojmë duke përmirësuar këtë teknikë, duke përfshirë në të edhe sulmet UDP Flood dhe NTP Amplication.

Në këtë punim do të bazohemi tek siguria në Cloud Computing për shkak të rëndësisë të madhe që po merr përdorimi i kësaj teknologjie në ditët e sotme. Duke u nisur edhe nga situata e shkaktuar nga pandemia e Covid-19, përdorimi i teknologjisë Cloud Computing është parë si rruga e shpëtimit ekonomik për kompanitë të cilat e kanë orientuar fuqinë e tyre punëtore të punojnë nga shtëpia me të njëjtin efikasitet sikur të ishin duke punuar nga zyra.

Siguria e përdorimit të këtyre platformave është vendosur në plan të parë për shkak të numrit të lartë të përdoruesve si dhe numrit të lartë të shërbimeve tashmë thelbësore që ato ofrojnë (si p.sh. aplikacionet e komunikimit të biznesit Teams, Zoom etj).

Analiza e propozuar bazohet në studimin e kësaj teknike duke e zgjeruar atë që të funksionojë edhe për sulmet e sigurisë UDP Flood dhe NTP Amplication. Ky modifikim i kësaj teknike do ta bëj këtë teknikë më të plotë dhe më të sigurtë për një përdorim gjithëpërfshirës. Gjithashtu ajo do të na mundësojë të shikojmë ndryshimet në performancën e ekzekutimit të kësaj metode si pasojë e modifikimit të saj duke shtuar mbrojtjen edhe nga nje sulm sigurie më shumë.

Qëllimi i kësaj pune është të demonstrojë se teknika e modifikuar është një teknikë e cila do të arrijë një mbrojtje ndaj më shumë lloje sulmesh sigurie më të njëjtin efekasitet.

Për të realizuar këtë punim do të përdoret sistemi për dedektimin e ndërhyrjeve në nivel rrjeti i quajtur SNORT[2]. Gjithashtu për të analizuar aktivitetet jonormale (sulme jo të njohura) do të përdoret një dedektor anomalie i bazuar në Teknikën me Vendim Pemë (ang. Decision Tree) dhe algoritmin e Përmirësimit Ekstrem të Gradientit (ang. eXtreme Gradient Boosting – XGBoost) . SNORT është sistemi i dedektimit të ndërhyrjeve (ang. Intrusion Detection System – IDS) më efektiv. Teknika të ndryshme të mësimit të makinës (ang. Machine Learning – ML) përdoren për IDS-të e bazuara tek anomalitë por XGBoost është dedektori më i përdorur i anomalisë në bazë të studime të fundit [3], [4].

Të dy këto mekanizma do të na garantojnë performancën dhe besueshmërinë e kësaj metode si dhe do të sigurojnë rezultatin e dëshiruar.

Për të zgjeruar këtë metodë do të modifikohet gjeneruesi i sulmeve duke shtuar në gjeneratorin e sulmeve edhe një gjenerues sulmesh përmbytja UDP (ang. UDP Flood) dhe amplifikimi NTP (ang. NTP Amplification). Gjithashtu do të shtohet edhe një modul sulmesh UDP Flood dhe NTP Amplication në modulin e sulmeve të sigurisë.

Duke analizuar teknikën SECURE [5] do të vihet re se kjo teknikë do të mbrojë sistemet nga ekzekutimi i pesë lloje sulmesh të ndryshme sigurie që përfshijnë Sulmet e Mohimit të Shërbimit (ang. Denial of Service DoS), sulmet Sondë (ang. Probing), sulmet nga Distanca në Ambjentin Lokal (ang. Remote to Local - R2L), sulmet nga përdoruesi në rrënjë (ang. User to Root - U2R) dhe sulmet e Shpërndara të Mohimit të Shërbimit (ang. Distributed Denial of Service - DDoS).

Kjo punë mund të zgjerohet në të ardhmen për të përdorur këtë teknikë si teknikë mbrojtëse ndaj llojeve të tjera të sulmeve siç mund të jenë sulmet ransomware, slowloris, etj. Pamvarësisht dëshirës për zgjerim duhet të kihet parasysh gjithmonë fakti se zgjerimi i kësaj teknike duhet të realizohet pa cënuar në asnjë moment performancën dhe besueshmërinë, për të qenë realisht një teknikë gjithëpërfshirëse e besueshme dhe rezultative.

1.3 TEKNOLOGJIA CLOUD COMPUTING, KONCEPTET THEMELORE

Cloud është një teknologji informatike e bazuar në Internet, ku burimet e përbashkëta të tilla si softueri, platforma, hapësira ruajtëse dhe informacioni u ofrohen klientëve sipas kërkesës. Cloud Computing është një platformë informatike për ndarjen e burimeve që përfshijnë infrastrukturat, programet kompjuterike, aplikacionet dhe proceset e biznesit. Cloud Computing është një grup virtual burimesh kompjuterike [6]. Ai siguron burime kompjuterike në grup për përdoruesit përmes internetit. Cloud Computing si një paradigmë kompjuterike në zhvillim, synon të ndajë hapësirën ruajtëse, llogaritjen dhe shërbimet në mënyrë transparente midis përdoruesve masivë. Sistemet aktuale të llogaritjes Cloud paraqesin kufizime serioze në mbrojtjen e konfidencialitetit të të dhënave të përdoruesve. Meqenëse të dhënat e ndjeshme të përdoruesve paraqiten në forma të paenkriptuara në makinat e largëta në pronësi dhe të operuara nga ofruesit e shërbimeve të palëve të treta, rreziqet e zbulimit të paautorizuar të të dhënave të ndjeshme të përdoruesve nga ofruesit e shërbimeve mund të jenë mjaft të larta. Ka shumë teknika për të mbrojtur të dhënat e përdoruesve nga sulmuesit e jashtëm. Paraqitet një qasje për të mbrojtur konfidencialitetin e të dhënave të përdoruesve nga ofruesit e shërbimeve dhe siguron që ofruesit e shërbimeve nuk mund të mbledhin të dhëna konfidenciale të përdoruesve, ndërsa të dhënat përpunohen dhe ruhen në sistemet Cloud Computing. Sistemet Cloud Computing sigurojnë ruajtje dhe shërbime të ndryshme të bazuara në internet. Për shkak të shumë përfitimeve të tij kryesore, duke përfshirë efektivitetin e kostos dhe shkallëzimin dhe fleksibilitetin e lartë, Cloud computing po fiton vrull të rëndësishëm kohët e fundit si një paradigmë e re e informatikës së shpërndarë për aplikacione të ndryshme, veçanërisht për aplikimet e biznesit së bashku me rritjen e shpejtë të internetit [7]. Me rritjen e epokës së "Cloud computing", shqetësimet rreth "Internet Security" vazhdojnë të rriten. Si do ta dinë klientët e "Cloud" se informacioni i tyre do të jetë i disponueshëm për ta, si dhe i sigurt dhe i paprekshëm nga të tjerët?

Termi "Cloud" në Cloud Computing është rrjeti i komunikimit ose një rrjet i cili është i Kombinuar me infrastrukturën informatike. Sistemi i Cloud Computing aksesohet duke përdorur rrjetin i cili siguron përdoruesin softuer, pajisje, fuqi përpunuese etj, kur gjenerohet kërkesa. Cloud Computing është një grup virtual burimesh kompjuterike, i cili u ofrohet grupeve të përdoruesve përmes internetit. Cloud Computing siguron shërbime të ndryshme për përdoruesit duke krijuar një ose disa grupe dhe rrjeta kompjuterësh. Qëllimi kryesor mbrapa kësaj është të ofrojë shërbime në mënyrë të virtualizuar për të zvogëluar barrën e përdoruesit për të ruajtur gjithçka në vetvete. Ai i referohet gjithashtu përpunimit të të dhënave të bazuara në internet, e cila siguron pajisje me burime të përbashkëta, informacion ose softuer sipas kërkesës dhe mënyrës së pagimit sipas përdorimit. Në vend që të kenë servera lokalë ose pajisje të veta për të menaxhuar aplikacionet, njerëzit përdorin modelin e ndarjes (ose bashkë përdorimit) të burimeve kompjuterike në Cloud.

1.3.1 Modelet e Shërbimit të Përdorura në Teknologjinë Cloud Computing

Cloud computing siguron një mjedis në të cilin përdoruesi mund të ketë infrastrukturën e tij virtuale duke e përdorur atë dhe mund të kryejë detyra pa u varur nga kufiri gjeografik. Për shkak të mjedisit fleksibël dhe kostos më të lirë, njerëzit tërhiqen drejt përdorimit të shërbimeve Cloud që mund të lidhen me platformën, softuerin ose infrastrukturën. Bazuar në përdorimin e Cloud, ekzistojnë tre modele ofrimi: Cloud Publike, Cloud Private dhe Cloud Hibride [8].

Cloud Computing siguron përparësi të shumta për përdoruesit e saj, por ana e errët e saj është që vuan nga shumë çështje si Integriteti ose Korrektësia e Të Dhënave në pajisjet Storage, Disponueshmëria, Konfidencialiteti dhe më tepër. Këto çështje e bëjnë disi të vështirë përshtatjen me mjedisin cloud për përdoruesit. Prandaj nevojiten më shumë kërkime ose studime në këtë drejtim për të vendosur një besim midis përdoruesve të platformave Cloud Comouting dhe ofruesve te shërbimeve Cloud Computing.

1.4 TEKNOLOGJIA CLOUD COMPUTING NË SHQIPËRI

Cloud Computing ka marrë një zhvillim thelbësor ditët e sotme duke dirigjuar pothuajse të gjitha zhvillimet teknologjike në fushën e teknologjisë së informacionit. Vlen për t'u përmendur se në vendin tonë kjo teknologji akoma nuk po gjen mbështetje dhe përdorim të gjerë midis përdoruesve, ofruesëve të shërbimeve të teknologjisë së informacionit dhe atyre të kompanive të telekomunikoacionit [9]. Kjo situatë ka disa faktorë të cilët influencojnë direkt mbi zhvillimin e kësaj teknologjie në Shqipëri:

- ✓ Së pari, tregu Shqiptar është i vogël dhe si rrjedhojë kerkesa është jashtëzakonisht e papërfillshme.
- ✓ Së dyti, investimet e kërkuara për këtë teknologji janë relativish të konsiderueshme dhe nuk justifikojnë kërkesën e ulët që vjen nga tregu.
- ✓ Së treti, nuk ekziston një kuadër rregullator ligjor i cili të mbrojë dhe stimulojë zhvillimin e kësaj teknologjie brenda terrritorit të Shqipërisë.

Situatë totalisht e ndryshme ekziston sot në botë, ku kompani ndërkombëtare të themeluara në Amerikë të tilla si: Amazon, Google, Microsoft etj, operojnë fuqimisht në tregjet e gjithë botës me shërbimet e tyre Cloud Computing. Për t'u përmendur është fakti që Amazon në fillimin e shërbimeve të saj Cloud, më 19 Mars 2006 investoi rreth 2 miliard dollar amerikane në infrastrukturën fizike të burimeve kompjuterike. Dukshëm shikohet përparësia që ekziston në këtë treg global të këtyre kompanive dhe zgjerimit të tyre në të gjitha vendet me potencial të lartë ekonomik.

Në Shqipëri janë realizuar disa investime në këtë fushë kryesisht në sektorin shtetëror të inicializuara dhe të implementuara nga AKSHI si dhe ne sektorin privat të realizuara nga kompania ALBtelecom [10]. Vlen për t'u përmendur këtu fakti se edhe kompania Vodafone Albania ka realizuar disa iniciativa në këtë teknologji, por më së shumti kanë

qenë tentativa të huazuara në nivel grupi nga shtete të tjera se sa investime direkte të realizuara në Shqipëri. Në këtë kuadër Vodafone në nivel grupi ka nënshkruar një marëveshje me Microsoft për të qenë ofrues i shërbimeve cloud të këtij të fundit, dhe së fundmi ka nënshkruar një marëveshje me Amazon për të qenë ofrues i shërbimeve web të Amazon.

1.4.1 Rregulloret për Mbrojtjen e të Dhënave Personale

Zhvillimi i teknlogjisë Cloud sot në botë përveç faktit që ka sjell shumë të mira ekonomike dhe teknike ka mbartur edhe shumë pikëpyetje në lidhje me sigurinë e informacionit që ofrojnë këto platforma. Shqetësimi më i madh i përdoruesve të këtyre platformave është përdorimi i të dhënave të tyre për qëllime të tjera. Për këtë qëllim, kompanitë të cilat operojnë në këtë treg kanë investuar në zhvillimin e teknologjive të cilat ofrojnë siguri dhe garanci për përdoruesit e rrjeteve Cloud. Megjithatë vlen për t'u përmendur fakti se siguria dhe privatësia e të dhënave të përdoruesit në këto platforma është e rregulluar në mënyrë të ndryshme, në vende të ndryshme. Aktualisht në Europë ligji për mbrojtjen e të dhënave personale në anglisht termi GDPR (General Data Protection Regulation – Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave) aplikohet në mënyrë detyruese mbi të gjitha kompanitë Amerikane të cilat operojnë në Europë. Me anë të këtij ligji të gjitha këto kompani janë të detyruar që të ruajnë, përpunojnë dhe transmetojnë të dhënat e përdoruesve Europiane brenda kufijve të Bashkimit Europian. Si rrjedhojë, të gjitha kompanitë janë detyruar që të ndërtojnë dhe të operojnë infrastrukturat e tyre kompjuterike në vendet e Bashkimit Europian për shërbimet që i'u ofrohen shtetasve europianë.

1.4.2 Legjislacioni Shqiptar

Legjislacioni Shqiptar, për mbrojtjen e të dhënave personale nuk është detyrues për të përpunuar, ruajtur edhe transmetuar të dhënat e përdoruesve Shqiptarë brenda territorit të Shqipërisë por është më shumë një përafrim me ligjet europiane të mbrojtjes së të dhënave personale duke lejuar që përdoruesit Shqiptarë të mund të përdorin shërbimet e ofruesve ndërkombëtarë të cilët operojnë sipas kushteve të Bashkimit Europian. Në këtë mënyrë cënohet drejtpërdrejtë veprimtaria ekonomike e operatorëve Shqiptarë, si dhe të ardhurat që mund të përfitojnë institucionet shtetërore nga ofrimi dhe marrja e këtyre shërbimeve brenda territorit të vendit [11].

M.q.se siguria është një nga pikat ku sot po mëshohet më fort në infrastrukturën Cloud ne do të përqendrohemi në këtë tematikë duke tentuar që të kontribuojmë në përmirësimin e saj në favor të përdorimit të teknologjisë Cloud Computing. Aspektin e sigurisë do ta trajtojmë në kuadrin e teknikës SECURE [5], një teknikë vet-mbrojtëse dhe me performancë më të mirë se teknikat e tjera, në termat e shpejtësisë së dedektimit të ndërhyrjes, kohës së përgjigjes dhe të shpejtësisë false pozitive. Më pas do të zgjerojmë këtë teknikë për dy lloje sulmesh të quajtura UDP Flood dhe NTP Amplication.

1.5 KONCEPTET BAZË TË SIGURISË NË CLOUD COMPUTING

Siguria e informacionit është një ansambël kompleks i teknikave, teknologjive, rregulloreve dhe sjelljeve që në bashkëpunim mbrojnë integritetin dhe aksesin në sistemet kompjuterike dhe të dhënat. Masat e sigurisë të aplikuara nga Teknologjia e Informacionit synojnë të mbrohen nga kërcënimet dhe ndërhyrjet që vijnë si nga qëllimi i keq, ashtu edhe nga gabimi i paqëllimtë i përdoruesit. Seksionet e ardhshme përcaktojnë termat themelorë të sigurisë që lidhen me Cloud Computing dhe përshkruajnë konceptet e ndërlidhura midis tyre [12].

- *Konfidencialiteti*

Konfidencialiteti është karakteristikë e diçkaje që bëhet e arritshme vetëm për palët e autorizuara (Figura 1-1). Brenda mjediseve cloud, konfidencialiteti ka të bëjë kryesisht me kufizimin e hyrjes në të dhëna gjatë tranzitit dhe ruajtjes.

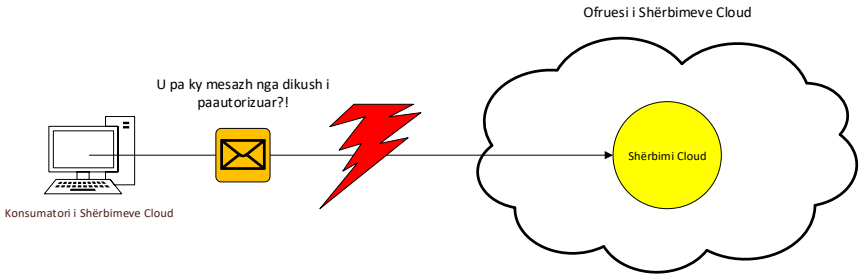

Figura 1-1 Mesazhi i lëshuar nga konsumatori i cloud për shërbimin cloud konsiderohet konfidencial vetëm nëse nuk arrihet ose lexohet nga një palë e paautorizuar

- *Integriteti*

Integriteti është karakteristikë e mosndryshimit nga një palë e paautorizuar (Figura 1-2). Një çështje e rëndësishme që ka të bëjë me integritetin e të dhënave në cloud është nëse një konsumator cloud mund të garantohet që të dhënat që ai transmeton në një shërbim cloud përputhen me të dhënat e marra nga ai shërbim cloud. Integriteti mund të shtrihet në mënyrën se si ruhen, përpunohen dhe merren të dhënat nga shërbimet cloud dhe burimet e IT të bazuara në Cloud.

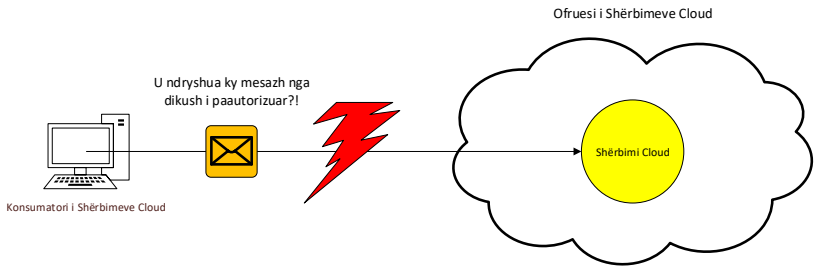

Figura 1-2 Mesazhi i lëshuar nga konsumatori i cloud për shërbimin cloud konsiderohet të ketë integritet nëse nuk është ndryshuar

- *Autenticiteti*

Autenticiteti është karakteristikë e diçkaje që është siguruar nga një burim i autorizuar. Ky koncept përfshin mos-mohim, që është paaftësia e një pale për të mohuar ose sfiduar vërtetimin e një ndërveprimi. Vërtetimi në bashkëveprime të pakontestueshme siguron prova se këto ndërveprime janë të lidhura në mënyrë unike me një burim të autorizuar. Për shembull, një përdorues mund të mos jetë në gjendje të hyjë në një skedar të pakontestueshëm pas marrjes së tij, pa krijuar gjithashtu një regjistrim të këtij aksesi.

- *Disponueshmëria*

Disponueshmëria është karakteristikë e të qenit e arritshme dhe e përdorshme gjatë një periudhe kohore të specifikuar. Në mjediset tipike të cloud-it, disponueshmëria e shërbimeve të cloud-it mund të jetë një përgjegjësi që ndahet nga ofruesi i cloud-it dhe transportuesi i cloud-it. Disponueshmëria e një zgjidhjeje të bazuar në cloud që shtrihet tek konsumatorët e shërbimeve cloud ndahet më tej nga konsumatori i cloud.

- *Kërcënimi*

Një kërcënim është një shkelje e mundshme e sigurisë që mund të sfidojë mbrojtjen në një përpjekje për të shkelur privatësinë dhe/ose për të shkaktuar dëm. Kërcënimet e nxitura manualisht dhe automatikisht janë krijuar për të shfrytëzuar dobësitë e njohura, të referuara gjithashtu si dobësi. Një kërcënim që kryhet rezulton në një sulm.

- *Prekshmëria ose Vulnerabiliteti*

Një dobësi është një dobësi që mund të shfrytëzohet ose sepse mbrohet nga kontrolle të pamjaftueshme të sigurisë, ose sepse kontrollet ekzistuese të sigurisë kapërcehen nga një sulm. Dobësitë e burimeve IT mund të kenë një sërë shkaqesh, përfshirë mangësitë në konfigurim, dobësitë e politikës së sigurisë, gabimet e përdoruesve, defektet e harduerit ose firmware, defektet e softuerit dhe arkitektura e dobët e sigurisë.

- *Rreziku*

Rreziku është mundësia e humbjes ose dëmtimit që rrjedh nga kryerja e një aktiviteti. Rreziku zakonisht matet në përputhje me nivelin e tij të kërcënimit dhe numrin e dobësive të mundshme ose të njohura. Dy metrika që mund të përdoren për të përcaktuar rrezikun për një burim IT janë:

1. probabiliteti i një kërcënimi që ndodh për të shfrytëzuar dobësitë në burimin e IT.
2. pritshmëritë e humbjes/dëmtimit nga burimi i IT-së që kompromentohet.

- *Kontrollet e Sigurisë*

Kontrollet e sigurisë janë kundërmasa të përdorura për të parandaluar ose përgjigjur kërcënimeve të sigurisë dhe për të zvogëluar ose shmangur rrezikun. Detajet mbi mënyrën e përdorimit të kundërmasave të sigurisë përshkruhen zakonisht në politikën e sigurisë, e cila përmban një sërë rregullash dhe praktikash që specifikojnë mënyrën e zbatimit të një

sistemi, shërbimi ose plani të sigurisë për mbrojtjen maksimale të burimeve të ndjeshme dhe kritike të IT.

- *Mekanizmat e Sigurisë*

Kundërmasat përshkruhen zakonisht në terma të mekanizmave të sigurisë, të cilët janë komponentë që përmbajnë një kornizë mbrojtëse që mbron burimet e IT, informacionin dhe shërbimet.

- *Politikat e Sigurisë*

Një politikë sigurie përcakton një sërë rregullash dhe rregulloreje të sigurisë. Shpesh, politikat e sigurisë do të përcaktojnë më tej se si këto rregulla dhe rregullore zbatohen dhe imponohen. Për shembull, pozicionimi dhe përdorimi i kontrolleve dhe mekanizmave të sigurisë mund të përcaktohet nga politikat e sigurisë.

Cloud Computing i siguron kompanive kursime të konsiderueshme të kostos, si për sa i përket shpenzimeve kapitale (CAPEX) dhe shpenzimeve operacionale (OPEX), dhe i lejon ata të përdorin teknologjitë kryesore për të përmbushur nevojat e tyre të përpunimit të informacionit. Në një mjedis cloud, siguria dhe privatësia janë një shqetësim ndër-sektorial, pasi që të dyja prekin të gjitha shtresat e arkitekturës referuese të cloud computing dhe ndikojnë në shumë pjesë të një shërbimi cloud. Prandaj, menaxhimi i sigurisë së burimeve të lidhura me shërbimet cloud është një aspekt kritik i cloud computing.

Shumë nga kërcënimet e sigurisë mund të zvogëlohen me zbatimin e proceseve dhe mekanizmave tradicionalë të sigurisë, ndërsa të tjerët kërkojnë zgjidhje specifike për platformat cloud. Meqenëse secila shtresë e arkitekturës referuese të cloud computing mund të ketë një siguri jo shumë efikase dhe mund të ekspozohet ndaj kërcënimeve të ndryshme, arkitektura e një shërbimi të mundësuar nga cloud ndikon drejtpërdrejt në pozicionin e tij të sigurisë dhe aspektet kryesore të menaxhimit të sistemit.

Për secilin model të shërbimit, Figura 1-3 përdor një qasje “bllok-ndërtesash” për të përshkruar një paraqitje grafike të aksesit të konsumatorit në shtresat e ndryshme të një mjedisi cloud. Siç tregon figura, në një model të shërbimit Infrastruktura si një Shërbim (IaaS) konsumatori cloud ka shikueshmëri të lartë në gjithçka mbi shtresën e Ndërfaqes së Programit të Aplikimit (ang. Application Program Interface-API), ndërsa ofruesit e shërbimeve cloud zbatojnë kontrollet nën shtresën API (të cilat zakonisht janë të paqarta për konsumatorët).

Konsumatori i cloud ka një shikueshmëri të kufizuar dhe kontroll të kufizuar të menaxhimit të çelësit në një model Platforma si një Shërbim (PaaS), mbasi ofruesi i shërbimeve cloud aplikon funksionet e sigurisë në të gjitha shtresat duke përfshirë nën shtresën e integrimit dhe atë middleware. Konsumatori i cloud computing humbet shikueshmërinë dhe kontrollin në një model Softwari si një Shërbim (SaaS), dhe në përgjithësi, kontrollet në nën shtresën e prezantimit janë jo të dukshme për konsumatorin

cloud, pasi ofruesi i shërbimeve cloud implementon të gjitha funksionet e sigurisë. Konsumatorët cloud janë përgjegjës për:

- Identifikimin e duhur të të dhënave.
- Vlerësimin e rrezikut nga çdo ekspozim ose keqpërdorim i të dhënave.
- Identifikimin e kërkesave të sigurisë të krahasueshme me ndjeshmërinë e të dhënave.
- Miratimin e zvogëlimeve të nevojshme të rrezikut.

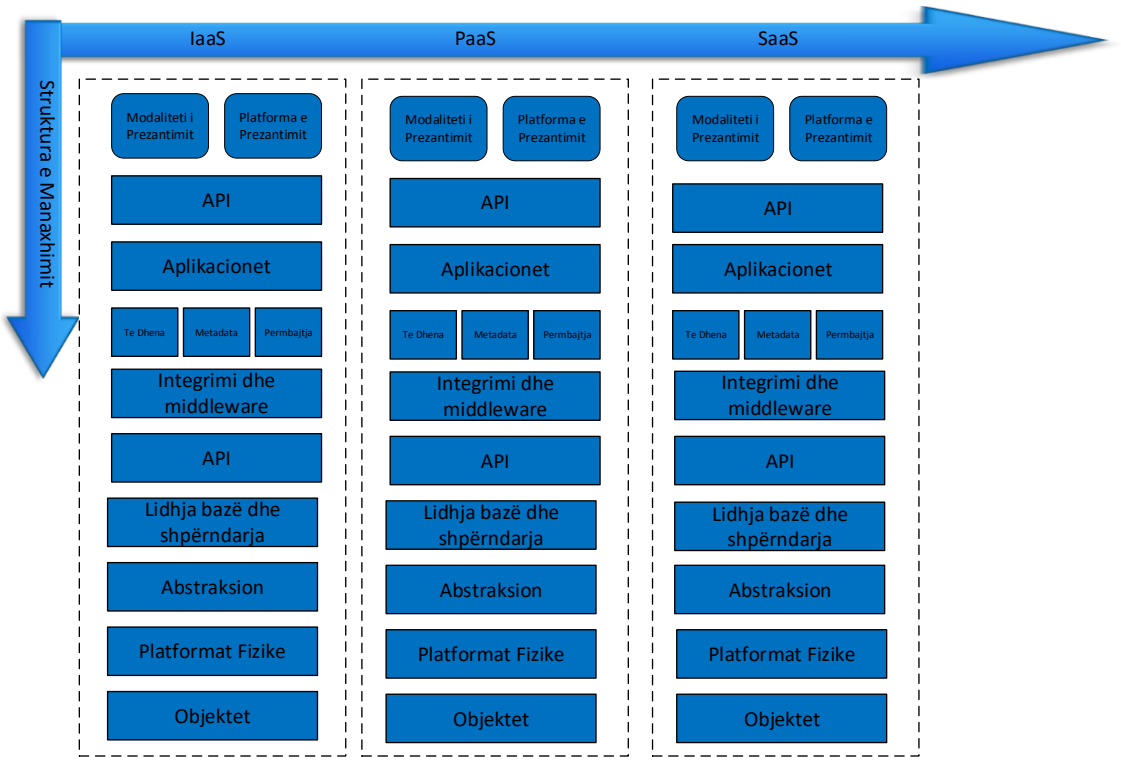

Figura 1-3 Niveli i kontrollit të konsumatorit

Siguria në cloud computing i referohet tërësisë së procedurave, proceseve dhe standardeve të krijuara për të na dhënë sigurinë e informacionit në një eko-sistem cloud. Përqëndrimi i burimeve të specializuara në një eko-sistem cloud ka mundësinë të sigurojë, nga njëra anë mbrojtje më të fuqishme dhe ana tjetër me kosto efektive. Siguria e cloud computing adreson çështje fizike dhe logjike të sigurisë në të gjitha modelet e ndryshme të shërbimit të software-it, platformës dhe infrastrukturës. Ai adreson gjithashtu mënyrën e ofrimit të këtyre shërbimeve në modelet e shpërndarjes publike, private dhe komunitare.

Modeli i Privatësisë: Cloud computing ka shqetësime për privatësinë sepse ofruesit e shërbimeve kanë akses në të dhënat që janë të ruajtura në infrastrukturat e tyre. Ofruesit e shërbimeve cloud mund të ndryshojnë, fshijnë aksidentalisht ose qëllimisht informacionin. Shumë ofrues të shërbimeve cloud mund të ndajnë informacione me palë të treta nëse është e nevojshme qoftë edhe pa një urdhër. Leja ofrohet sipas rregullave të

tyre të privatësisë, për të cilën përdoruesit bien dakord para se të fillojnë të përdorin shërbimin cloud (i pranojnë ose në kundërt nuk marrin shërbim).

Meqenëse përdorues të ndryshëm ndajnë një platformë të ofruesve të shërbimeve cloud, mund të ekzistojë një mundësi që informacioni që i përket klientëve të ndryshëm të jetë në të njëjtin server të të dhënave. Prandaj, rrjedhja (humbja) e informacionit mund të lindi pa dashje kur informacioni për një klient i jepet një klienti tjetër. Për më tepër, hakerat po kalojnë kohë dhe përpjekje të konsiderueshme në kërkim të mënyrave për të gjetur dobësi në infrastrukturat cloud që do ti lejonte ata të depërtonin në këto platforma. Për shkak se të dhënat nga qindra ose mijëra kompani mund të ruhen në servera me burime kompjuterike shume të mëdhaja në cloud, hakerat mund të fitojnë teorikisht kontrollin e informacionit përmes një sulmi të vetëm të hipervizorit (kontrolluesit të burimeve kompjuterike në shtresën virtuale) - një proces i referuar si “hyperjacking”.

Një çështje tjetër e platformave cloud është pronësia ligjore e të dhënave, përgjegjësitë dhe privilegjet e zotëruesit të të dhënave dhe ruajtësit e tyre. Meqenëse konsumatorët cloud mbajnë pronësinë e të dhënave që qëndrojnë në një platformë cloud, ata zakonisht mbajnë autorizimin e sigurisë brenda dhe janë përgjegjës për identifikimin e të gjitha kërkesave të sigurisë që kanë të bëjnë me pritjen dhe përpunimin e platformave cloud të këtyre të dhënave. Gjithmonë rekomandohet që konsumatorët cloud të rishikojnë zbatimin e të gjitha kontrolleve të sigurisë dhe privatësisë dhe të sigurojnë që të gjitha kërkesat janë përmbushur përpara se të autorizojnë përdorimin e një sistemi informacioni të bazuar në plaftormat cloud.

1.6 PUNIME TË NGJASHME

Sipas një raporti të Forbes [13] të botuar në 2015, shpenzimet e sigurisë të bazuara në Cloud pritet të rriten me 42%. Sipas një studimi tjetër, shpenzimet e sigurisë së IT ishin rritur në 79.1% deri në 2015, duke treguar një rritje prej më shumë se 10% çdo vit [13]. Korporata Ndërkombëtare e të Dhënave (IDC) në vitin 2011 tregoi se 74.6% e klientëve të ndërmarrjeve e renditën sigurinë si një sfidë të madhe. Ky punim përmbledh një numër artikujsh të rishikuar nga kolegët mbi kërcënimet e sigurisë në Cloud Computing dhe metodat parandaluese. Objektivi i hulumtimit është të kuptojmë përbërësit e Cloud, çështjet e sigurisë dhe rreziqet, së bashku me zgjidhjet në zhvillim që mund të zbusin potencialisht dobësitë në Cloud. Eshtë një fakt i pranuar kryesisht që nga viti 2008, që Cloud Computing është një platformë e vlefshme hostimi; megjithatë, perceptimi në lidhje me sigurinë në Cloud është se ajo ka nevojë për përmirësime të konsiderueshme të realizuara në nivele më të larta të përshtatjes në nivelin e kompanisë.

Siç është identifikuar nga një hulumtim tjetër, shumë prej çështjeve me të cilat përballen Cloud Computing duhet të zgjidhen urgjentisht. Industria ka bërë përparime të konsiderueshme në luftën kundër kërcënimeve ndaj Cloud Computing, por ka edhe më shumë për të bërë për të arritur një nivel pjekurie që ekziston aktualisht me hostimet tradicionale on-premise[14].

Siguria në Cloud Computing po zhvillohet hap pas hapi me rreziqe pasi ato zbulohen shpesh herë tepër vonë për të parandaluar incidentet. Cloud Computing për shkak të natyrës së tij të shpërndarë, arkitekturës komplekse dhe burimeve të shfrytëzuara paraqet një rrezik unik dhe të rëndë për të gjithë aktorët. Për të gjithë aktorët është kritike të kuptojnë rrezikun dhe ta zbusin atë në mënyrë të përshtatshme. Siguria duhet të ndërtohet në çdo shtresë në një platformë të Cloud Computing duke përfshirë praktikat më të mira dhe teknologjitë e reja për të zbutur në mënyrë efektive rrezikun.

Në cloud, konsumatori, ofruesi, ndërmjetësi, transportuesi, auditori dhe të gjithë të tjerët duhet të marrin masat e nevojshme paraprake kundër rreziqeve për të siguruar me të vërtetë platformën e Cloud Computing ose për t'u ekspozuar ndaj rrezikut të rëndësishëm dhe ndonjëherë kritik të biznesit. Sipas një studimi të fundit, industria njeh që inxhinieria e sigurisë ofron praktikat, metodat dhe teknikat më të mira për zhvillimin e sistemeve dhe shërbimeve, të cilat janë ndërtuar për sigurinë, qëndrueshmërinë dhe disponueshmërinë. E rëndësishme është ta çojmë përpara këtë hulumtim për të siguruar praktika të tilla më të mira për më shumë aplikime dhe raste përdorimi.

Thelbësore është gjithashtu që të kryhet hulumtim i mëtejshëm në ciklin jetësor të zhvillimit të sistemeve (SDLC) për konsumatorët e platforms Cloud Computing në mënyrë që të përfshijnë modele të ndryshme të zhvillimit dhe përparimit teknologjik dhe sistemeve të kontejnerëve të tillë si Docker për të përmirësuar sigurinë në një nivel themelor. Për më tepër, ka një studim shumë të kufizuar mbi trajnimin dhe ndikimin e njerëzve në siguri. Mund të bëhet punë për të kuptuar sfidat, kërkesat dhe ndikimin e trajnimit efektiv të sigurisë për konsumatorët dhe ofruesit e tjerë.

Cloud Computing lejon firmat të transferojnë tërë procesin e tyre të teknologjisë së informacionit (IT), duke i'u dhënë atyre mundësinë që të përqëndrohen më shumë në biznesin e tyre kryesor për të rritur produktivitetin dhe inovacionin e tyre në ofrimin e shërbimeve për klientët. Kjo i lejon bizneset të ulin koston e rëndë të kryer mbi infrastrukturën e IT pa humbur përqendrimin në nevojat e klientit [15].

Sidoqoftë, deri në një kufi të caktuar, adoptimi i Cloud Computing ka filluar të rritet në mesin e shumë organizatave të mëdha dhe të ketë zhvillim për shkak të disa çështjeve që lidhen me sigurinë dhe privatësinë. Si rrjedhojë u zhvilluan disa intervista, me zhvillues të platformave Cloud Computing dhe me ekspertë të sigurisë, si dhe u rishikua literatura përkatëse. Ky studim na mundësoi të kuptojmë, sfidat aktuale dhe të ardhshme, të sigurisë dhe privatësisë me Cloud Computing. Rezultati i këtij studimi çoi në identifikimin e gjithsej 18 çështjeve aktuale dhe të ardhshme të sigurisë që ndikojnë në disa atribute të Cloud Computing.

Përdorimi i llogaritjes cloud është i ngadaltë midis NVM-ve, pasi NVM-të kërkojnë shërbime më shumë në fushën e ofrimit të infrastrukturës dhe aplikacioneve si shërbim. Studimi dhe analiza e këtyre çështjeve të sigurisë kanë çuar në kuptimin e dobësive të sigurisë në Cloud Computing që ekzistojnë dhe kjo do të ndihmojë ndërmarrjet të zhvendosen drejt cloud computing. U rishikuan aplikacione tradicionale të

ueb-it, mbajtjen e të dhënave dhe virtualizimin sipas shfaqjes së tyre në modelet e shërbimit: IaaS, PaaS dhe SaaS.

Siç përshkruhet në këtë paragraf, shumica e çështjeve të sigurisë janë për shkak të dobësive në virtualizim, ruajtjen e të dhënave dhe rrjetin data të cilat janë gjithashtu mundësuesit kryesorë të teknologjisë së Cloud Computing. Shpjegimi i çështjeve të sigurisë në Cloud nuk është i mjaftueshëm, prandaj kemi paraqitur dobësi të cilat mund të çojnë në kërcënim, në mënyrë që të jetë e lehtë të formulohet kontributi i këtyre kërcënimeve. Ne besojmë se kjo do të inkurajojë dhe përshpejtojë miratimin e cloud computing midis ndërmarrjeve të vogla dhe të mesme.

Duke ekspozuar [16] dhe eksploruar çështje teknike dhe të besimit që lindin në marrjen e informacioneve teknike nga platforma Cloud Computing si një shërbim dhe duke analizuar disa strategji për adresimin e këtyre sfidave ne mund të:

- Së pari, krijojmë një model për të treguar shtresat e besimit të kërkuara në Cloud Computing.
- Së dyti, paraqesim kontekstin gjithëpërfshirës për një provim ligjor në Cloud Computing dhe analizojmë zgjedhjet e disponueshme për një ekzaminues.
- Së treti, ofrojmë për herë të parë një vlerësim të pervetesimit të mjeteve të njohura ligjore, duke përfshirë kompletet ligjore te pajisjeve Guidance EnCase dhe AccesData, dhe tregojmë se ata mund të kthejnë me sukses të dhëna të paqëndrueshme dhe qëndrueshme nga Cloud.

Megjithatë, ne arrijmë të shpjegojmë, se me këto teknika gjyqtari dhe juria duhet të pranojnë një besim të madh në vërtetësinë dhe integritetin e të dhënave nga shumë shtresa të modelit Cloud Computing. Përveç kësaj, ne do të shqyrtojmë katër zgjidhje të tjera për përvetësimin e nje Moduli Platforme të Besuar (Trusted Platform Module – TPM), platformën e menaxhimit, parashikimin-si-një-shërbim, dhe zgjidhjet ligjore, të cilat supozojnë më pak besim, por kërkojnë më shumë bashkëpunim nga ofruesi i shërbimit cloud.

Në këtë rast hidhet një themel për zhvillimin në të ardhmen të metodave të reja të blerjes për platformat Cloud që do të jenë të besueshme dhe të bazuara në kuadret ligjore respektive. Gjithashtu kjo do të ndihmojë ekspertët ligjorë, zbatuesit e ligjit dhe gjykatën që të vlerësojnë besimin në provat e marra nga Cloud-i.

Kemi demonstruar se mjetet e sotme ligjore më të përdorura janë teknikisht të afta për marrjen në largësi të të dhënave nga Amazon EC2. Gjithashtu kemi treguar që duke pasur parasysh kërkesën për më shumë shtresa të besimit, atëherë vetëm teknologjia është e pamjaftueshme për të prodhuar të dhëna të besueshme dhe për të zgjidhur problemin e përvetësimit ligjor në cloud. Katër alternativat që janë paraqitur ofrojnë mundësi që të lidhin teknologjinë me mbështetjen e ofruesit të shërbimit.

Rekomandimi për përvetësimin ligjor të modelit IaaS ne Cloud Computing është plani i menaxhimit. Ky opsion ofron ekuilibrin më të kënaqshëm të shpejtësisë dhe kontrollit me

besimin. Inkurajojmë ofruesit e shërbimeve Cloud që të vendosin të dhëna ligjore në dispozicion të përdoruesve sipas kësaj mënyre, në mënyrë që të fillohet zbatimi për ta bërë këtë të mundur. Ndërsa EnCase dhe FTK realizuan dhe ofruan me sukses provat, nuk rekomandojmë përdorimin e tyre për ligjshmërinë në distancë në Cloud sepse kërkohet shumë besim përkatësisht.

Disa fusha mbeten për punë në të ardhmen. Së pari, eksperimentet e realizuara janë specifike për Infrastruktura si Shërbim (IaaS) duke përdorur platformën komerciale EC2. Këto rezultate nuk aplikohen në modele dhe mjedise të tjera të platformave Cloud, të tilla si Microsoft Azure ose Google AppEngine, ku aplikacioni ligjor nuk mund të instalohet dhe ekzekutohet siç mund të bëhet në EC2 [17].

Do të nevojitet punë e ardhshme për të gjetur paralele të përshtatshme në ato platforma. Së dyti, përdoruesit e cloud-it do të përfitonin nga aftësitë ligjore të drejtuara nga konsumatorët dhe të ekspozuara ndaj tyre nga vet ofruesi i shërbimeve. Synojmë të punojmë me ofruesit e shërbimit për t'i lejuar klientët qe të rimarrin të dhënat e regjistruara (logs) ligjore dhe metadata (*p.sh.,* kontrollet e kriptografisë të vëllimeve të diskut) direkt online nga konsola e menaxhimit. Së treti, nevojiten zgjidhje për të ruajtur provat dhe për të parandaluar humbjen e provave ligjore kur burimet e platformave Cloud lihen të lira. Së fundmi, planifikojmë të shqyrtojmë më tej çështjet ligjore të blerjes, veçanërisht ato që dalin nga shqetësimet e ndryshimit të katërt në lidhje me kërkimin dhe konfiskimin, juridiksionin dhe pronësinë.

Cloud Computing po përjeton momentin dhe së bashku me të shkojnë njerëzit, të dhënat dhe paratë, po kështu edhe krimi. Ky paragraph është një themel dhe rrugë për t'u dhënë mundësi ekspertëve ligjorë të ndërmarrin hapat fillestarë në hetimin kriminalistik të krimeve të bazuara në Cloud [18].

Teknika e Cloud Computing përdoret kryesisht nga aplikacione me rritje të shpejtë të bazuara në Internet. Kalimi në Cloud Computing rezulton në uljen e kostos së menaxhimit dhe mirëmbajtjes së infrastrukturës IT. Organizata të ndryshme kontrollojnë burimet Cloud përmes internetit duke ulur koston e menaxhimit dhe mirëmbajtjes së infrastrukturës IT. Gjithashtu këto organizata kontrollojnë burimet Cloud përmes internetit duke përdorur protokollet dhe standardet e rrjetave të të dhënave. Kjo e bën infrastrukturën IT të shpërndarë në natyrë, por të kontrolluar në mënyrë qëndrore, e cila u hap derën sulmuesve për ndërhyrje.

Sulmet e Shpërndara të Mohimit të Shërbimit (DDoS) është një nga ndërhyrjet më popullore në platformat Cloud Private që shkakton degradimin e shërbimeve ose mohimin e shërbimeve. Në këtë kuadër fokusi i vetëm është mbi sulmin DDoS i cili synohet specifikisht drejt zbulimit të okupimit të gjerësisë së brezit dhe bllokimit të aksesit. Sulme të tilla synojnë shtresën e rrjetit të platformave Cloud të shoqëruara me kërkesa të pavlefshme duke sjell mohim të kërkesave legjitime. Kështu, i gjithë konfigurimi i platformave Cloud bëhet e cënueshme dhe mund të difektohet nga këto sulme DDoS. Për

të kapërcyer këtë, kërkohet një sistem operativ cloud i cili ka një mur zjarri (firewall) mbrojtës të integruar me sistemin e zbulimit DDoS.

Në këtë rast është propozuar një sistem OpenStack me firewall të integruar dhe programim të papërpunuar të CPUs për monitorimin e trafikut të rrjetit. Bazuar në të dhënat e krijuara në mjedisin e kontrolluar të sulmit DDoS, algoritmet si pema e Vendimit, fqinji më i afërt K (KNN), algoritmet e Naive Bayes dhe Deep Neural Network (DNN) krahasohen përkundrejt modelit të trajnuar. Si përfundim, zbulohen sulmet DDoS, dhe njoftohet administratori i platformës Cloud Private [19].

Cloud-i është më i avantazhuar sepse të dhënat mund të mirëmbahen në distancë. Gjithashtu, Cloud ka fituar rëndësi për shkak të tiparit të tij të 'hapësirës së ruajtjes së të dhënave të pakufizuar'. Cloud-i OpenStack është një tjetër fushë në zhvillim. Ai mund të sigurojë privilegje shtesë për konfigurimin e cloud si p.sh. administrimi i përdoruesve të shumtë, ndërfaqja e manaxhimit, duke krijuar topologjinë e vet. Por firewall-i ekzistues në OpenStack nuk trajton në mënyrë specifike sulmet DDoS.

Kështu që kërkohet një modul i evidentimit DDoS së bashku me firewall për të pasur sistemin e duhur të sigurisë në OpenStack. Do të ishte gjithashtu e përshtatshme që administratori i rrjetit të marrë një njoftim ku dhe kur ndodh një sulm DDoS. Në këtë rast tregohet një përmbledhje e sulmeve DDoS, në mënyrë specifike okupimi i gjerësisë së brezit dhe ndalimi i aksesit si dhe skemat e zbulimit. Për më tepër, është dhënë një krahasim midis metodave aktuale të evidentimit dhe një mënyrë për të njoftuar administratorin për adresat IP që shkaktojnë sulmin DDoS. Ky studim mund të shtrihet për të mësuar se si disa sulme të tjera DDoS mund të mbingarkojnë kontrolluesin në Cloud dhe kështu të shkaktojnë probleme në Cloud-in Privat të bazuar në OpenStack. Algoritmet mund të modifikohen për të zbuluar një gamë më të gjerë të sulmeve DDoS sesa është diskutuar tashmë. Algoritmet e optimizuara në arkitekturën Hadoop mund të përdoren në mënyrë që të marrim efikasitet dhe saktësi më të mirë për të zbuluar më tej lloje të ndryshme të sulmeve DDoS.

Cloud Computing është duke u bërë gjithnjë e më i modës në mjedisin e informatikes së shpërndarë. Përdorimi i mjedisit Cloud për përpunimin dhe ruajtjen e të dhënave po bëhet një lëvizje universale. Softueri si një Shërbim (SaaS) ndodhet në shumë aplikacione biznesi, si dhe në jetën tonë të përditshme, ne thjesht mund të themi se kjo është teknologji përçarëse. Cloud Computing mund të shihet që nga informatika e bazuar në Internet, në të cilën burimet e përbashkëta, aplikacioni dhe informacioni vihen në dispozicion të pajisjeve sipas kërkesës. Ai lejon burimet drejt komandimit mbi bazën e përdorimit. Zvogëlon koston dhe kompleksitetin e ofruesve të shërbimeve përmes mjeteve dhe kostove operacionale [20].

Kjo i lejon përdoruesit të kenë qasje në aplikacione në mënyrë të vazhdueshme. Në emër të përdoruesit, ky konstrukt u siguron ofruesve të shërbimit cloud mundësinë për të aplikuar përditësimet e softuerit dhe koston e serverave etj. Për të dyja palët, ofruesit e

shërbimit cloud dhe konsumatorëve; disponueshmëria, integriteti, vërtetësia, konfidencialiteti dhe privatësia janë shqetësimi më i rëndësishëm. Infrastruktura si Shërbim (IaaS) shërben si shtresë bazë për shumë modele të tjera të modeleve Cloud si dhe Platformës si Shërbim (PaaS). Siguria në Cloud-et PaaS konsiderohet nga perspektiva të shumëfishta duke përfshirë kontrollin e hyrjes, vazhdimësinë e shërbimit dhe privatësinë, ndërsa mbrojnë së bashku si ofruesin e shërbimit ashtu edhe përdoruesin. Problemet e sigurisë të Cloud-it PaaS janë hulumtuar dhe klasifikuar. Në këtë perspektivë do të shkojmë në disa çështje kryesore të sigurisë së mjediseve aktuale në Cloud Computing.

Cloud Computing ka një mundësi të madhe për kursimet e kostos për ndërmarrjet dhe kompanitë, por rreziku i sigurisë është gjithashtu shumë i madh. Ndërmarrjet të cilat konsiderojnë hyrjen në teknologjinë Cloud Computing si një taktikë për të ulur koston dhe për të rritur përfitimin, duhet të analizojnë seriozisht rrezikun e sigurisë në Cloud Computing. Vlera e Cloud Computing në administrimin e rrezikut të informacionit është lehtësia për të menaxhuar rrezikun në mënyrë më efektive nga një pikë e vetme integrimi. Megjithëse Cloud Computing mund të konsiderohet si një mrekulli e re e cila është vendosur të reformojë mënyrën se si ne përdorim Internetin, ka shumë më tepër për të menduar dhe marrë në konsideratë.

Ka shumë teknologji të reja që shfaqen me një shpejtësi të menjëhershme, secila me zhvillimet e veta teknologjike dhe me potencialin për ta bërë më të lehtë jetën e njeriut. Sidoqoftë, duhet të jemi shumë të kujdesshëm për të vlerësuar rreziqet dhe sfidat e sigurisë në zbulimin e këtyre teknologjive. Në këtë kontekst nuk bën përjashtim as teknologjia Cloud Computing. Në këtë kuadër theksohen çështjet e sigurisë në modelin e shërbimit të mjedisit në Cloud Computing, të cilat aktualisht trajtohen në platformat Cloud Computing. Cloud Computing ka mundësi të bëhet e preferuara në stimulimin e një zgjidhjeje të sigurt, virtuale dhe të mundshme ekonomikisht të IT-së në të ardhmen.

Problemet e sigurisë në internet mbeten një sfidë e madhe me shumë shqetësime në lidhje me sigurinë, të tilla si worm-et, spam-et si dhe sulmet phishing të realizuara në Internet. Botnet-et, sulmet e mirë organizuara përkundrejt rrjeteve të shpërndara, konsistojnë në një numër të madh bot-esh që gjenerojnë vëllime të mëdha spam-esh ose fillojnë sulme të Shpërndara të Mohimit të Shërbimit (DDoS) ndaj pajisjeve të viktimave. Sulmet e reja në zhvillim, botnet degradojnë statusin e sigurisë së Internetit. Për të adresuar këto probleme, është propozuar një sistem bashkëpunimi praktik i menaxhimit të sigurisë së rrjetit me një bashkëpunim efektiv të Menaxhimit të Unifikuar të Kërcënimit (UTM) dhe prober-ave të trafikut. Një rrjet i shpërndarë sigurie dhe i mbivendosur me një qendër të centralizuar sigurie drejton një protokoll të komunikimit pikë-më-pikë duke përdorur modulin bashkëpunues të UTM-ve duke i lidhur ato virtualisht për të shkëmbyer ngjarjet e rrjetit dhe rregullat e sigurisë [21].

Funksionet e sigurisë për UTM janë rikonstruktuar për të shpërndarë rregullat e sigurisë. Në këtë rast, është propozuar një model dhe implementimi i një qendre sigurie

me bazë cloud-in për analizën parashikuese të sigurisë në rrjet. Në këtë kontekst është propozuar të përdoret hapësira e ruajtjes së të dhënave në storage për të mbajtur trafikun e mbledhur dhe më pas ta përpunojmë atë me platforma Cloud Computing dhe për të zbuluar sulmet me qëllim të keq. Si një shembull praktik, paraqitet analiza parashikuese e sulmit phishing dhe burimet e kërkuara të procesimit dhe magazinimit të të dhënave, të cilat vlerësohen bazuar në gjurmimin real të të dhënave. Qendra e sigurisë e mbështetur në Cloud mund të udhëzojë secilin UTM dhe pikë trafiku (probe) bashkëpunuese për të mbledhur ngjarjet dhe trafikun e papërpunuar, t'i kthejë ato mbrapa për analiza të thelluara dhe të gjenerojë rregulla të reja për qendrën e sigurisë. Këto rregulla të reja të sigurisë zbatohen nga UTM-të bashkëpunuese dhe feedback-u i ngjarjeve të këtyre rregullave kthehen në qendrën e sigurisë. Me anë të këtij lloji të kontrollit me qark të mbyllur, sistemi i menaxhimit të sigurisë së rrjetit me bashkëpunim mund të identifikojë dhe adresojë sulmet e reja të shpërndara më shpejt dhe në mënyrë më efektive.

CNSMS është shumë i dobishëm për të ndërmarrë kundërmasa përkundrejt sulmeve të shpërndara në rrjet. Funksionimi i tij rezulton në rezultate me të dhëna shumë të mëdha, të tilla si trafiku i rrjetit, ngjarjet e sigurisë, etj [22]. Në këtë rast, propozohet përdorimi i sistemeve Cloud Computing për të eksploruar vëllimin e madh të të dhënave të mbledhura nga CNSMS dhe për të gjurmuar ngjarjet e sulmeve. Arkivimi i trafikut është implementuar në UTM bashkëpunuese për të mbledhur të gjitha të dhënat e gjurmimit të rrjetit dhe teknologjia Cloud Computing është përdorur për të analizuar të dhënat eksperimentale në paralel.

Një platform Cloud IaaS u ndërtua me aplikacionin Eucalyptus dhe platformat ekzistuese të cloud-it si Amazon EC2 dhe S3, të cilat u përdorën për qëllime krahasimore. Analiza parashikuese e sulmeve Phishing u prezantua si një rast praktik dhe burimet e kërkuara kompjuterike dhe ruajtjes së të dhënave (storage) u vlerësuan duke përdorur të dhëna reale gjurmimi. Operacionet e filtrimit të sulmeve phishing janë të bazuara në Cloud dhe operojnë në paralel, si dhe vlerësohet procedura e përpunimit të të dhënave. Rezultatet tregojnë se skema e propozuar është praktike dhe mund të përgjithësohet për të analizuar parashikimin e sulmeve të tjera të rrjetit në të ardhmen.

Ndjeshmëria e sistemeve Cloud Computing (CCS) ndaj kërcënimeve të avancuara të vazhdueshme (APTs) është një shqetësim i rëndësishëm për qeverinë dhe industrinë. Po paraqesim një model referimi të arkitekturës Cloud që përfshin një gamë të gjerë të kontrolleve të sigurisë dhe praktikave më të mira, si dhe një model të vlerësimit të sigurisë në Cloud – Besimi ne Cloud (Cloud-Trust) - që vlerëson nivelet e larta të sigurisë për të vlerësuar shkallën e konfidencialitetit dhe integritetit të ofruar nga një CCS ose ofruesi i shërbimit cloud (Cloud Service Provider CSP). Cloud-Trust është përdorur për të vlerësuar nivelin e sigurisë së katër arkitekturave cloud me shumë përdorues të njëkohshëm IaaS, të pajisura me kontrolle alternative të sigurisë në Cloud [23].

Rezultatet tregojnë se probabiliteti i depërtimit të CCS (kompromis i të dhënave me vlerë të lartë) është i lartë nëse zbatohen një grup minimal i kontrolleve të sigurisë. Probabiliteti

i depërtimit të CCS bie ndjeshëm nëse miratohet një mbrojtje e thellë cloud në arkitekturën e sigurisë që mbron imazhet e makinës virtuale (VM) jo në gjendje pune, forcon CSP dhe kontrollet e hyrjes së administratorit të sistemit si dhe përdor kontrolle të tjera të sigurisë së rrjetit për të minimizuar mbikëqyrjen e rrjetit cloud dhe zbulimin e makina virtuale (VM-ve) që janë në gjendje pune.

Kemi demonstruar se si Cloud-Trust mund të vlerësojë statusin e sigurisë të shërbimit të ofruar IaaS CCS dhe IaaS CSP dhe të përdoret për të vlerësuar mundësitë e mundshme të infiltrimit dhe zbulimit të APT. Këto përcaktojnë sasinë e dy metrikave të sigurisë të nivelit të lartë: konfidencialitetin dhe integritetin e IaaS CCS.

Cloud-Trust gjithashtu mund të përcaktojë sasinë e vlerës së kontrolleve specifike të sigurisë CCS (përfshirë karakteristikat opsionale të sigurisë të ofruara nga CSP-të kryesore komerciale). Ajo mund të përdoret gjithashtu për të kryer analiza të ndjeshmërisë së vlerës duke shtuar kontrolle specifike të sigurisë në një IaaS të CCS, kur ekziston pasiguri në lidhje me vlerën e një kontrolli specifik të sigurisë (i cili mund të jetë opsional dhe të rrisë koston e shërbimeve të CSP, ose të cilat mund të mos kërkohen nga industria ose standardet e qeverisë) [24].

Synimi i versionit fillestar të Cloud-Trust është aktualisht e kufizuar në IaaS CCS dhe CSP. Ai gjithashtu nuk përfshin të gjithë vektorët e mundshëm të brendshëm të sulmeve dhe metodat e tyre. Hapat e tjerë të mundshëm në të ardhmen janë për të zgjeruar Cloud-Trust që të përfshijë gamën e plotë të sulmeve të brendshme, si për CSP-të që ofrojnë Platformë si një Shërbim (PaaS) ashtu dhe Software si një Shërbim (SaaS).

Do të ishte gjithashtu e dobishme të zhvillohej një seri e plotë e hapave të sulmit APT të eksfiltrimit të të dhënave që përfshin hapësirën e rrugëve të mundshme të daljes së të dhënave CCS dhe CSP. Do të ishte e dobishme të eksploroni se si të dhënat CVSS mund të përdoren për të vlerësuar probabilitetin e sulmit APT. Një analizë e fortë ndjeshmërie mund të kryhet gjithashtu duke përdorur një version të përmirësuar të Cloud-Trust që përfshin sulme të brendshme për të parë se cilat nyje CCS dhe rrugëve të sulmit paraqesin dobësitë më të mëdha dhe avantazhet për sulmuesit.

Cloud Computing është akoma në fillimet e tij, pavarësisht nga fitimi i një vrulli të jashtëzakonshëm kohët e fundit, siguria e lartë është një nga pengesat kryesore për hapjen e epokës së re të vizionit të ëndërruar prej kohësh të informatikës si një gjë e dobishme. Ndonëse aplikacionet dhe të dhënat e ndjeshme zhvendosen në qendrat e të dhënave cloud, ekzekutimi i burime kompjuterike virtuale realizohet në formën e makinës virtuale. Sidoqoftë, këto atribute unike paraqesin shumë sfida të reja të prekshme dhe të paprekshme të sigurisë. Mund të jetë e vështirë të gjurmohen çështjen e sigurisë në mjediset e Cloud Computing [25].

Pra, në këtë rast kryesisht do të synojmë të nxjerrim në pah çështjet kryesore të sigurisë, privatësisë dhe besimit në mjediset aktuale ekzistuese të Cloud Computing dhe të ndihmojë përdoruesit të njohin kërcënimet e prekshme dhe jo-te prekshme të lidhura me përdorimin e tyre, e cila përfshin: (a) studimin e çështjeve më të rëndësishme të sigurisë,

privatësisë dhe besimit që paraqesin kërcënime në mjediset aktuale ekzistuese të Cloud Computing; dhe (b) analizimin e mënyrës që mund të adresohet për të eleminuar këto kërcënime të mundshme të privatësisë, sigurisë dhe besimit, dhe të sigurojë një mjedis me nivel të lartë sigurie, të besueshëm dhe të varur në mjedisin Cloud Computing. Në një të ardhme të afërt, do të analizojmë dhe vlerësojmë më tej çështjet e privatësisë, sigurisë dhe besimit në mjedisin e Cloud Computing me një qasje të matshme, do të zhvillojmë dhe vendosim më tej një siguri të plotë, vlerësimin e besimit të privatësisë, kornizën e menaxhimit në mjediset e vërteta Cloud Computing.

Siguria e lartë është një nga pengesat kryesore për hapjen e epokës së re të vizionit të ëndërruar prej kohësh të kompjuterit si një gjë e dobishme. Ndërsa aplikacionet e ndjeshme dhe të dhënat zhvendosen në qendrat e të dhënave cloud, ekzekutimi i burimeve kompjuterike virtuale në formën e makinës virtuale. Sidoqoftë, këto atribute unike paraqesin shumë sfida të reja të sigurisë si dobësitë e aksesit, dobësitë e virtualizimit dhe dobësitë e aplikacioneve në internet.

Me avancimin e Cloud Computing dhe rritjen e numrit të përdoruesve të Cloud-it, siguria, privatësia dhe dimensionet e besimit do të rriten vazhdimisht. Për të mbrojtur të dhëna private dhe të ndjeshme që përpunohen në qendrat e të dhënave, përdoruesi i Cloud-it duhet të verifikojë:

(a) ekzistencën reale të mjedisit Cloud Computing në botë;

(b) sigurinë e informacionit në Cloud; dhe

(c) besueshmërinë e sistemeve në mjedisin Cloud Computing.

Në këtë rast, synohet kryesisht të nxjerrim në pah çështjet kryesore të sigurisë, privatësisë dhe besimit në mjediset aktuale ekzistuese Cloud Computing dhe të ndihmojmë përdoruesit të njohin kërcënimet e prekshme dhe jo-te prekshme që lidhen me përdorimin e tyre. Ne mbulojmë dy aspekte kryesore të sigurisë, çështjet e privatësisë dhe besimit, të cilat përfshijnë: (a) sondazhin e çështjeve më të rëndësishme të privatësisë, sigurisë dhe besimit që paraqesin kërcënime në mjediset aktuale ekzistuese të informatikës dhe (b) analizimin e mënyrës që mund të adresohet për të eleminuar këto kërcënime të mundshme të sigurisë, privatësisë dhe besimit dhe sigurimin e një mjedisi të lartë të sigurt, të besueshëm dhe të varur në mjediset e Cloud Computing.

Punimet e ardhshme duhet të përqëndrohen në sa vijon:

(a) analizimi dhe vlerësimi i çështjeve të privatësisë, sigurisë dhe besimit në mjedisin e Cloud Computing nga një qasje e vlerësueshme, metoda e qasjes së vrojtimit dhe analizimit e sugjeruar në këtë dokument është hapi i parë drejt analizimit të çështjeve të privatësisë, sigurisë dhe besimit,

(b) zhvillimi i një vlerësimi të plotë të sigurisë, të privatësisë, besimit dhe kornizës së menaxhimit si pjesë e shërbimeve Cloud Computing për të përmbushur kërkesat e sigurisë; dhe

(c) vendosjen e kornizës në mjediset reale Cloud Computing.

Cloud Computing është duke futur shumë ndryshime të mëdha në stilin e jetës dhe mënyrën e punës së njerëzve kohët e fundit për përfitimet e tij të shumta. Sidoqoftë, siguria e Cloud Computing është gjithmonë në qendër të vëmendjes të përdoruesve të shumtë të mundshëm në Cloud, dhe një pengesë e madhe për aplikimet e tij të përhapura.

Në këtë rast, për të lehtësuar klientët për të kuptuar status quo-në e sigurisë në Cloud Computing dhe për të kontribuar në disa përpjekje për të përmirësuar nivelin e sigurisë në Cloud Computing, ne vëzhguam modelet ekzistuese të njohura të sigurisë të Cloud Computing, p.sh. modeli me përdorim të shumëfishtë, modeli me akumulim rreziku, modeli kub i Cloud Computing dhe si përmbledhje rreziqet kryesore të sigurisë në Cloud Computing që rrjedhin nga organizata të ndryshme. Më në fund, ne paraqesim disa strategji sigurie nga perspektiva e ndërtimit, operimit dhe reagimit të incidentit të sigurisë për të lehtësuar çështjet e zakonshme të sigurisë në Cloud Computing [26].

Cloud Computing është një lloj paradigme informatike që mund të aksesojë në mënyrë të leverdisshme një grup dinamik dhe publik të konfigurueshëm të burimeve informatike (p.sh. serveri, hapësira ruajtëse e të dhënave, rrjeti, aplikacioni dhe shërbimet përkatëse), i siguruar dhe publikuar me shpejtësi dhe sipas kërkesës me më pak menaxhim dhe ndërhyrje.

Sidoqoftë, përhapja e Cloud Computing në një masë të madhe është bllokuar nga siguria e tij. Për të kontribuar disa përpjekje për të përmirësuar sigurinë e Cloud Computing, ne vëzhguam modelet kryesore ekzistuese të sigurisë në Cloud Computing, dhe përmblodhëm rreziqet kryesore të sigurisë në Cloud Computing nga organizata të ndryshme. Në fund, u dhanë disa strategji sigurie kundër këtyre çështjeve të zakonshme të sigurisë në Cloud Computing. Në të ardhmen, ne do t'i përmbushim këto strategji sigurie me teknologji dhe mënyra të menaxhimit.

Evolucioni i Cloud Computing ka revolucionarizuar mënyrën se si informatika është përhumbur dhe është përdorur në infrastrukturën e largët të palëve të treta. Tani është e mundur të provohen ide të reja mbi Cloud-in me kosto fillestare zero ose shumë të ulëta. Cloud Computing është tërheqëse për kompanitë dhe organizatat pasi eliminon kërkesën që ata të planifikojnë përpara për sigurimin e infrastrukturës, dhe i lejon ata të fillojnë me burime të vogla dhe të rriten gradualisht me rritjen e kërkesës për shërbime [27].

Ekzistojnë sfida në adaptimin e cloud computing; por me pengesa, ne kemi mundësi për hulumtime në disa aspekte të Cloud Computing. Një nga çështjet kryesore është siguria e të dhënave dhe privatësia e informacionit të ruajtur dhe përpunuar në sistemet e ofruesit të shërbimit cloud. Në këtë aspekt, janë inspektuar disa punë kërkimore mbi Cloud Computing që lidhen me sfidat e sigurisë dhe çështjet e privatësisë.

Qëllimi kryesor i këtij dokumenti është të sigurojë një kuptim më të mirë të sfidave të sigurisë në Cloud Computing dhe të identifikojë qasjet dhe zgjidhjet të cilat janë propozuar dhe miratuar nga industria e shërbimit cloud.

Revolucioni në Cloud Computing ka ofruar mundësi për kërkime shkencore në të gjitha aspektet e cloud computing. Në këtë kuadër janë paraqitur pesë karakteristikat thelbësore të Cloud Computing, tre modelet e shërbimeve Cloud dhe katër modelet e shpërndarjes në Cloud.

Hulumtimi në hapësirën e sigurt të ruajtjes së të dhënave në Cloud përbëhet nga fakti që të dhënat e përdoruesve mund të mbahen në disa vende ose për tepricë/për tolerancë ndaj gabimeve, ose për shkak se shërbimi sigurohet përmes një zinxhiri të ofruesve të shërbimeve. U exploruan masat e sigurisë të miratuara nga ofruesi më i madh i shërbimeve cloud (shërbimet e Web të Amazon ose AWS) duke përfshirë sigurinë e tyre të infrastrukturës dhe praktikat më të mira të sigurisë të ndjekura nga AWS.

Cloud Computing është bërë një pjesë e rëndësishme në tregun konkurrues sot. Ofrues të ndryshëm të shërbimeve Cloud Computing janë të disponueshëm me shërbimet e tyre në mjedisin Cloud. Teknikat e miratuara nga ofrues të ndryshëm për të arritur sigurinë janë të natyrave të ndryshme. Analizimi dhe matja e një shërbimi të veçantë bazuar në vetitë e tij të sigurisë është një sfidë më vete [28].

Ky rast paraqet një matje të tillë duke përdorur një model besimi. Një model besimi mat fuqinë e sigurisë dhe llogarit një vlerë të besimit. Një vlerë besimi përfshin parametra të ndryshëm që janë dimensionet e nevojshme përgjatë të cilave mund të matet siguria e shërbimeve Cloud. Sfidat e shërbimit CSA (Aleanca e Sherbimit Cloud - Cloud Service Alliance) përdoren për të vlerësuar sigurinë e një shërbimi dhe vlefshmërinë e modelit. Përshtatshmëria e modelit verifikohet gjithashtu duke vlerësuar vlerën e besimit për shërbimet ekzistuese në Cloud. Modeli i besimit vepron si një pikë referimi dhe renditjeje për të matur sigurinë në një mjedis Cloud Computing.

Vlerësimi i bazuar në besim propozohet në formën e modelit të besimit. Vlera e besimit është rezultati i modelit të besimit që mat fuqinë e sigurisë. Modeli i besimit mund të përdoret në mënyrë efektive nga përdoruesit për të zgjedhur një shërbim të veçantë. Mund të përdoret gjithashtu nga ofruesit si një pikë referimi për të gjetur mangësitë dhe fushat e përmirësimit të një shërbimi cloud ose aplikacioneve përkatëse. Modeli i besimit mund të integrohet me shërbimet Cloud dhe përshkrimet e tyre si menaxher i shërbimit Cloud. Menaxheri i shërbimit Cloud ruan sasinë e vlerës së besimit të ofruesve të regjistruar të reve dhe shërbimeve të tyre. Masat e vlerës së besimit mund të përdoren nga përdoruesit për të zgjedhur një shërbim në mënyrë globale.

Kërcënimet rrezikojnë disa kërkesa themelore të sigurisë në një platform Cloud. Këto kërcënime zakonisht përbëjnë shkelje të privatësisë, rrjedhje të të dhënave dhe qasje të paautorizuar të të dhënave në shtresa të ndryshme të reve. Në këtë rast paraqitet një model i ri klasifikimi, me shumë nivele të sulmeve të ndryshme të sigurisë, përgjatë shërbimeve

të ndryshme Cloud në secilën shtresë. Ai gjithashtu identifikon llojet e sulmeve dhe nivelet e rrezikut të shoqëruara me shërbime të ndryshme Cloud në këto shtresa [29].

Rreziqet renditen si të ulta, të mesme dhe të larta. Intensiteti i këtyre niveleve të rrezikut varet nga pozicioni i shtresave të Cloud-it. Sulmet bëhen më të ashpra për shtresat e ulëta ku përfshihen infrastruktura dhe platforma. Intensiteti i këtyre niveleve të rrezikut shoqërohet gjithashtu me kërkesat e sigurisë së kriptimit të të dhënave, shumë-përdorues, privatësisë së të dhënave, vërtetimit dhe autorizimit për shërbime të ndryshme në Cloud. Modeli i klasifikimit në shumë nivele çon në sigurimin e kontratës dinamike të sigurisë për secilën shtresë cloud që vendos në mënyrë dinamike në lidhje me kërkesat e sigurisë për konsumatorin dhe ofruesin e platformave Cloud.

Një klasifikim i ri në shumë nivele i shqetësimeve të sigurisë në Cloud Computing duke theksuar efektin e sulmeve të ndryshme të sigurisë në secilën shtresë të Cloud është paraqitur. Ky klasifikim me shumë nivele siguron një dimension të ri për të adresuar shqetësimet e sigurisë në nivele të shumëfishta dhe minimizimin e efekteve të tyre.

Niveli i ashpërsisë së sulmit vlerësohet gjithashtu si i ulët, i mesëm dhe i lartë për çështje të ndryshme të sigurisë. Kërkesat e sigurisë për shërbime të ndryshme në Cloud përshkruhen gjithashtu për llogaritjen e sigurt në Cloud. Këto kërkesa të sigurisë përfshijnë kriptimin e të dhënave, shumë-përdorues, privatësinë e të dhënave, vërtetimin dhe autorizimin. Këto kërkesa të sigurisë janë të lidhura me shërbime të ndryshme Cloud për të arritur integritetin dhe koherencën në sistemin Cloud.

Paraqitet një koncept i ri i kontratës dinamike të sigurisë për të përcaktuar nivelin e rrezikut dhe llojin e sigurisë që kërkohet për secilin shërbim në shtresa të ndryshme Cloud për një konsumator cloud dhe ofruesin e shërbimit Cloud.

Trendi i Cloud Computing është në rritje të shpejtë që ka një lidhje teknologjike me Grid Computing, Utility Computing, Distributed Computing. Ofruesit e shërbimeve Cloud si Amazon IBM, Google's Application, Microsoft Azure etj. u ofrojnë përdoruesve zhvillimin e aplikacioneve në mjedisin cloud dhe për t'i aksesuar ato nga kudo ne botë [30].

Të dhënat në Cloud ruhen dhe aksesohen në një server në distancë me ndihmën e shërbimeve të ofruara nga ofruesit e shërbimeve Cloud. Ofrimi i sigurisë është një shqetësim i madh pasi të dhënat transmetohen në serverin në distanceë përmes një kanali transmetimi (në këtë rast është Interneti). Para se të implementohet Cloud Computing në një organizatë, së pari duhet të adresohen sfidat e sigurisë. Ne nxjerrim në pah sfidat e sigurisë në lidhje me të dhënat në mjedisin e bazuar në Cloud dhe zgjidhjet për të tejkaluar këtë problem.

Edhe pse Cloud Computing është teknologji e re në zhvillim që paraqet një numër të kënaqshëm përfitimesh për përdoruesit, ajo përballet me shumë sfida të sigurisë. Në këtë rast sfidat dhe zgjidhjet e sigurisë së të dhënave janë dhënë për këto platforma si dhe për

të kapërcyer rrezikun e përfshirë në Cloud Computing. Në të ardhmen mund të zhvillohen standarde konkrete për sigurinë në Cloud Computing.

Për të siguruar një hyrje të sigurt të të dhënave në cloud, teknikat e përparuara të enkriptimit mund të përdoren për ruajtjen dhe rigjenerimin e të dhënave nga Cloud. Gjithashtu teknikat e duhura të menaxhimit të çelësave mund të përdoren për të shpërndarë çelësin tek përdoruesit e Cloud, në mënyrë që vetëm personat e autorizuar të mund të hyjnë në të dhëna.

Në këtë rast synojmë të zbulojmë praktikat më të mira të menaxhimit të një zhvillimi të ri të teknologjisë siç është rasti i Cloud computing. Menaxhimi i një mjedisi të tillë varet shumë nga marrëdhënia e besimit midis ofruesve të shërbimeve Cloud dhe klientëve të tyre (dhe / ose bizneseve të tjera). Ky besim nuk varet vetëm nga mjetet më të fundit teknologjike, por gjithashtu varet edhe nga strategjia e menaxhimit në një mjedis kaq kritik [31].

Për të arritur këtë objektiv, u krye një studim në lidhje me pranueshmërinë e shërbimeve cloud, e cila ka rezultuar në tre seksione kryesore. Këto ishin: siguria, mbrojtja e të dhënave dhe etika në mjedisin kompjuterik në Cloud. Madhësia e shembullit ishte 441 ku rezultoi në një marrëdhënie shumë të rëndësishme midis etikës dhe sigurisë, si dhe etikës dhe mbrojtjes së të dhënave të cilat janë dy motivacionet kryesore për çdo biznes për t'u bashkuar në Cloud. Bazuar në këtë studim, u përshkrua një udhëzues për menaxhimin e Cloud Computing për të mirëmbajtur këto tre çështje. Dhjetë hapa u propozuan për të mbrojtur shërbimet Cloud nga sjelljet e mundshme joetike, si dhe për të mbrojtur sistemet nga thyerrja e mundshme e sigurisë.

Në këtë studim u hetua marrëdhënia e mirëbesimit në mjedisin Cloud Computing. Mbrojtja e të dhënave, siguria dhe etika ishin variabli më i rëndësishëm në studimin e kryer. Marrëdhënia e besimit do të ishte faktori kryesor para se të pranohet Cloud Computing nga ndërmarrjet e vogla dhe të mesme në përgjithësi dhe për ndërmarrjet ndërkombëtare në veçanti.

Analiza e vëzhgimit dhe e të dhënave u diskutua ku rezultatet tregojnë lidhje të forta midis mbrojtjes së të dhënave, sigurisë dhe etikës në mjedisin kompjuterik në Cloud. Si rezultat i analizës së vëzhgimit, ky punim gjithashtu propozon një udhëzues menaxherial IT të mjedisit teknik të shërbimit Cloud. Ky udhëzues propozohet në një formë hapash drejt menaxhimit të profesionistëve të IT (problemet e ndërgjegjësimit të njerëzve) si dhe menaxhimit të stafit të IT në një mjedis teknik si Cloud Computing për të shmangur çdo shkelje të mundshme të sigurisë dhe / ose humbjes së të dhënave që drejtohen kryesisht nga sjellje joetike. Udhëzimi i propozuar po bëhet një domosdoshmëri për shkak të mjedisit të ri Cloud Computing dhe globalizimit të IT. Udhëzuesi paraqitet në një formë të tre kritereve kryesore, i cili është përcaktuar në dhjetë nën kritere (hapa) të ndryshëm për të arritur sigurinë dhe mbrojtjen e të dhënave.

Rritja e kërkesave të klientëve, analiza e të dhënave të mëdha dhe presionet mbi kohën e reagimit, kostot e larta të platformave të rrjetit i shtynë kompanitë të migrojnë në Cloud

Computing duke ofruar shërbime të IT të vendosura/hostuara në internet. Rritja e përdoruesve të Cloud dhe ndërveprimet e tyre me infrastrukturën Cloud rrit rrezikun e defekteve të burimeve. Një problem i tillë mund të çojë në një reputacion të keq të mjedisit Cloud, i cili ngadalëson evolucionin e kësaj paradigme. Arkitektura dinamike dhe sistemi kompleks i Cloud duhet të merren parasysh. Në fakt, kjo paradigmë Cloud kërkon që mbrojtja dhe sigurimi i burimeve të jenë efektive, transparente dhe pa ndërhyrje të jashtme [32].

Kështu, është thelbësore përdorimi i aspekteve themelore të llogaritjes autonome në cloud për t'u marrë me vet-aktivizimin e sigurisë në cloud. Shkalla e lartë e përputhjes midis sistemeve të llogaritjes autonome dhe sistemeve me shumë agjentë lejojnë krijimin e një arkitekture cloud inteligjente që mbështet aspektet autonome. Prandaj, propozohet një kornizë bashkëpunuese e bazuar në sistemin e zbulimit hibrid të ndërhyrjeve (Hy -IDS), Agjentët celularë dhe Firewall, të cilat lejojnë të zbulojnë sulmet e brendshme dhe të jashtme me saktësi të lartë të zbulimit në mjedisin Cloud. Në këtë rast, propozohet një kornizë Cloud Computing që ofron sigurinë e hyrjes, lehtësinë e menaxhimit të burimeve duke përdorur agjentët mobil dhe disponueshmërinë e shërbimit në një strukturë të besueshme me kosto më të ulët.

Në këtë paragraf, është propozuar një kontribut i ri për zbulimin e ndërhyrjeve për të siguruar arkitekturën e cloud computing kundër kërcënimeve të brendshme. Hy-IDS bazohet në agjentë mobile fleksibël dhe të ndërveprueshëm, të përdorur për të rimarrë dhe analizuar të dhëna të dëmshme, për të gjeneruar dhe vendosur veprime të reja të përgjigjeve. Xen bazohet në firewall-in e vet virtual që kontrollon hyrjen në instancat që përdorin Script-e Shell. Agjentët bashkëpunues të drejtuar nga interesi e bëjnë sistemin më të pa ndikueshëm ndaj difekteve.

Për më tepër, autonomia e dhënë agjentëve i bën detyrat e administrimit të oficerit të sigurisë shumë më të lehta. Sidoqoftë, fleksibiliteti, përshtatshmëria dhe shpërndarja janë tiparet kryesore që adresohen për të ndërtuar një arkitekturë të përshtatshme që mund të jetë e dobishme për zbulimin e sulmeve komplekse dhe të shpërndara. Eksperimentet e kryera mbi arkitekturën kanë prodhuar rezultate që tregojnë efektivitetin e kornizës sonë.

Gjatë shpërthimit të pandemisë të shkaktuar nga koronavirusi i ri COVID-19, kompanitë dhe institucionet kanë udhëzuar punonjësit e tyre të punojnë nga shtëpia si një masë paraprake për të zvogëluar rrezikun e infektimit. Megjithatë, punonjësit kanë qenë të ekspozuar ndaj rreziqeve të ndryshme të sigurisë për shkak të punës nga shtëpia.

Për më tepër, përhapja e shpejtë globale e COVID-19 ka rritur vëllimin e të dhënave të gjeneruara nga burime të ndryshme. Puna nga shtëpia varet kryesisht nga aplikacionet në Cloud Computing (CC) që ndihmojnë punonjësit të përmbushin me efikasitet detyrat e tyre. Mjedisi i Cloud Computing (CCE) është një hero i panjohur në krizën pandemike COVID-19. Ai përbëhet nga praktika të shpejta për shërbimet që pasqyrojnë trendin e aplikacioneve të zhvilluara me shpejtësi për mirëmbajtjen e të dhënave [1].

Përkundër rritjes së përdorimit të aplikacioneve Cloud Computing, ekziston një sfidë e vazhdueshme kërkimore në fushat e Mjedisit Cloud Computing (CCE) në lidhje me të dhënat, garantimin e sigurisë dhe disponueshmërinë e aplikacioneve Cloud Computing. Ky punim, është i pari i ketij lloji që shpjegon hollësisht ndikimin e pandemisë COVID-19 në Mjedisin Cloud Computing. Për më tepër, ky dokument thekson gjithashtu rreziqet e sigurisë së punës nga shtëpia gjatë pandemisë COVID-19.

Varësia nga aplikimet Cloud Computing dhe teknologjitë e tjera është rritur në mënyrë dramatike për shkak të situatës aktuale të pandemisë COVID-19. Padyshim, kjo krizë pandemike ka ndikuar pothuajse në të gjithë sektorët, të tilla si turizmi, kujdesi shëndetësor, arsimi dhe të tjerë. Për më tepër, kriza COVID-19 mund të shkaktojë një ndryshim të përhershëm drejt punës nga shtëpia si masa paraprake për kufizimin e virusit.

Përhapja e shpejtë globale e COVID-19 ka rritur gjithashtu vëllimin e të dhënave të gjeneruara nga burime të ndryshme. Rritja e vëllimit të të dhënave ka nevojë për sisteme shtesë të ruajtjes së të dhënave, mekanizma ruajtjeje të të dhënave, mjedise të reja dhe teknologji të reja, të gjitha këto krijojnë një sfidë kritike. Në këtë rast, jemi përpjekur të tregojmë qartë ndikimet aktuale dhe të mundshme të krizës COVID-19 në Mjediset Cloud Computing dhe teknologjitë e tjera për shkak të rritjes së papritur të punës nga shtëpia. Për më tepër, ky punim analizon rreziqet e sigurisë për të punuar nga shtëpia.

Nga perspektiva e sigurisë, situata aktuale mund të ekspozojë si Mjediset Cloud Computing ashtu edhe përdoruesit e saj ndaj llojeve të ndryshme të sulmeve për shkak të mungesës së gatishmërisë për t'u përballur me një situatë kaq të papritur. Për Mjediset Cloud Computing, sulme të tilla si Mohimi Ekonomik i Shërbimit (ang. Economical Denial of Service-EDoS), mund të jenë të spikatura gjatë periudhës së COVID-19. Përdoruesit mund të jenë të prekshëm ndaj llojeve të ndryshme të sulmeve pasi ato operojnë aplikacione të pakuptueshme të Internetit në pajisjet e tyre shtëpiake, të cilat mund të mos përditësohen ose rregullohen me politikat e fundit të sigurisë. Prandaj, punonjësit në shtëpi mund të bëhen shënjestër e sulmuesve për të vjedhur (kopjuar) sasi të mëdha të të dhënave.

Si rezultat, ekziston nevoja për të adresuar rreziqet e sigurisë me të cilat përballen Mjediset Cloud Computing dhe përdoruesit, si dhe për të rritur ndërgjegjësimin e përdoruesve në lidhje me kërcënimet e përdorimit të pajisjeve të pasigurta për të hyrë në internet kur ata janë duke punuar nga shtëpia.

2 SIGURIA KOMPJUTERIKE NË CLOUD COMPUTING

Siguria kompjuterike përfshin tre shtylla kryesore të cilat janë tepër të njohura si KID: Konfidencialiteti, Integriteti dhe Disponueshmëria (ang. Confidentiality, Integrity and Availability – CIA). Konfidencialiteti përfshin fshehjen e një informacioni të rëndësishëm nga palët e paautorizuara. Gjithsej janë tre mekanizma që ndihmojnë në zbatimin e konfidencialitetit. E para është kriptografia, e cila konsiston në fshehjen e një informacioni të thjeshtë, duke përdorur transformimet matematikore. E dyta është "kontrolli i hyrjes", e cila përcakton palët e lejuara për të patur akses në pjesë të ndryshme të sistemit apo të informacionit. E treta është "autorizimi", e cila përcakton se çfarë veprimesh lejohet të bëjë secila palë e autorizuar me një pjesë të të dhënave [33], [34], [35].

Shtylla e integritetit nënkupton që një sistem dhe të dhënat e tij nuk kanë mundur të ndryshohen nga palët e paautorizuara. Mekanizmat e mbrojtjes së integritetit përpiqen të ndalojnë që një ndryshim apo ndërhyrje të ndodhë ose ta zbulojnë atë pasi të ketë ndodhur.

Shtylla e tretë, disponushmëria i referohet një tipari që një sistem apo të dhënat e tij duhet të kenë në dispozicion, në lidhje me palët e autorizuara, në një kohë të caktuar. Ekzistojnë dhe koncepte të tjera të rëndësishme si "autenticiteti", që është një tipar i të dhënave dhe transaksioneve, dhe gjithashtu "jo-mohimi", që është siguria se një palë nuk mund të mohojë një transaksion, deklaratë apo nënshkrim. Proceset e implementimit dhe projektimit të software-ve, firmware-ve dhe hardware-ve, mund të kenë gabime të cilat mund të shfrytëzohen nga një sulmues.

Në sigurinë kompjuterike i cilësojmë këto gabime si dobësi. Sistemet kompjuterike gjithmonë do të përmbajnë dobësi , sepse ato janë të projektuara, të implementuara dhe të testuara nga njerëzit në fund të fundit. Kështu që një dobësi apo një gabim është një kërcënim për sigurinë.

Sfidat e sigurisë në cloud computing nuk kanë shumë ndryshim nga ato të sitemeve tradicionalë, përveç se në rastin e mjedisit cloud kemi një përkeqësim të numrit të dobësive dhe impaktit ndaj sulmeve.

E ndërsa një mjedis cloud përfshin shtresat si aplikimin, sistemin e operimit, arkitekturën dhe rrjetin, një sulmues përdor disa mënyra për kompromentimin e sigurisë në një shërbim cloud.

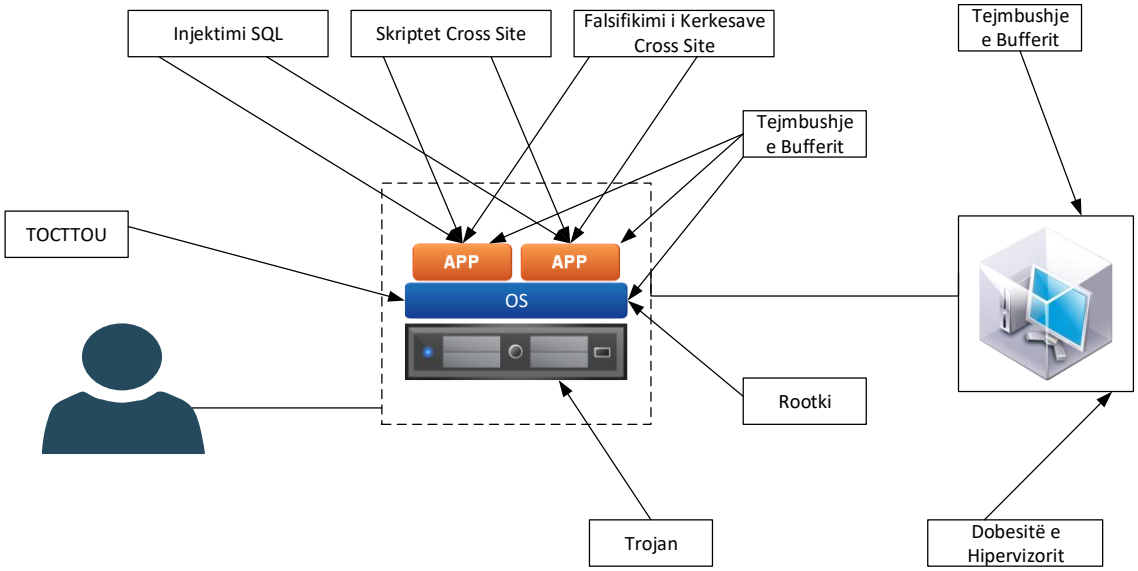

Figura 2-1 Dobësitë e sigurisë në Cloud Computing

2.1 DOBËSITË DHE SULMET

Ashtu sikurse dhe e përmendëm, shërbimet e cloud computing mund të disponojnë dobësi në të gjitha shtresat e strukturës së saj [72]. Figura 2-1 tregon dobësitë e sigurisë në cloud computing duke u bazuar në shtresën e strukturës ku ato mund të ndodhin.

2.1.1 Shtresa e Aplikimit

Në nivelin e aplikacionit, një aplikacion cloud mund të ketë shumë dobësi , të cilat lejojnë që një kundërshtar të kompromentojë një sistem. Shumë nga aplikacionet cloud janë "të bazuara në web" dhe kanë dobësitë tipike të internetit ashtu sikurse është "higjena e të dhënave të përdoruesit" i pamjaftueshëm, i cili lejon sulmet si injektimi SQL [73]. Ky i fundit lejon që një sulmues të injektojë kodin në një motor skriptues që do të ekzekutohet nga një interpretues i kontrolluesit SQL. Për të kuptuar këtë dobësi, së pari marrim parasysh një skenar tipik të një përdoruesi që bashkëvepron me një server web-i që pret një aplikacion web që ruan të dhënat e tij në një bazë të dhënash. Zakonisht kodi për aplikacionin web dhe bazën e të dhënave ruhen në "makina" të ndryshme. Në një skenar tipik, një aplikacion web i vendosur nga një shitës me pakicë librash (p.sh. Amazon) lejon përdoruesit të kërkojnë libra bazuar në autorin, titullin, botuesin, etj. I gjithë katalogu i librit mbahet në një bazë të dhënash dhe aplikacioni përdor pyetje SQL për të marrë detajet e librit. Supozoni se një përdorues kërkon të gjithë librat e botuar nga Wiley. Motori i skriptit të webit në anën e aplikacionit në internet pranon, manipulon dhe vepron mbi këto të dhëna duke i interpretuar ato si të dhëna të furnizuara nga përdoruesi. Motori i skriptit web më pas ndërton një komandë SQL që është një përzierje e udhëzimeve të shkruara nga programuesi dhe e dhëna e përdoruesit. Kjo pyetje bën që baza e të dhënave të kontrollojë çdo rresht brenda tabelës së librave, të nxjerrë secilin nga rekordet ku kolona e botuesit ka vlerën "Wiley" dhe të kthejë grupin e të gjitha këtyre rekordeve. Ky

grup të dhënash përpunohet nga aplikacioni web dhe i paraqitet përdoruesit brenda një faqe HTML. Tani, marrim parasysh një skenar në të cilin një sulmues mund të shkaktojë një thyerje në interpretimin e të dhënave dhe të dalë nga konteksti i tyre. Në këtë skenar, një komandë të re SQL modifikon pyetjen që një programues synon të zbatojë tek aplikacioni. Ekziston një ndarje e qartë se si interpretohet hyrja në kufirin midis gjuhës të skriptit web dhe interpretuesit të kontrolluesit SQL. Viza dyshe (- -) në hyrjen e sulmuesit i thotë interpretuesit të kontrolluesit që të injorojë pjesën e mbetur të linjës edhe pse mund të ketë komanda të tjera të përfshira nga programuesi.

Në këtë rast, pasoja e këtij sulmi është fshirja e të gjithë tabelës "books" nga baza e të dhënave siç ilustrohet në Figurën 2-2. Dobësitë e tjera të aplikacioneve të bazuara në web përfshijnë skripte cross site(ang. Cross Site Scripting - XSS) [74] dhe falsifikim të kërkesave cross site [75]. Për më tepër, kodi i aplikacionit mund të jetë i prekshëm nga injektimi i kodit në distancë përmes tejmbushjes së buffer-it[76] nëse është i shkruar në një gjuhë programimi që nuk verifikon kufijtë e vargjeve, të tilla si C ose C ++. Aplikacioni mund të jetë gjithashtu i prekshëm nga zbulimi i të dhënave nëse nuk përdor kriptografi për të ruajtur konfidencialitetin e tyre. Kodi i aplikimit mund të jetë gjithashtu i prekshëm ndaj kompromentimit nëse vërtetimi i tij dhe procedurat e kontrollit të aksesit kanë të meta. Një burim tjetër i cënueshmërisë në shtresën e aplikacionit janë funksionet e gabuara të Ndërfaqes të Programuar të Aplikacionit (ang. Application Programming Interface - API).

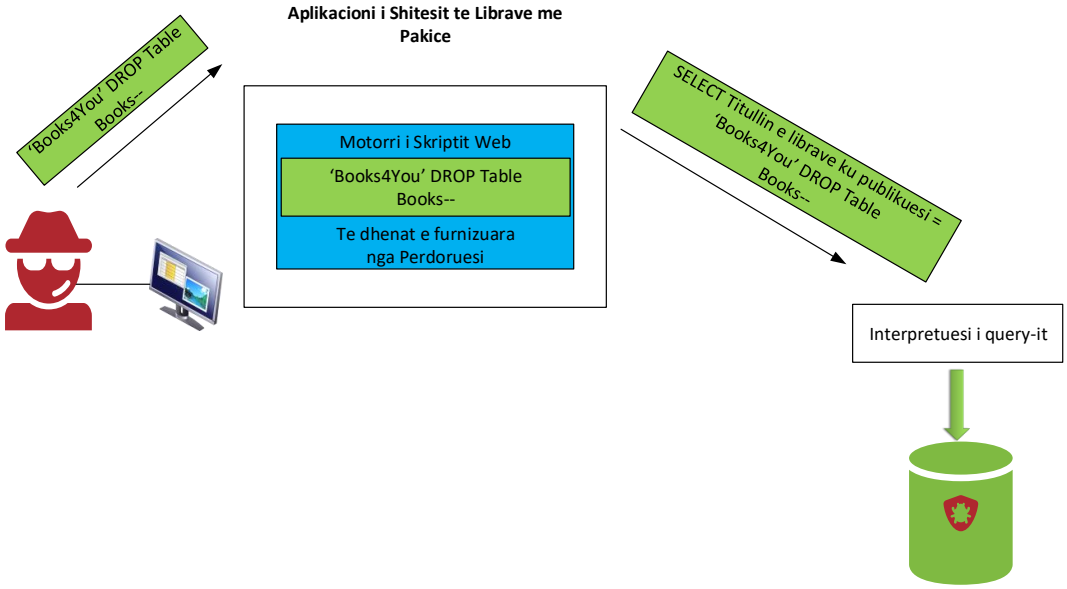

Figura 2-2 Dobësitë e injektimit SQL

2.1.2 Shtresa e Sistemit të Operimit

Dobësitë në nivelin e sistemit operativ gjithashtu mund të rrezikojnë platformat Cloud Security. Sistemi operativ (OS), si çdo pjesë e softwarit e shkruar në C / C ++, është e

prekshme nga dobësitë e tejmbushjes së buffer-it. Sistemet operative janë gjithashtu të ndjeshme ndaj dobësive që lidhen me kushtet e përdorimit, siç është cënueshmëria nga koha e kontrollit deri në kohën e përdorimit (ang. Time to Check To Time of Use - TOCTTOU). Cënueshmëria TOCTTOU shkaktohet nga ndryshimet në një sistem që ndodhin midis kontrollit të një gjendjeje (siç është p.sh. siguria e kredencialeve) dhe përdorimit të rezultateve të këtij kontrolli. TOCTTOU përbëhet nga një fazë kontrolli, e cila përcakton një parakusht të pandryshueshëm (p.sh., lejen e aksesit), dhe një fazë përdorimi, e cila vepron mbi objektin duke supozuar se parakushti i pandryshueshmërisë është akoma i vlefshëm. TOCTTOU zakonisht ndodh në proceset SETUID, të cilat kanë të drejta administratori, por mund të thirren nga përdorues të pa privilegjuar, në mënyrë që procesi të kryejë veprime në emër të përdoruesit. Për shembull, një program printimi është zakonisht SETUID-root për të pasur akses në pajisje, e cila është një veprim që kërkon të drejta administrative. Duke ekzekutuar sikur përdoruesi të kishte privilegjet root, programi i printerit zbulon nëse një përdorues që thirret në ekzekutimin e tij ka leje për të lexuar dhe shtypur një skedar të caktuar duke përdorur funksionin e hyrjes nga sistemi operativ. Një shembull klasik i TOCTTOU jepet nga sekuenca e thirrjeve të sistemit.

Proceset ekzekutohen nga OS, pasi ai cakton një proces në të njëjtën kohë për CPU. Kështu, një proces nuk ekzekutohet në CPU nga fillimi në fund pa u ndërprerë. CPU ekzekuton një proces për një periudhë të caktuar kohe dhe më pas OS bën pauzë procesin aktual dhe rifillon ekzekutimin e një procesi të pezulluar. Supozoni se procesi kodi i të cilit jepet në Figurën 2-3 është pezulluar para *fopen (),* është ekzekutuar pasi fitohet akesimi për të hyrë në dosjen *file/home/bob/symlink*. Pastaj supozoni se procesi i një kundërshtari është zgjedhur për ekzekutim dhe ndryshon lidhjen simbolike për të treguar dosjen e fjalëkalimeve */etc/passwords*.

Kur procesi i parë ekzekutohet përsëri, ai do të hapë një dosjen fjalekalimet (*passwords*) që nuk kishte leje për ta bërë. Sistemet operative janë gjithashtu të prekshme nga instalimet keqdashëse. Zgjerimet e Kernel-it, veçanërisht aplikacionet e pjesëve përbërëse, përbëjnë aktualisht një pjesë të madhe të kodit Kernel (afërsisht 70% në Linux dhe një përqindje më e madhe në Windows) [77].

Shumica e këtyre zgjerimeve janë “beninje” dhe lejojnë sistemin të komunikojë me një numër në rritje të pajisjeve të ndryshme I/O pa nevojën e rindezjes ose rikompilimit të OS. Sidoqoftë, ato përbëjnë një kërcënim për sistemin sepse funksionojnë me një nivel të lartë të drejtash dhe mund të jenë të prekshme.

Zbulimi i zgjerimeve me qëllim të keq është shumë sfidues dhe shumica e propozimeve në literaturë nuk janë miratuar nga sistemet operative bashkëkohore [78], [79], [80].

```
if (access ("/home/test/symlink", R_OK | W_OK) != -1)
  {
    //Linku Simbolik mund te ndryshoje ketu
    f = fopen ("/home/test/symlink", "rw");
  ...

  }
```

Figura 2-3 Dobësitë e TOCTTOU

2.1.3 Hipervizori, Storage, Hardware dhe Rrjeti

Meqenëse cloud computing varet nga teknologjia e virtualizimit, dobësitë në imazhet e makinës virtuale (VM) gjithashtu mund të rrezikojnë sigurinë. Çdo dobësi ose e metë në kodin kompleks të hipervizorit mund të rrezikojë izolimin midis makinave virtuale që ndodhen në të njëjtin server. Cloud computing është gjithashtu e ndjeshme ndaj defekteve në kodin që kryen lëvizjen e makinave virtuale midis serverave, fotografimi i makinës virtuale dhe kthimi mbrapa [81]. Këto dobësi mund të çojnë në kompromentime të integritetit, zbulimit të të dhënave dhe sulmeve të mohimit të shërbimit (DoS). Imazhet e makinave virtuale në publik mund të përmbajnë malware, ose kode të prekshëm. Ka disa dobësi referuar të dhënave që janë unike për cloud computing. Të dhënat mund të vendosen në vende të ndryshme që kanë ligje të ndryshme në lidhje me pronësinë e të dhënave [82].

Gjithashtu, zbulimi i të dhënave mund të ndodhë nëse të dhënat nuk pastrohen siç duhet nga hapësira sekondare kur zhvendosen ose fshihen [81]. Në shtresën e arkitekturës, ashtu si në një mjedis kompjuterik tradicional, hardware-i në cloud computing është e prekshme nga Trojan-e që prezantojnë funksionalitete me qëllim të demshëm në nivelin e hyrjes [83]. Në shtresën e rrjetit, cloud computing është gjithashtu e ndjeshme ndaj dobësive të gjetura në protokollet e rrjetit, zakonisht duke shkaktuar një sulm mohimi shërbimi (DoS) siç është rasti i TCPSYN flood, ku një kundërshtar dërgon më shumë paketa me kërkesë për lidhje (paketat SYN) sesa një server mund të përpunojë, dhe si pasojë e bën atë të padisponueshëm për klientët e ligjshëm [84].

Cloud computing është gjithashtu e ndjeshme ndaj përgjimit në rrjetet virtuale: një makinë virtuale me qëllim të keq mund të dëgjojë rrjetin virtual ose madje të përdorë mashtrime të Protokollit të Përzgjedhjes së Adresës (ang. Adress Resolution Protocol-ARP) për të ridrejtuar paketat nga dhe drejt makinave virtuale të tjera [85].

2.2 MEKANIZMAT E SIGURISË NË CLOUD

Ka shumë mekanizma sigurie që kur zbatohen në mjedisin cloud mund të ndihmojnë në zvogëlimin e disa prej dobësive të përshkruara në seksionin e mëparshëm. Më poshtë do

të diskutojmë disa prej tyre duke përfshirë mekanizmat për sigurinë e të dhënave dhe virtualizimit.

2.2.1 Siguria e të dhënave

Enkriptimi zakonisht përdoret për të mbrojtur konfidencialitetin e të dhënave cloud. Ai përfshin transformimin (kriptimin) e informacionit duke përdorur metoda matematikore dhe një çelës sekret, të quajtur çelës kriptimi. Informacioni i koduar mund të zbulohet palëve të autorizuara vetëm me përdorimin e një çelësi dekriptimi. Kriptimi parandalon që një kundërshtar të përgjojë të dhëna cloud të ndjeshme kur ato ruhen në një qendër të dhënash dhe në tranzit përmes rrjetit. Ekzistojnë dy lloje të teknikave të kriptimit: simetrike dhe asimetrike [86], [87].

- *Kriptografia simetrike* përdor çelësa identikë për të kriptuar dhe dekriptuar të dhënat, gjë që i bën algoritmet më pak komplekse sesa homologët e tyre asimetrik. Kështu, ata kanë performancë më të mirë sesa algoritmet e kriptografisë asimetrike, zakonisht 100 deri në 1000 herë më shpejt [87]. Niveli i sigurisë varet nga gjatësia e çelësit. Instituti i Standarteve dhe Teknologjisë në Amerikë (NIST) rekomandon 160–512 bit. Kriptografia simetrike zakonisht miratohet për enkriptimin në masë të të dhënave dhe zbatohet në protokollet si Siguria në Protokollin Internet (IPSec) dhe Siguria në Shtresën e Transportit (TLS). Një sfidë për kriptografinë simetrike është mënyra e shpërndarjes së sigurt të çelësave.
- *Kriptografia asimetrike* përdor dy çelësa të ndryshëm: një çelës privat për enkriptim dhe një çelës publik për dekriptim. Për shembull, supozoni se Klea dëshiron ti dërgojë një mesazh sekret Keltit duke përdorur kriptografinë asimetrike. Klea fillimisht enkripton mesazhin duke përdorur çelësin publik të Keltit, i cili është publik dhe i disponueshëm për këdo. Për shembull, Kelti mund ta bëjë çelësin e tij publik të disponueshëm në një direktori në organizatën e tij ose në një faqe në internet. Kelti gjithashtu ka një çelës privat të njohur vetëm për të, i cili është i ndryshëm nga çelësi i tij publik. Pavarësisht se janë të ndryshëm, këto çelësa janë të përputhshëm në funksion sepse Kelti do të përdorë çelësin e tij privat për të dëshifruar mesazhin e Kleas. Me fjalë të tjera, informacioni në tekst të thjeshtë që është i koduar me një çelës publik mund të deshifrohet vetëm me çelësin privat korrespondues. Kriptografia asimetrike përdoret për të zgjidhur sfidën e shpërndarjes së çelësave në kriptografinë simetrike dhe gjithashtu si një mekanizëm për të zbatuar nënshkrimet dixhitale.

2.2.2 Nënshkrimi dixhital

Nënshkrimi dixhital është një mënyrë që një palë të sigurojë vërtetësinë e një mesazhi. Nënshkrimet dixhitale duhet të arrijnë mos-mohimin; domethënë duhet të jetë e vështirë për një palë të falsifikojë një nënshkrim dixhital dhe të përdorë një nënshkrim të vlefshëm për një mesazh tjetër. Kriptografia asimetrike zakonisht përdoret si një mekanizëm i

nënshkrimit dixhital në mjediset cloud. Në kriptografinë e çelësit publik / privat, të dhënat e koduara me çelësin privat të dikujt mund të dëshifrohen vetëm me çelësin publik të atij personi. Pra, nëse për shembull, Kelti ka çelësin publik të Kleas dhe dëshiron nënshkrimin e saj dixhital të besuar në një dokument të dërguar në rrjet (një kanal zakonisht jo i besueshëm), ai mund të kërkojë nga Klea që të "nënshkruajë" ose të kriptojë të dhënat ose dokumentin me çelësin e saj privat. Nëse Kelti është në gjendje të dëshifrojë të dhënat me çelësin publik të Kleas, ai mund të jetë i sigurt se vetëm Klea mund ta kishte enkriptuar dokumentin, sepse vetëm ajo e njeh çelësin e saj privat. Tani le të shqyrtojmë një aplikacion tipik në internet në mjedisin cloud. SSL është një protokoll rrjeti që përdoret për të siguruar të dhëna ndërmjet dy nyjeve të rrjetit me enkriptim. Për të kuptuar rëndësinë e SSL për sigurinë e aplikacioneve në internet, merrni parasysh një skenar kur keni dashur të blini një libër nga Amazon. Ndërsa jeni duke kërkuar në site-in, web browser juaj dhe serveri Amazon janë të lidhur përmes protokollit standard TCP. Përmes kësaj lloji lidhjeje, të dhënat e shkëmbyera midis shfletuesit tuaj (d.m.th., artikujt që kërkohen) dhe serverit të Amazon (d.m.th., të dhënat në lidhje me artikujt e Amazon) nuk janë të koduara. Për shkak se ky shkëmbim nuk është i koduar, një kundërshtar që ndodhet në rrjetin tuaj lokal mund të përdorë programe të nuhatjes së rrjetit që shqyrtojnë të dhënat e papërpunuara në paketat e rrjetit të shkëmbyera midis jush. Për shembull, një kundërshtar mund të mësojë se përdoruesi i një nyjeje specifike është i interesuar për libra rreth Jul Çezarit. Duket se përdoruesi duhet të parandalojë që një kundërshtar të jetë në gjendje të "nuhasë" të dhënat e tij të ndjeshme si numrat e kartave të kreditit dhe informacionin e transportit. Një sfidë tjetër është që shfletuesi juaj nuk ka asnjë garanci që serveri me të cilin "po flet" është në të vërtetë Amazon.com. Për shembull, një përdorues mund të ketë shtypur Amazom.com gabimisht dhe mund të komunikojë me një browser jo real. Pra, përdoruesi gjithashtu do të duhet të jetë i sigurt se serveri që merr informacionin është në të vërtetë Amazon.com.

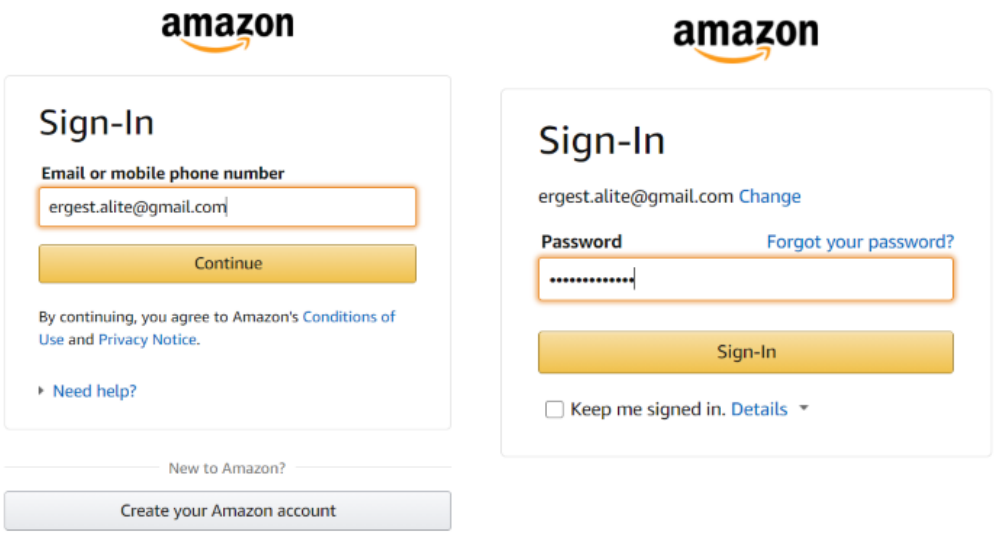

Figura 2-4 Shembull i autentikimit të sigurtë me SSL

Protokolli SSL përmbush të dyja nevojat duke përdorur metoda kriptografike për të fshehur atë që po dërgohet nga një kompjuter në tjetrin dhe duke përdorur teknika identifikimi që sigurojnë se shfletuesi me të cilin komunikon kompjuteri të jetë i besueshëm. Me fjalë të tjera, duke përdorur SSL për të blerë një libër nga Amazon, përdoruesi mund të jetë i sigurt se asnjë kundërshtar nuk do të zbulojë informacionin e kartës së tij të kreditit dhe se çdo informacion shkëmbehet ekskluzivisht me Amazon.com të vërtetë.

Siç tregohet në Figurën 2-4, kur një përdorues bën një transaksion financiar me Amazon.com, browser dhe serveri krijojnë një lidhje SSL nën HTTP (https). Vini re se si mbyllja bëhet jeshile duke treguar se është një lidhje e besuar. Gjithashtu vini re që lexon https dhe jo http. Kur përdoruesi shtyp butonin "login" ose "sign in" në serverat e-commerce (p.sh. Amazon), shfletuesi i tij dhe serveri do të krijojnë një lidhje SSL përmes një "handshake" dhe më pas një fazë pasuese. Në fazën e "handshake", browseri dhe serveri bien dakord për një algoritëm të veçantë të kriptimit dhe serveri i dërgon një çertifikatë klientit. Kjo çertifikatë është një pjesë e të dhënave të lëshuara nga një autoritet i besueshëm çertifikimi (ang, Certificate Authority - CA) që lidh një çelës publik kriptografik me një entitet të veçantë (p.sh., Amazon.com) dhe është krijuar për të legjitimuar që serveri është në të vërtetë ai që pretendon të jetë.

2.2.3 Hashing

Hashing përdoret për të gjeneruar një përfaqësim një-drejtimesh të pakthyeshëm të të dhënave të sigurisë [35], [84], [88]. Një hash shndërron një mesazh të thjeshtë teksti *m* në një kod hash me madhësi fikse, H(*m*), që zakonisht quhet hash. Një karakteristikë interesante e një funksioni hash është se dy mesazhe të ndryshme nuk mund të kenë të njëjtin hash. Gjithashtu, sapo një informacion të jetë bërë hashed, nuk ka asnjë mënyrë për ta kthyer atë, pasi nuk ka asnjë "çelës johash". Hashing mund të informojë nëse të dhënat e ruajtura në një qendër të dhënash ose në tranzit janë të kompromentuara [88]. Për shembull, mund të nxirret një kod hash me gjatësi fikse për disa të dhëna. Përmbledhja e mesazhit është zakonisht më e vogël se vetë mesazhi. Nëse një palë duhet të dërgojë mesazhin përmes rrjetit në një palë tjetër, ajo mund ti bashkëngjisë mesazhit përmbledhjen e tij. Pala marrëse verifikon integritetin e mesazhit duke aplikuar të njëjtin funksion hash në mesazh dhe duke verifikuar që "kuptimi i mesazhit" është i njëjtë me mesazhin. Nëse një kundërshtar ka ngatërruar të dhënat, përmbledhja e mesazhit do të ndryshojë.

2.2.4 Siguria e virtualizimit

Wang dhe Jiang prezantuan HyperSafe [89], një qasje që siguron integritetin e rrjedhës së kontrollit për hipervizorët. Kjo teknikë kyç faqet e kujtesës me mbrojtje nga ndryshimet dhe nuk lejon që ato të manipulohen gjatë kohës së ekzekutimit, gjë që mbron integritetin e kodit të hipervizorit. Santos [90] ka propozuar një qasje për një platformë të

besuar të cloud computing (ang. Trusted Cloud Computing Platform-TCCP) që mundëson infrastrukturën si një shërbim (IaaS), shërbime të tilla si Amazon EC2 për të siguruar një mjedis ekzekutimi në qark të mbyllur. Zhang [91] prezantoi PALM, një kornizë lëvizje të drejtpërdrejtë per makinat virtuale. Kjo strategji përbëhet nga tre module për privatësinë dhe mbrojtjen e integritetit të të dhënave të ndjeshme, të metadatave, si dhe vetë procesit të lëvizjes.

2.3 PRIVATËSIA DHE SIGURIA NË SHËRBIMET CLOUD STORAGE

Në ditët e sotme gjithnjë e më shumë kompanitë kanë miratuar marrjen e shërbimeve cloud publike për të ruajtur të dhënat e tyre (p.sh., Microsoft Skydrive dhe Dropbox), si dhe Amazon EC2 bashkë me MapReduce Framework, për të procesuar të dhënat e tyre. Rezultatet e sondazhit kanë treguar një rritje të qëndrueshme të adaptimit (marrjes) me shërbimet cloud, ku 75% e të anketuarve në 2013 përdorën platforma cloud krahasuar me 67% në 2012 [92]. Përdorimi i teknologjisë cloud do të jetë gjithashtu thelbësor në shpërndarjen e të dhënave në shumë organizata (p.sh., organizata qeveritare), të cilat do të jenë të dobishme për shumë aplikime kritike shoqërore, të tilla si mbrojtja e vendit, siguria kibernetike, kontrolli i përhapjes së sëmundjeve infektive (pandemitë) dhe ekonomia.

Situata pandemike e shkaktuar nga virusi Covid-19 tregoji se shërbimet dhe aplikacionet e ofruara nga ofruesit e shërbimeve cloud ishin jetësore për tejaklimin e kësaj situate si në aspektin shoqëror ashtu edhe në atë eknomik, ku puna nga shtëpia nuk do të ishte e mundur nëse nuk do të ekzistonin shërbimet cloud.

Sidoqoftë, çështjet kritike të konfidencialitetit të të dhënave [93], [94], [95], [96] pengojnë përvetësimin e gjerë të teknologjisë cloud, veçanërisht të cloud publike. Gjithashtu, është e rëndësishme që të dhënat e ruajtura dhe të ndara në platformat cloud të sigurohen nga aksesimi i paautorizuar. Kjo do të thotë se këto të dhëna duhet të ndahen në mënyrë selektive midis përdoruesve të ndryshëm, ndoshta brenda organizatave të ndryshme, bazuar në politikat e kontrollit të aksesimit. Kur zbatohet Kontrollet e Aksesit, është gjithashtu e rëndësishme të mbrohen informacionet e profilit të përdoruesve të autorizuar (p.sh., rolin dhe vendndodhjen e përdoruesit), përndryshe mund të çojë në përfundime në lidhje me përmbajtjen e të dhënave. Kjo sepse sistemet e përparuara të Kontrollit të Aksesit, siç është modeli tepër i njohur me bazë veçorinë [97], kërkojnë zbulimin e informacionit të sistemit të zbatimit në lidhje me përdoruesit tek Kontrolli i Aksesit.

Për më tepër, të dhënat në cloud mund të transferohen midis qendrave të të dhënave të cilat mund të jenë të vendosura në rajone të ndryshme (ose madje edhe vende), ku përdoruesit e cloud nuk kanë shumë informacion se ku ruhen dhe përpunohen të dhënat e tyre. Kështu, sigurimi i pajtueshmërisë së privatësisë gjatë veprimeve në ditët e sotme është një detyrë shumë sfiduese si për ofruesit e shërbimeve në cloud (CSP) ashtu edhe për klientët e tyre. Ekziston një nevojë e qartë për të zhvilluar teknika specifike për

sigurimin e të dhënave në cloud. Në vijim do të paraqesim një model të përgjithshëm të mbrojtjes së të dhënave cloud dhe më pas do të rishikojmë teknikat e mbrojtjes së tyre. Si përfundim do të pasqyrojmë disa shkaqe të tjera të mundshme të rrjedhjes së të dhënave në cloud.

2.3.1 Modelet e mbrojtjes së të dhënave në Cloud

Në cloud, ne vëzhgojmë dy karakteristikat e mëposhtme të rëndësishme që vendosin sfidat për zhvillimin e teknikave të mbrojtjes së të dhënave. Një shërbim cloud mund të sigurohet përmes një zinxhiri të ofruesve të shërbimeve [95]. Le të shënojmë ofruesin e shërbimeve direkte me S, duke patur parasysh që është një shërbim i drejtëpërdrejtë dhe kontraktorët e tij indirekt si S_1, S_2, Sn.

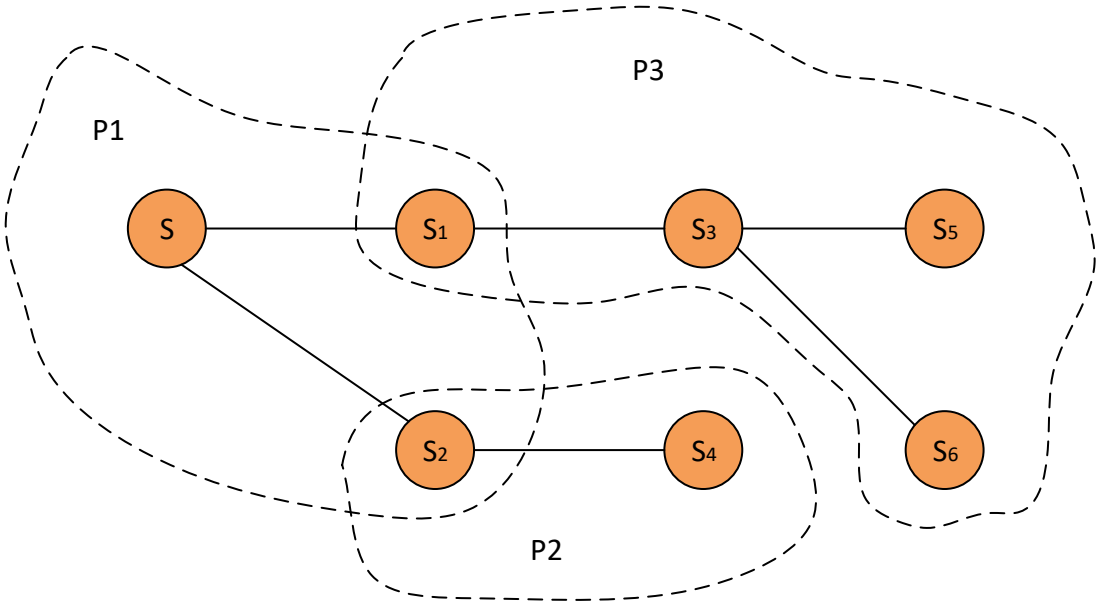

Figura 2-5 Shërbimi zinxhir në Cloud

Siç tregohet në Figurën 2-5, ofruesi direkt i shërbimit është i lidhur me gjashtë ofrues të tjerë shërbimesh, ku P1, P2, P3 tregojnë politikat përkatëse brenda nëngrupeve të ofruesve të shërbimeve. Që një përdorues të zgjedhë një ofrues shërbimi, ka disa rregulla të cilat duhet të kontrollohen për tu siguruar që ato përputhen me kërkesat e privatësisë së përdoruesve.

Në mënyrë më rigoroze, rregullat e kontraktorëve, indirekt mund të kenë nevojë të verifikohen për të përmbushur këto kërkesa. Kur vendosni marrëdhënien e shërbimit, marrëveshja e rregullave duhet të arrihet jo vetëm midis përdoruesit dhe S, por edhe midis S dhe S1, S1 dhe S2, etj. Gjithashtu është edhe më sfiduese të garantoni dhe zbatoni kërkesat e privatësisë së përdoruesit në shumë palë gjatë gjithë periudhës së shërbimit.

Disa ndryshime të mundshme për palët e përfshira në një shërbim cloud duhet të konsiderohen siç diskutohet në literaturë [94]: një palë pjesëmarrëse mund të duhet të përditësojë politikat e saj të privatësisë, ose një ofrues shërbimi mund të ketë nevojë të transferojë veprimet e tij së bashku me të dhënat e përdoruesve, diku tjetër për shkak të shitjes së ndërmarrjes, bashkimit, konfiskimit nga qeveria, etj.

Të gjitha këto ngjarje mund të ndikojnë në politikat aktuale që kanë rënë dakord të gjitha palët. Sfida është se si të reflektohet në mënyrë efikase dhe efektive një ndryshim i tillë në mënyrë që ndikimi në arritjen e marrëveshjes së rregullave dhe zbatimin e tyre të minimizohet.

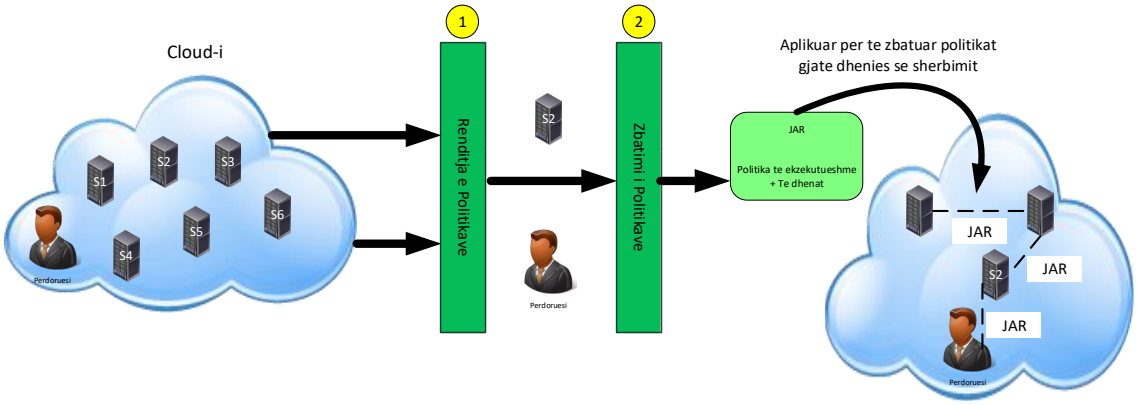

Figura 2-6 Modeli i mbrojtjes së të dhënave cloud

Bazuar në vëzhgimet e mësipërme, është propozuar një strukturë për mbrojtjen e të dhënave [97]. Kjo strukturë, siç ilustrohet në Figurën 2.6, përbëhet nga tre komponentë kryesorë: renditja e rregullave, integrimi dhe zbatimi i tyre. Në veçanti, një përdorues bashkohet në cloud dhe përballet me disa ofrues të shërbimeve cloud, ku secili prej tyre është në gjendje të ofrojë shërbimin që i nevojitet. Për të gjetur ofruesin e shërbimit, rregullat e privatësisë së të cilit përshtaten më mirë me kërkesat e privatësisë së përdoruesit, këto kërkesa dhe politikat aktuale të privatësisë të ofruesit të shërbimit futen së bashku në modulin e renditjes së rregullave. Moduli i renditjes ndihmon përdoruesin të zgjedhë ofruesin e shërbimit që ka politikat më të përputhshme të privatësisë. Meqenëse ofruesi i shërbimit të zgjedhur ende mund të mos ketë rregulla që përputhen saktësisht me kërkesat e përdoruesit, hapi i dytë është dërgimi i rregullave të tyre në modulin e integrimit, i cili automatikisht do të gjenerojë një rregull të integruar siç është rënë dakord nga të dy palët. Rregulli i integruar do të jetë në dy formate. Njëra është në një format aktual, d.m.th një rregull i shkruar në një gjuhë të caktuar. Tjetra është në një format të ekzekutueshëm (si një dosje Java, ang. JAR) i cili do të përdoret për zbatimin e rregullit pasues. Gjatë gjithë shërbimit, privatësia e të dhënave të përdoruesit do të mbrohet nga politika e ekzekutueshme, e cila mund të lëvizë gjithashtu midis kontraktorëve të lidhur drejtpërsëdrejti me ofruesin e shërbimeve.

2.3.2 Zbatimi i rregullave të kontrollit të aksesit në Cloud

Siç tregohet në modelin e mësipërm të mbrojtjes së të dhënave, komponenti i zbatimit të "politikës" është kritik për sigurinë e përgjithshme të të dhënave në cloud [93], [94]. Ka pasur disa përpjekje ekzistuese që synojnë të adresojnë këtë çështje. Disa mënyra [98], [99], [100] përdorin skemat kryesore të menaxhimit të çelësave për të siguruar Kontrollin e Aksesit në të dhënat cloud. Një lloj i tillë qasjesh grupon zërat e të dhënave bazuar në rregullat e Kontrollit të Aksesit dhe kriptojnë secilin grup me një çelës të ndryshëm. Më pas përdoruesve u jepen vetëm çelësat për zërat e të dhënave në të cilat lejohen të kenë qasje. Për shembull, nëse një përdorues anulohet, atij do t'i duhet të shkarkojë të dhënat e prekura nga ky ndryshim nga cloudi, të gjenerojë një çelës të ri kriptimi, të rikriptojë të dhënat e shkarkuara me çelësin e ri dhe pastaj të ngarkojë të këto të dhëna në cloud. Përveç menaxhimit të transmetimit të çelësit, kriptimi i bazuar në karakteristikat (ang. Attribute Base Encription - ABE) [101] është aplikuar gjithashtu për të ruajtur privatësinë e të dhënave në cloud. Sidoqoftë, kjo qasje nuk është efikase as në trajtimin e anëtarësimeve dhe largimeve të shpeshta të përdoruesve. Për të përmirësuar performancën, disa procese prezantojnë një palë të tretë të quajtur "autorizuesi ose lejuesi" [96] për të kryer rikriptimin në rast të ndryshimit të marrësit të të dhënave. Sidoqoftë, ato nuk mbrojnë karakteristikat e identitetit të përdoruesve.

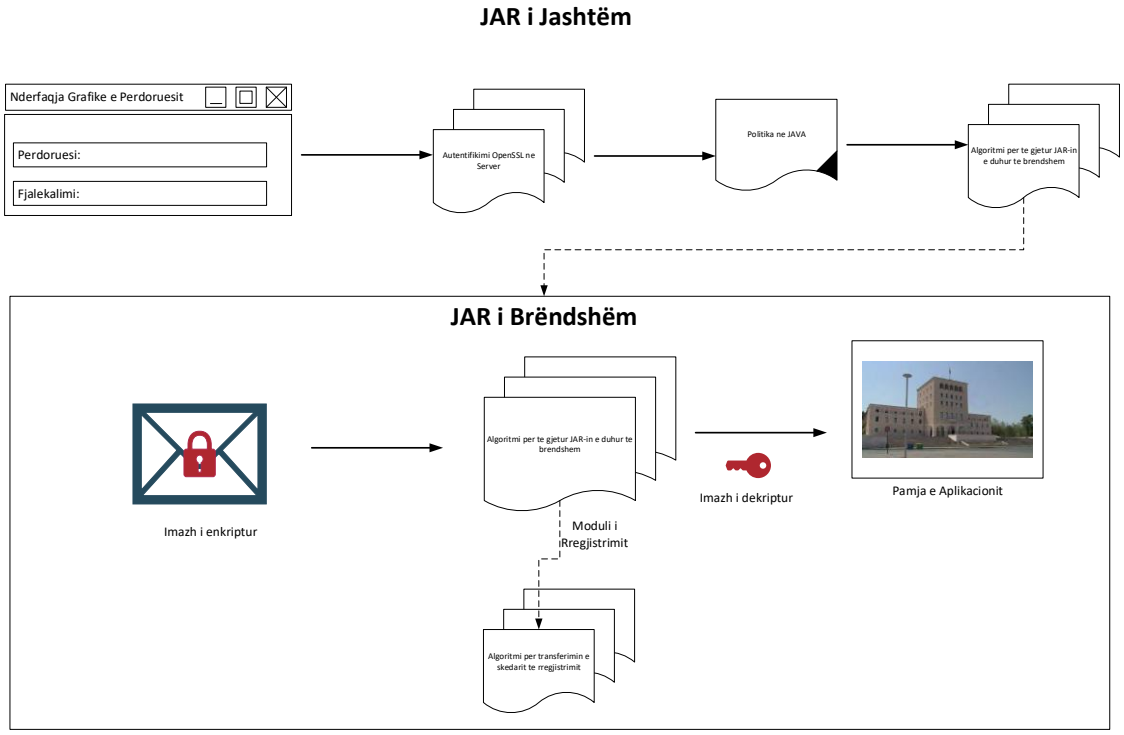

Figura 2-7 Procesi i JARs (i brendshëm dhe i jashtëm)

Një kategori tjetër interesante e procesit [102] synon të lidhë ngushtë të dhënat me rregullat e Kontrollit të Aksesit për të siguruar që këto rregulla do të zbatohen automatikisht kurdo dhe kudo ku të dhënat të jenë aksesuar. Ideja themelore është të

përdorësh arkivat Java (JAR-et), siç paraqitet në Figurën 2-7. Përparësitë e përdorimit të teknikave Java janë kryesisht të dyfishta. Së pari, JAR-et sigurojnë një "mbartës" të thjeshtë dhe të lëvizshëm për të dhënat, si dhe motorin e zbatimit. Së dyti, JAR-et kanë kërkesa minimale të infrastrukturës (d.m.th., një mjedis zbatimi Java të vlefshëm) për JRE-të të cilat lejojnë që sksesi jonë të adoptohet lehtësisht. Zërat e të dhënave të përdoruesit referuar rregullave të ndryshme do të ruhen në JAR-e të ndryshëm të koduar së bashku me skedarin e rregjistrave po ashtu të koduara. JAR-i i jashtëm përmban modulin e vërtetimit dhe motorin e zbatimit të rregullave. Ai është përgjegjës për vërtetimin e njësive që dëshirojnë të përdorin të dhënat, zgjedhjen e saktë të JAR-it të brendshëm dhe zbatimin e politikave përkatëse.

2.4 Shkaqe të tjera të Rrjedhjes së të Dhënave në Cloud

Përveç zbatimit të rregullave të privatësisë së përdoruesve në skedarin e të dhënave të tyre aktuale, ekziston një tjetër problem interesant dhe shumë i rëndësishëm i privatësisë i shkaktuar nga indeksimi i të dhënave. Indekset mund të përmbajnë një sasi të madhe informacioni në lidhje me vetë të dhënat. Meqenëse ato zakonisht ndërtohen pasi ofruesi i shërbimit të marrë të dhënat e përdoruesit dhe vendos ti ndërtojë për të përmirësuar performancën e kërkimit, përdoruesit mund të mos jenë të vetëdijshëm për përdorimin e tillë të të dhënave të tyre që ndoshta rrjedhin shumë më shumë informacion sesa ato të synuara nga përdoruesit. Diskutimi më i hollësishëm është si vijon. Skema më e zakonshme për mbështetjen e kërkimit efikas mbi përmbajtjen e shpërndarë është ndërtimi i një indeksi qëndror të përmbysur. Indeksi harton secilin term në një grup dokumentesh që e përmbajnë dhe kërkohet nga kërkuesi për të marrë një listë të dokumenteve që përputhen. Kjo skemë zakonisht miratohet nga motorat e kërkimit web dhe ndërmjetësuesit. Siç sygjerohet në [103], skema mund të zgjerohet për të mbështetur kërkimin e Kontrollit të Aksesit duke zbatuar rregullat e kontrollit të aksesit së bashku me përmbajtjen në nyjen indeksuese. Nyja indeksuese duhet të zbatojë këto rregulla për secilin kërkues për të filtruar rezultatet e kërkimit në mënyrë të përshtatshme. Meqenëse vetëm ky indeks duhet të kontaktohet për të ekzekutuar plotësisht një kërkim, kërkimet janë shumë efikase. Shkeljet e Kontrollit të Aksesit mund të mos jenë të tolerueshme në cloud, ku supozimet mbi besimin e serverit të indeksimit nuk ekzistojnë më. Më tej, kompromizimi i nyjes se indeksit nga hakerat mund të çojë në një humbje të plotë dhe shkatërruese të privatësisë. Indeksimi jo i qëndërzuar është një arkitekturë alternative e përdorur për të identifikuar një sërë dokumentesh që përputhen me kërkesën e kërkuesit. Këto nyje më pas kontaktohen drejtpërdrejt nga kërkuesi për të marrë dokumentet që përputhen. Kontrolli i Aksesit mund të mbështetet thjesht duke i bërë ofruesit e shërbimeve të zbatojnë politikat e tyre të hyrjes përpara se të sigurojnë dokumentet. Për të kapërcyer çështjet e lartpërmendura, disa procese kanë hulumtuar mundësinë e krijimit të indekseve private duke u mbështetur në kriptografinë të bazuar në predikim [104], [105].

Ndërsa janë të dukshme, këto procese kanë mungesë të zbatueshmërisë për shkak të kërkesave kryesore të menaxhimit dhe shpenzimeve të përgjithshme kompjuterike. Bawa et al. [103] propozoi një qasje interesante për indeksimin privat duke prezantuar një protokoll zbatues të shpërndarjes së Kontrollit të Aksesit. Një punim i fundit [106] merret me problemin e privatësisë nga një këndvështrim tjetër duke i fuqizuar përdoruesit për të fituar kontroll më të mirë mbi indekset. Në veçanti, u propozua një strukturë e tre-fishtë për mbrojtjen e të dhënave, e cila siguron mbrojtje të fortë, të mesme dhe të ulët, në përputhje me nevojat e zotëruesit të të dhënave. Kjo arrihet duke ndërtuar një skedar të ngjashëm JAR siç u diskutua më lart. File-i JAR përfshin të dhëna, rregulla, si dhe zbaton nivele të ndryshme të mbrojtjes si më poshtë:

- Mbrojtje e Fortë: Ofruesi i shërbimit nuk lejohet të lexojë pjesë të skedarit të përdoruesit, në mënyrë që të eleminojë rrezikun e indeksimit që kryhet në një pjesë të dokumentit dhe që mund të çojë në rrjedhje të privatësisë. Përdoruesit duhet të sigurojnë fusha në lidhje me skedarët e tyre të të dhënave. Më pas JAR kryen funksionin e zgjedhjes se cilat fusha do të lexohen nga ofruesit e shërbimeve cloud. Fushat e mbrojtura thjesht anashkalohen gjatë leximit vijues të skedarit duke identifikuar pozicionin ku fillon fusha e mbrojtur.
- Mbrojtje e Mesme: Ky opsion nuk lejon hyrjen e rastësishme në skedarin e të dhënave në mënyrë që të parandalojë indeksimin efektiv të file-it. Ofruesi i shërbimeve cloud do të zbatohet për të lexuar skedarin në një rend të njëpasnjëshëm përpara se të gjejë pëmbajtjen që i nevojitet.
- Mbrojtje e Ulët: Përdoruesi specifikon qartë në rregullat e tij, përdorimin e skedarit të të dhënave dhe përdorimin e indeksimit. Ofruesi i shërbimit supozohet i besuar dhe do të informojë dhe negociojë me përdoruesit fjalët kyçe që do të përdoren për qëllime indeksimi.

2.5 Makina e Vektorit Mbështetës (SVM)

Makina e Vektorit Mbështetës (ang. Support Vector Machine-SVM), është zhvilluar fillimisht nga Cortes dhe Vapnik (1995), është pa dyshim një nga algoritmet më të suksesshme të një mësimi automatik të zhvilluar gjatë dekadës së fundit. SVM-të kanë disa karakteristika tërheqëse për modeluesit; për shembull, ato bazohen më shumë në statistika sesa në analogji me sistemet e të mësuarit dhe ato teorikisht na garantojnë performancën. SVM-të përdorin një marrëdhënie funksionale të njohur si një Kernel për të hartuar të dhëna në një hapësirë të re në të cilën modelet e komplikuara mund të përfaqësohen më thjeshtë. Një analizë e plotë e SVM kërkon tre hapa, dhe idealisht në secilin nga këto tre hapa, përdoret një pjesë e veçantë e të dhënave:

1. Zgjedhja e modelit.
2. Përshtatja.
3. Vërtetimi.

Si funksionojnë SVM-të? Një shembull i thjeshtë mund të jetë që SVM-të do të grumbullojnë pikat e të dhënave në dy grupe të dukshme. Ajo që do të bënte modeluesi SVM është të gjejë ekuacionin për kufijtë për të ndarë maksimalisht dy grupe. Për të vizatuar më shumë variabla, linja e ndarjes do të bëhej një plan. Nëse do të përfshiheshin edhe më shumë variabla, ndarja do të ishte një hiperplan, e cila përcaktohet nga një nëngrup i pikave të dy klasave, të quajtur vektorët mbeshtetës. Formalisht, algoritmi SVM krijon një hiperplan që ndan të dhënat në dy klasa me marzhin maksimal - që do të thotë që distanca midis hiperplan-it dhe shembujve më të afërt (marzhi) të maksimizohet. SVM mund të përdoren për të kryer klasifikimin jolinear duke përdorur një kernel jolineare, i cili është një funksion matematikor që transformon të dhënat nga një hapësirë e tipareve lineare në një hapësirë të tipareve jolineare. Zbatimi i kernel-ve të ndryshëm në grupe të ndryshme të të dhënave mund të përmirësojë në mënyrë dramatike performancën e një klasifikuesi SVM.

2.5.1 SVM për klasifikim

SVM është një teknikë e dobishme për klasifikimin e të dhënave. Edhe pse konsiderohet se Rrjetet Neurale janë më të lehta për t'u përdorur sesa kjo, megjithatë, ndonjëherë janë fituar rezultate të pakënaqshme. Një detyrë klasifikimi zakonisht përfshin trajnimin dhe testimin e të dhënave të cilat përbëhen nga disa raste të tyre [66]. Çdo rast në grupin e trajnimit përmban një objektiv vlerash dhe disa karakteristika. Qëllimi i SVM është të prodhojë një model i cili parashikon vlerat e synuara të instancave të të dhënave në grupin e testimit të cilave u jepen vetëm karakteristikat. Klasifikimi në SVM është një shembull i një "të mësuarit me mbikqyrje". Etiketat e njohura ndihmojnë të kuptohet nëse sistemi po performon në një mënyrë të duhur apo jo. Një hap në klasifikimin e SVM përfshin identifikimin që janë të lidhura ngushtë me klasat e njohura. Kjo quhet përzgjedhje e karakteristikave. Kjo përzgjedhje dhe klasifikimi SVM së bashku kanë një përdorim edhe kur parashikimi i mostrave të panjohura nuk është i nevojshëm. Ato mund të përdoren për të identifikuar grupe kryesore të cilat përfshihen në çfarëdolloj procesi që dallon klasat.

2.5.2 SVM për regres

SVM-të mund të zbatohen edhe për problemet e regresit duke prezantuar një funksion alterativ "humbje" [67] [68]. Funksioni "humbje" duhet të modifikohet për të përfshirë një masë distance. Regresi mund të jetë linear dhe jo linear. Modelet lineare kryesisht përbëhen nga funksionet e mëposhtme: funksionet humbëse e-intensive, kuadratike dhe humbjet Huber. Njësoj si me problemet e klasifikimit edhe këtu zakonisht kërkohet një model jo-linear. Në metodën e regresit ka konsiderata të bazuara në njohjen paraprake të problemit dhe shpërndarjen e zhurmës. Në mungesë të një informacioni të tillë, funksioni humbjet Huber, ka vërtetuar se është një alternativë e mirë.

2.5.3 Aplikime të SVM-së

SVM ka treguar të jetë e suksesshme kur përdoret për problemet e klasifikimit të modeleve. Zbatimi i qasjes me vektor mbështetës për një problem të veçantë praktik përfshin zgjidhjen e një numri pyetjesh bazuar në përcaktimin e problemit dhe modelin e përfshirë me të. Një nga sfidat kryesore është ajo e zgjedhjes së një Kernel-i të përshtatshëm për aplikimin e dhënë. Ekzistojnë zgjedhje standarde siç është një kernel Gaussian ose polinomial që janë opsionet e paracaktuara, por nëse këto rezultojnë joefektive ose nëse të dhënat hyrëse janë diskrete do të nevojiten struktura më të hollësishme. Duke përcaktuar hapësirën e tiparit, kernel siguron gjuhën e përshkrimit të përdorur nga makina për të parë të dhënat. Pasi të jetë bërë zgjedhja e kernelit dhe kriteri i optimizimit, përbërësit kryesorë të sistemit janë vendosur.

Le të shohim disa shembuj të aplikimeve të SVM:

- "Dedektimi i Fytyrës" – SVM klasifikon pjesë të një imazhi si fytyrë ose jo-fytyrë dhe krijon një kufi përreth saj.
- Kategorizimi i tekstit dhe hipertextit – SVM lejon kategorizimin e tekstit dhe hipertekstit për të dy modelet induktive dhe ato përcjellëse. Ata përdorin të dhënat e mësuara për të klasifikuar dokumentet në kategori të ndryshme. Ai kategorizohet në bazë të rezultatit të gjeneruar dhe pastaj krahasohet me vlerën e pragut.
- Klasifikimi i imazheve – Përdorimi i SVM ofron saktësi më të mirë të kërkimit për klasifikimin e imazheve, në krahasim me teknikat tradicionale të kërkimit të bazuara në pyetje.
- Bioinformatika – SVM përdoret për identifikimin e klasifikimit të gjeneve, pacientëve në bazë të gjeneve dhe problemeve të tjera biologjike.
- Njohja e shkrimit të dorës - SVM përdoret gjithashtu për të njohur karaktere të shkruara me dorë të përdorura gjerësisht.

2.5.4 Avantazhe dhe disavantazhe të përdorimit të SVM

Gjithsej kemi 4 avantazhe kryesore , të cilat janë:

- SVM punon relativisht mirë kur ekziston një diferencë e qartë e ndarjes midis klasave.
- SVM është më efektive në hapësirat me dimensione të larta.
- SVM është efektive në rastet kur numri i dimensioneve është më i madh se numri i mostrave.
- SVM është relativisht efikase ndaj kujtesës.

Më poshtë listojmë disavantazhet e saj:

- Algoritmi SVM nuk është i përshtatshëm për grupe të mëdha të të dhënave.

- SVM nuk performon shumë mirë kur grupi i të dhënave ka më shumë zhurmë, dmth: klasat e synuara mbivendosen.
- Në rastet kur numri i karakteristikave për secilën pikë të të dhënave tejkalon numrin e mostrave të të dhënave të mësuara, SVM do të performojë më pak.
- Ndërsa klasifikuesi i vektorit mbështetës funksionon duke vendosur pika të dhënash, mbi dhe nën hiperplanin klasifikues, si dhe nuk ka asnjë shpjegim probabilistik për klasifikimin.

2.6 ALGORITMI MAPE-K

Algoritmi i qarkut Monitorim, Analizim, Planifikim, Ekzekutim mbi Njohurinë e përbashkët (ang. Monitorim -Analyze-Plan-Execute over a shared Knowledge – MAPE-K) është modeli kontrollues me ndikimin më të madh për sistemet autonome dhe vetë-përshtatëse. Sistemet moderne të softwerëve zakonisht funksionojnë në mjedise dinamike dhe trajtojnë kushte shumë të ndryshueshme operacionale: përbërësit mund të shfaqen dhe zhduken, mund të bëhen përkohësisht ose përgjithmonë të padisponueshëm, mund të ndryshojnë sjelljen e tyre, etj. Vetë-përshtatja është njohur gjerësisht si një qasje efektive për tu marrë me kompleksitetin, pasigurinë dhe dinamikën në rritje të këtyre sistemeve. Një qasje inxhinierike e mirënjohur për të realizuar vetë-përshtatjen është me anë të një qarku me kontroll të rezultatit të quajtur MAPE-K dhe konceptuar si një sekuencë e katër hapave Monitoro-Analizo-Planifiko-Ekzekuto mbi një Njohuri të dhënë.

Për të siguruar garantimin e korrektësisë funksionale të logjikës së adaptimit, metodat formale mund të përdoren si një mjet rigoroz për specifikimin dhe arsyetimin e sjelljes së sistemeve vetë-adaptuese, si në kohën e krijimit ashtu edhe në kohën e ekzekutimit. Sidoqoftë, sondazhi tregon se, megjithëse vëmendja për sistemet e softwarit vetë-adaptues po rritet gradualisht, numri i studimeve që përdorin metoda zyrtare mbetet i ulët, dhe kryesisht lidhen me verifikimin e kohës së ekzekutimit. Modelet e krijuara zyrtarisht të krijimit që mbulojnë të dyja aspektet strukturore si të sjelljes të vetë-përshtatjes dhe të qasjeve për të vërtetuar dhe verifikuar vetitë e sjelljes janë shumë të kërkuara.

2.6.1 Arkitektura MAPE-K për vetë-adaptimin

Vet-rikuperimi është një nga katër vetitë kryesore të një sistemi vetë-përshtatës [69]. Për realizimin e sistemit vetë-përshtatës, IBM prezantoi mekanizmin e qarkut të kontrollit MAPE-K. MAPE-K qarku i kontrollit [70]. Figura 2-8, përfshin Monitorimin, Analizimin, Planifikimin e proceseve, Ekzektimin dhe një Njohuri të dhënash. Procesi i monitorit mbledh detajet, tregon informacionin mbi topologjinë, dhe konfiguron parametrat nga burimet e menaxhuara. Procesi i analizës kryen analizën e të dhënave dhe arsyetimin e "simptomave" të siguruara nga procesi i monitorimit. Procesi i analizës ndikohet nga të dhënat e ruajtura të njohurive. Nëse kërkohen ndryshime, një kërkesë

ndryshimi i kalohet procesit të planit. Procesi i planit strukturon veprimet e nevojshme për të arritur qëllimet. Procesi i planit krijon ose zgjedh një procedurë për të miratuar një ndryshim të dëshiruar në burimet e menaxhuara. Ai mund të marrë shumë forma, duke filluar nga një urdhër i vetëm të një pune komplekse. Procesi i ekzekutimit ndryshon sjelljen e burimit të menaxhuar bazuar në veprimet e rekomanduara nga procesi i planit. Të katër proceset ndajnë një njohuri bazë që përfshin të dhëna, të tilla si regjistrat historikë apo politikat. Njohuritë bazë mund të përditësohet nga proceset në varësi të rezultateve të tyre.

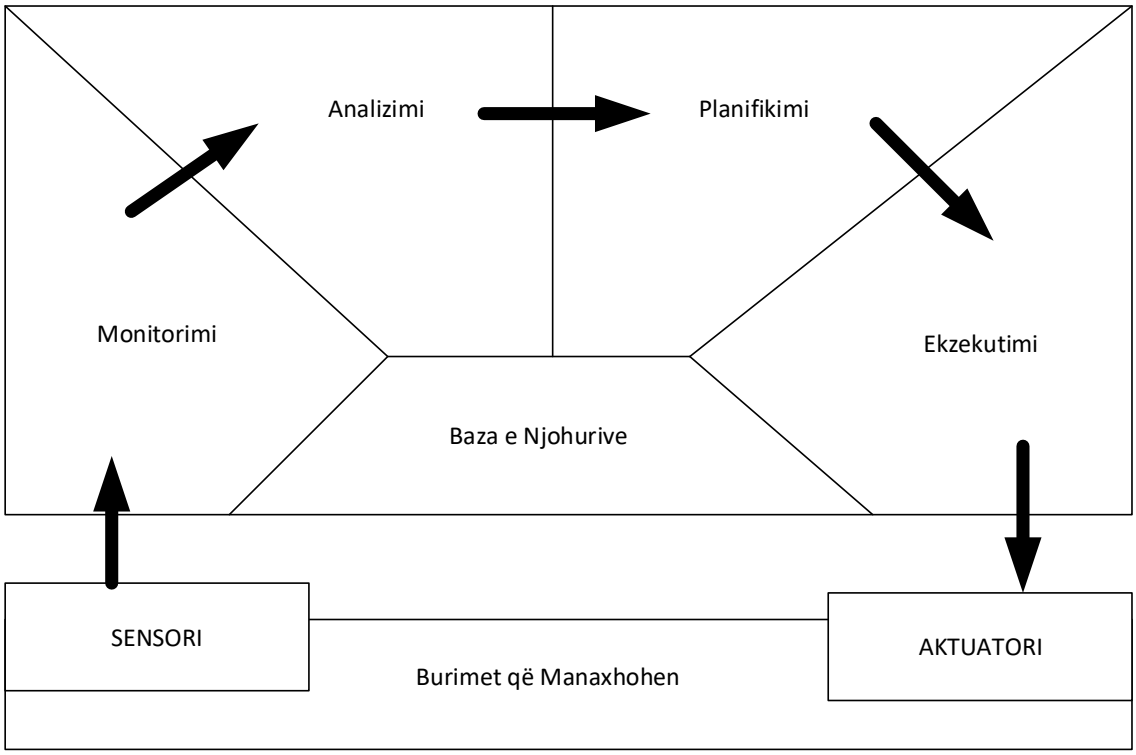

Figura 2-8 Arkitektura e algoritmit MAPE-K

Shumë studime të kohëve të fundit kanë studiuar modalitetin MAPE-K të vetë-menaxhimit të rrjetave pa tel të sensorëve si sisteme kompjuterike autonome, duke adresuar "veçoritë-vetjake" të ndryshme. Sidoqoftë, shumica e studimeve synojnë vet-konfigurimin, vetë-optimizimin ose vetitë e vetë-mbrojtjes. Agilla ofron një model programimi me të cilin aplikacionet në secilën nyje të sensorit në rrjet veprojnë si një agjent që mund të migrojë në mënyrë të qartë ose klonuar nga nyja në nyjen tjetër.

2.7 Algoritmi i Përmirësimit Ekstrem të Gradientit (XGBoost)

Algoritmi i përmirësimit ekstrem të gradientit (ang. eXtreme Gradient Boosting - XGBoost) është një algoritëm relativisht i ri që u prezantua nga Chen & Guestrin në 2016,

i cili përdor konceptin e përmirësimit pemë të gradientit. XGBoost u krijua për të rritur shpejtësinë dhe performancën, ndërsa prezantoi parametrat e rregullimit për të zvogëluar tejmbushjen. Përmirësimi pemë i gradientit përdor pemët e klasifikimit dhe kthimit për mësimin automatik (ang. Classification And Regression Trees for Machine Learning - CART) në një proces sekuencial mësimi si nxënësit e dobët. Këto pemë kthimi janë të ngjashme me pemët e vendimit, megjithatë, ato përdorin një rezultat të caktuar dhe të vazhdueshëm për secilën fletë (d.m.th. nyja e fundit pasi pema të ketë mbaruar së rrituri) e cila përmblidhet dhe siguron parashikimin përfundimtar. Për çdo cikël ***i*** i cili rrit një pemë ***t***, llogariten rezultatet ***w*** të cilat parashikojnë një rezultat të caktuar ***y***. Procesi i mësimit synon të minimizojë rezultatin e përgjithshëm i cili përbëhet nga funksioni i humbjes në ***i-1*** dhe një strukturë të re pemë të ***t***. Kjo lejon që algoritmi të rritë pemët në mënyrë sekuenciale dhe të mësojë nga ciklet e mëparshme. Zbritja e gradientit përdoret më pas për të llogaritur vlerat optimale për secilën fletë dhe rezultatin e përgjithshëm të pemës ***t***. Rezultati quhet edhe papastërtia e parashikimeve të një peme siç paraqitet në Figurën 2-9.

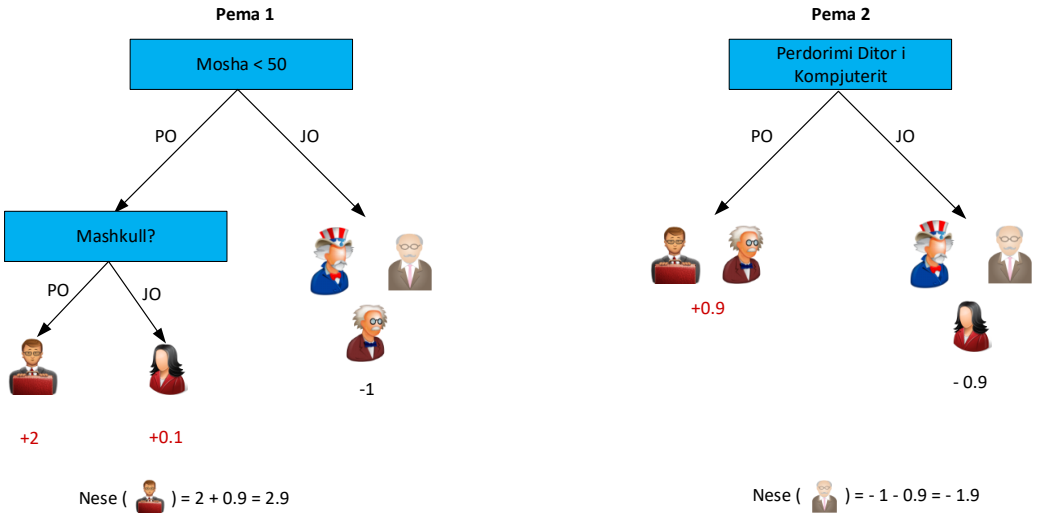

Figura 2-9 Vizualizimi i algoritmit XGBoost

Funksioni i humbjes në algoritmin e mësipërm përmban një model rregullim ose penaliteti **Ω** qëllimi i të cilës është të zvogëlojë kompleksitetin e funksioneve të pemës së kthimit. Ky parametër mund të ndryshohet dhe mund të marrë vlera të barabarta ose më të mëdha se **0**. Nëse vendoset në **0**, atëherë nuk ka asnjë ndryshim midis rezultateve të parashikimit midis metodave të pemëve me përmirësim të gradientit dhe XGBoost.

Përveç kësaj, Chen & Guestrin prezantojnë tkurrjen (d.m.th. një normë të të mësuarit) dhe nënkampionimin e kolonës (duke zgjedhur rastësisht një nëngrup të tipareve) në këtë algoritëm të pemës me përmirësim të gradientit, i cili lejon uljen e mëtejshme të tejmbushjes.

Përparësia kryesore e XGBoost është shpejtësia e tij e madhe krahasuar me algoritmet e tjerë, siç është SVM, dhe parametri i tij i rregullimit që zvogëlon ndryshimin me sukses. Por edhe përveç parametrit të rregullimit, ky algoritëm përdor një normë të të mësuarit (tkurrjen) dhe nën-shembujt, gjë e cila rrit aftësinë e tij për të përgjithësuar edhe më tej. Sidoqoftë, XGBoost është më e vështirë për t'u kuptuar, vizualizuar dhe për t'u akorduar në krahasim me SVM. Ekziston një mori hiperparametrash që mund të akordohen për të rritur performancën.

Për të përmendur disa nga hiperparametrat përkatës: niveli i të mësuarit, nën-kampionimi i kolonës dhe niveli i rregullimit të përmendur më sipër. Për më tepër, nën-shembulli (i cili po përgatit modelin e trajnimit), thellësia maksimale e pemëve, peshat minimale në shënimet fëmijë për ndarje dhe numri i vlerësuesve (pemëve) përdoren gjithashtu shpesh për të adresuar shkëmbimin midis ndryshimeve dhe paragjykimeve.

Ndërsa vlerat më të larta për numrin e vlerësuesve, rregullimi dhe peshat në shënimet fëmijë shoqërohen me ulje të mbingarkesës, shkalla e të mësuarit, thellësia maksimale, marrja e mostrave dhe marrja e mostrave nga kolona duhet të kenë vlera më të ulëta për të arritur reduktimin e tejmbushjes. Megjithatë, vlerat ekstreme do të çojnë në çmontimin e modelit.

XGBoost është një algoritëm veçanërisht interesant kur shpejtësia dhe saktësia e lartë janë thelbësore. Sidoqoftë, kërkohen më shumë burime në trajnimin e modelit sepse rregullimi i modelit kërkon më shumë kohë dhe ekspertizë nga përdoruesit për të arritur rezultate domethënëse.

2.8 Mbrojtja e Duhur e Informacionit të të Dhënave

Të dhënat e konsumatorit, të cilat mund të jenë të çdo lloji si të strukturuar ose të pastrukturuar dhe të ruajtura në çdo format (të koduar ose të pakriptuar) në media janë pjesa më e rëndësishme e një korporate. Sigurisht, kur një korporatë merr një vendim për të marë shërbimet e një njësie kompjuterike cloud, ajo duhet të jetë e vetëdijshme për ekspozimin ndaj rrezikut në lidhje me të dhënat e tyre.

Korporata mund të vendosë të lëvizë vetëm të dhëna jokritike në cloud, dhe të mbajë të dhëna kritike në nivel lokal brenda infrastrukturës së tyre të IT-së, duke zvogëluar kështu faktorin e rrezikut.

Me kalimin e kohës, korporatat mund ta konsiderojnë këtë ndarje në të dhëna jo praktike, prandaj marrin një vendim për të zhvendosur të gjitha të dhënat e tyre të korporatave në cloud. Ofruesi i shërbimit të shërbimeve cloud computing mund të ketë një rregull për shpërndarjen e të dhënave të klientit nëpër qendrat e tyre të të dhënave.

Cloud computing ka rritur fushën e sigurisë si për të dhënat që janë statike ashtu edhe për ato që lëvizin përgjatë rrjetit, për pasojë një korporatë duhet të marrë auditimin e grupeve të të dhënave të saj.

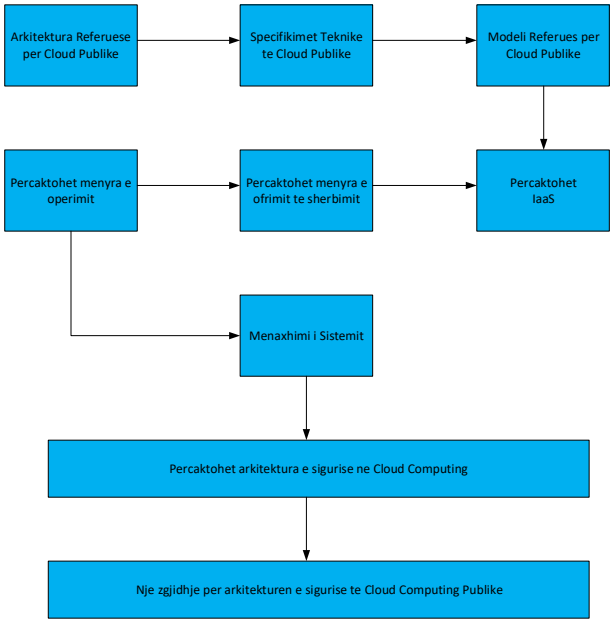

Figura 2-10 Arkitektura referuese për cloud publike

Të dhënat (të strukturuara si dhe të pastrukturuara) duhet të kategorizohen në grupe, ku secili prej tyre korrespondon me funksione të përcaktuara, të cilat do të përfaqësonin procese biznesi me departamente të ndryshme brenda një korporate të caktuar. Secili prej departamenteve do të kishte të drejta të caktuara përpunimi për ato procese biznesi, pra për grupet e të dhënave. Këtu duhet të përcaktojmë privilegjet e sigurisë duke përdorur një lloj algoritmi refleksiv të caktuar për secilin nga këto procese apo grupe; ekzekutivi përgjegjës për informacionin (ang. Chief Information Officer-CIO) do të kishte nivelin më të lartë të privilegjit për të gjitha grupet e të dhënave. Algoritmi refleksiv gjithashtu identifikon departamentet që kanë qasje të përbashkët (përfshirëse) në grupet e të dhënave, dhe ato që kanë qasje ekskluzive, nën menaxhimin e qasjes. Kështu, rregullat e sigurisë përcaktohen tani duke përdorur algoritmin refleksiv dhe zbatohen kontrollet e sigurisë. Hapi tjetër është monitorimi i proceseve të biznesit.

Politika e sigurisë e përcaktuar dhe kontrollet e zbatuara duhet të sigurojnë privatësinë e grupeve të të dhënave në përputhje me rregulloret lokale të pajtueshmërisë siç jepet në Figurën 2-10. Sigurisht, ofruesi i shërbimit të cloud computing do të duhet të ketë gjithashtu kontrolle sigurie për të mbrojtur grupet e të dhënave të konsumatorëve të tyre. Konsumatorët duhet të marrin një vendim në lidhje me grupet e të dhënave që duhet të kriptohen. Ky vendim do të varet nga natyra e të dhënave, dhe sa shpesh mund të aksesohen. Me algoritmin aktual të kriptimit, të dhënat do të duhej të dëshifroheshin gjatë procesit për përpunim, duke shtuar kështu koston dhe vonesën në biznes.

2.9 ASPEKTET E SIGURISË SË RRJETEVE CLOUD

Çdo ofrues i shërbimeve internet (ang. Internet Service Provider-ISP) që ofron shërbime kompjuterike për klientët e saj është gjithashtu e ndjeshme ndaj hakimit dhe formave të tjera të sulmeve të mohimit të shërbimit (DoS). Prandaj, ISP-të duhet të ketë një sistem të zbulimit të ndërhyrjeve (ang. Intrusion Detection System-IDS) dhe një sistem parandalimi të ndërhyrjeve (ang. Intrusion Prevention System-IPS) të instaluar për të monitoruar trafikun e rrjetit dhe për të marrë masat e duhura nëse zbulohet një ndërhyrje.

Njësoj si ekspozimi i një ISP ndaj trafikut "të dëmshëm" të rrjetit, çdo ofrues i shërbimit cloud mund të jetë gjithashtu i ekspozuar ndaj të njëjtit nivel rreziku. Prandaj edhe ofruesi i shërbimit cloud do të duhet të ketë IDS dhe IPS të instaluara për të siguruar masat e sigurisë, kështu që të jetë në gjendje të zbulojë çdo trafik të dëmshëm të rrjetit.

Projektimi logjik i rrjetit të burimeve të cloud computing duhet të ketë një router fundor me një lidhje me internetin për të siguruar ofrimin e shërbimeve tek konsumatorët. Fundi i pasëm i routerit do të lidhet me një perimetër firewall i cili do të mbështesë një zonë të demilitarizuar (ang. Demilitarized Zone-DMZ).

Kjo DMZ do të suportojë ndoshta shërbime të bazuara në web, postë elektronike dhe servera për shërbime të jashtme. Firewall-i rrethues do të sigurojë një masë të kontrollit të hyrjes dhe mbrojtjes së shërbimeve në DMZ. Fundi i pasëm i firewall-it do të lidhet me një mur të brendshëm, prapa të cilit do të vendosen të gjitha burimet e cloud computing, siç demonstrohet në Figurën 2-11.

Këto burime do të konfigurohen në rrjete të segmentuara. Secili prej këtyre segmenteve mund të konfigurohet si Rrjet Virtual me Zonë Lokale (ang. Virtual Local Area Networks-VLAN) për të siguruar një masë mbrojtjeje të burimeve nga aksesi i paautorizuar, si dhe për të siguruar një shkallë të privatësisë midis konsumatorëve, siç ilustrohet në Figurën 2-12.

Trafiku i rrjetit duhet të jetë "i rregjistruar" për të përmbushur pajtueshmërinë siç kërkohet nga ligjet e shtetit. Raportet e gjeneruara nga kjo vihen në dispozicion të klientëve në mënyrë të rregullt.

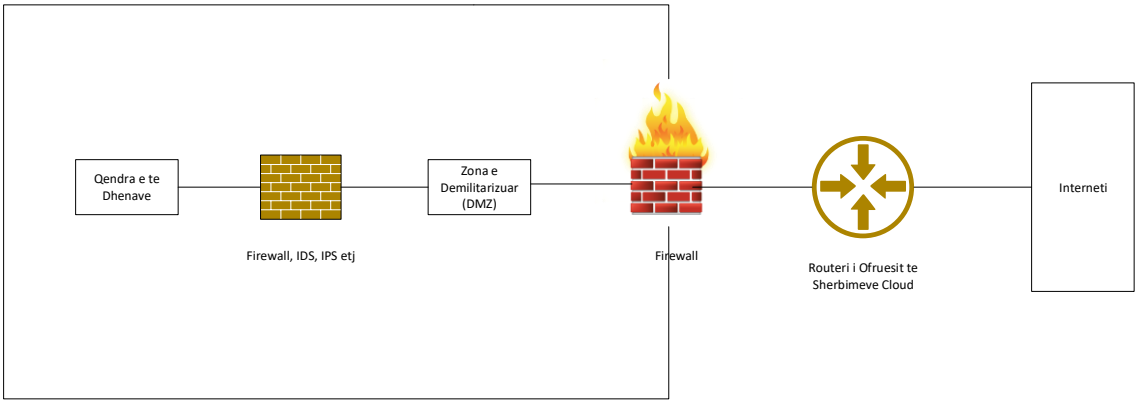

Figura 2-11 Projektimi logjik i rrjetit të Cloud provider

- Routeri fundor duhet të konfigurohet për të bllokuar trafikun hyrës dhe dalës sipas parametrave të konfigurimit të Kontrollit të Aksesit, siç janë adresa e rrjetit IP, numri i portës dhe protokollet përkatëse. Kjo do të filtrojë trafikun e rrjetit në modelin e shtresës së rrjetit.
- "Perimeter router" duhet të ketë në mënyrë rigoroze "filtrimin e paketave" të trafikut të rrjetit brenda/jashtë. Kjo mundëson aksesin e kërkuar në burimet e serverave në DMZ.
- Burimet e rrjetit duhet të jenë të sigurta nga sulmet e mohimit të shërbimit (DoS). Sulmet e shpërndara të mohimit të shërbimit (ang. Distributed Denial of Service-DDOS) do të kishin kërkesa të mëtejshme të një routeri me konfigurimin e duhur.
- Një kombinim i IDS dhe IPS të vendosura në mënyrë strategjike do të lejonte inspektim më të thellë të paketave për të identifikuar ngarkesat e dëmshme si worm-at (worms), kuajt Trojan dhe viruset. IDS/IPS-të të bazuar në nyje do të parandalonin modifikimin e burimeve të sistemit. IDS/IPS-të të bazuar në web do të përdorin zbulimin e nënshkrimit dhe anomalisë.
- Raportimi i incidenteve tek konsumatorët duhet të jetë përparësi, pasi konsumatorët janë përgjegjës për të dhënat e klientëve të tyre. Procedurat e trajtimit të incidenteve duhet të përcaktohen qartë, duke minimizuar ndikimin e tyre në një akses joproduktiv të shërbimit.
- Rregjistrimi i informacionit të rrjetit do të vihej në dispozicion të konsumatorëve, në të njëjtën kohë duke mbrojtur privatësinë e secilit prej konsumatorëve nga njëri-tjetri. Kjo do të varet nga mënyra se si pajisjet e ruajtjes konfigurohen dhe bëhen të disponueshme në të gjithë rrjetet e segmentuara.

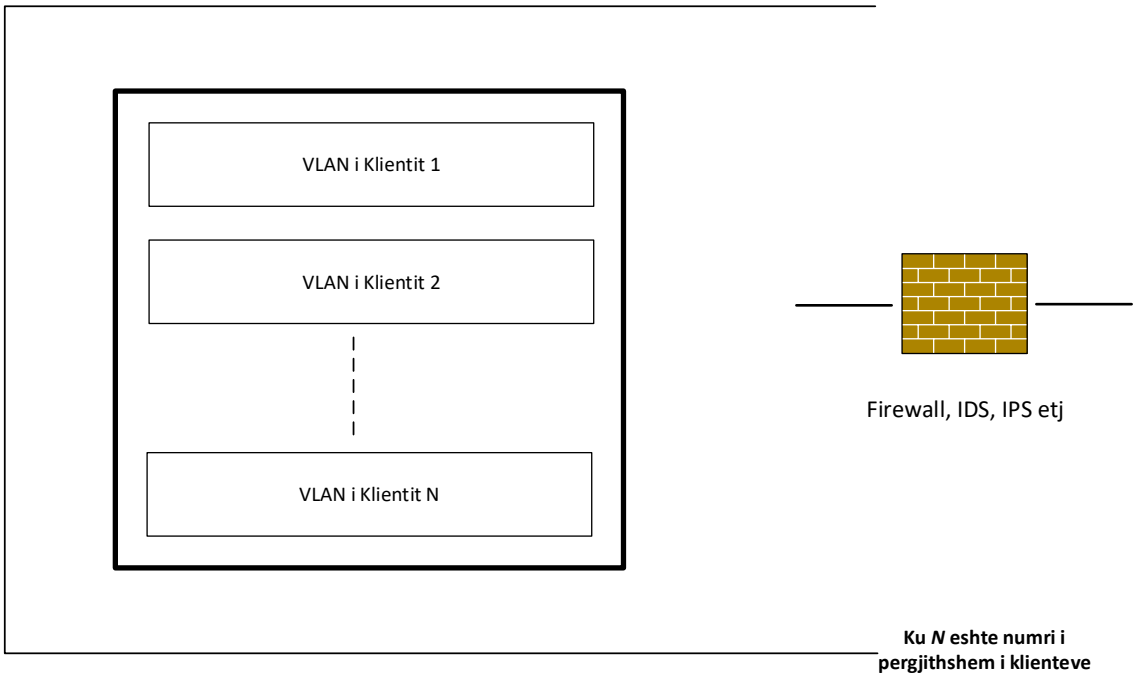

Figura 2-12 Segmentimi i rrjetit të data center-it

Marrëveshja e nivelit të shërbimit (ang. Service Level Agreement-SLA) duhet të deklarojë politikën e sigurisë të përshtatur nga ofruesi i shërbimit në terma të qarta. Dëmet e shkaktuara nga konsumatori në rast të një prishjeje të rrjetit duhet të përcaktohet po ashtu në një mënyrë sa më të qartë. Meqenëse ofruesi i shërbimit cloud ka shumë konsumatorë, shkelja e të dhënave në një llogari të konsumatorit nuk duhet të ndikojë në privatësinë dhe sigurinë e të dhënave të llogarive të konsumatorëve të tjerë - natyrisht, kjo do të varet nga konfigurimet e brendshme të rrjetit të të dhënave siç janë VLAN-et, "muret e zjarrit" mbrojtës dhe aksesi në ruajtjen e të dhënave.

2.10 Kontrollet e Sigurisë në Infrastrukturën Fizike

Rrjetat me zonë lokale (ang. Local Area Network-LAN) do të konfiguroheshin si VLAN, kështu që konsumatorët në një VLAN kurrë nuk do të shihnin ose monitoronin trafikun (kapërcimin e VLAN-eve) në një VLAN tjetër. Në këtë mënyrë është mjaft e mundshme që një konsumator mund të përdorë një aplikacion software-ik që mund të monitorojë dhe regjistrojë trafikun në këtë VLAN, duke shkelur kështu sigurinë e rrjetit për qëllime spiunazhi.

Konsumatorët mund të përdorin shërbimet cloud duke përdorur rrjetet virtuale private (ang. Virtual Private Network-VPN) nga vendndodhja bazë dhe më pas në VLAN siç paraqitet në Figurën 2-13. Kjo do të na ofronte siguri dhe privatësi pikë-më-pikë. Sigurisht, përdorimi i VPN-së do të kërkonte që konsumatorët të siguronin çertifikata dixhitale të sigurta (SSL/ IPSec) nga ofruesi i shërbimit. Ofruesit e shërbimit duhet ti

kujtojnë përdoruesve se në këtë pikë ata janë duke hyrë në shërbime nga serverat e parregjistruar. Konsumatorë të shumtë mund të kenë akses në një server ose në projektimin e një server-i të shpërndarë.

A mund të sigurojë ofruesi i shërbimit cloud një VLAN privat (ang. Privat VLAN-PVLAN)? Shtresa e lidhjes së të dhënave nga modeli OSI transmeton domain-e përveç qarqeve VPN që funksionojnë në shtresën 3 (shtresën e rrjetit). Kështu, PVLAN shton edhe një shtresë tjetër sigurie. Rrjeti i brendshëm i segmentuar duhet të projektohet në mënyrë që rrjeti i ofruesit të shërbimit cloud të jetë i izoluar nga rrjeti i konsumatorëve. Ofruesi i shërbimit cloud do të duhet të mbajë regjistrat e klientëve të tyre, të ruajtura në një bazë të dhënash ose në një bazë të dhënash të shpërndarë diku në rrjet.

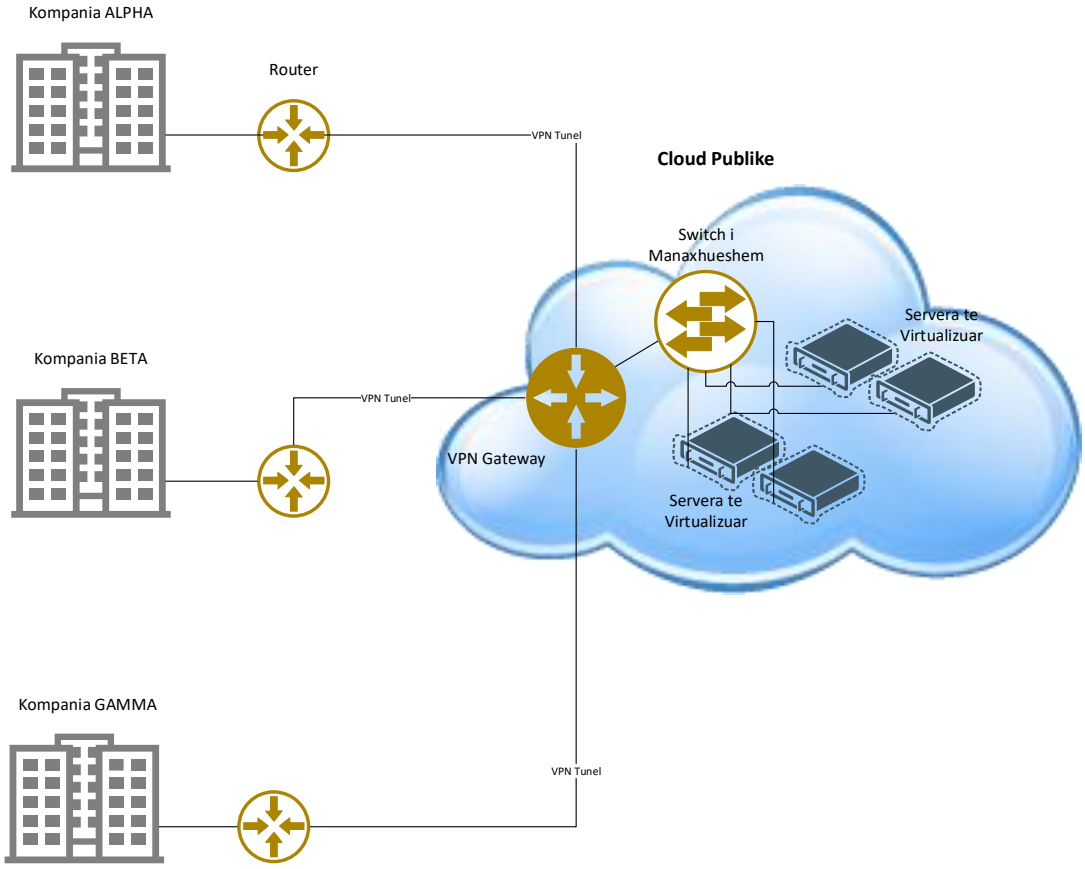

Figura 2-13 Zgjerimi i data center-it të një cloudi publik

Rrjeti i ofruesit të shërbimit cloud duhet të integrohet minimalisht me rrjetin e konsumatorëve dhe të ndërlidhet me një switch të shtresës së tretë. Aktivitetet e monitorimit të trafikut do të zhvilloheshin në rrjetin e konsumatorëve, por të dhënat e gjeneruara duhet të transferohen në rrjetin e ofruesit të shërbimit dhe më pas në pajisjet e ruajtjes së të dhënave. Kjo do të kërkonte planifikim dhe vlerësim të kujdesshëm në rast të një shkeljeje, izolimin e segmenteve të rrjeteve, pa pasur nevojë të mbyllni të gjithë

shërbimet cloud. Ofruesi i shërbimit cloud dhe konsumatorët e tij jo vetëm që do të pësonin humbje të të ardhurave, por edhe integritet dhe besueshmëri të shërbimit. Arkitektura e re dhe e shkallëzuar cloud është jashtëzakonisht e rëndësishme për një ofrues të shërbimit publik cloud, ku të ardhurat gjenerohen në miliona dollarë — ekonomitë e cloud computing publike duhet të adresojnë koston/përfitimin nga perspektiva e konsumatorëve.

Siguria në cloud computing publike është më e dëshiruar [71], pasi që cloud computing publike është një platformë ku të dhënat e rëndësishme të konsumatorëve ruhen ose në një vend ose në shumë vende.

Kombet kanë nocione dhe ligje të ndryshme në lidhje me privatësinë dhe sigurinë. Pyetjet që ne paraqesim janë si më poshtë - A janë të dhënat të koduara në pajisjen e ruajtjes së të dhënave, apo janë në format të thjeshtë? Nëse të dhënat janë të koduara, atëherë sa të sigurta janë ato, dhe kush është mbrojtësi i teknologjive të kriptimit? Ofruesi i shërbimit cloud ndan detajet e teknologjisë së kriptimit me konsumatorët e tyre si çelësat, çertifikatat dixhitale dhe algoritmet hash. Ne mund të konkludojmë se privatësia dhe siguria duhet të shihen si një integrim gjithnjë në zhvillim i artit dhe teknologjive të informacionit.

Platforma cloud computing duhet të jetë e vendosur fizikisht, edhe pse është në cloud. Infrastruktura fizike duhet të jetë e sigurt. Punonjësit e ofruesit të shërbimit duhet të kenë një qasje të kontrolluar në objekt me regjistrat e të gjitha hyrjeve/daljeve të mbajtura, dhe të disponueshme për konsumatorët për qëllime të auditimit. Infrastruktura fizike duhet të mbrohet nga fatkeqësitë natyrore të tilla si përmbytjet, tërmetet dhe zjarri.

Mirëmbajtja apo azhornimi i duhur i infrastrukturës duhet të kryhet për të siguruar nivelin e shërbimit sipas detyrimeve kontraktuale. Shërbimet cloud computing duhet të kenë qasje të pandërprerë në furnizimin me energji elektrike. Çdo qendër të dhënash duhet të ketë kopje të të dhënave ose plane rezervë dhe po kështu duhet të ketë qasjen edhe ofruesi i shërbimit të cloud computing - sipas planit të tyre të biznesit.

3 KLASIFIKIMI I SULMEVE NË CLOUD COMPUTING DHE PREZANTIMI I TEKNIKAVE VET-MBROJTËSE TË ZHVILLUARA NDAJ KËTYRE SULMEVE

Sulmet kompjuterike kanë treguar se janë një kërcënim i vazhdueshëm për përdoruesit, organizatat dhe infrastrukturat në Internet. Ato kategorizohen në tre kategoritë kryesore të mëposhtme: Sulmet e Mohimit të Shërbimit (DoS), Sondë dhe Kompromisit. Qëllimet kryesore të këtyre sulmeve janë ndalimi i aksesit, përfitimi i akseseve të paautorizuara për të kompromentuar sistemet e përdoruesit si dhe përfitimi i akseseve të paautorizuara për të shkatërruarr rjetin e përdoruesit. Në këtë kapitull do të flasim për klasat kryesore të sulmeve të kryera mbi Infrastrukturat Cloud. Në pjesën e dytë do të prezantohen teknikat e zhvilluara nga kërkues shkencor të ndryshëm gjatë këtij dhjetëvjeçari për të bërë të mundur, dedektimin, parandalimin dhe mbrojtjen e Infrastrukturave Cloud nga këto sulme dhe nga ndikimet që mund të kenë keto sulme mbi përdoruesit e këtyre rrjeteve dhe ofruesit e tyre.

3.1 KATEGORIA E PARË E SULMEVE – MOHIMI I SHËRBIMIT (ANG. DENIAL OF SERVICE - DOS)

Sulmet e mohimit të shërbimit (DoS) kanë provuar të jenë një kërcënim serioz dhe i përhershëm për përdoruesit, organizatat dhe infrastrukurat e Internetit. Qëllimi kryesor i këtyre sulmeve është parandalimi i aksesit në një burim të veçantë si për shembull një server në Internet [36]. Një numër tepër i madh mbrojtjesh kundër sulmeve DoS janë propozuar në literaturë, por asnjë nga këto nuk siguron një mbrojtje të besueshme. Gjithmonë do të ketë hoste të prekshëm në Internet që do të përdoren për qëllime të DoS. Për më tepër është shumë e vështirë të njohësh dhe të filtrosh vetëm trafikun e sulmit pa shkaktuar ndonjë dëm kolateral në trafikun e ligjshëm.

Një sulm DoS mund të kryhet ose si një "përmbytje" ose si një sulm logjik [37]. Një sulm përmbytjeje DoS bazohet në forcën brutale. Të dhëna me pamje reale, por të panevojshme i dërgohen viktimës sa më shumë që të jetë e mundur. Si rezultat gjerësia e brezit të rrjetit është okupuar plotësisht, hapësira e diskut është mbushur me të dhëna të panevojshme (për shembull: e-mail te padëshiruar, të dhëna junk FTP, mesazhe gabimi të qëllimshme),

strukturat e të dhënave me madhësi fikse brenda softuerit host janë të mbushura me informacion fals, ose fuqia e përpunimit është harxhuar për qëllime të padobishme. Një sulm i logjikshëm DoS, bazohet në një përdorim inteligjent të dobësive të synuara. Një datagram i fragmentuar IP, i ndërtuar me shkathtësi, mund të rrëzojë një sistem për shkak të një problemi serioz në softuerin e sistemit të operimit (OS). Një shembull tjetër i sulmi logjik është përdorimi i kërkesave të munguara për vërtetim duke injektuar informacione false të ruterit, në mënyrë që të parandalojë arritjen e trafikut në rrjetin e viktimës.

Ka dy arsye kryesore që i bën sulmet DoS tërheqës për përdoruesit. Arsyeja e parë është se ka mjete efektive automatike të disponeshme për të sulmuar një viktimë [38], për shembull, ekspertiza nuk është domosdoshmërisht e kërkuar. Arsyeja e dytë është se zakonisht është e pamundur të gjesh një sulmues pa ndërveprim të gjerë njerëzor [39], [40], ose pa karakteristika të reja në shumicën e ruterave të Internetit [41].

3.1.1 Mekanizmat e sulmit të përmbytjes

Sulmet DoS nga përmbytja zakonisht ndahen në sulme direkte dhe sulme reflektuese [41]. Në sulmet direkte, paketa të falsifikuara dërgohen në mënyrë të drejtpërdrejtë tek viktima. Në sulmet reflektuese paketat me adresën e viktimës në zonën e adresës IP të burimit, dërgohen tek një palë e tretë e pafajshme, e cila, nga ana tjetër do ti kthejë një përgjigje viktimës. Shembuj të palëve të treta të pafajshme janë serverat e Internetit, serverat DNS, dhe route-rat. Sulmet e reflektorëve kanë të paktën dy viktima në të njëjtën kohë [42].

Në thelb, çdo sjellje e zakonshme e protokollit, mund të përdoret si mekanizmi kryesor për sulmet e përmbytjes. Çdo shtresë protokolli është e përshtatshme për qëllime sulmi. Sulmet direkte përdorin zakonisht vetëm disa mekanizma të quajtura përmbytja TCP SYN, përmbytja ICMP Echo, ose ndonjëherë përmbytja e të dhënave UDP[43]. Në përmbytjen TCP SYN, viktimës i dërgohen paketa me një adresë të një hosti jo-ekzistent në fushën e adresës IP të burimit, e cila rezulton në shumë lidhje gjysmë të hapura që mbushin strukturat e të dhënave statike dhe parandalojnë lidhjet e ligjshme. Këto lidhje gjysmë të hapura do të skadojnë në 75 sekonda [44]. Në përmbytjen ICMP Echo, viktima është e detyruar të mbajë një sasi të madhe paketash-ping.

Në përmbytjen e të dhënave UDP, një objektiv i mundshëm është lidhja e ngarkesave dhe echo- portave ndërmjet dy viktimave. Këto sulme nuk konsumojnë burime për një kohë të gjatë, kështu që të paktën në teori, viktima duhet të jetë në gjendje të vazhdojë shërbimin drejt përdoruesve të ligjshëm normalisht pasi sulmi të ketë mbaruar. Sidoqoftë, disa sulme përmbytjesh, mund të kenë efekte të gjata. Pë shembull, përmbytja e fragmentit IP mund të konsumojë të gjithë memorien e disponueshme për ruajtjen e datagramave të pjesshëm të IP, pas së cilës çdo host mund të difektohet për shkak të mosdisponueshmërisë së memories së lirë.

Sulmet e reflektorëve shfrytëzojnë çdo sjellje protokolli, ku një paketë sulmuese shkakton një paketë përgjigjeje që t'i dërgohet viktimës përfundimtare [45]. Sulmet e reflektorit gjithashtu mund të përfshijnë përdorimin e një teknike të quajtur bandë gjerë ose

amplifikim i paketës. Pala e tretë e pafajshme ose do të përgjigjet me një pako më të gjatë, ose me disa paketa përkatësisht në një paketë të vetme sulmi. Një formë e amplifikimit të paketës është amplifikimi i transmetimit ku një paketë sulmuese dërgohet në një adresë transmetimi të drejtuar nga një nën-rrjet.

Të gjithë hostet që marrin paketën sulmuese do ti dërgojnë përgjigjen e tyre viktimës përfundimtare. Një shembull i mirënjohur i kësaj është sulmi i smurfit [46], ku një Echo e vetme përforcohet në disa paketa të Përgjigjes së Echo të ICMP-së. Sulmet nga përmbytja kundër routerëve mund të jenë efektive, sepse routerët zakonisht janë të optimizuar për përcjelljen e trafikut në vend që të trajtojnë të dhënat e dërguara direkt tek ata [47]. Sulmet nga përmbytjet kundër DNS mund të shkaktojnë ngadalësime të përhapjes të Internetit ose ndërprerje efektive.

Një rrjedhë e gjerë e gjerësisë së brezit të paketave nuk është domosdoshmërisht e nevojshme për një sulm përmbytjeje. Gjerësia e brezit, e cila është më pak se një shpejtësi tipike e një modemi analog mund të jetë e mjaftueshme në shfrytëzimin e mangësive në zbatimin e strukturave të të dhënave [48]. Këto lloj sulmesh të kompleksitetit algoritmik mund, për shembull, të degjenerojnë pemët binare dhe tabelat e hashit në listat e lidhura. Për shkak të kërkesës së inteligjencës në zgjedhjen e trafikut të sulmit, këto sulme të kompleksitetit algoritmik mund të klasifikohen si sulme logjike të përshkruara më poshtë.

3.1.2 Mekanizmat e sulmit logjik

Objektivi i sulmeve logjike DoS është të ndërtojë një numër të vogël të paketave specifike që shfrytëzojnë dobësitë që e bëjnë viktimën të bëjë gjëra anormale. Paketat normalisht dërgohen direkt tek një viktimë, sepse kërkohet njohuri e veçantë për një dobësi. Ka një larmishmëri të sulmeve logjike. Në mënyrë tipike një sulm bazohet në më shumë se një nga çështjet e mëposhtme në të njëjtën kohë:

- Shfrytëzimi i të metave: I gjithë softueri përmban të meta të cilat mund p.sh., të shkaktojnë prishjen e një host për shkak të gabimeve në trajtimin e strukturës dinamike të kujtesës, si në sulmin Tear drop bazuar në fragmente të mbivendosura të IP [46].
- Shfrytëzimi i gabimeve sintaksore: Implementimet nuk janë gjithmonë në gjendje të trajtojnë të dhëna të pasakta, si në sulmin e Protokollit të Menaxhimit të Grupit të Internetit (IGMP) bazuar në kokat e keqformuara [49].
- Shfrytëzimi i gabimeve semantike: Zbatimet mund të përpunojnë normalisht të gjitha mesazhet e sakta nga ana sintaksore edhe nëse këto mesazhe janë semantikisht të pasakta. Për shembull, në helmimin me memorie të DNS një hartë false (një përgjigje e DNS) mund t'i bashkëngjitet një mesazhi kërkimi të pafajshëm [47].
- Shfrytëzimi i kërkesave të munguara të vërtetimit: Mungesa e vërtetimit bën të mundur futjen e informacionit të rremë në shumë protokolle (p.sh., protokollet dinamike të rutimit) dhe shërbimet (p.sh., DNS) [50].

Implementimet e protokolleve mund të përfshijnë tipare jo standarde ose karakteristika që mungojnë të cilat mund të shfrytëzohen. Për shembull, disa implementime të makinës shtetërore TCP janë jo standarde dhe përfshijnë kalime të jashtme të gjendjes, ose jo të gjitha shtetet kanë kohë të përcaktuar mirë. Në këto lloj hostesh është e mundur të detyrojmë makinerinë që të hyjë në një gjendje nga e cila nuk mund të dalë, ose ka një ndërprerje shumë të gjatë. Këto dobësi në disa implementime mund të shfrytëzohen nga rrjedhat e paketave TCP SYN-FIN ose duke iu përgjigjur një pakete TCP SYN me një paketë TCP SYN [44].

Sulmet logjike kundër routerëve dhe pajisjeve të sigurisë mund të ndikojnë në pjesë të mëdha të infrastrukturës së Internetit dhe të mundësojnë lloje të tjera sulmesh, kur një pjesë e mbrojtjes nuk është më operacionale. Sulmet DoS kundër infrastrukturës së Internetit po bëhen gjithnjë e më të zakonshme. Infrastruktura e rutimit konsiderohet të jetë një shënjestër e shkëlqyer për sulmet DoS, sepse një sulmues është në gjendje të shkaktojë ndërprerje të rënda të rrjetit pa një përpjekje të rëndësishme thjesht duke injektuar informacion të rremë të rutimit [50]. DNS është një tjetër shërbim infrastrukture i prekshëm nga sulmet DoS, për shembull kur një domain rrëmbehet [47].

3.2 Klasa e dytë e sulmeve – Mohimi i Shpërndarë i Shërbimit (ang. Distributed Denial of Service - DDoS)

Për të amplifikuar efektet, sulmet DoS mund të drejtohen në një mënyrë të koordinuar nga disa burime në të njëjtën kohë (Distributed DoS, DDoS). Në një sulm DDoS një sulmues përdor hoste të shumtë burimesh për të dërguar trafik sulmi tek një ose më shumë viktima njëkohësisht. Në mënyrë tipike pjesëmarrësit në një sulm DDoS formojnë një rrjet hierarkik DDoS, ku një sulmues kontrollon disa administrues, të cilët nga ana tjetër kontrollojnë një numër shumë më të lartë të agjentëve (ose demonëve ose zombive) për të kryer një sulm të vërtetë kundër një viktime.

Fillimisht mjetet e sulmit DDoS u vendosën manualisht, por tani worm-et përdoren zakonisht për këtë. Worm-et janë softuer me qëllim të keq vet-përhapës, i cili shpesh përfshin ose drejtpërdrejt aftësinë e sulmit DDoS (p.sh., Code Red I [51] dhe Slapper [52]) ose përmban mundësinë për të ekzekutuar kod arbitrar (p.sh., Code Red II [53]). Sidoqoftë, disa worm-e janë krijuar për tu përhapur shpejt pa ndonjë ngarkesë të dëmshme (p.sh., Slammer [54]) ose funksionaliteti i tyre i plotë është i panjohur (p.sh., Nimda [55]). Viruset mund të përdoren gjithashtu për fazën e vendosjes për të ndërtuar një rrjet të madh DDoS, por ata nuk mund të kopjohen automatikisht vetë.

Në mënyrë tipike kërkohet inxhinieria sociale për të nxitur një njeri që të fillojë një program që përmban një virus (p.sh., një shtojcë E-mail). Një shënjestër për një sulm DDoS ka zakonisht pak kohë për t'u përgatitur, sepse viruset identifikohen dhe inxhinierohen në mënyrë të kundërt sapo të gjenden në natyrë. Pritësit e infektuar gjithashtu mund të dezinfektohen sapo të jenë të disponueshme azhornimet e antivirus.

Përkundrazi, një worm përhapet shpejt dhe mund të shkaktojë një sulm të papritur. Kjo e bën një worm një mjet më serioz të vendosjes për sulmet e DoS.

Kombinimi i një mjeti DDoS me një mekanizëm efikas të përhapjes së worm-ave bën që instalimi i rrjeteve DDoS të jetë i shpejtë. Praktikisht çdo mjet DDoS mund të mbështillet brenda një worm-i vetë-përhapës [36]. Gjithashtu, worm-at bëjnë të mundur krijimin e shpejtë të rrjeteve DDoS multiplatformë. Disa worm-a mund të lëshohen në të njëjtën kohë për të instaluar një mjet identik DDoS në host me sisteme operative ose aplikacione të ndryshme.

Ekzistojnë dy klasa kryesore të sulmeve DDoS (Figura 3-1): sulmet e zbrazjes së gjerësisë së brezit dhe sulmet e zbrazjes së burimeve. Një sulm i zvogëlimit të gjerësisë së brezit është krijuar për të përmbytur rrjetin e viktimës me trafik të padëshiruar që parandalon trafikun e ligjshëm për të arritur sistemin e viktimës. Sulmet e gjerësisë së brezit mund të ndahen në sulme nga përmbytjet dhe sulme të amplifikimit. Një sulm i zbrazjes së burimeve është një sulm që është krijuar për të lidhur burimet e një sistemi viktimë. Ky lloj sulmi mund të ndahet në sulmet e shfrytëzimit të protokollit dhe sulmet e paketave të keqformuara [56].

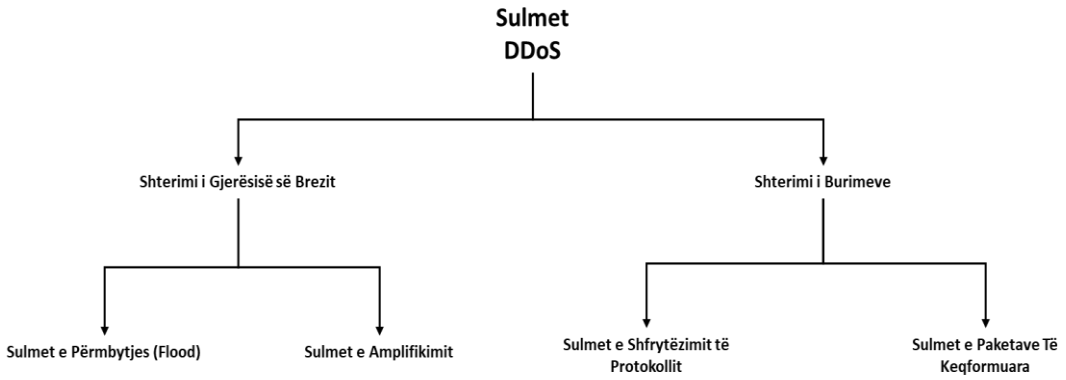

Figura 3-1 Klasifikimi i Sulmeve DDoS

Sulmet DDoS gjithashtu mund të klasifikohen në dy kategori të përgjithshme: sulme të drejtpërdrejta dhe sulme reflektuese të cilat janë përshkruar tashmë në seancën e mëparshme.

3.2.1 Sulmet nga përmbytja HTTP

Një sulm përmbytjeje HTTP është një lloj sulmi volumetrik i shpërndarë i mohimit të shërbimit (DDoS) i krijuar për të mbingarkuar një server të synuar me kërkesa HTTP sipas Fig. 3-2. Pasi objektivi të jetë ngopur me kërkesa dhe nuk është në gjendje ti përgjigjet trafikut normal, mohimi i shërbimit do të ndodhë për kërkesa shtesë nga përdoruesit aktualë.

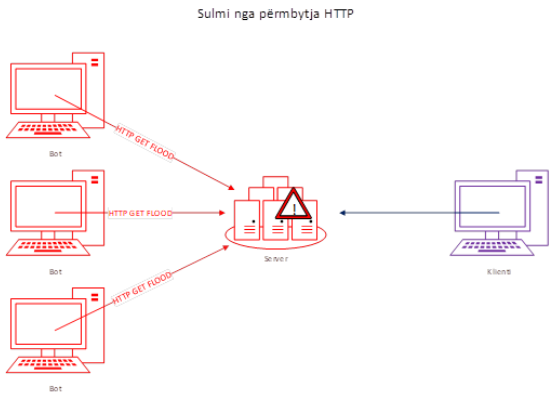

Figura 3-2 Sulmet nga përmbytja HTTP

Sulmet nga përmbytja HTTP janë një lloj sulmi DDoS të "shtresës 7". Shtresa 7 është shtresa e aplikimit të modelit OSI dhe i referohet protokolleve të internetit si HTTP. HTTP është baza e kërkesave të internetit të bazuara në shfletues dhe zakonisht përdoret për të ngarkuar faqe në internet ose për të dërguar përmbajtjen e formularit në Internet. Zbutja e sulmeve të shtresës së aplikimit është veçanërisht komplekse, pasi trafiku keqdashës është i vështirë të dallohet nga trafiku normal. Në mënyrë që të arrihet një efikasitet maksimal, aktorët me qëllim të keq do të përdorin ose krijojnë botnets në mënyrë që të maksimizojnë ndikimin e sulmit të tyre. Duke përdorur shumë pajisje të infektuara me malware, një sulmues është në gjendje të përdorë përpjekjet e tyre duke nisur një vëllim më të madh të trafikut sulmues.

Ekzistojnë dy lloje të sulmeve të përmbytjeve HTTP:

- Sulmi HTTP GET - në këtë formë sulmi, shumë kompjuterë ose pajisje të tjera koordinohen për të dërguar kërkesa të shumta për imazhe, skedarë ose ndonjë pasuri tjetër nga një server i synuar. Kur objektivi përmbytet me kërkesa dhe përgjigje në hyrje, mohimi i shërbimit do të ndodhë për kërkesa shtesë nga burime të ligjshme të trafikut.
- Sulmi HTTP POST - zakonisht kur një formë dorëzohet në një faqe në internet, serveri duhet të trajtojë kërkesën hyrëse dhe ti shtyjë të dhënat në një shtresë të qëndrueshmërisë, më shpesh një bazë të dhënash. Procesi i trajtimit të formës së të dhënave dhe ekzekutimi i komandave të nevojshme të bazës së të dhënave është relativisht intensiv në krahasim me sasinë e fuqisë përpunuese dhe gjerësinë e brezit që kërkohet për të dërguar kërkesën POST. Ky sulm shfrytëzon pabarazinë në konsumin relativ të burimeve, duke dërguar shumë kërkesa për postë drejtpërdrejt në një server të synuar derisa kapaciteti i tij të ngopet dhe të ndodhë mohimi i shërbimit.

3.2.2 Sulmet e Ditës Zero

Një sulm me zero ditë (referuar gjithashtu si Dita Zero) është një sulm që shfrytëzon një dobësi potencialisht serioze të sigurisë së softuerit për të cilën shitësi ose zhvilluesi mund të mos ketë dijeni. Zhvilluesi i softuerit duhet të nxitojë për të zgjidhur dobësinë sa më shpejt që të zbulohet në mënyrë që të kufizojë kërcënimin për përdoruesit e softuerit. Zgjidhja quhet një fashë softueri. Sulmet zero-ditore mund të përdoren gjithashtu për të sulmuar internetin e gjërave (ang. Internt of Things - IoT).

Një sulm me ditë zero merr emrin e tij nga numri i ditëve që zhvilluesi i softuerit ka qenë në dijeni për problemin. Një sulm me ditë zero mund të përfshijë malware, adware, spyware ose qasje të paautorizuar në informacionin e përdoruesit. Përdoruesit mund të mbrojnë veten nga sulmet e ditës zero duke vendosur softuerin e tyre - përfshirë sistemet operative, programin antivirus dhe shfletuesit e internetit - për të azhornuar automatikisht dhe duke instaluar menjëherë çdo azhornim të rekomanduar jashtë azhornimeve të planifikuara rregullisht. E thënë me fjalë të tjera, azhornimi i softuerit të antivirusit, nuk do të mbrojë një përdorues nga sulmi me ditë zero, sepse deri ne momentin që dobësitë e softuerit do të jenë publikisht të njohura, softueri i antivirusit mund të mos ketë një mënyrë për ta dalluar atë. Sistemet e parandalimit të ndërhyrjeve të hostit gjithashtu ndihmojnë në mbrojtjen nga sulmet e ditës zero duke parandaluar dhe mbrojtur nga ndërhyrjet dhe duke mbrojtur të dhënat.

Mendoni për një dobësi të ditës zero si një derë e hapur e makinës për të cilën pronari mendon se është mbyllur por një hajdut zbulon se është e zhbllokuar. Hajduti mund të futet pa u zbuluar dhe të vjedhë gjëra në kroskotin ose bagazhin e pronarit të makinës që mund të mos vërehen deri disa ditë më vonë kur dëmi është bërë tashmë dhe hajduti është zhdukur prej kohësh.

Ndërsa dobësitë e ditës zero njihen si të shfrytëzuara nga hakerat kriminelë, ato gjithashtu mund të shfrytëzohen nga agjencitë qeveritare të sigurisë që duan ti përdorin ato për mbikëqyrje apo sulme. Në fakt, ka një kërkesë të madhe për dobësitë e ditës zero nga agjencitë qeveritare të sigurisë që ato ndihmojnë për të nxitur tregun për blerjen dhe shitjen e informacionit në lidhje me këto dobësi dhe mënyrën e shfrytëzimit të tyre.

Përdorimet zero-ditore mund të zbulohen publikisht, vetëm për tek shitësi i softuerit, ose ti shitet një pale të tretë. Nëse ato shiten, ato mund të shiten me ose pa të drejta ekskluzive. Zgjidhja më e mirë për një defekt sigurie, nga këndvështrimi i kompanisë softuerike përgjegjëse për të, është që një haker etik ose me kapelë të bardhë të zbulojë privatisht të metën tek kompania në mënyrë që të rregullohet përpara se hakerat kriminelë ta zbulojnë atë. Por në disa raste, më shumë se një palë duhet të adresojë cënueshmërinë për ta zgjidhur plotësisht, kështu që një zbulim i plotë privat mund të jetë i pamundur.

3.3 KLASA E DYTË E SULMEVE – KOMPROMISIT

Këto sulme paraqiten me të dhënat e grupuara në dy nënkategori: Nga Distanca në Ambjentin Lokal (ang.Remote to Local - R2L) dhe nga përdoruesi në rrënjë (ang. User to Root - U2R).

3.3.1 Sulmet nga Distanca në Ambientin Lokal (R2L)

Në këto lloj sulmesh, sulmuesit ekzekutojnë komanda për të marrë aksesin e sistemit për të kompromentuar rrjetin (në terma të cilësisë së shërbimit ang. QoS).

Sulmet R2L janë sulmues të paautorizuar, të cilët përmes rrjeteve fitojnë akses lokal pasi si përdorues të makinave lokale. Sulmet mund të fillojnë nga kudo në internet. Sapo sulmuesi fillon të ketë akses në sistemet e informacionit, ata mund të shfrytëzojnë dobësitë e makinës dhe të shkaktojnë dëme serioze të tilla si vjedhja e të dhënave të rëndësishme ose shkatërrimi i sistemeve të informacionit. Për shembull, sulmi ftp_write është që sulmuesi krijon skedar host për të bërë të shkruar dosjen anonime FTP dhe më në fund merr hyrjen lokale në sistem. Sulmi Guess_passwd është se sulmuesi përpiqet të fitojë akses në llogarinë e një përdoruesi duke supozuar vazhdimisht fjalëkalimet e mundshme. Çdo shërbim që ka nevojë për fjalëkalim për të hyrë shpesh bëhet një objektiv i sulmuar.

Tre nga teknikat më të spikatura për këtë lloj sulmi janë:

- Spiuni: Instalohet vetë fshehurazi në një sistem dhe funksionon në sfond për phishing.
- Supozimi i Fjalëkalimit: Sulmuesit i marrin me mend fjalëkalimet në vend ose në distancë.
- IMAP (Protokolli i Aksesit në Mesazhe në Internet): Gjen një server IMAP Mail.

3.3.2 Sulmet nga Përdoruesi në Ambientin Rrënjë (U2R)

Sulmet U2R janë sulmuesit që shtiren si një përdorues i ligjshëm i sistemit pa autorizim dhe më pas shfrytëzojnë dobësitë e sistemit për të marrë qasje rrënjësore të këtij sistemi. Për shembull, sulmuesi mund të shfrytëzojë dobësitë e një sistemi për të fituar privilegjet e rrënjës dhe për të instaluar një program backdoor në një sistem për akses në të ardhmen. Rezultati mund të shkaktojë prishjen e sistemit ose ta bëjë sistemin të ekzekutojë programin e sulmuesit sikur të jetë pjesë e programeve origjinale të sistemit. Një shembull tjetër është sulmi PHF që shfrytëzon një defekt sigurie të shkrimit CGI në një server në internet. Pasi identifikohet dobësia, sulmuesi mund të ekzekutojë komandat lokale në serverin e largët të sulmuar. Synimi i këtyre sulmeve është për të shkatërruar rrjetin, sulmuesit marrin aksesin rrënjë brenda sistemit.

Dy nga teknikat më të spikatura për këtë lloj sulmi janë:

- Rootkits: Ofron qasje të vazhdueshme të privilegjuar në një sistem duke fshehur në mënyrë aktive ekzistencën e tij.
- Buffer Overflow: Ndodh kur një program kopjon një sasi të madhe të të dhënave në një buffer statik.

3.4 KLASA E DYTË E SULMEVE – SONDË (ANG. PROBING)

Për të shkelur informacionin personal të viktimës, një sulmues përdor gjuhë të ndryshme programimi. Sulmet e hetimit kryhen nga sulmuesit që përdorin programe për të skanuar automatikisht adresat IP të rrjetit me një sasi të madhe në mënyrë që të gjejnë dobësi që mund të shfrytëzohen. Sapo të zbulohet ndonjë cënueshmëri, sulmuesit mund të fitojnë kështu hyrjen në sistem dhe të fillojnë të mbledhin informacion pa autorizim. Një nga sulmet më të zakonshme të hetimit quhet skanimi i portës, i cili lejon sulmuesit të skanojnë të gjitha portat në hostet e rrjetit dhe të zbulojnë se cilat janë në dispozicion për lidhje. Metodat popullore të skanimit përfshijnë skanimin TCP, skanimin UDP, skanimin SYN, skanimin ACK, skanimin FIN, skanimin ICMP, skanimin e protokollit dhe skanimin bosh. Për shembull, sulmi i portsweep zbulon kanalet e shfrytëzueshme të komunikimit në hostet e largëta duke kërkuar sistematikisht lidhje me shumë porta TCP.

Dy nga teknikat më të spikatura për këto kategori sulmi janë:

- Ports Sweep: Pritës të shumtë skanohen për një port të veçantë dëgjimi.
- NMAP (Network MAPper): Kryen skanimin e portës.

3.5 PREZANTIMI I TEKNIKAVE VET-MBROJTËSE TË ZHVILLUARA NDAJ KËTYRE SULMEVE

Një Teknikë e Sigurt Autonome (SAT) u propozua për të siguruar një mjedis të sigurt cloud për ekzekutimin e aplikacioneve të përdoruesve [57]. SAT zbulon sulmet DoS (përmbytjen SYN) me saktësi të shkëlqyeshme të të dhënave gjatë menaxhimit të shërbimeve cloud. Carpen-Amarie [58] propozoi sistemin e Menaxhimit të Vetë-Përshtatjes së të Dhënave (SADM), i cili menaxhon sasi të mëdha të të dhënave përmes mjedisit cloud të Nimbus. SADM gjithashtu integron një politikë sigurie si pjesë e kornizës së saj për të detektuar sulmet e sigurisë DoS (Teardrop) që të zbulojë klientë me qëllim të keq. Wailly dhe kolegët prezantuan një Mjedis Virtual bazuar në Arkitekturë Vetë-Mbrojtëse (VESPA) [59] për të mbrojtur burimet e infrastrukturës duke përdorur qarqe sigurie autonome. Performanca e VESPA matet në terma të kohës së përgjigjes ndërsa zbulon sulmet e sigurisë U2R (rootkit). Sulistio dhe Reich [60] propozuan një arkitekturë të Shërbimit Cloud të Vetë-Mbrojtjes (CPCS) për të zvogëluar pengesën për adoptimin cloud, e cila ul shkeljet e Marrëveshjes së Nivelit të Shërbimit (SLA). Shërbimet cloud të ofruesve të ndryshëm (p.sh. Microsoft Azure, Amazon EC2 dhe

Google App Engine) krahasohen bazuar në sulmin e sigurisë R2L (SPY) për konfigurime të ndryshme të infrastrukturës.

Për të mbrojtur një rrjet kundër malware si sulmet e sigurisë DoS (LAND), Benkhelifa dhe Welsh [61] propozuan një mekanizëm të quajtur Malware Inspired Cloud Self-Protection (MICSP), i cili përdor analizën e nënshkrimeve për të zbuluar malware dhe për të parandaluar sistemin nga sulmet e tilla në të ardhmen. Paul [62] propozoi një Cloud të bazuar në Sistem të Menaxhimit të Mirëbesimit (CTMS) për të adresuar vërtetimin, autorizimin dhe integritetin e të dhënave të sigurisë së Cloud; gjithashtu mat efektin e sulmeve të sigurisë DoS në vonesën e futur gjatë përpunimit të vendeve të punës.

Tabela 3-1 Krahasimi i Teknikës SECURE me Teknikat Ekzistuese

Viti	Teknika	Mekanizëm Autonom	Lloji i Sulmeve	Analiza e Impaktit të Sigurisë sipas Cilësisë së Shërbimit	Parametrat e Performancës
2010	SAT	Po	DoS	Jo	Përdorimi i Burimeve
2011	SADM	Po	DoS	Jo	Përdorimi i Burimeve
2012	VESPA	Po	U2R	Jo	Koha e Përgjigjes
2013	CPCS	Po	R2L	Jo	Shkelje ndaj SLA
2014	MICSP	Po	DoS	Jo	Përdorimi i Burimeve
2015	CTMS	Jo	DoS	Jo	Vonesë
2016	SMVR	Po	U2R	Jo	Përdorimi i Burimeve
2017	SPDS	Po	R2L	Jo	Përdorimi i Burimeve
2018	SECURE (teknika e propozuar)	Po	Probing, DoS, R2L, U2R dhe DDoS	Po	Shpejtësia e dedektimit të ndërhyrjes, Koha e përgjigjes, Shpejtësia e gjenerimit të nënshkrimit, Shpejtësia Fals Pozitive

Di Pietro dhe kolegët e tij propozuan një teknikë të Menaxhimit të Sigurt për Burimet e Virtualizuara (SMVR) [63], nga të cilat zbulojnë sulmet e sigurisë U2R (buffer overflaw) gjatë kohës së ekzekutimit për të përmirësuar sigurinë e virtualizimit. SMVR zvogëlon shkeljen e sigurisë dhe përmirëson përdorimin e kujtesës. Sarhan dhe Carr propozuan një Skemë të Vetë-Mbrojtjes së të Dhënave (SPDS), [64] nga të cilat përdorin batch-eve aktive të të dhënave dhe agjenti siguron një llogaritje shumëpalëshe për të mbrojtur burimet e ndjeshme të të dhënave në një Cloud për përpunim. Më tej siguron një menaxhim të sigurt të çelësit duke përdorur algoritmin RSA për të mbrojtur sulmet e sigurisë së formës R2L (IMAP).

Tabela 3-1 tregon një krahasim kritik të sigurisë me qasjet ekzistuese bazuar në kritere të ndryshme. Teknikat ekzistuese të menaxhimit të burimeve marrin në konsideratë vetëm një lloj të sulmeve të sigurisë nga DoS, R2L, U2R, por gjithë tre llojet e sulmeve të sigurisë nuk janë marrë në konisderatë në të njëjtën kohë mesa dimë. Për më tepër, ekziston nevoja për parandalimin e sulmeve së sigurisë së DDoS dhe Hetimit.

SECURE mbron një sistem kompjuterik të bazuar në cloud nga pesë lloje të ndryshme të sulmeve të sigurisë duke përfshirë DDoS, Hetimet, U2R, R2L dhe DoS dhe analizon ndikimin e sigurisë në QoS. Më tej, performanca e Sigurisë është testuar në drejtim të kohës së përgjigjes, shkallës së rreme pozitive dhe shkallës së zbulimit të ndërhyrjeve. Vlerësimi i performancës tregon se Siguria performon në mënyrë efektive.

4 TEKNIKA SECURE DHE PËRMIRËSIMI I KËSAJ TEKNIKE DUKE PËRFSHIRË EDHE MBROJTJEN NGA SULMET UDP FLOOD DHE NTP AMPLIFICATION

Vitet e fundit, studiuesit janë përqendruar në identifikimin e teknikave të reja për zbulimin dhe parandalimin e ndërhyrjeve në sistemet kompjuterike dhe kanë zbuluar se Sistemi i Zbulimit të Ndërhyrjeve (IDS) është një mënyrë efektive për të mbrojtur rrjetin nga sulmet. IDS ndalon sulmet, kryen rikuperimin pas sulmeve dhe heton boshllëqet e sigurisë për të ndihmuar në shmangien e problemeve të tilla në të ardhmen. IDS-të mund të kategorizohen në dy lloje bazuar në anomali dhe nënshkrim. IDS e bazuar në nënshkrim përdoret për të zbuluar nënshkrimet e sulmeve të njohura në bazën e të dhënave, ndërsa IDS e bazuar në anomali analizon aktivitetet anormale. SNORT [2] është IDS-ja më efektive që mund të përdoret për zbulimin e sulmit. Për IDS-të e bazuara në anomali përdoren teknika të ndryshme të të mësuarit të makinës, por Makineria e Vektorit të Gjendjes (SVM) është detektori më i zakonshëm i bazuar në anomali.

Në këtë kapitull do të flasim për një teknikë e cila trajton sulmet e sigurisë, e cila quhet SECURE, Teknika me Vet-Mbrojtje në Manaxhimin e Burimeve Cloud (ang. **S**elf-prot**E**ction approa**C**h in clo**U**d **R**esource management) [5].

SECURE mund të krijojë nënshkrime të reja automatikisht dhe të ofrojë siguri kundër sulmeve të sigurisë DDoS, Hetimit, U2R, R2L dhe DoS. Bazuar në lakun MAPE-K, është zhvilluar një algoritëm për faza të ndryshme për të monitoruar, analizuar, planifikuar dhe ekzekutuar. SECURE monitoron vazhdimisht sulmet e sigurisë gjatë ekzekutimit të ngarkesave të punës, kryen analiza për të kuptuar alarme në rastin e sulmeve të sigurisë, bën një plan për të kryer veprime për të menaxhuar kërcënimet dhe ekzekuton veprimin. Agjentët e sigurisë (sensorët) krijohen në SVM si detektor anomalie. SECURE rrit sigurinë e shërbimeve të bazuara në cloud dhe rrit shkallën e zbulimit të ndërhyrjeve nëse i njëjti kërcënim arrin përsëri.

4.1 PREZANTIMI I TEKNIKAVE VET-MBROJTËSE TË ZHVILLUARA NDAJ KËTYRE SULMEVE

Më poshtë do të paraqesim arkitekturën e teknikës SECURE, e cila ofron vet-mbrojtje kundër sulmeve të sigurisë. Figura 4-1 tregon arkitekturën e teknikës SECURE dhe përfshin nën-njësitë e mëposhtme:

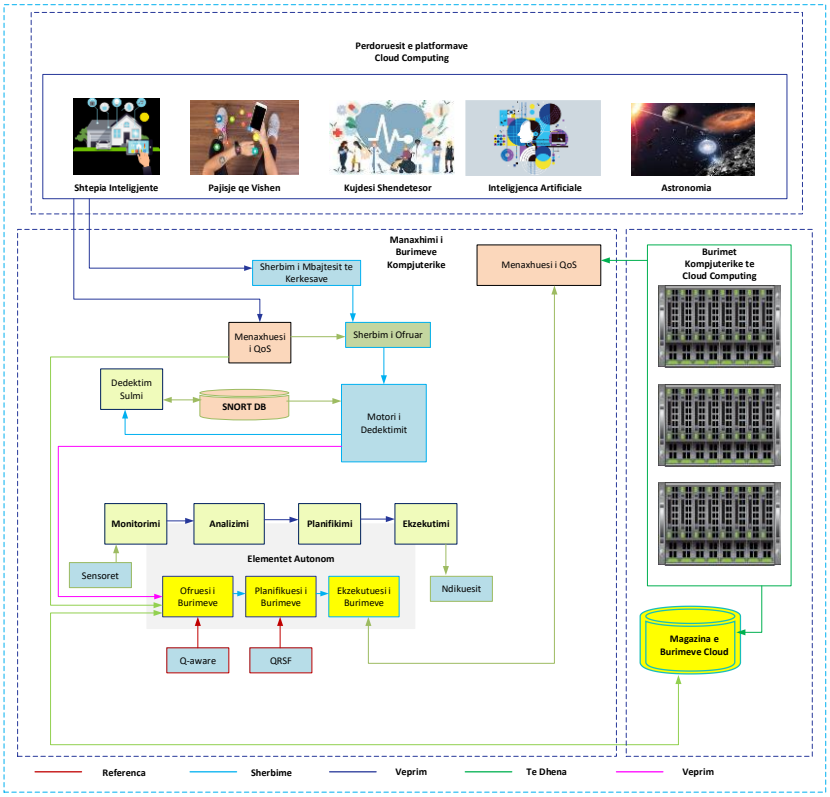

Figura 4-1 Arkitektura e Teknikës SECURE

- Përdoruesi i Cloud: Përdoruesit e Cloud paraqesin kërkesat e tyre për ekzekutim.
- Mbajtësi i shërbimit të kërkesave: Një mbrojtës për të ruajtur informacionin në lidhje me çdo kërkesë dhe për të kaluar ngarkesat e ndryshme të punës të Shërbimit Dispeçer.
- Menaxheri QoS: Identifikon kërkesat e ndryshme QoS të një kërkese të përdoruesit dhe ia përcjell Shërbimit Dispeçer.
- Shërbimi Dispatcher: Dërgon ngarkesat e punës së përdoruesit së bashku me kërkesat e tyre QoS te Motori i Zbulimit.
- Motori i Zbulimit: Përdor dy lloje IDS, i cili përdor kërkimin SNORT për nënshkrime të sulmeve të njohura në bazën e të dhënave (SNORT DB) dhe përdor një detektor anomalie të bazuar në SVM për të analizuar aktivitetet anormale (sulme të panjohura). Databaza e trajnimit përdoret për të hartuar SVM për të gjetur dhe diagnostikuar të dhëna të trafikut të rrjetit hyrës për të identifikuar sulmin. Një veprim merret sapo një sulm zbulohet dhe ruhet në bazën e të dhënave.
- Siguruesi i burimeve: Burimet sigurohen duke përdorur Q-aware [4], në të cilin identifikohen burime të përshtatshme për një ngarkesë të veçantë pune bazuar në kërkesat e tyre për QoS siç përcaktohet nga Menaxheri i QoS. Këto burime sigurohen më pas sipas kërkesave të përdoruesit.
- Planifikuesi i burimeve: QRSF [65] përdoret për të planifikuar burimet e siguruara me koston dhe kohën minimale të ekzekutimit.

- Ekzekutuesi i burimeve: Ekzekuton ngarkesat e punës duke përdorur burimet e planifikuara.
- Elementi Autonomik: Përfshin gjashtë përbërës: sensorin, monitorin, analizimin, planifikimin, ekzekutuesin dhe efektin.
- Monitori i Përdorimit të Burimeve: Mat vlerën e shfrytëzimit të burimeve gjatë ekzekutimit të ngarkesës së punës.
- Vendi i Burimeve Cloud: Ruan konfigurimin e burimeve Cloud.

Teknika SECURE mbron veten nga sulmuesit duke dalluar sjellje të paligjshme nga legjitime dhe duke kryer veprimet e kërkuara për të bllokuar ato kërcënime pa vetëdijen e përdoruesit. Kërcënimet e mbuluara nga SECURE janë DDoS, Hetimi, U2R, R2L dhe DoS. Për të qenë efikas, motori i zbulimit zbulon vazhdimisht sulmet e sigurisë gjatë përpunimit të ngarkesave të punës. Alarmet mund të stimulohen gjatë sulmeve të sigurisë. Figura 4-2 përshkruan hapat e sistemit autonom d.m.th. monitorimin, analizimin, planifikimin dhe ekzekutimin. Gjatë ekzekutimit të ngarkesave të punës në burimet e planifikuara, sensorët zbulojnë vlerën e QoS për sa i përket kohës së përgjigjes së ekzekutimit të detyrës. Pastaj, nyja e menaxherit mbledh informacion nga sensorët dhe përcjell informacionin e azhornuar drejt modulit të analizës.

4.1.1 Mekanizmi vet-mbrojtës – pseudo_kodi.

Figura 4.2 paraqet pseudo_kodin në lidhje me hapat që realizohen për të realizuar një sistem autonom si p.sh. monitorimi, analizimi, planifikimi dhe ekzekutimi.

```
# MONITORIMI
FILLIMI
Kapja e Paketes
Kryerja e analizes ne paketat e kapura
per te gjitha Pakeata
Do
   n.q.se Gjatesia e Ngarkeses se Paketes!= Varg (MIN, MAX) atehere
   ruaj informacionin e paketes ne log file
 end if
end for
#ANALIZIMI dhe PLANIFIKIMI
# Krijimi i log-ut
# kontrollo per Sulm Sigurie
Mblidh te gjitha alarmet e reja te gjeneruara nga AE [Elementi Automatik]
per te gjitha alarmet
 do
  Kryej analizen per te mare URL, Porten dhe detajet e Ngarkeses
  Kategorizo te dhenat te bazuara nga URL, Porta dhe Ngarkesa
  Per te gjetur nenstringen me te madhe te perbashket apliko LCS (Nensekuenca me e madhe e perbashket)
end for
#EKZEKUTIMIN
for te gjithe Nenshkrimet e Analizuara [SIGN_ANA]
do
  if SIGN_ANA Te Dhenat Ekzistuese atehere
     Nenshkrimi i bashkohet ekzistuesit
  else if SIGN_ANA = Ekziston tashme atehere
   'INJOROJE'
  else
    Shto nenshkrimin si e dhene e re
  end if
  end for
```

Figura 4-2 Hapat e sistemit Autonom si p.sh. monitorimi, analizimi dhe planifikimi, dhe ekzekutimi

Një agjent i sigurisë i bazuar në SVM zbulon anomalitë e reja dhe ruan informacionin në bazën e të dhënave për të mbajtur një regjistër rreth sulmeve. SECURE mbron nga sulmet

e sigurisë: DDoS (Përmbytja HTTP dhe Sulmi me ditë Zero), Hetimi (NMAP dhe Portet sweep), U2R (Buffer Overflow dhe Rootkits), R2L (IMAP, Guess password and SPY) dhe DoS (Teardrop, SYN Flood, LAND dhe Smurf) siç diskutohet në Tabelën 3.1. Për të zbuluar një sulm sigurie, do të regjistrohen vetëm ato paketa që përshtaten në intervalin siç është specifikuar. Motori i zbulimit zbulon modelin e çdo pakete që transferohet përmes rrjetit dhe krahasohet me modelin e paketave ekzistuese në bazën e të dhënave për të gjetur vlerën e gjatësisë së ngarkesës së paketës (diapazoni i paketës). Alarmi do të gjenerohet nëse gjatësia aktuale e ngarkesës është jashtë rrezes [Vlera (Min, Max)] dhe zbulohet sulmi.

Moduli i Analizimit dhe Planifikimit analizon sulmet e zbuluara dhe gjeneron një nënshkrim për zbulimin e sulmeve në të ardhmen. Figura 4-3 tregon funksionet e kryera për të gjeneruar nënshkrimin.

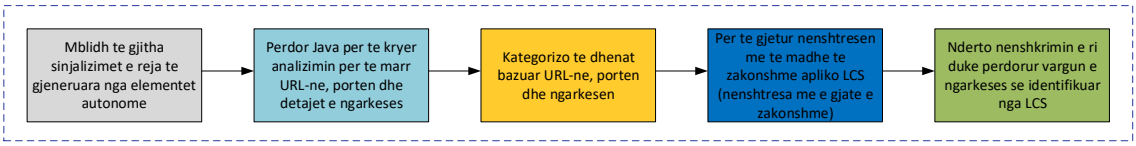

Figura 4-3 Procesi i gjenerimit të nënshkrimit

Për Modulin e Ekzekutimit, SNORT IDS përmirëson nënshkrimet e marra nga modulet e mëparshme dhe krahason nënshkrimet e krijuara rishtas me nënshkrimet ekzistuese të ruajtura në bazën e të dhënave SNORT. Nënshkrime të reja shtohen në bazën e të dhënave SNORT dhe informacioni i ri bashkohet me nënshkrimet ekzistuese. Informacioni i azhornuar midis elementeve autonome shkëmbehet nga Effector, i cili komunikon informacione të azhornuara rreth sinjalizimeve, rregullave dhe politikave të reja.

4.2 VLERËSIMI I PERFORMANCËS

Figura 4-4 tregon konfigurimin eksperimental, i cili përdoret për të vlerësuar performancën e SECURE. SNORT është një detektor i bazuar në nënshkrime dhe punon në Rrjetet e Protokollit të Internetit për të ekzaminuar rrjetin në kohë reale për identifikimin e aktivitetit me qëllim të keq. Ajo gjeneron "nënshkrime analize" duke krahasuar nënshkrimet e ruajtura tashmë në bazën e të dhënave SNORT dhe përsos, finalizon dhe ruan nënshkrime të reja në bazën e të dhënave SNORT. SVM përdoret për të zbuluar sjellje anormale (sulme të panjohura). Mjete të ndryshme (NMAP për hetim, DAVOSET për DDoS, NetCat për L2R, Hydra për R2L dhe metasploit për DoS) përdoren në këtë punë kërkimore për të nisur sulme të ndryshme.

Eksperimentet janë kryer për pesë lloje të ndryshme sulmesh (DDoS, Sondë, U2R, R2L dhe DoS) duke krahasuar SECURE me teknikat ekzistuese të menaxhimit të burimeve të vetëdijshëm për sigurinë, dmth Skema e të Dhënave të Vetë-Mbrojtjes (SPDS) [64] Ngarkesa e punës është shndërrimi i skedari të madh të imazhit me madhësi 713 MB nga formati JPEG në formatin PNG.

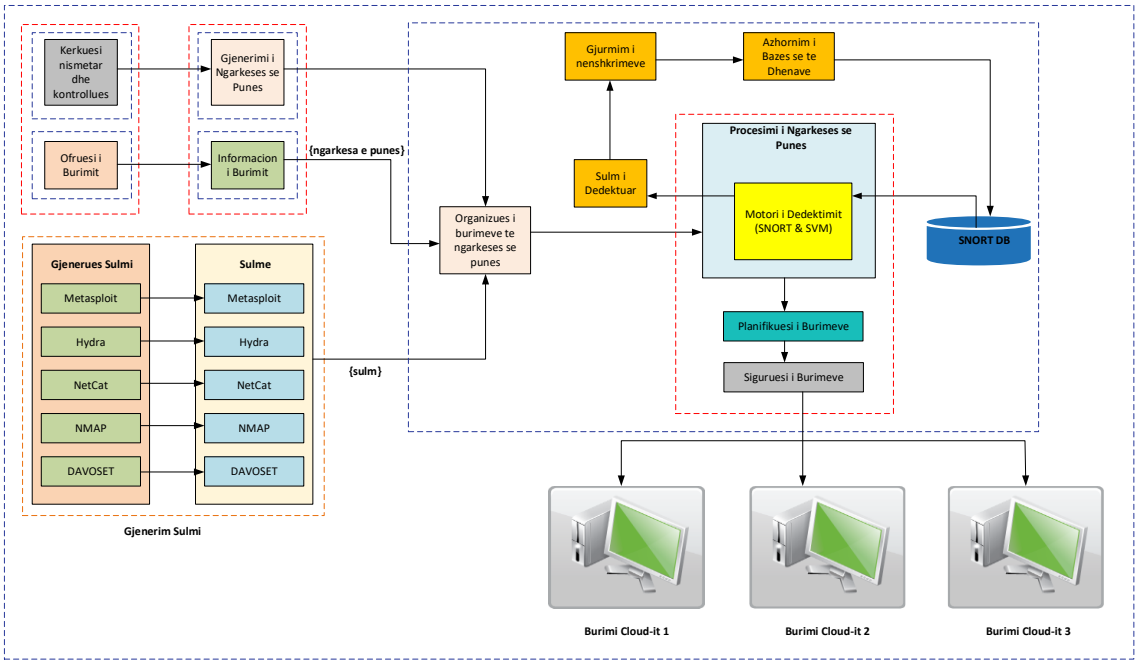

Figura 4-4 Konfigurimi Eksperimental i Teknikës SECURE

Ekuacioni 1 përshkruan shpejtësinë fals pozitive (ang. False Positive Rating - FPR), i cili është raporti i *Fals Pozitive* ndaj mbledhjes së *Fals Pozitive* dhe *Vertetë Pozitive*.

$$FPR = \frac{\text{FalsPozitive}}{\text{FalsPozitive} + \text{VertetePozitive}} \quad (1)$$

FPR zvogëlohet në SECURE me kalimin e kohës dhe është minimumi në 50 orë siç tregohet në Figurën 4-5. Ne kemi konsideruar pesë lloje sulmesh (DDoS, Sondimi, U2R, R2L dhe DoS) dhe kemi matur vlerën e FPR për secilin sulm. Vlera e FPR është më e lartë për R2L krahasuar me sulmet DDoS, Sondime, U2R dhe DoS.

Ekuacioni 2 përshkruan Shkallën e Zbulimit të Ndërhyrjes (IDR), e cila është "raporti i numrit të përgjithshëm të *Vertetë Pozitive* me numrin e përgjithshëm të ndërhyrjeve".

$$IDR = \frac{\text{NumriTotalVertetePozitive}}{\text{NumriTotaliNderhyrjeve}} \quad (2)$$

IDR konsideron numrin e sulmeve të zbuluara dhe të bllokuara dhe vlera e tij rritet në lidhje me kohën. Për të shmangur të njëjtin sulm, nënshkrimet e reja ruhen në bazën e të dhënave vazhdimisht. Për sulmet e njohura, ky eksperiment është kryer. Figura 4-6 tregon qartë se SECURE jep rezultate më të mira krahasuar me SPDS për sa i përket IDR.

Më tej, për më shumë verifikime të SECURE, nënshkrimet e disa sulmeve të njohura janë hequr nga baza e të dhënave SNORT.

Figura 4-7 tregon që IDR po rritet në lidhje me kohën. Një eksperiment për 144 orë është kryer për verifikimin e SECURE dhe rezultatet tregojnë se SECURE performon më mirë sesa SPDS për sa i përket IDR dhe performanca SECURE është e jashtëzakonshme pas 120 orësh. Figura 4-8 tregon ndryshimin e IDR në lidhje me numrat e ndryshëm të ngarkesave të punës dhe llojet e ndryshme të sulmeve të sigurisë. Me ndryshimin e numrit të ngarkesave të punës, vlera e IDR gjithashtu po rritet. Figura 4-8 tregon që SECURE performon më mirë në hetim.

Niveli i Gjenerimit të Nënshkrimit (SGR) përcaktohet si përqindja e nënshkrimeve të krijuara me kalimin e kohës. Figura 4-9 tregon sesi llogaritet SGR si për SECURE ashtu edhe për SPDS dhe tregon se SECURE ka shkallë më të lartë të gjenerimit të nënshkrimeve sesa SPDS.

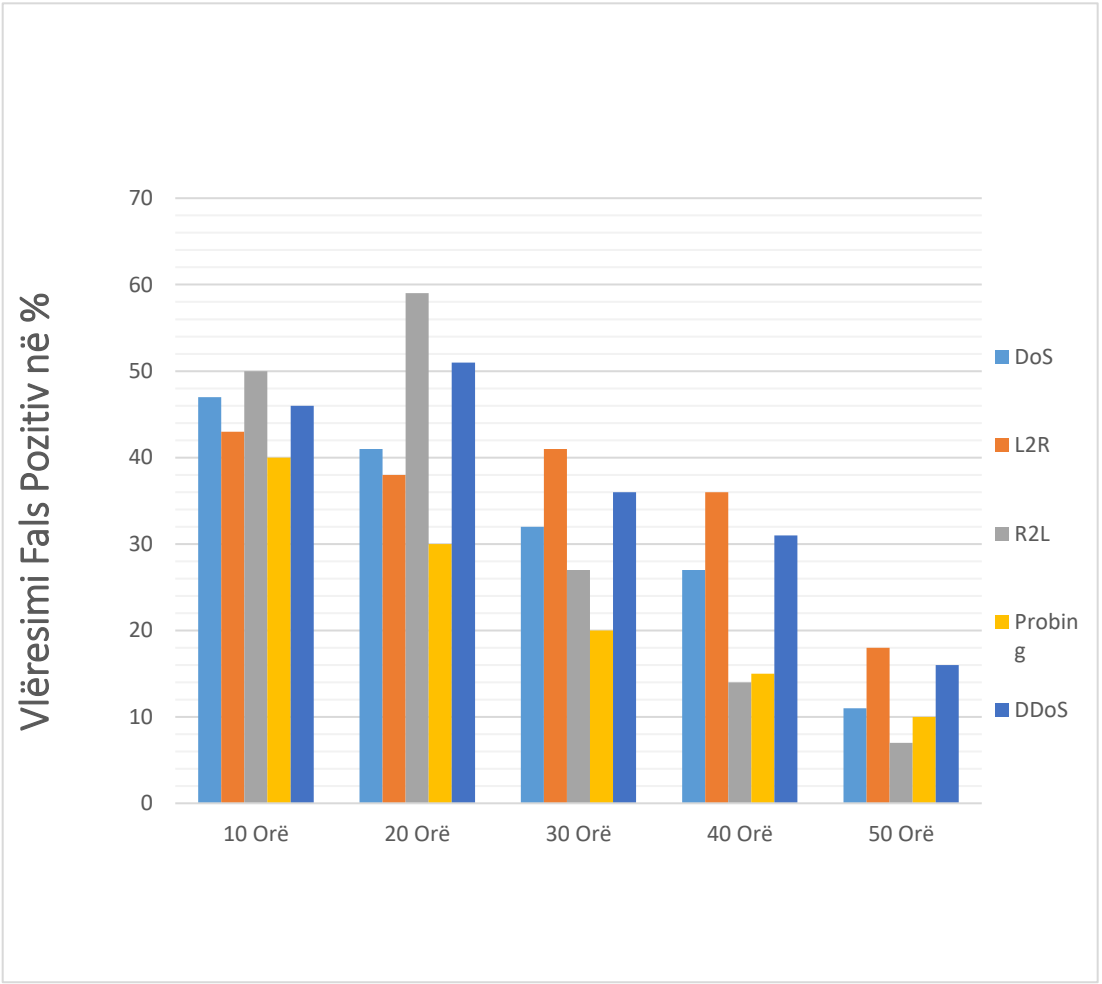

Figura 4-5 Shpejtësia Fals Pozitve përkundrejt Kohës

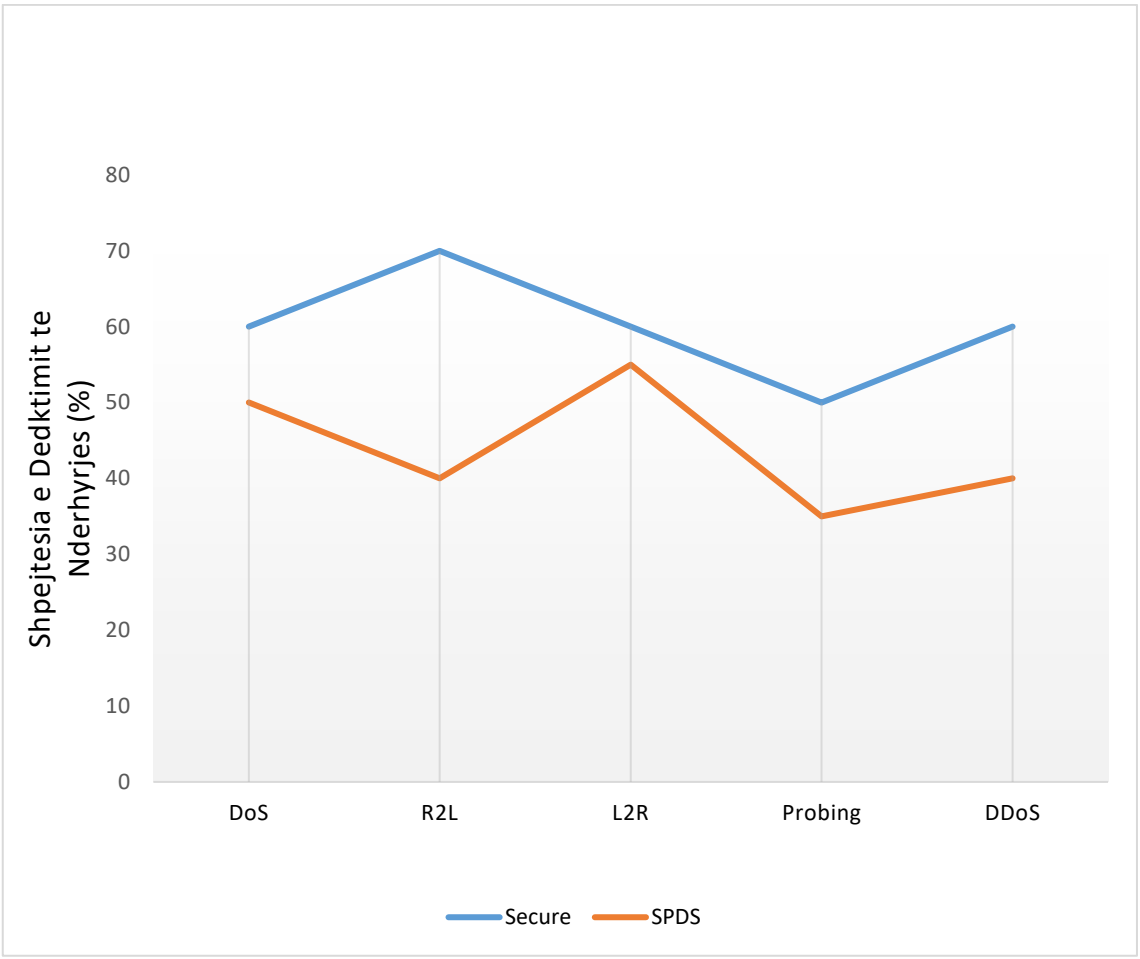

Figura 4-6 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Sulmeve

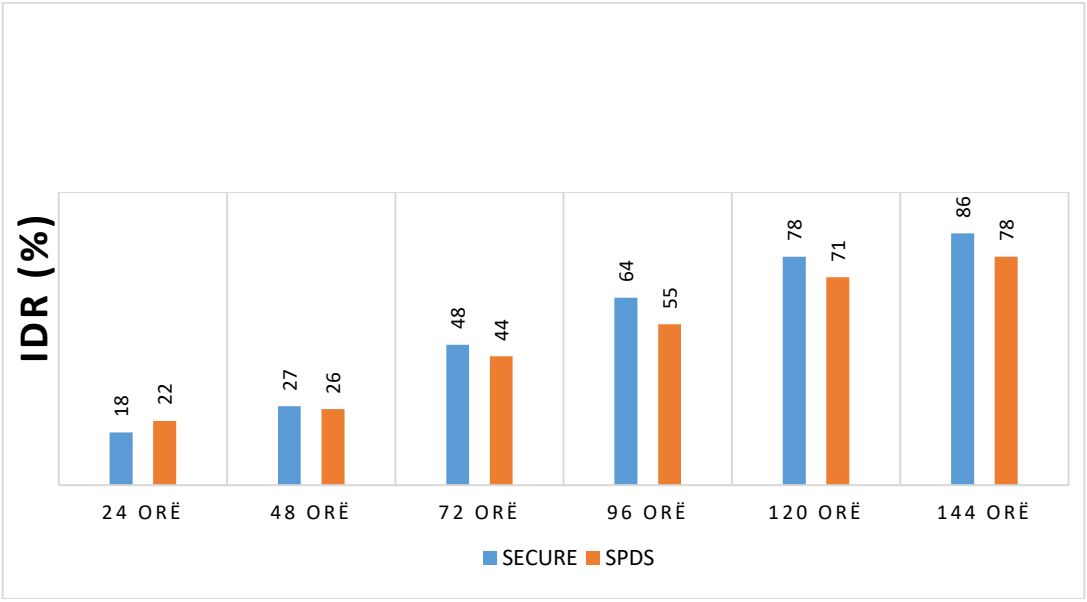

Figura 4-7 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Kohës

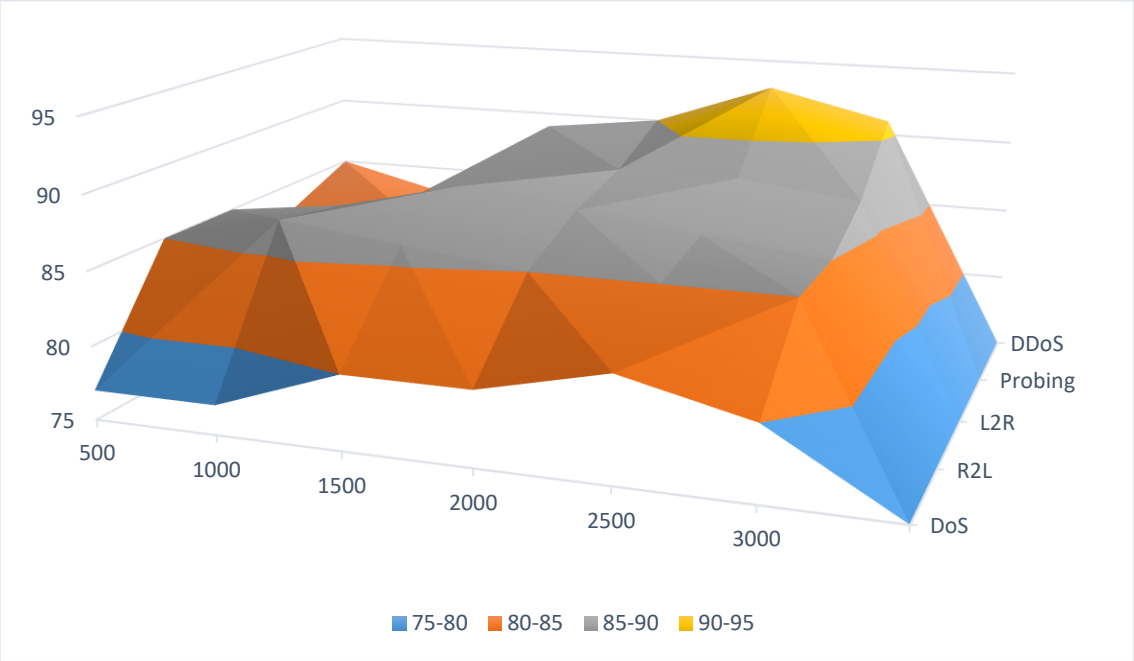

Figura 4-8 Shpejtësia e Dedektimit të Ndërhyrjes (IDR) përkundrejt Sulmeve

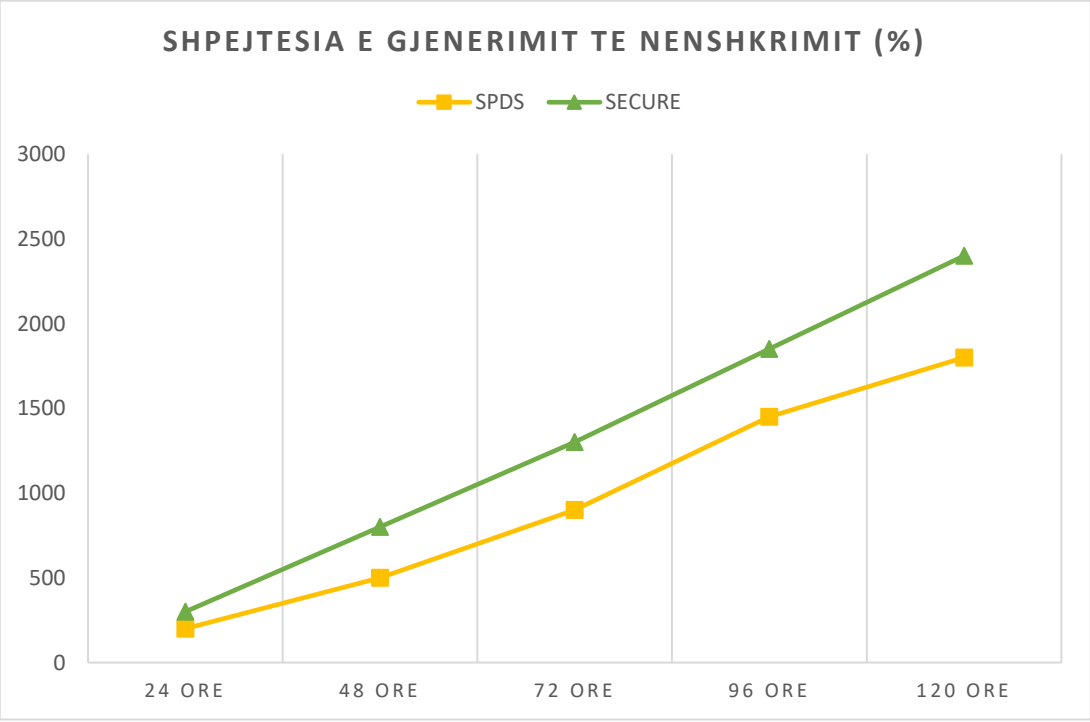

Figura 4-9 Shpejtësia e Gjenerimit të Nënshkrimit (SGR) përkundrejt Sulmeve.

4.3 Zgjerimi i Teknikës SECURE për Mbrojtjen Nga Sulmet e Tjera DDoS (UDP Flood dhe NTP Amplification)

Ne propozojmë qasjen SECURE për vetëmbrojtje ndaj sulmeve të sigurisë. SECURE mbron ekzekutimin e sistemit nga pesë lloje të ndryshme të sulmeve të sigurisë duke përfshirë DDoS, Probing, U2R, R2L dhe DoS, dhe analizon ndikimin e sigurisë në QoS gjatë përpunimit të kërkesave të përdoruesve. Rezultatet eksperimentale tregojnë se performanca e SECURE është më e mirë se teknikat ekzistuese, të cilat ofrojnë shërbime të sigurta të bazuara në Cloud duke mbrojtur nga sulmet e sigurisë.

Studimin tonë do ta bazojmë në përmirësimin e kësaj teknike duke përfshirë edhe sulmet e tjera DDos si UDP Flood dhe NTP Amplification. M.q.s këto sulme janë bërë më të vështira për t'u dedektuar dhe ndaluar atëherë përmirësimi i kësaj teknike duke konsideruar këto sulme bëhet më i rëndësishëm.

5 TEKNIKA E MBROJTJES SECURE+ NË PLATFORMAT CLOUD COMPUTING

Siç e kemi përmendur qëllimi kryesor i këtij punimi doktoral është krijimi i një mekanizmi vetmbrojtës dhe automatik ndaj ndërhyrjeve dhe sulmeve (të njohura dhe të panjohura) të kryera ndaj platformave Cloud. Në këtë punim ne do të propozojmë një teknikë me vet mbrojtje dhe ndërveprim automatik në menaxhimin e burimeve cloud të quajtur SECURE+. Kjo teknikë do të përmirësojë teknikën SECURE duke ndikuar mbi metrikët e rëndësishëm si Norma e Dedektimit të Ndërhyrjeve (IDR), Normën Fals Pozitive (FPR) si dhe në përdorim më të ulët të burimeve kompjuterike (CPU, RAM dhe gjerësi brezi). SECURE+ do të krijojë nënshkrime automatike dhe do të ofrojë siguri përkundrejt sulmeve të sigurisë të llojeve DoS, DDoS, Probing, U2R dhe R2L. Ky studim do të bazohet në metodën XGBoost (ang. eXtreme Gradient Boosting). XGBoost është një algoritëm i të Mësuarit Automatik me një bashkësi vendimesh të bazuara në strukturën pemë, i cili përdor një kornizë përforcimi të gradientit. Motivimi kryesor është ndërtimi i një modeli klasifikues të fuqishëm, i cili në bashkëpunim me sistemin SNORT IDS të mundet të klasifikojë të dhënat e futura në rrjet me sa më shumë saktësi të jetë e mundur, sa më shpejtë dhe me një përdorim sa më të ulët të burimeve kompjuterike te vendosura në dispozicion.

Në këtë punim, ne do të japim rezultate të cilat na vërtetojnë se XGBoost është më i përshtatshëm për të ndërtuar një model të fuqishëm klasifikimi. Kjo do të çojë në një sistem dedektimi të ndërhyrjes më të saktë dhe si rrjedhojë një mjedis më të sigurtë për të ndarë informacionin në platformat cloud.

Teknika SECURE+ do të ndërtohet për të evidentuar sulmet nga nje kombinim midis sistemit të dedektimit të sulmeve i quajtur SNORT dhe teknikës XGBoost. SNORT do të përdoret për të evidentuar sulmet e njohura mbi bazën e të dhënave që kjo teknikë zotëron (sulme të njohura). Ndërsa për të evidentuar aktivitetet anormale (pra sulmet e panjohura) do të përdoret një nga teknikat më të reja të algoritmit me vendimarrje pemë (ang. Decision Tree) të Mësimit Automatik (ang. ML - Machine Learning) e quajtur Fuqizimi Ekstrem i Gradientit (ang. XGBoost-eXtreme Gradient Boosting). Me anë të këtij algoritmi do të bëhet e mundur krijimi i një baze të dhënash e cila do të quhet databaza e trajnimit dhe do të projektojë XGBoost për të identifikuar dhe diagnostikuar sulmet nga

të dhënat e trafikut të rrjetit hyrës. Teknika SECURE+ do të krijojë automatikisht një nënshkrim të ri dhe do të ofrojë siguri ndaj sulmeve të tipeve DoS, DDoS [UDP Flooding dhe NTP Amplification], Probing, U2R dhe R2L. Kjo teknikë do të ofrojë një sistem dedektimi të ndërhyrjes dhe shmangieje të sulmeve kompjuterike me mënyrën e përmirësimit të gradientit sipas teknikës të vendimit pemë siç paraqitet në Figurën 5-1, në mënyrë automatike, duke realizuar një analizë inteligjente të rrjedhës së paketave në rrjet, si dhe duke u ndjekur nga veprimet e shmangies, të cilat janë në përputhje me vendimarrjen e komponentëve të dedektimit të ndërhyrjes. Dedektimi pikë-më-pikë i ndërhyrjes dhe procesit të shmangies bazohet në tre aplikacione bazë të quajtura, Krijimi i Karakteristikave, Rritja/Përmirësimi e/i Gradientit dhe Shmangia e Sulmit.

Ne kemi zgjedhur të perdorim metodën e Përmirësimit të Gradientit për shkak se kjo metodë është konsideruar metoda me efektive dhe më e vlefshme në rastin kur bëhet fjalë për detyra me të dhëna të strukturuara (siç është dhe rasti i studimit tonë).

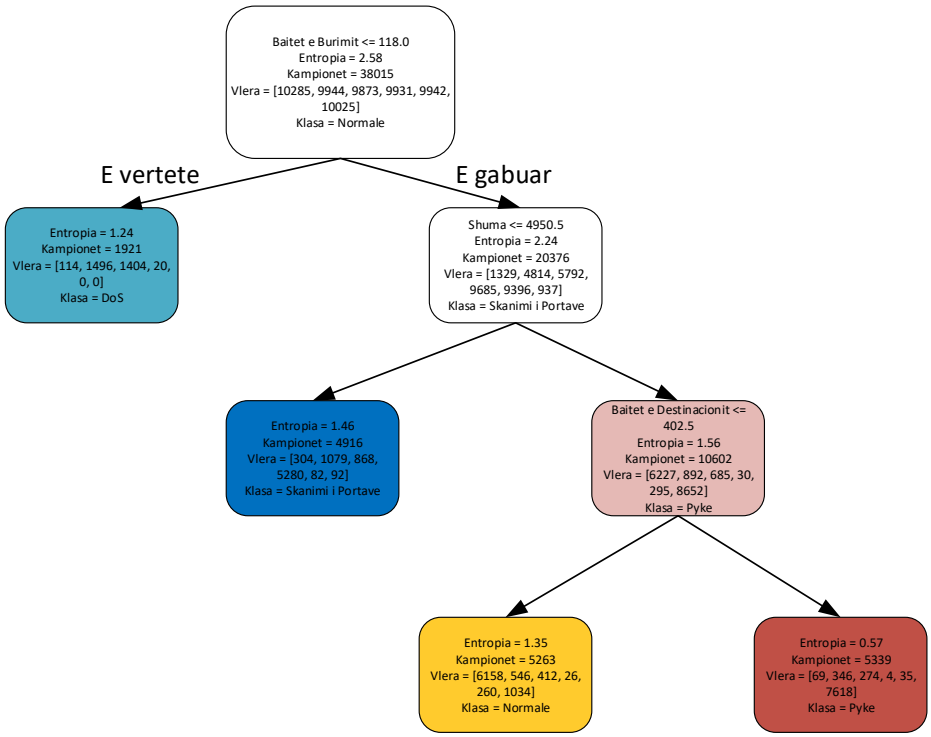

Figura 5-1 Shembull Vendimi Pemë për Përmirësimin e Gradientit gjatë Detyrës së Dedektimit të Ndërhyrjes së Rrjetit

5.1 BLLOQET FUNKSIONALE TË TEKNIKËS SECURE+

Në këtë seksion do të paraqesim arkitekturën e teknikës SECURE+ e cila do të ofrojë një mekanizëm vet-mbrojtës, automatik dhe autonom ndaj sulmeve kibernetike të përmendura më lart. Arkitektura e teknikës SECURE+ jepet në Figurën 5-2 dhe komponentët kryesor të saj paraqiten më poshtë:

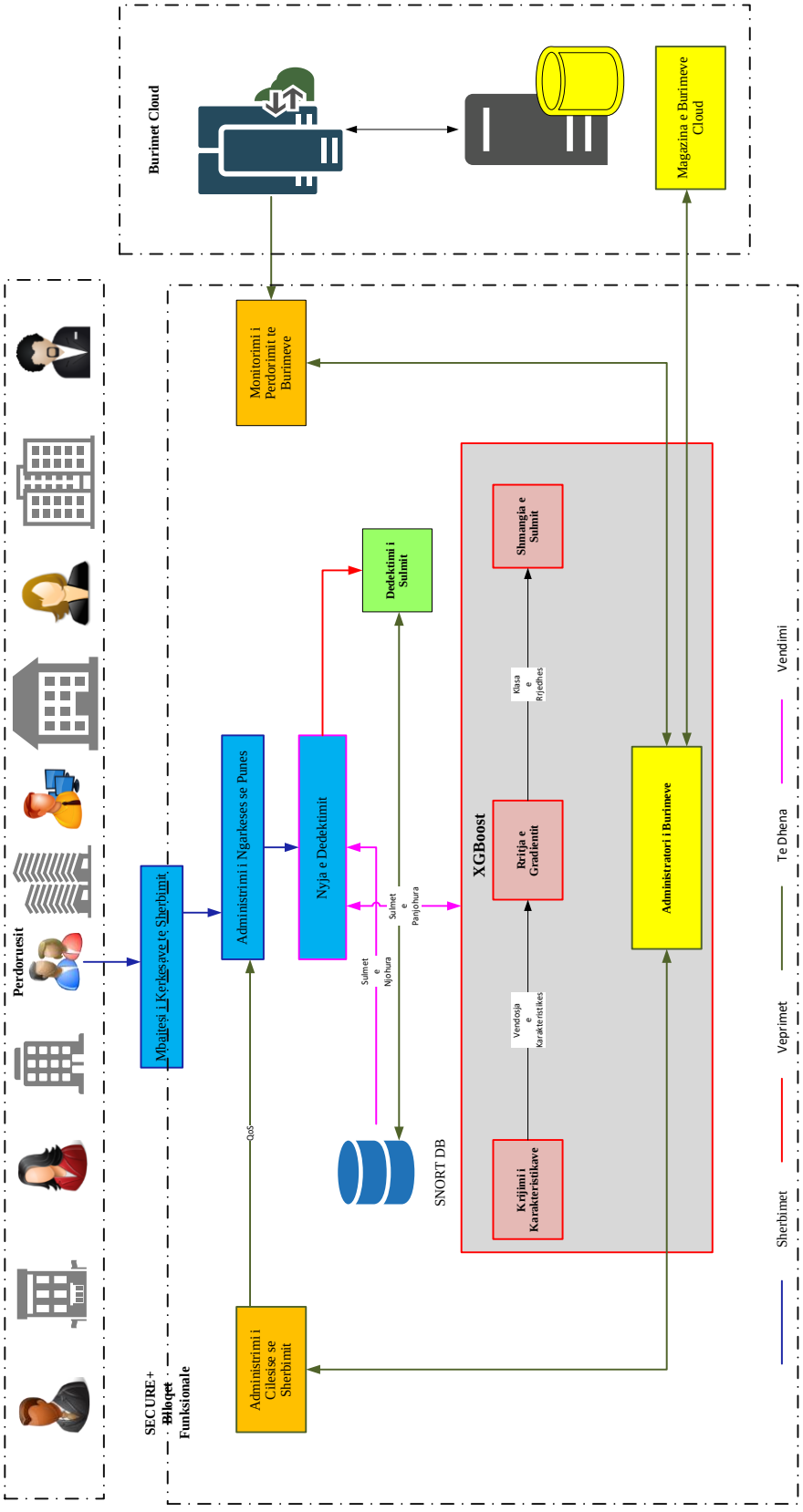

Figura 5-2 Arkitektura e teknikës SECURE+

- Përdoruesit e platformës cloud paraqesin kërkesat e tyre për ekzekutim.
- Të gjitha kërkesat e përdoruesve ruhen nga një buffer i cili quhet Mbajtësi i Kërkesave të Shërbimit. Ky buffer më pas përcjell ngarkesën e punës drejt Administratorit të Ngarkesës së Punës.
- Administratori i ngarkesës së punës shpërndan ngarkesën e punës sëbashku me kërkesat e tyre për Cilësinë e Shërbimit (ang. QoS - Quality of Service) tek Nyja e Dedektimit.
- Nyja e dedektimit për t'u mbrojtur nga sulmet realizon një mbrojtje me dy nivele. Niveli i parë aplikohet për sulmet e njohura dhe kryhet nga aplikacioni i dedektimit të ndërhyrjeve SNORT. Ndërsa Niveli i Dytë është për sulmet e panjohura dhe kryhet nga algoritmi i mësimit automatik me vendimarrje pemë (ML), i bazuar mbi teknikën më të fundit XGBoost.
- Administratori i Burimeve mban informacionin e burimeve ku përfshihen numri i përdorur i CPU-ve, kapaciteti i përdorur i RAM dhe numrat e burimeve. Ai gjithashtu, ruan informacionin rreth burimeve të disponueshme dhe atyre të rezervuara me përshkrimet respektive (emri i burimit, tipi i burimit, konfigurimi, informacioni i disponueshmërisë dhe informacioni i përdorimit) sipas ofruesit të shërbimeve cloud.
- Niveli autonom përbëhet nga 3 elemente të cilët janë: krijimi i karakteristikave, përmirësimi i gradientit dhe shmangësi automatik i sulmit.
- Monitoruesi i Përdorimit të Burimeve i cili mat vlerën e përdorimit të burimeve gjatë ekzekutimit të ngarkesës së punës.
- Magazina e Burimeve Cloud ruan konfigurimin e burimeve cloud.

5.1.1 Sistemi i Dedektimit të Sulmeve të Njohura nëpërmjet SNORT

SNORT është një Sistem Dedektimi i Ndërhyrjeve në Rrjet (ang. NIDS- Network Intrusion Detection System). Ai përdor një strukturë monitorimi të quajtur Libpcap, për të gjurmuar dhe rregjistruar paketat në rrjet. Karakteristika e tij e modelit të njëjtë të bazuar në rregulla të përcaktuara, dedekton sulmet në kohe reale të tillat si tej mbushja e buffer-it, sulmet DoS dhe sulmet DDoS. Teknikat e filtrimit që ofrohen nga Snort e bëjnë atë një sistem efektiv të dedektimit të ndërhyrjeve (IDS). Snort kryesisht ofron ekzekutimin në tre mënyra të ndryshme. Ato janë:

1- mënyra e gjurmimit,

2- mënyra e rregjistrimit të paketës dhe

3- mënyra e sistemit të dedektimit të ndërhyrjes në nivel rrjeti (NIDS).

Mënyra e tretë është edhe mënyra ku ne do të bazohemi për realizimin e punimit tonë. Në mënyrën NIDS, Snort gjeneron mesazhe alarmesh për dedektimin dhe analizën e realizuar mbi trafikun e rrjetit. Rregullat e shkruara në [107], [108] gjenden në mënyrën NIDS.

Konfigurimet për të filtruar paketat e dëmshme nga ato legjitime të dhëna nga snort janë filtrimi “Normë” dhe filtrimi “Ngjarje”. Në këtë punim ne do të bazohemi tek teknika e filtrimit “Normë”.

Ekzistojne mënyra të shumta për të gjeneruar mesazhe alarmi, në rastin e mënyrës të dedektimit të ndërhyrjes në nivel rrjeti. Midis tyre shumë autorë dhe kërkues të ndryshëm i përdorin ato në literaturë si “Alarm” dhe “Filtri_i_Normës” për të dedektuar dhe filtruar paketat e dëmshme nga ato legjitime në nivel rrjeti. Mënyra “Alarm” përdoret për të gjeneruar mesazhet e alarmit të cilat përmbushin vlerat e atributit të përdorura në dosjen e rregullit të paracaktuar. Mënyra “Filtri_i_Normës” është një parametër konfigurimi i përdorur për të filtruar paketat. Ekzistojnë shumë attribute në këtë parametër.

Midis tyre, dedektimi nga burimi dhe dedektimi nga destinacioni janë dy mënyrat e ndryshme për të rrëzuar paketat të cilat do të përdoren në rastin tonë në teknikën SECURE+.

Mesazhi i alarmit në teknikën SECURE+ do të hartohet sipas [107] dhe jepet më poshtë:

*“drop TCP any any -> any 80 (*
*Msg:”Reset outside window”, *
*Detection_filter:track by_src, count 30, seconds 1; *
New_action drop; timeout 50; sid:100001;)”

Rregulli i mësipërm i specifikon snortit të rrëzojë paketat e tipit TCP të cilat vijnë nga çdo adresë IP dhe çdo portë të destinuar për çdo adresë IP në portën 80 nëse ai dhunon sekuencë ID-në sid: 1000001 tridhjetë herë në një sekondë. Dedektimi i paketave bëhet duke përdorur mënyrën “dedektimin nga burimi”. Atributi i përdorur për këtë mënyrë është “by_src”. Kjo mënyrë i tregon snort-it të gjurmojë paketat nga adresa IP e burimit. Për të shkaktuar rregullin për këtë mënyrë, snort do të rrëzojë paketat pa marë parasysh destinacionin.

Rregullin tjetër që do të implementohet në teknikën SECURE+, i cili bazohet në [108] jepet si më poshtë:

*“rate_filter *
*gen_id 1, sig_id 100001, track by_dst, *
count 30, seconds 5, new_action drop, timeout 30”

Rregulli i mësipërm i tregon snort-it që të gjurmojë adresën IP të destinacionit kur filtri bëhet aktiv dhe rrëzon paketat pavarësisht nga burimi.

Rregulli i dedektimit i implementuar në këtë rast përshkruhet si më poshtë:

 # TCP rule that detects TCP packet with the SYN flag on in destination of an FTP server.
*"alert tcp $EXTERNAL_NET any -> $HOME_NET 21 *
(flags: s; msg:"FTP – TCP FLAG"; classtype:attempted-dos;
sid:100001; rev:1;)"

Rregulli i mësipërm specifikon që snort të krijojë një rregull me sekuencë ID sid 100001. Ai gjeneron mesazhet e alarmit për paketat TCP të cilat vijnë nga rrjeti i jashtëm EXTERNAL_NET (adresa IP e sistemeve të përdoruesit) me çdo portë të destinuar drejt rrjetit të brendshëm HOME_NET (adresa IP e serverit që duhet të mbrojë IPS).

5.1.2 Sistemi Autonom i Dedektimit të Sulmeve të Panjohura nëpërmjet Teknikës me mësim automatik (ML)

Teknika SECURE+ konsideron 3 hapa në lidhje me sistemin autonom të dedektimit dhe ndërveprimit. Ndërveprimi i këtyre nën-njësive përshkruhet në Figurën 5-3 siç janë: Krijimi i Karakteristikave, Përmirësimi/Rritja e Gradientit dhe Shmangësi i Sulmit.

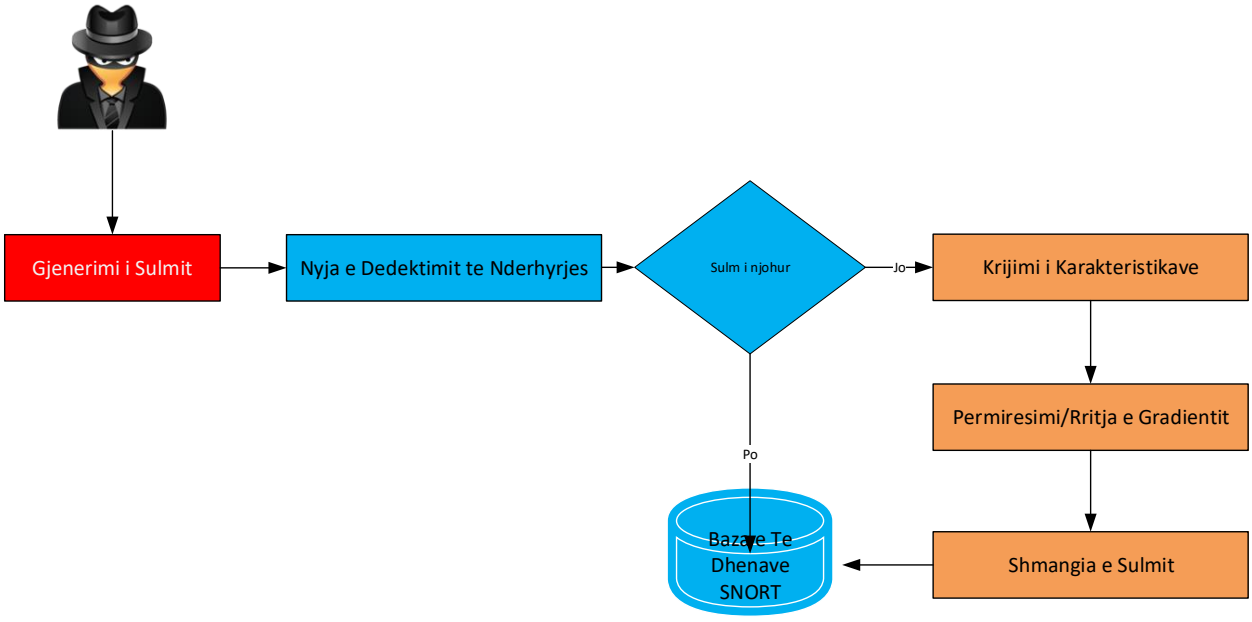

Figura 5-3 Ndërveprimi i nën-njësive të sistemit autonom

Krijuesi i karakteristikave mbledh trafikun e rrjetit nga nyja e dedektimit të ndërhyrjes në rast se sulmi është i panjohur për snort dhe përllogarit vlerat e karakteristikave që kërkohen nga Përmirësuesi i Gradientit për fluksin respektiv. Përmirësuesi i Gradientit

aplikon modelet e tij të para-ndërtuara të dedektimit të ndërhyrjes mbi shembullin e fluksit dhe e kalon rezultatin drejt Shmangësit të Sulmit. Pastaj shmangësi i sulmit përcakton veprimin që duhet të marrë, të bazuar në rezultatin klasifikues dhe instalon rregullat e fluksit në dedektuesin e sulmit për të parandaluar sulmin nëse është e nevojshme.

5.1.3 Menaxhimi i Burimeve Kompjuterike

Në bazë të informacionit të burimeve, informacionit të ngarkesës së punës dhe informacionit të Cilësisë së Shërbimeve, burimet kompjuterike provizionohen nga teknika e provizionimit të burimeve Q-aware për ekzekutimin e ngarkesës së punës [110]. Mbas provizionimit të burimeve, caktimi i burimeve aktuale realizohet në bazë të teknikës së planifikimit QRSF [109]. Mbas planifikimit dhe caktimit të burimeve, fillon ekzekutimi i ngarkesës aktuale të punës. Gjatë ekzekutimit të ngarkesës së punës, performanca e përdorimit të burimeve monitorohet në mënyrë të vazhdueshme duke përdorur njësinë e Monitorimit të Përdorimit të Burimeve, kjo për të siguruar efektivitetin e teknikës SECURE+ e cila gjeneron alarme në rast të degradimit të performancës. Alarmi mund të gjenerohet në rast se nuk ka burime të mjaftueshme në dispozicion për të ekzekutuar ngarkesën e punës (veprimi: ricaktimi i burimeve). Në Figurën 5-4 jepet ndërveprimi i përdoruesit cloud dhe ofruesit të shërbimeve cloud në caktimin e burimeve.

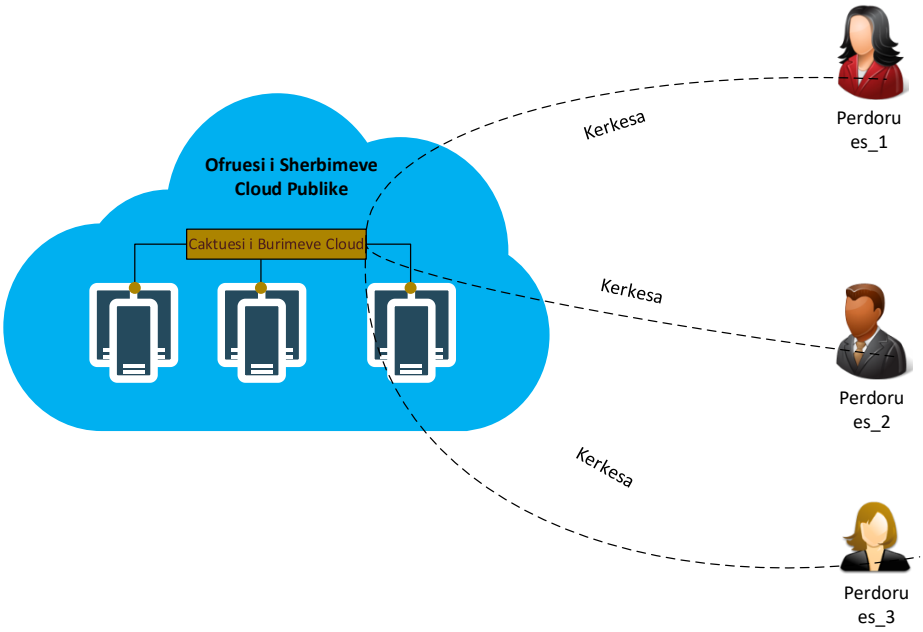

Figura 5-4 Caktimi i Burimeve në platformat Cloud

5.2 METRIKËT BAZË TË TEKNIKËS SECURE+

Më poshtë pasqyrohen metrikët të cilët do të studiohen për të vlerësuar efektivitetin dhe performancën e teknikës SECURE+ përkundrejt teknikës SECURE. Ekuacioni 1 përshkruan Normën Fals Pozitive (NFP) (ang. FPR – False Positive Rate) e cila është raporti Fals Pozitive përkundrejt shumës Fals Pozitive dhe E Vërtetë Negative.

$$Norma\ Fals\ Pozitive\ (NFP) = \frac{Fals\ Pozitive}{Fals\ Pozitive + E\ Vertete\ Negative} \quad (1)$$

Ekuacioni 2 përshkruan Normën Fals Negative (NFN) (ang. FNR – False Negative Rate) e cila është raporti Fals Negative përkundrejt shumës Fals Negative dhe E Vërtetë Pozitive.

$$Norma\ Fals\ Negative\ (NFN) = \frac{Fals\ Negative}{Fals\ Negative + E\ Vertete\ Pozitive} \quad (2)$$

Metrika e tretë që do të përdoret për krahasimin jepet në ekuacionin 3. Ky ekuacion përshkruan Normën e Dedektimit të Ndërhyrjes (ang. IDR – Intrusion Detection Rate), e cila është raporti i numrit të përgjithshëm fals pozitive me numrin e përgjithshëm të ndërhyrjeve.

$$Norma\ e\ Dedektimit\ te\ Nderhyrjes\ (IDR) = \frac{Numri\ Total\ Fals\ Pozitive}{Numri\ Total\ i\ Nderhyrjeve} \quad (3)$$

IDR konsideron numrin e sulmeve të dedektuara dhe të bllokuara dhe vlera e tij rritet me kalimin e kohës. Për të shmangur të njëjtin sulm, nënshkrimet e reja ruhen në mënyrë të vazhdueshme në databazën e aplikacionit SNORT.

Metrika e katërt që do të studiohet është përdorimi i burimeve cloud në teknikën SECURE+ dhe krahasimi i tyre me ato të përdorura në teknikën SECURE. Ky metrik do të llogaritet duke monitoruar kohën e ekzekutimit ndërmjet dy teknikave gjatë ngarkesës së punës. Ekuacioni 4 përdoret për të përllogaritur kohën e ekzekutimit (Et_i)

$$Koha\ e\ Ekzekutimit\ (Et_i) = \sum_{i=1}^{n} \left(\frac{PN_i - SN_i}{n}\right) + \Delta t_i \quad (4)$$

Ku PN_i është koha e përfundimit të ngarkesës së punës dhe SN_i është koha e paraqitjes/shfaqjes së ngarkesës së punës dhe Δt_i është koha për fikjen-ndezjen e nyjes dhe n është numri i ngarkesave të punës. Koha e ekzekutimit përfaqëson në këtë mënyrë përdorimin e burimeve.

5.3 FUNKSIONIMI I TEKNIKËS SECURE+

Synimi kryesor vet-mbrojtës në teknikën SECURE+ është mbrojtja e komunikimit klient – platform cloud nga sulmet e qëllimshme. Në thelb, teknika SECURE+ punon duke gjurmuar aktivitetet e dyshimta dhe përgjigjet në përputhje me rrethanat për të mbajtur të paprekur komunikimin klient-platformë cloud dhe të mos cënohet siguria në të dyja anët e komunikimit.

Sistemi trajnohet për të diferencuar sjelljet legjitime dhe keqdashëse në mënyrë që të zbatoj mbrojtjen në mënyrën e duhur. Siç është përmendur, SECURE+ është projektuar për të mbrojtur një komunikim cloud ndaj sulmeve DoS, DDoS [UDP Flooding dhe NTP Amplification], Probing, U2R dhe R2L. Në rastin e sulmit DoS, mohimi i shërbimit (ang. Denial of Service), gjenerohet një sasi e madhe trafiku nga sulmuesit për të shkaktuar dëmtim nga përmbytja e rrjetit të viktimës [111].

Këtu mund të përmendim llojin e sulmit të ashtëquajtur SMURF (për krijuar mohim shërbimi, sulmuesit përdorin protokollin e mesazhit të kontrollit internet ICMP) e cila gjeneron kërkesa eko duke specifikuar paketat drejt adresave IP të transmetuara.

Lloj tjetër sulmi është i ashtuquajturi Mohimi i Rrjetit me Zonë Lokale (ang. LAND-Local Area Network Denial) dhe ndodh në rastin kur adresa e burimit dhe destinacionit është e njëjtë, në këtë rast sulmuesit dërgojnë paketa sinkronizimi (SYN) mashtruese në rrjetin TCP/IP dhe Përmbytja SYN ose (ang. SYN Flood) ndodh në rastin kur sulmuesit dërgojnë paketa mashtruese IP të cilat mund të rrëzojnë funksionin e memories duke e tejmbushur atë.

Në rastin e sulmeve nga Distanca në Mbjentin Lokal (R2L), sulmuesit aksesojnë lokalisht sistemin pa autorizim për të shkatërruar rrjetin duke ekzekutuar komandat e tyre [112]. Në këtë rast përfshihen sulme si protokolli i aksesit të mesazhit internet (ang. IMAP), supozimi i fjalëkalimit (ang. Guess Password) dhe spiunimi (ang. SPY) [113].

Për sulmet nga përdoruesi në rrënjë (U2R), sulmuesit marrin aksesin e burimit të sistemit për të shkatërruar rrjetin. Në këtë rast përfshihen sulme të tilla si tejmbushja e buffer-it

dhe rootkits [114]. Në rastin e sulmeve sondë, sulmuesit përdorin gjuhët e programimit për të vjedhur informacione private. Në këtë rast përfshihen sulme të tilla si fshirja e portës dhe NMAP (Network MAPper).

SECURE+ ofron siguri gjatë ekzekutimeve të sulmeve të ndryshme në mënyrë automatike. Gjatë kohës së sulmeve, siguria monitorohet duke përdorur një nën-njësi të monitorimit të performancës ose ndryshe moduli i monitorimit. Me anë të kësaj nën-njësie ruhet efektiviteti i teknikës SECURE+, e cili gjeneron alarm në rast të një sulmi sigurie [115].

SECURE+ ofron vet-mbrojtje dhe siguron komunikim të sigurtë ndërmjet elementeve autonom gjatë ndodhisë të sulmit [111]. SECURE+ përbehet nga 3 komponente të modelit autonom: krijuesi i karakteristikave, përmirësuesi i gradientit dhe shmangësi automatik i sulmit.

Krijuesi i karakteristikave merr informacionin rreth performances të gjendjes aktuale të nyjes në termat e parametrave të Cilësisë së Shërbimit si p.sh. Norma e Dedektimit të Ndërhyrjes (IDR) apo Norma Fals Pozitive (FPR) [116].

Së pari, informacioni i përditësuar që merret nga nyja e dedektimit transferohet tek administratori i burimeve, më pas administratori i burimeve e transferon këtë informacion tek monitoruesi. Informacioni i përditësuar përfshin informacionin rreth kërcënimeve të sigurisë.

5.3.1 Konfigurimet SNORT

Rregullat e përmendura në seksionin 5.1.1 janë implementuar në shumë raste nga kërkues dhe autorë të ndryshëm në varësi të mjediseve të simulimit. Po në rastin tonë ne do të krijojmë një mjedis më të përgjithshëm [108], [117]. Mjedisi që ne kemi projektuar është si vijon në varësi të rregullave të implementuara.

Rregullat e projektuar për këtë punë kerkimore janë si më poshtë:

#TCP rule to detect TCP packet with SYN flag in the network.
alert tcp !$HOME_NET any -> $HOME_NET 80 (flags: s; msg:"Attempt to access server is made with TCP packets"; classtype:attempted-dos; sid:1000990; rev:1;)

#UDP rule to detect UDP packets in the network
alert udp !$HOME_NET any -> $HOME_NET 80 (msg:" Attempt to access server is made with UDP packets"; classtype:attempted-dos; sid:1000991; rev:1;)

Rregullat e mësipërme janë hartuar për të gjeneruar mesazhet e alarmit për paketat që kalojnë në sistemin IDS. Nuk kemi realizuar një rregull të shkruar shprehimisht për përmbytjen e paketave HTTP, sepse paketat HTTP komunikojnë duke përdorur protokollin TCP.

Gjithashtu për të filtruar paketat e dëmshme rregullat e shkruara për dedektimin e përmbytjes nga paketat TCP dhe UDP janë si më poshtë:

- Dedektimi i paketave nga burimi dhe filtrimi i tyre (metoda sipas burimit) [107]: Kjo i tregon snort-it që të gjurmojë paketat e adresave IP të burimit dhe të aktivizojë filtrin nëse është plotësuar kushti. Në këtë mënyrë, rregulli i tregon snort-it që të gjurmojë paketat të cilat vijnë nga burimi dhe të aktivizojë filtrin nëse është plotësuar kushti.

Rregulli i filtrit IDS në këtë rast është i shkruar si më poshtë:

```
# IPS rule to filter TCP packets
                    rate_filter \
                            gen_id 1, sig_id 1000990, \
                            track by_src, \
                    count 30, seconds 1, \
                    new_action drop, timeout 30

# IPS rule to filter UDP packets
rate_filter \
            gen_id 1, sig_id 1000991, \
            track by_src, \
            count 10, seconds 2, \
            new_action drop, timeout 30
```

Teknika e mësipërme e filtrimit i tregon snort-it që të gjurmojë paketat e të dhënave të cilat vijnë nga burimi dhe nëse shpejtësia e kërkesave drejt serverit arrijnë 30 brënda një sekonde atëherë rrëzon paketat dhe shkëput lidhjen për 30 sekonda.

- Dedektimi i paketave nga destinacioni dhe filtrimi (metoda sipas destinacionit) [108]: Kjo i tregon snort-it që të gjurmojë paketat drejt adresës IP të destinacionit dhe të aktivizojë filtrin nësë është plotësuar kushti. Në këtë metodë, rregulli i tregon snorti-it që të gjurmojë paketat të cilat arrijnë destinacionin dhe aktivizojnë filtrin nëse është plotesuar kushti.

Rregulli i filtrit IPS në këtë teknikë shkruhet si më poshtë:

```
# IPS rule to filter TCP packets
rate_filter \
        gen_id 1, sig_id 1000990, \
        track by_dst, \
        count 30, seconds 1, \
        new_action drop, timeout 30

# IPS rule to filter UDP packets
rate_filter \
        gen_id 1, sig_id 1000991, \
        track by_dst, \
        count 10, seconds 2, \
        new_action drop, timeout 30
```

Teknika e filtrit të mësipërm i tregon snort-it që të gjurmojë paketat e të dhënave të cilat arrijnë destinacionin nga çdo burim dhe nëse shpejtësia e kërkesave në server arrin 30 brënda një sekonde pastaj rrëzon paketat dhe shkëput lidhjen për 30 sekonda.

5.3.2 Konfigurimet dhe Algoritmet e përdorur në teknikën SGBoost

Figura 5-5 e mëposhtme prezanton bllok-skemën e funksionit pikë-me-pikë të zgjidhjes së propozuar të sigurisë.

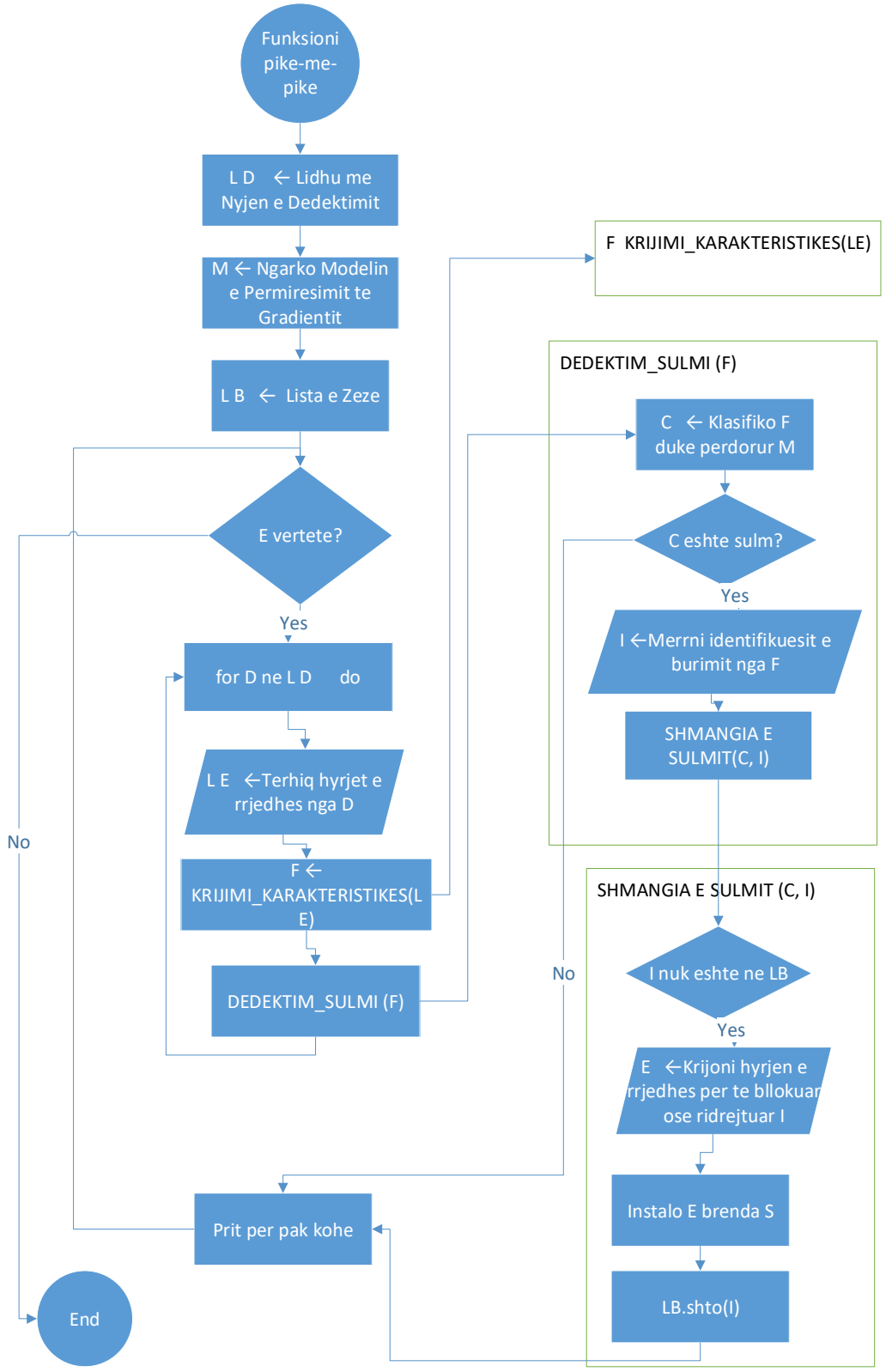

Figura 5-5 Bllok-skema e funksionit pikë-më-pikë

Nyja e dedektimit mbledh të dhënat e trafikut të rrjetit dhe nëse ato i përkasin sulmeve të panjohura merren nga Krijuesi i Karakteristikave. Mbas marrjes, krijohen karakteristika për çdo rrjedhë siç tregohet në mënyrë të përmbledhur në bllok-skemën e paraqitur në Figurën 5-6.

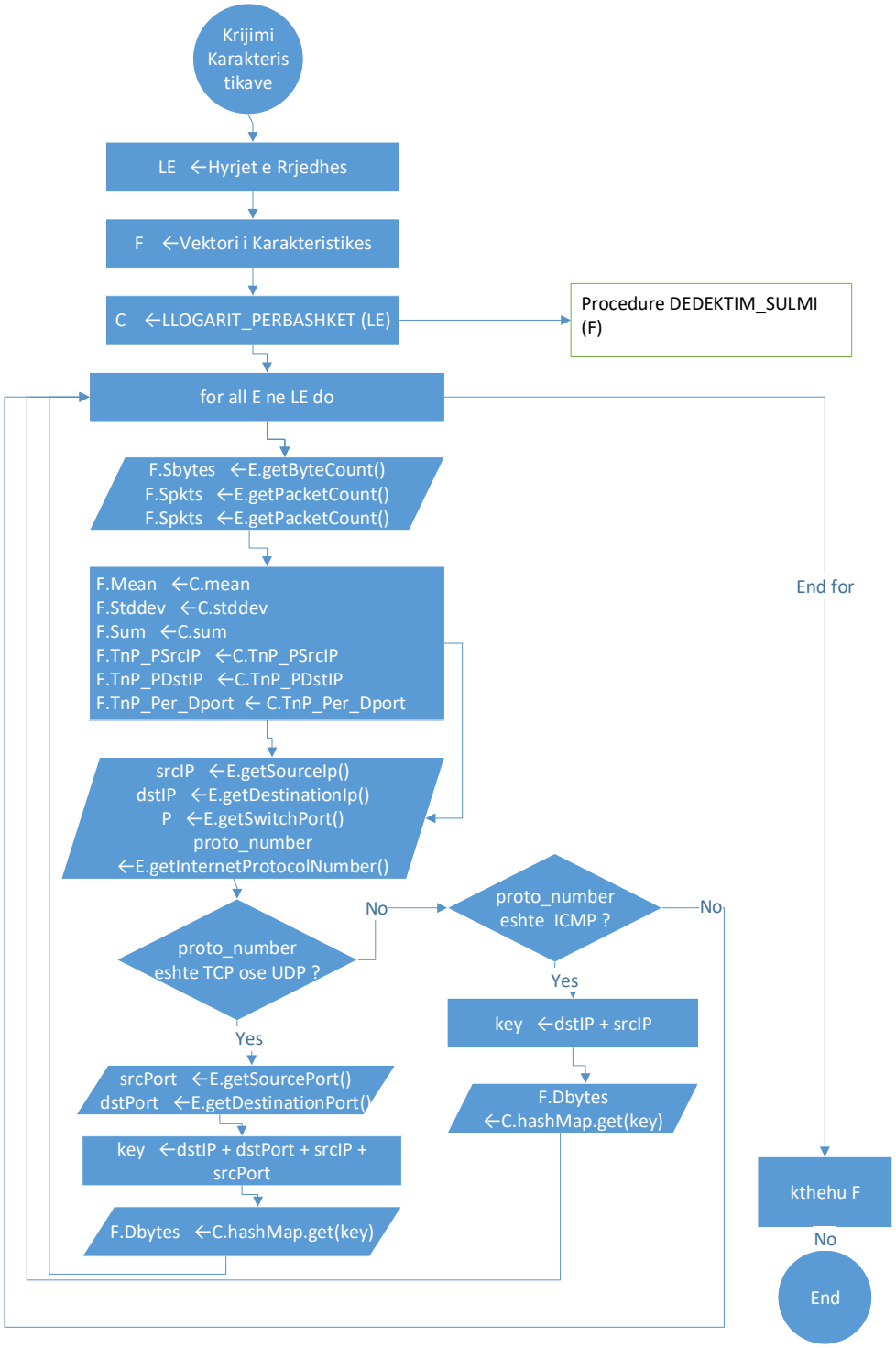

Figura 5-6 Bllok-skema e funksionit të krijimit të Karakteristikave

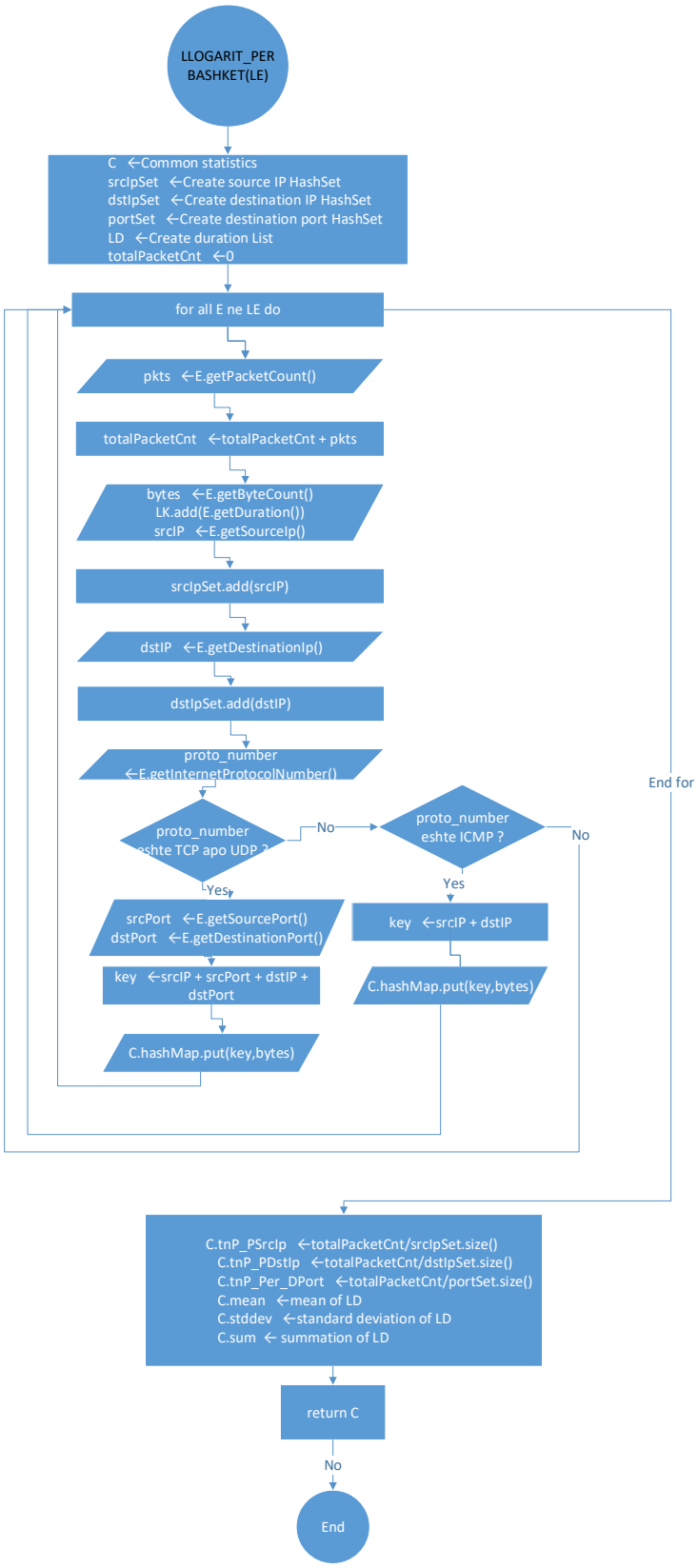

Figura 5-7 Bllok-skema e funksionit të përllogaritjes së karakteristikave dhe statistikave të përbashkëta

Në këtë mënyrë gjenerohen karakteristika të përbashkëta për çdo rrjedhë, duke rrethuar çdo rrjedhë hyrëse në nyjen dedektuese dhe përdorur bllok-skemën e paraqitur në Figurën 5-7, p.sh. kohëzgjatja mesatare e rrjedhës dhe numrit total të paketave në një transaksion krijohen me një kalim fillestar mbi hyrjet e rrjedhës. Si rrjedhojë, karakteristika specifike të rrjedhës, si p.sh. kohëzgjatja e rrjedhës dhe përllogaritja e paketave nga burimi në destinacion, merren duke kaluar mbi hyrjet e rrjedhës.

Ndërsa shikojmë mbi hyrjet e rrjedhës, vektori i tiparit të krijuar për një rrjedhë dërgohet menjëherë tek Përmirësuesi i Gradientit, pa pritur të përfundojë krijimin e veçorisë për hyrjet e tjera të rrjedhës.

- Krijuesi i Karakteristikave gjithashtu tërheq fushat e përputhjes së rrjedhës, si adresat IP dhe MAC të burimit, si dhe portën fizike nga vjen paketa. Shmangësi i Sulmit përdor si përfundim këto karakteristika. Karakteristikat e përbashkëta përfshijnë Mean, Stddev, Sum, TnP_PSrcIP, TnP_PDstIP, dhe TnP_Per_Dport. Përshkrimet e detajuara përkatëse gjenden në Tabelën 5-1. Grupet *hash* përdoren për të ruajtur IP-të unike të burimeve dhe destinacioneve dhe numrat e portave të destinacionit. Zbatohet një listë për të ruajtur kohëzgjatjen e rrjedhës së hyrjes. Ndërsa rrethon hyrjen e rrjedhës, numërimi i paketave në rrjedhën e hyrjes shtohet në përllogaritjen totale të paketave. Kohëzgjatja e rrjedhës së hyrjes shtohet në listën e kohëzgjatjes. IP-të e burimit, IP-të e destinacionit dhe numrat e portave të destinacionit shtohen në grupin hash respektiv. Numërimi i biteve të rrjedhës shtohet në një hartë hash. Çelësat e kësaj harte përbëhen prej IP-ve të burimit, portës së burimit, IP-së së destinacionit dhe portës së destinacionit për paketat TCP dhe UDP.

- Për paketat ICMP, çelësat përbëhen nga IP-ja e burimit dhe IP-ja e destinacionit, m.q.se në këtë rast ato nuk kanë numra të portës. Kjo hartë përdoret më vonë për të marrë statistikat e rrjedhës së kundërt. Mbas rrethimit të nyjes së dedektimit, llogariten karakteristikat kryesore duke përdorur numërimin total të paketave, grupet hash dhe listën e kohëzgjatjes.

- Përmirësuesi i Gradientit merr vektorët e karakteristikave nga "Krijuesi i karakteristikave" një e nga një dhe i klasifikon ato duke përdorur modelin e tij të parandërtuar të dedektimit të ndërhyrjes. Nëse rezultati i klasifikimit është ndonjë tip sulmi, atëherë "Shmangësi i Sulmit merr tipin e sulmit të dedektuar dhe identifikuesit e burimit si p.sh. IP-në e burimit dhe MAC adresën e burimit. Modeli i përdorur i mësimit automatik përditësohet në mënyre dinamike nga përfshirja e të dhënave të reja të mësuara për të njëjtat tipe ekzistuese të sulmeve sapo ato zbulohen. Ndërtimi i modelit me përmirësim të gradientit është një model

me klasifikim shumë-klasësh, i cili formohet duke përdorur të dhënat e mësuara që ekzistojnë në tipe të ndryshme sulmesh përveç trafikut normal.

Tabela 5-1 Përshkrimi i karakteristikave të rrjedhës

Karakteristika	**Pershkrimi**
Dur	Kohëzgjatja e përgjithshme e rastit
Mean	Kohëzgjatja mesatare e rasteve të grumbulluara
Stddev	Devijimi standard i kohëzgjatjes për rastet e grumbulluara
Spkts	Llogaritja e paketave nga burimi në destinacion
Sbytes	Llogaritja e byte-eve nga burimi në destinacion
Dbytes	Llogaritja e byte-eve nga destinacioni në burim
Sum	Kohëzgjatja totale e rekordeve të grumbulluara
TnP_PSrcIP	Numri total i paketave për IP-në e burimit
TnP_PDstIP	Numri total i paketave për IP-në e destinacionit
TnP_Per_Dport	Numri total i paketave për portën e destinacionit

5.4 Përshkrimi i Metodologjisë së Kërkimit

Kemi projektuar skenarët e eksperimentit për të vëzhguar dhe për të përfituar rezultatet e matjeve. Në këtë studim ne do të demostrojmë krahasimet e performancës midis dy teknikave në mënyrë rigoroze, të ripërsëritura dhe sasiore. Eksperimentet do të bazohen në një ambjent testues i cili do të krahasojë teknikat SECURE me SECURE+. Ky ambjent do të ketë një rrjet me gjerësi brezi 100Gbps dhe disa tipe të ndryshme trafiku të dëmshëm. Tipet e trafikut të dëmshëm janë zgjedhur sepse rregullat e paracaktuara mund të aplikohen njëkohësisht mbi SECURE dhe SECURE+. Për më tepër, këto janë tipet më të hasura dhe mbulojnë një numër shumë më të madh të llojeve të sulmeve.

Eksperimentet e ralizuara do të krahasojnë performancën e të dy teknikave duke matur, normën fals pozitive, normën e dedektimit të ndërhyrjes, kohëzgjatjen e ekzekutimit, si dhe përqindjen e CPU-së, përdorimin e memorjes RAM si dhe përqindjen e paketave të rrëzuara në rrjet. Trafiku normal i rrjetit për kryerjen e ekperimenteve është realizuar duke përdorur një gjenerues trafiku në rrjet me burim të hapur të quajtur Hping3 [118]. Ky

aplikacion do të gjenerojë trafikun në rrjet deri në 20 Gbps. Trafiku i dëmshëm është gjeneruar duke përdorur aplikacionet:

- Metasploit për sulmet DoS,
- NMAP për sulmet sondë,
- Hydra për sulmet R2L,
- NetCat për sulmet L2R dhe
- DDoSIM për sulmet DDoS.

Në Snort janë përdorur rregullat siç është përshkruar në seksionin 5.3.1. Gjithashtu trafiku i rrjetit legjitim dhe i dëmshëm janë gjeneruar si trafik i kombinuar dhe pastaj futen tek nyja dedektuese. Disa nga pyetjet që ne kemi ngritur janë si vijon. Cila teknikë ka performancë më të mirë kur procesojmë trafik rrjeti deri në 10 Gbps? A ka ndikim arkitektura e teknikës për këtë? Cilat janë diferencat në normën e rrëzimit të paketave ndërmjet teknikës SECURE+ dhe asaj SECURE kur CPU, memorja RAM dhe përdorimi i gjerësisë së brezit rritet? Sa të sakta janë teknikat SECURE+ dhe SECURE në dedektimin e sulmeve kur trafiku i dëmshëm vjen bashkë me atë legjitim?

5.5 AMBJENTI EKSPERIMENTAL

Për të evidentuar rezultatet e Teknikës SECURE+ kemi ngritur një ambjent eksperimental i cili është i ndërtuar si vijon:

1- Shtresa HW janë dy Servera Blade HP ProLiant BL465c G7 me 2 x AMD Opteron CPU model 6172 (12 core dhe 12 thread), RAM 112GB dhe HDD 2x146GB SAS 10K RPM në konfigurimin RAID1
2- Shtresa Virtuale do të jetë e bazuar në aplikacionin VMware, eSXi version 5.5
3- Serveri i Parë ka dy makina Virtuale të cilat do të përdoren për Gjenerimin e Trafikut të:
   a- Gjeneruesi i trafikut të ligjshëm të rrjetit me aplikacionin Hping3 dhe NMAP v.7.91 me Sistem Operativ Centos 7.0, CPU – 4 vCPU, RAM- 20GB dhe HDD – 30 GB.
   b- Gjeneruesi i trafikut të dëmshëm me aplikacionet Metasploit, Struktura Metasploit, Hydra, NetCat, DAVOSET dhe DDoSIM me Sistem Operativ Centos 7.0, CPU – 4 vCPU, RAM- 20GB dhe HDD – 30GB
4- Serveri i Dytë ka dy makina virtuale të cilat do të përdoren për secilën teknikë si vijon:
   a- Serveri teknikës SECURE+, i cili ka të instaluar snort 2.9.17 dhe algoritmin e XGBoost me Sistem Operativ Centos 7.0, CPU – 6 vCPU, RAM- 40GB dhe HDD – 60 GB.

b- Serveri i teknikës SECURE, i cili ka të instaluar snort 2.9.17 dhe algoritmin MAPE-K me Sistem Operativ Centos 7.0, CPU – 6 vCPU, RAM- 40GB dhe HDD – 60GB.

Në mënyrë skematike ambjenti ekperimental paraqitet si në Figurën 5-8 në vijim

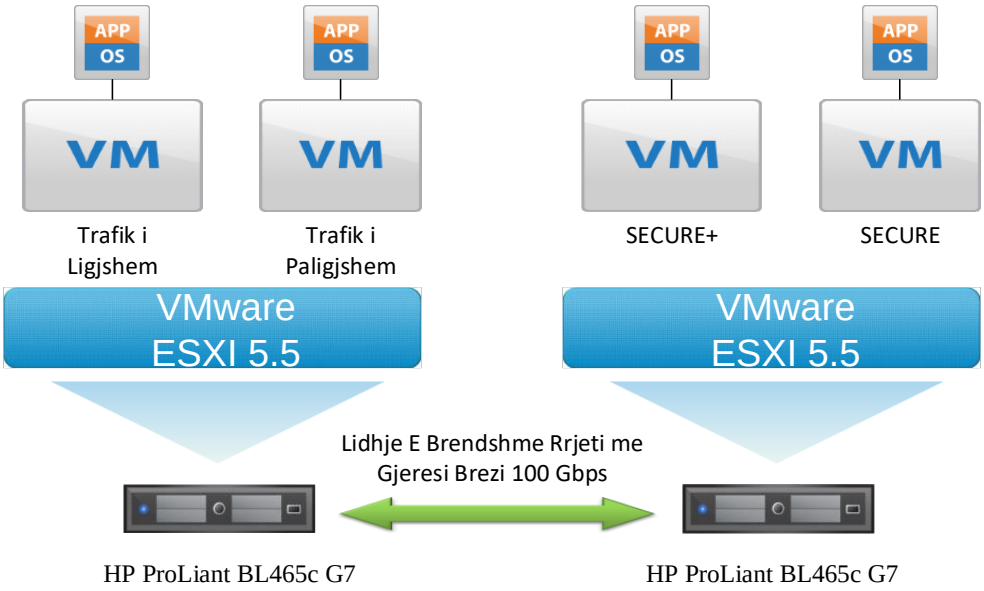

Figura 5-8 Ambjenti Eksperimental

5.6 KRYERJA E EKSPERIMENTEVE DHE ANALIZA PËRKATËSE

Eksperimentet janë kryer për të evidentuar avantazhet e teknikës SECURE+ përkundrejt asaj SECURE duke përdorur makina virtuale me të njëjta burime kompjuterike dhe me të njëjta kushte testimi siç tregohet në Tabelën 5-2.

Fillimisht kemi realizuar eksperimentin që vëren në kohë reale performancën e teknikave SECURE+ dhe SECURE duke procesuar një trafik legjitim me shpejtësi 10 Gbps nga gjeneruesi i trafikut të ligjshëm (Hping3).

Eksperimentin e parë e kemi realizuar për të krahasuar performancën e teknikës SECURE+ dhe asaj SECURE. Për të marrë rezultate të sakta, eksperimentin e kemi realizuar me paketa me madhësi 1,470 bajt për protokollet e llojit TCP, UDP dhe ICMP. Këto paketa i kemi injektuar në të dy teknikat me një shpejtësi rrjeti prej 10Gbps. Eksperimenti mbështetet në diagramën logjike të rrjetit siç tregohet në Figurën 5-9.

Çdo teknikë e kemi instaluar në mënyrë të ndarë në makina virtuale identike me parametra të njëjtë të burimeve kompjuterike dhe rregulla të njëjta për aplikacionin snort. Kemi

përdorur një aplikacion të quajtur Monitoruesi i Performancës së Rrjetit nga Solarwinds, i cili rregjistron dhe mat CPU-në, memorien dhe përdorimin e rrjetit. Përveç këtij aplikacioni kemi përdorur edhe disa aplikacione të tjera për të rregjistruat dhe matur karakteristikat e studiuara, siç janë struktura Metasploit, Snort logs, nmap etj.

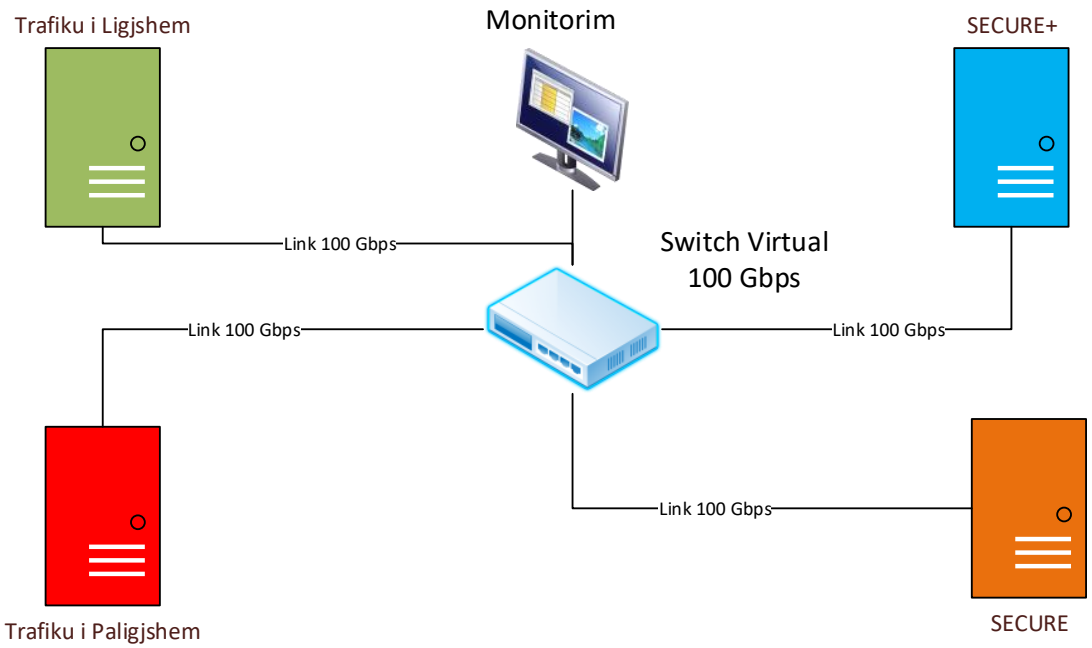

Figura 5-9 Paraqitja e rrjetit të ambjentit eksperimental

Eksperimentet janë kryer për cikle me kohëzgjatje 8 orëshe secili. Në total kemi realizuar 10 cikle testimesh dhe kemi arritur në total një kohëzgjatjeje eksperimentesh 80 orëshe, kjo për të rritur besueshmërinë e rezultateve tona. Paketat e mëposhtme janë injektuar si trafik bazë duke filluar nga 1 Gbps deri në 10 Gbps si vijon:

1- 1,000,000 paketa UDP me një shpejtësi prej 500 paketash/sekondë, çdo madhësi pakete përbëhet nga 1,470 bajte.
2- 1,000,000 paketa TCP me një shpejtësi prej 500 paketash/sekondë, çdo madhësi pakete përbëhet nga 1,470 bajte.
3- 1,000,000 paketa ICMP me nje shpejtësi prej 500 paketash/sekondë, çdo madhësi pakete përbëhet nga 1,470 bajte.

Tabela 5-2 Specifikimet teknike të ambjentit eksperimental

Tipi i Makinës dhe Sistemit Operativ	**Specifikimet e Burimeve Kompjuterike**	**Aplikacionet e Tjera të instaluara**
Gjeneruesi i trafikut të ligjshëm, Centos 7.0	Makinë virtuale, CPU 2.1 GHz 4 bërthama virtuale, RAM me kapacitet 20 GB Memorje, Rrjet Giga Ethernet me kapacitet 100 Gbps	Hping3
SECURE+, Centos 7.0	Makinë virtuale, CPU 2.1 GHz 6 bërthama virtuale, RAM me kapacitet 40 GB Memory, Rrjet Giga Ethernet me kapacitet 100 Gbps	Snort 2.9.17 build 199 IDS; Collectl, top, dstat, Snort logs, tcpdump, IPTRAF, XGBoost.
Gjeneruesi i trafikut të dëmshëm, Centos 7.0	Makinë virtuale, CPU 2.1 GHz 4 berthama virtuale, RAM me kapacitet 20 GB Memorje, Rrjet Giga Ethernet me kapacitet 100 Gbps	Struktura Metasploit, Hydra, NetCat, NMAP dhe DDoSIM
SECURE, Centos 7.0	Makinë virtuale, CPU 2.1 GHz 6 bërthama virtuale, RAM me kapacitet 40 GB Memorje, Rrjet Ethernet me kapacitet 100 Gbps	Snort 2.9.17 build 199 IDS; Collectl, top, dstat, Snort logs, tcpdump, IPTRAF, MAPE-K.
Switchi i Rrjetit	Switch Virtual 100 Gbps	

Mënyrën që zgjodhëm për të injektuar paketat ishte ajo me trafik normal, duke specifikuar numrin e paketave për sekondë dhe numrin total të paketave. Të dhënat e rezultateve të

eksperimenteve treguan se përdorimi i CPUs në Teknikën SECURE+ ishte më i ulët krahasuar me atë të teknikës SECURE kjo e matur gjatë procesimit të të njëjtit trafik rrjeti prej 10 Gbps. Figura 5-10 jep rezultatin mesatar të përdorimit të CPUs për të dy teknikat gjatë 80 orëve testim.

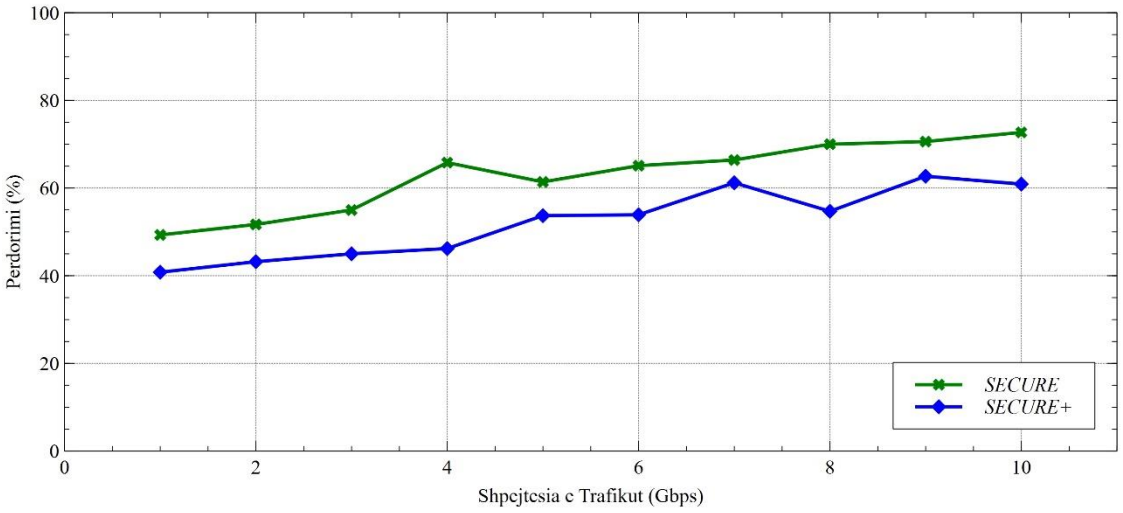

Figura 5-10 Mesatarja e përdorimi të CPUs.

Përdorimi mesatar i CPUs në teknikën SECURE+ është 51.04% për serverin me 6 bërthama CPU-je dhe me një shpejtësi 2.1GHz për çdo bërthamë, ndërsa teknika SECURE ka një përdorim mesatar të CPUs prej 60.58% për të njëjtat karakteristika të parametrave të përdorur të CPUs.

Si rrjedhoje teknika SECURE+ është përafërsisht 10% me efikase në përdorimin e CPUs krahasuar me teknikën SECURE. Tabela 9-1 në shtojcën B jep paraqitjen e të gjitha rezultateve të përfitura nga eksperimentet.

Të dhënat e mbledhura të performancës na tregojnë se përdorimi i memorjes në teknikën SECURE+ është më i ulët se ai i teknikës SECURE. Këto të dhëna jepen në mënyrë të grupuar në Tabelën 9-2 të shtojcës B.

Në këte tabelë shikohet qartë se përdorimi mesatar i memorjes në rastin e teknikës SECURE+ rritet nga 19 GB kur realizojme testime në 1Gbps dhe vazhdon të rritet me një shkallë të ndryshueshme deri në një maksimum prej 30 GB kur realizohen testet me shpejtësi rrjeti 10 Gbps. Në mënyrë grafike ky përdorim pasqyrohet në Figurën 5-11.

Përdorimi mesatar i memorjes në teknikën SECURE+ duket se është krahasimisht më i ulët krahasuar me vlerat mesatare të teknikës SECURE. Këto vlera fillojnë në 19 GB në testet me shpejtësi 1 Gbps dhe vazhdojnë të performojnë me memorje të reduktuar përgjatë gjithë testeve të realizuara në shpejtësitë e tjera.

Kulmi i përdorimit të memorjes arrihet në nivelin 30GB kur procesohet testi me shpejtësi rrjeti 10 Gbps. Nga këto rrezultate shikohet se përdorimi i memorjes në teknikën SECURE+ është rreth 7% më i ulët se teknika SECURE.

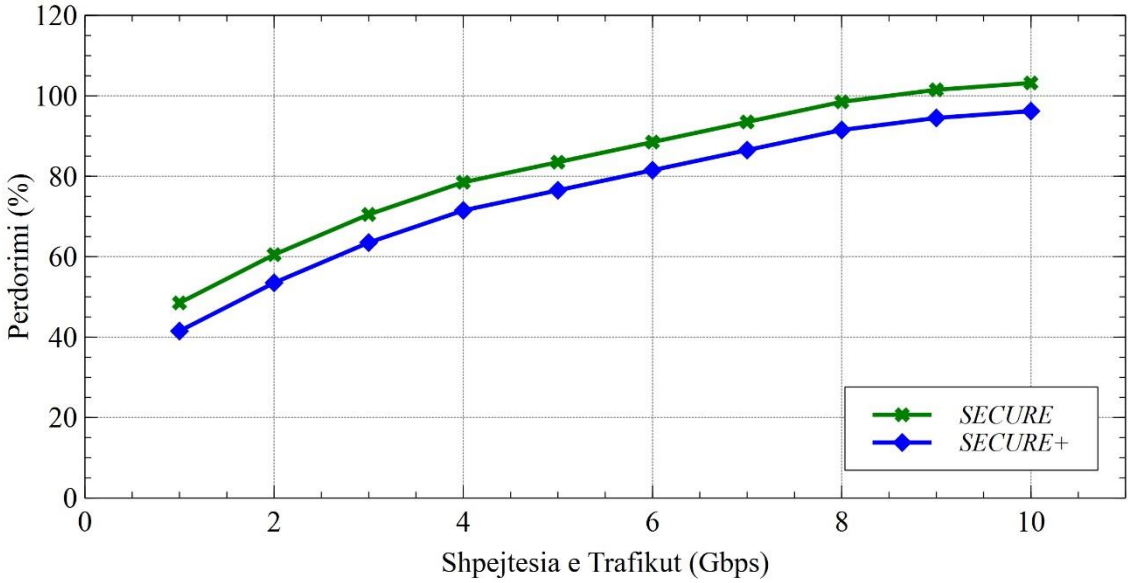

Figura 5-11 Mesatarja e përdorimi të memorjes RAM.

Nga këto testime vëmë re se kur shpejtësia e trafikut të rrjetit fillon e rritet ateherë si përdorimi i procesorit ashtu edhe përdorimi i memorjes fillon të rritet për të dyja teknikat. Teknika SECURE+ dhe SECURE i mbledhin të dhënat e testeve në skedarët e logeve dhe vazhdojnë procesin me paketat në një shpejtësi mesatare të ndryshueshme si për përdorimin e CPUs ashtu edhe të memorjes.

Procesimi i paketave në Teknikën SECURE+ është më i shpejtë se procesimi i paketave në Teknikën SECURE. Kjo e thënë ndryshe, për të njëjtën sasi paketash UDP, TCP dhe ICMP (1,000,000 paketa) të injektuara në të dyja teknikat për një periudhë kohore 80 orëshe (10 cikle testesh me nga 8 orë secila) vumë re se teknika SECURE+ tregoi një performancë më të mirë përkundrejt asaj SECURE.

Shpejtësia mesatare e procesimit për teknikën SECURE+ është 107,560 paketa në sekondë gjatë kohës së testit prej 80 orësh, ndërsa në rastin e teknikës SECURE shpejtësia

mesatare e paketave është 73,460 paketa në sekondë gjatë të njëjtës periudhë kohore. Figura 5-12 paraqet mesataren e procesimit të paketave në njësinë e kohës.

Tabela 9-3 tregon shpejtësinë e procesimit të paketave ndërmjet të dy teknikave SECURE+ dhe asaj SECURE. Nga kjo tabelë vërejmë lehtësisht se Teknika SECURE+ proceson rreth 30% më tepër paketa krahasuar me teknikën SECURE për shkak të përdorimit të shumë bërthamave në të njëjtën kohë.

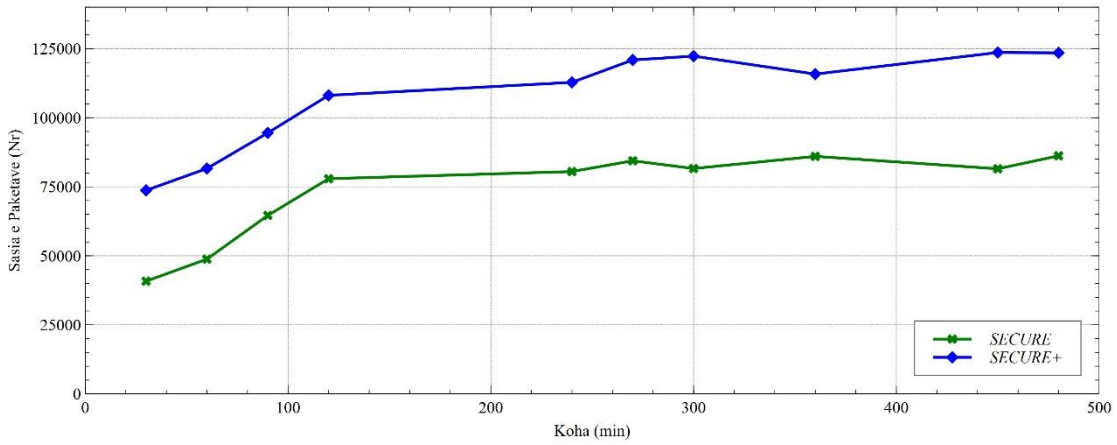

Figura 5-12 Mesatarja e shpejtësisë së procesimit (numri i paketave në njësinë e kohës) për të dy teknikat.

Figurat nga 5-13 deri në 5-15, tregojnë se performanca e rrjetit është më e mirë në teknikën SECURE+ krahasuar me teknikën SECURE, sepse në teknikën SECURE rrëzohen më shumë paketa në të gjitha shpejtësitë e rrjetit krahasuar me teknikën SECURE+.

Eksperimentin e kemi realizuar njësoj si në metodologjinë e përdorur më lart, me përdorimin e 5 testeve me nga 8 orë secili. Vlera mesatare është marrë nga tre vlerat e protokolleve UDP, TCP dhe ICMP për të dyja teknikat SECURE+ dhe SECURE.

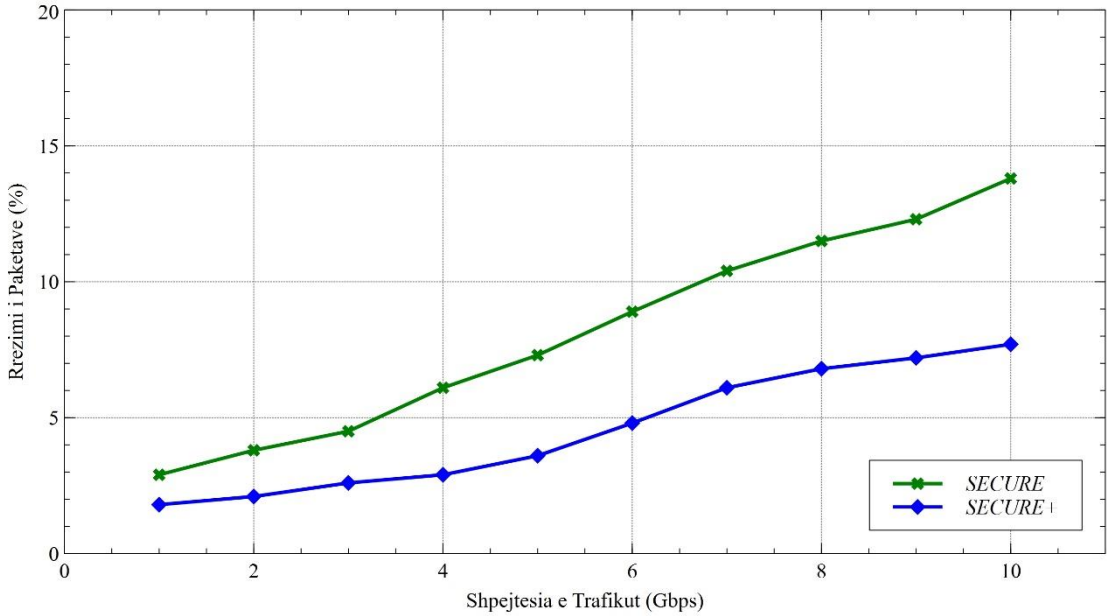

Figura 5-13 Shpejtësia mesatare e rrëzimit të paketave UDP

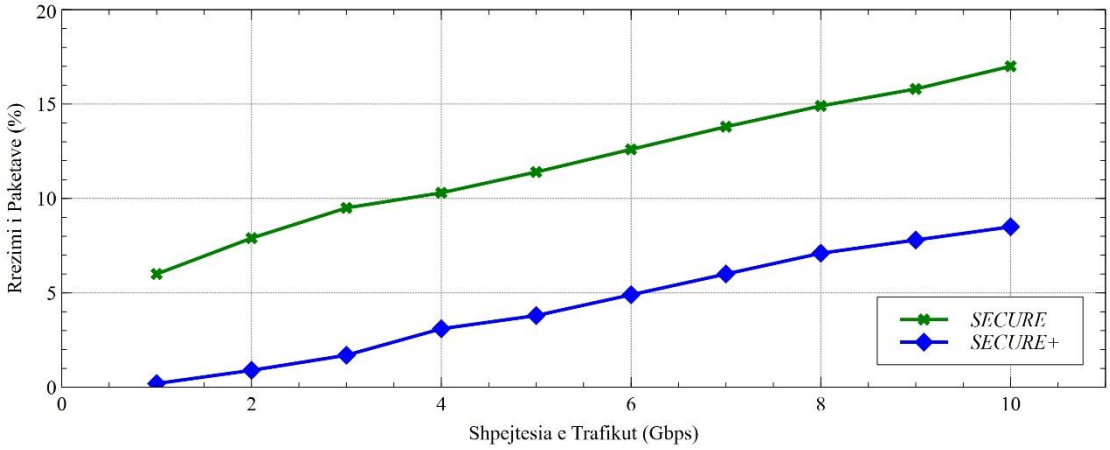

Figura 5-14 Shpejtësia mesatare e rrëzimit të paketave TCP

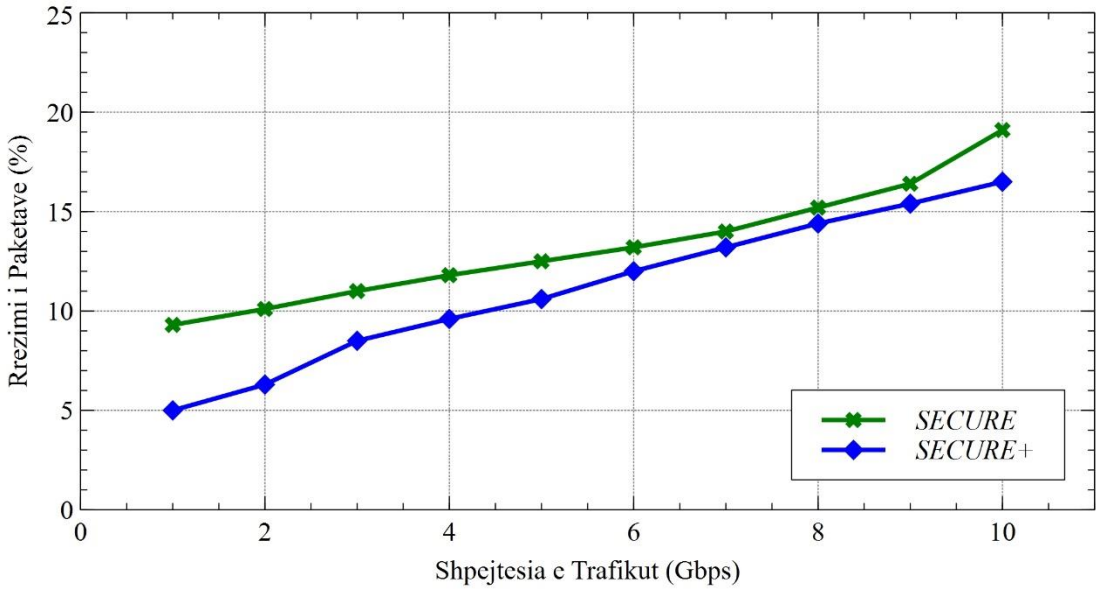

Figura 5-15 Shpejtësia mesatare e rrëzimit të paketave ICMP

Gjatë kryerjes së eksperimentit vumë re se sistemi i operimit (Centos 7.0) i instaluar në të dy teknikat ishte përgjegjës për numrin total të paketave të rrëzuara tek të dy teknikat për shpejtësi të larta të rrjetit nga 2 Gbps deri në 10 Gbps. Kjo u evidentua gjatë analizës që u realizua mbi loget e mbledhura në dosjen e mbikqyrësit të eventeve të sistemit operativ.

Kjo analizë nxorri në pah faktin se buferat e memorjes të sistemit operativ Centos 7.0 u konsumuan me paketa përpara se të dy teknikat të mund të lexonin të dhënat që ishin brenda tyre. Ky problem nuk ekziston në rastin e shpejtësive të ulta të rrjetit nga 100Mbps deri në 1Gbps. Kjo gjetje tregon në mënyrë të qartë se duhet patur memorje me kapacitete më të mëdha të bufferit në mënyrë që rrëzimi i paketave të reduktohet për këto shpejtësi rrjeti.

Për të krahasuar performancën e teknikave SECURE dhe SECURE+ ne kemi studiuar edhe dy metrikët më të rëndësishëm siç është Norma e Dedektimit të Ndërhyrjes (NDN) dhe Norma Fals Pozitive (NFP), të cilat janë gjithashtu kriteret më të rëndësishme të vlerësimit të algoritmave dhe teknikave të përdorura.

Rezultatet e përfituara për këto metrikë janë realizuar duke gjeneruar sulme nëpërmjet aplikacioneve Metasploit për sulmet DoS, NMAP për sulmet sondë, Hydra për sulmet R2L, NetCat për sulmet L2R dhe DDoSIM për sulmet DDoS.

Figurat nga 5-16 deri në 5-20, tregojnë në mënyrë grafike rezultatet e përfituara gjatë eksperimenteve të kryera për vlerat mesatare të normës fals pozitive (NFP) për të gjitha kategoritë e sulmeve (5 tipe sulmesh, DoS, L2R, R2L, Probing dhe DDoS).

Nga këto rezultate vihet re se NFP është më e ulët në teknikën SECURE+ krahasuar me vlerat e teknikës SECURE. U evidentua gjithashtu se kjo vlerë ka një trend rënës me zgjatjen e kohës së eksperimentit.

Vlen të theksohet gjithashtu fakti se NFP është më e madhe për sulmet R2L duke e krahasuar me sulmet DDos, Probing, U2R dhe DoS.

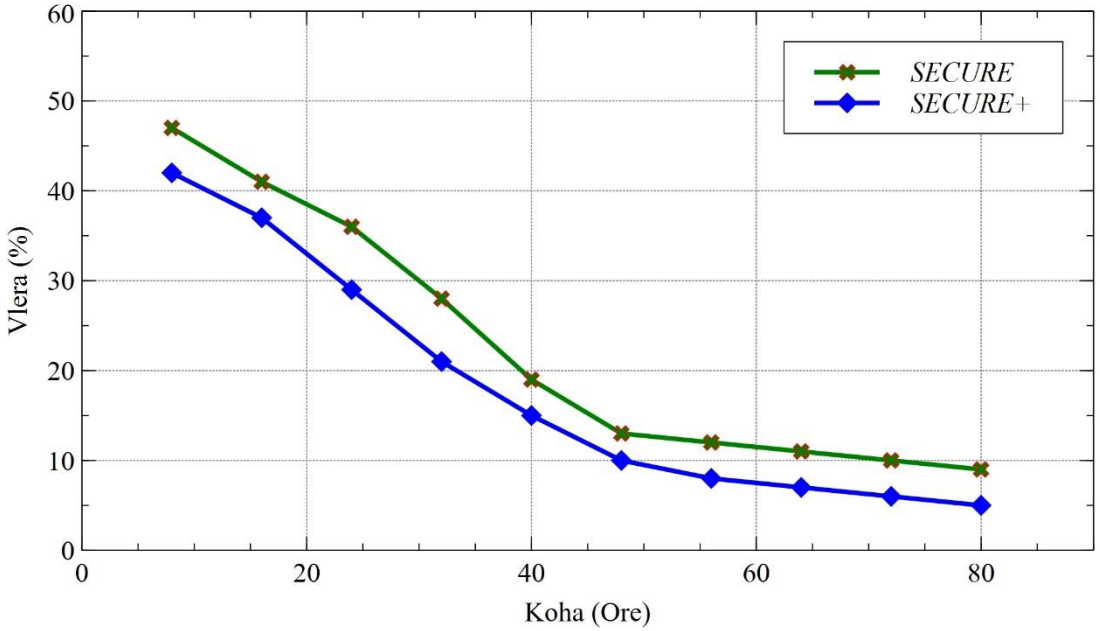

Figura 5-16 Norma Fals Pozitive për llojet e sulmit e Mohimit të Shërbimit (DoS)

NFP është një metrikë që aplikacioni SNORT e ka relativisht të lartë, prandaj për të përmirësuar këtë metrikë, kjo teknikë bashkëshoqërohet edhe me algoritma shtesë, siç është rasti i algoritmave Mape-K dhe XGBoost, që janë përdorur në dy teknikat që janë subjekt i këtij studimi.

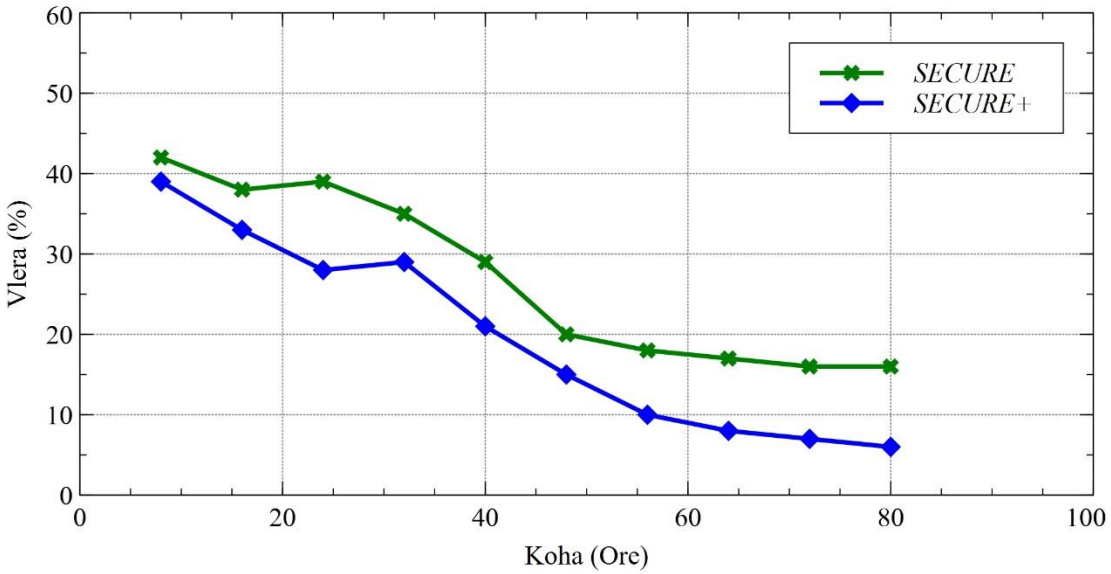

Figura 5-17 Norma Fals Pozitive për llojet e sulmit nga Ambjenti Lokal në Bërthamë (L2R)

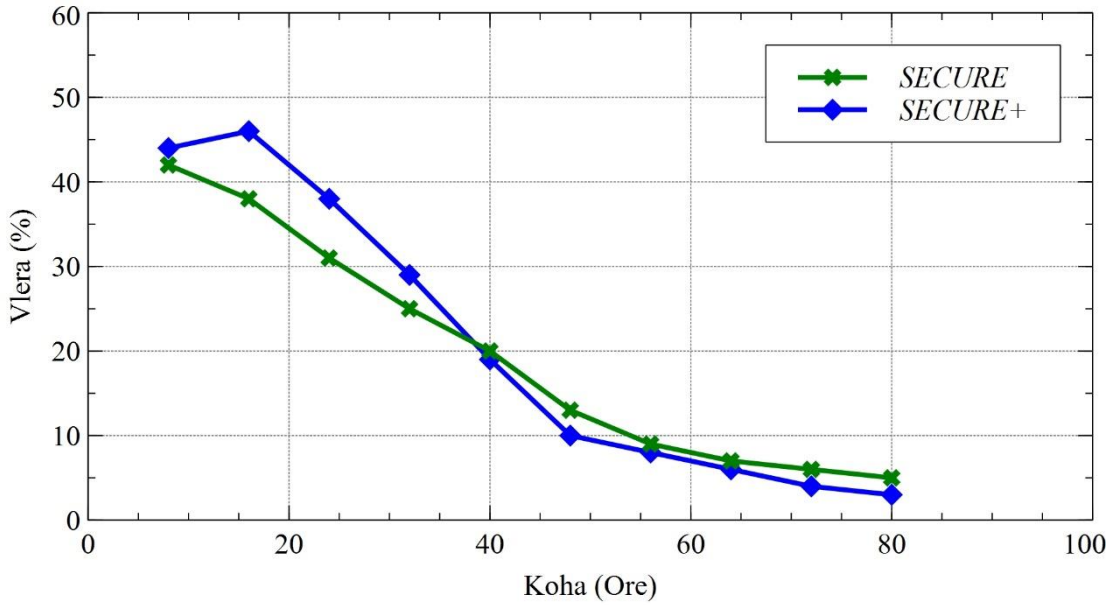

Figura 5-18 Norma Fals Pozitive për llojet e sulmit nga Distanca në Ambjentin Lokal (R2L)

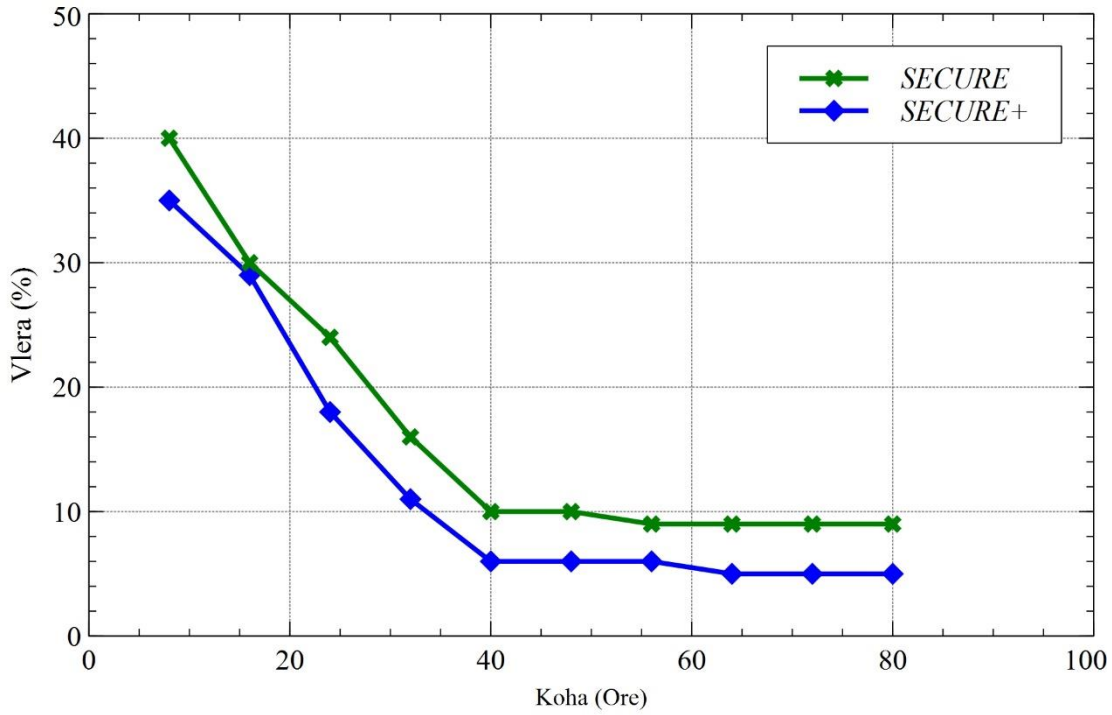

Figura 5-19 Norma Fals Pozitive për llojet e sulmit Sondë (Probing)

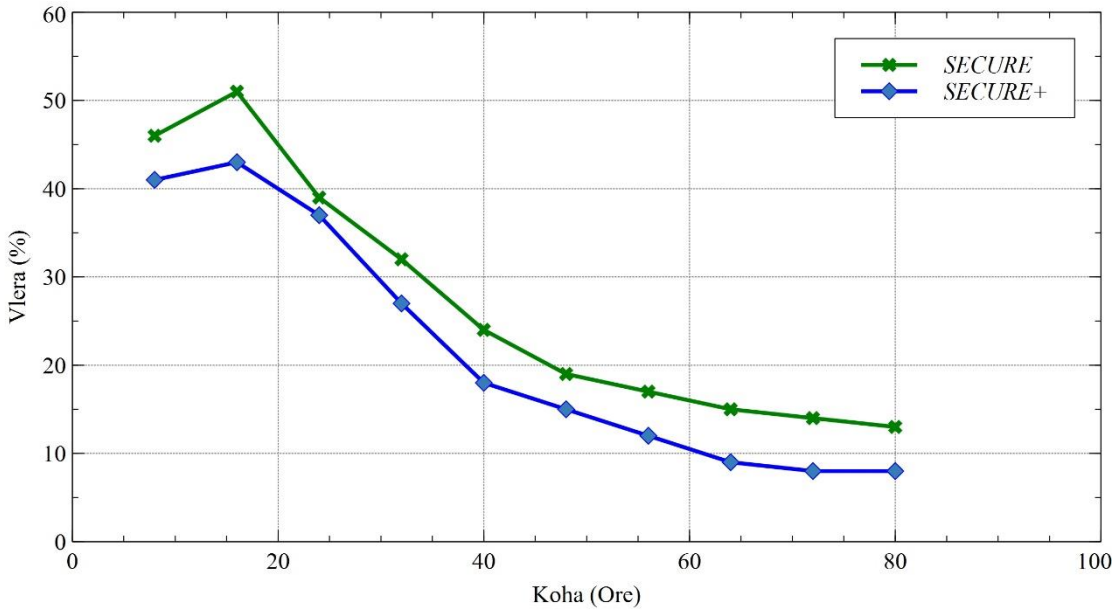

Figura 5-20 Norma Fals Pozitive për llojet e sulmit Mohimi i Shpërndarë i Shërbimit (DDoS)

Figurat nga 5-21 deri në 5-25, tregojnë në mënyrë grafike rezultatet e përfituara gjatë eksperimenteve të kryera për vlerat mesatare të Normës Fals Negative (NFN) për të gjitha kategoritë e sulmeve (5 tipe sulmesh, DoS, L2R, R2L, Probing dhe DDoS).

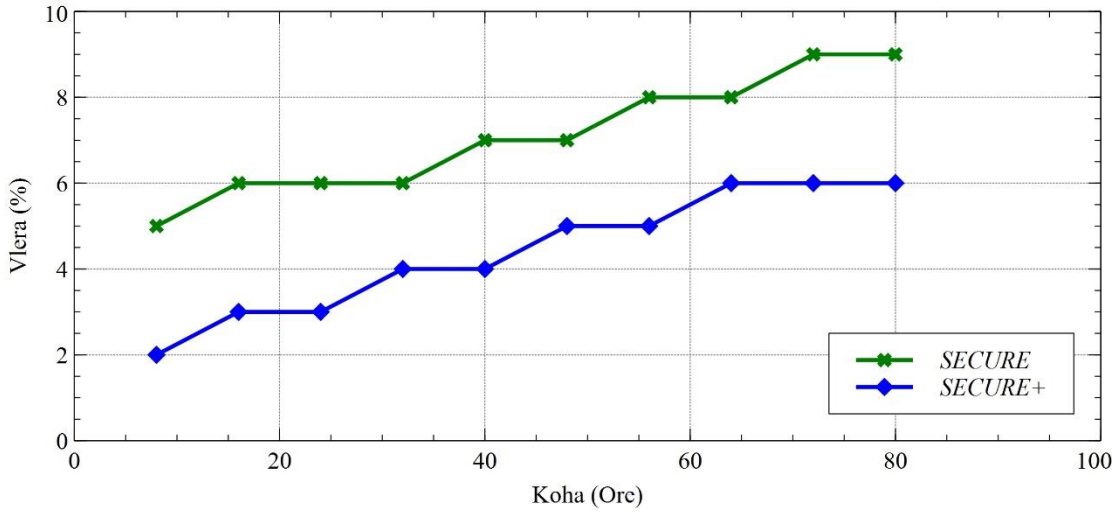

Figura 5-21 Norma Fals Negative për llojet e sulmit të Mohimit të Shërbimit (DoS)

Nga këto rezultate vihet re se NFN është më e ulët në teknikën SECURE+ krahasuar me vlerat e teknikës SECURE. U evidentua gjithashtu se kjo vlerë ka një trend ngritës me zgjatjen e kohës së eksperimentit. Vlen të theksohet gjithashtu fakti se NFN është më e madhe për sulmet DDoS dhe Sondë duke e krahasuar me sulmet R2L, U2R dhe DoS.

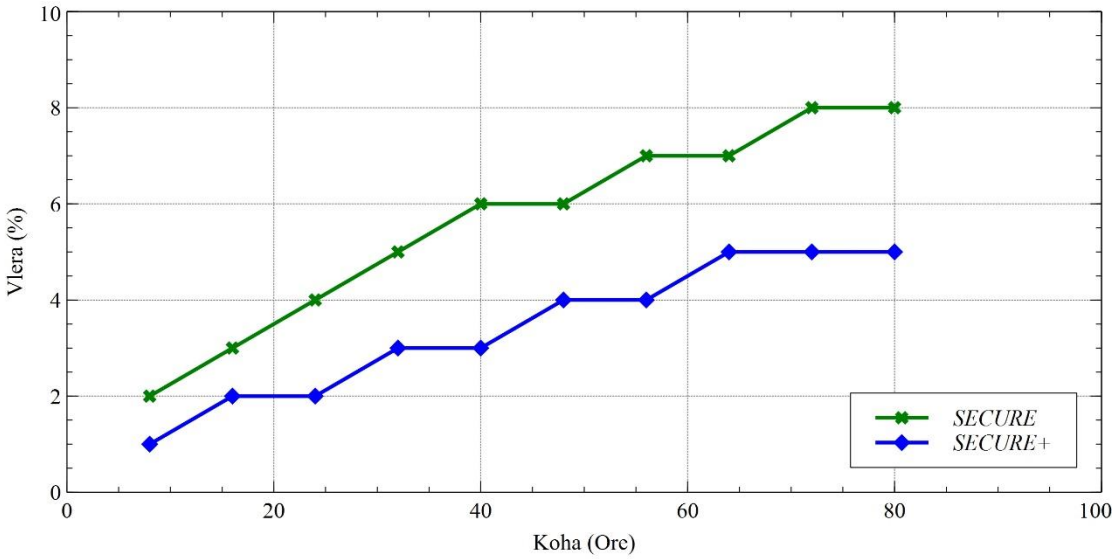

Figura 5-22 Norma Fals Negative për llojet e sulmit nga Ambjenti Lokal në Bërthamë (L2R)

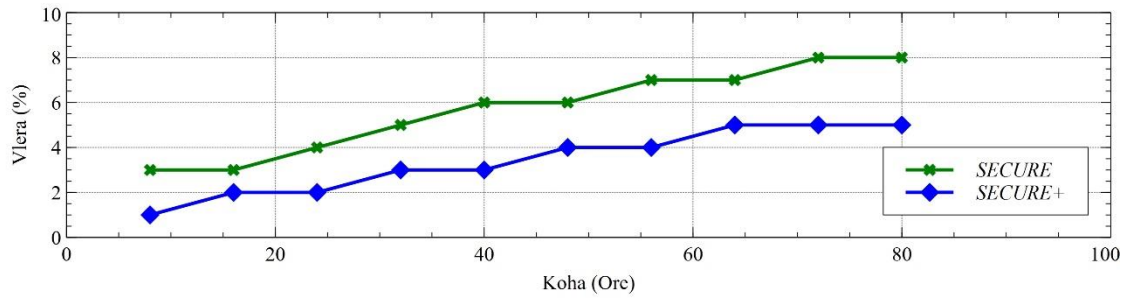

Figura 5-23 Norma Fals Negative për llojet e sulmit nga Distanca në Mbjentin Lokal (R2L)

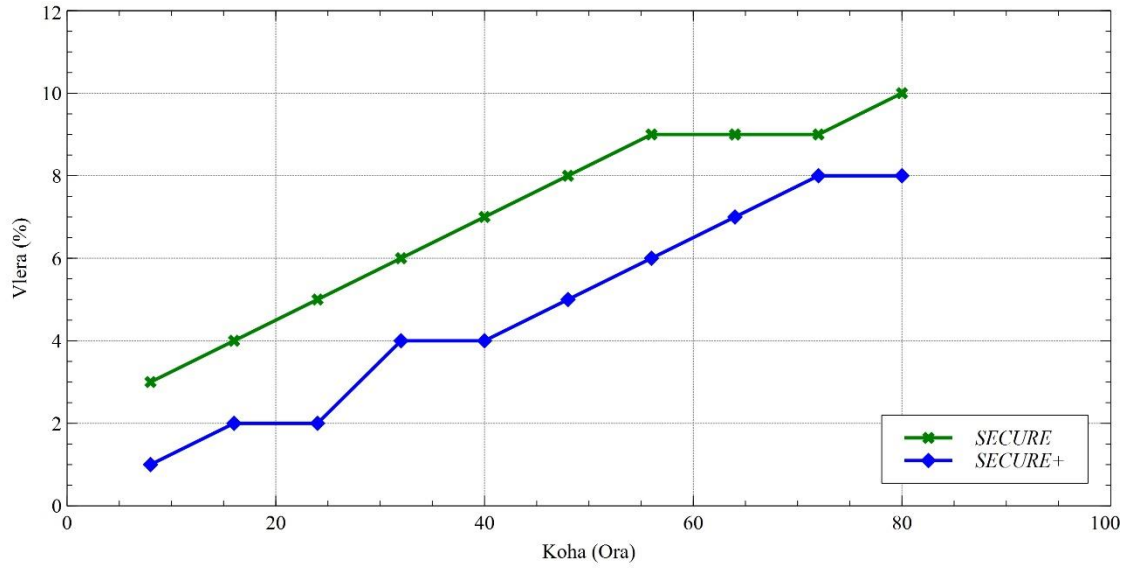

Figura 5-24 Norma Fals Negative për llojet e sulmit Sondë (Probing)

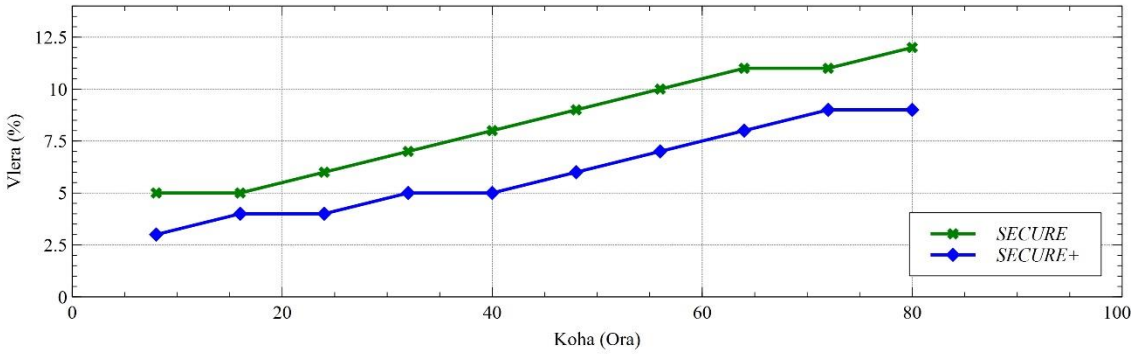

Figura 5-25 Norma Fals Negative për llojet e sulmit Mohimi i Shpërndarë i Shërbimit (DDoS)

Shumica e algoritmave kryesisht, përveç metrikave NFP dhe NFN kanë edhe metrikën Norma e Dedektimit të Ndërhyrjes (NDN) si një pikë referimi. Kryesisht algoritmat që

kanë vlerë të ulët të metrikës NDN nuk konsiderohen fare dhe nuk përdoren, sado të lartë ta kenë vlerën e NFP-së.

Dy figurat e paraqitura më poshtë, Figura 5-26 dhe Figura 5-27, tregojnë se Norma e Dedektimit të Ndërhyrjes (NDN) rritet në varësi të kohës. Në këtë rast ne kemi realizuar të njëjtin ekperiment të ndarë në 10 cikle me nga 8 orë secili. Nga rezultatet e përfituara shikojmë se teknika SECURE+ performon më mirë sesa teknika SECURE në terma të NDNs. Performanca e teknikës SECURE+ është më e kënaqshme mbas 40 orësh. Të gjitha tabelat përmbledhëse të rezultateve të përfituara nga eksperimentet janë pasqyruar në Shtojcën B.

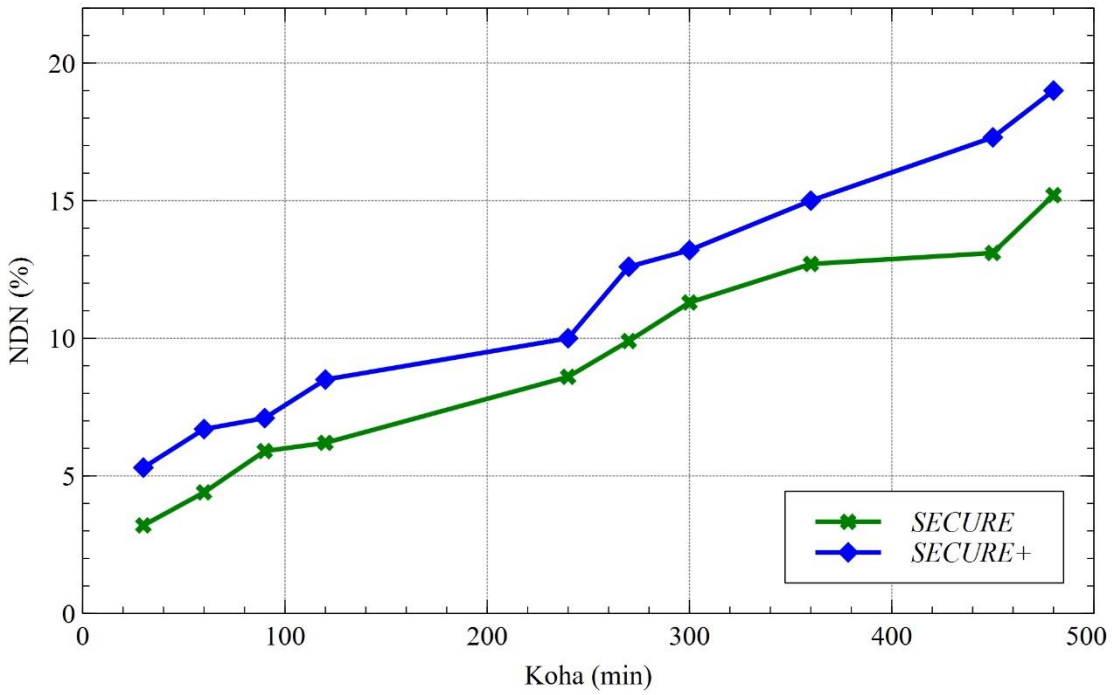

Figura 5-26 Norma e dedektimit të ndërhyrjes për 8 orët e para (në përqindje) për të dy teknikat

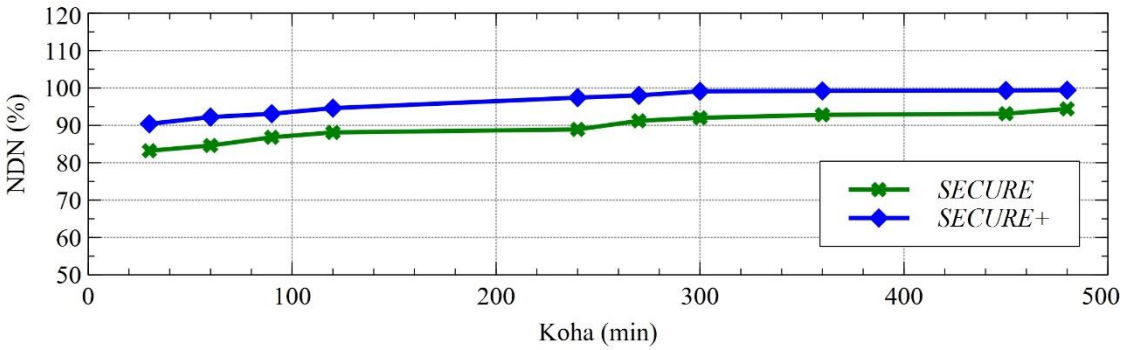

Figura 5-27 Norma e dedektimit të ndërhyrjes për 40 orët e fundit (në përqindje) për të dy teknikat

6 KONKLUZIONE, PUNA NË TË ARDHMEN

Në këtë punim ne kemi propozuar një teknikë me vet mbrojtje dhe ndërveprim automatik në menaxhimin e burimeve cloud të quajtur SECURE+. Kjo teknikë vetmbrojtëse dhe automatike dedekton ndërhyrjet dhe sulmet (të njohura dhe të panjohura) të kryera ndaj platformave Cloud. Teknika SECURE+ është e ndërtuar për të evidentuar sulmet nga një kombinim midis sistemit të dedektimit të sulmeve i quajtur SNORT dhe teknikës XGBoost. Ajo funksionon si një sistem i vetëm ndërhyrjesh ku një seri rregullash të SNORT funksionojnë paralelisht me logjikën e aplikuar nga algoritmi i mësimit automatik me vendim-marrje pemë i quajtur XGBoost.

XGBoost është algoritëm me përmirësim të gradientit në grupin me vendim-marrje pemë i cili ka avantazhet se është me burim të hapur, efikas dhe popullor. Kemi zgjedhur të përdorim metodën e Përmirësimit të Gradientit për shkak se kjo metodë është konsideruar metoda me efektive dhe më e vlefshme në rastin kur bëhet fjalë për detyra me të dhëna të strukturuara (siç është dhe rasti i studimit tonë).

Arsyeja për integrimin e SNORT me XGboost është sepse SNORT dedekton vetëm trafikun e dëmshëm që ka në bazën e të dhënave. Në këtë këndvështrim SNORT gjithashtu ka një normë dedektimi fals pozitiv të lartë. Trafiku i panjohur i cili mund të jetë një model i trafikut të dëmshëm që nuk ekziston në bazën e të dhënave të SNORT do të dedektohet nga mekanizmat e algoritmit XGBoost, e cila do të reduktojë edhe normën e alarmeve fals pozitive.

Ne kemi propozuar teknikën SECURE+, e cila është një teknikë me vet-mbrojtje përkundrejt sulmeve të sigurisë në platformat cloud computing. SECURE+ mbron platformat cloud computing nga pesë tipe të ndryshme sulmesh sigurie që përfshijnë sulmet DoS, DDoS (edhe UDP Flooding dhe NTP amplification), Probing, U2R, dhe R2L. Më tej, ne kemi testuar edhe performancën e teknikës SECURE+ në terma të normës së dedektimit të ndërhyrjes, kohës së ekzekutimit, normës fals pozitive si dhe përdorimit të burimeve kompjuterike.

Rezultatet eksperimentale treguan se performanca e teknikës SECURE+ është më e mirë se ajo e teknikës SECURE, duke na ofruar shërbime cloud të sigurta dhe duke na mbrojtur nga sulmet e sigurisë që mund të hasin këto platforma.

Në këtë studim krahasuam performancën e dy teknikave të dedektimit të ndërhyrjeve, të quajtura SECURE+ dhe SECURE. Të dyja këto teknika rezultuan të jenë sisteme dedektimi efikase dhe me performancë të lartë. Rezultatet e eksperimenteve treguan se teknika SECURE+ është më efektive dhe përdor më pak burime kompjuterike krahasuar me teknikën SECURE. Nga këto rezultate evidentuam se teknika SECURE+ përdor përafërsisht 10% më pak burime procesimi (CPU) dhe rreth 7% më pak memorje RAM. Gjithashtu teknika SECURE+ proceson një numër më të madh paketash rreth 30% me tepër paketa për sekondë krahasura me teknikën SECURE.

Teknika SECURE+ ka një normë rrëzimi paketash më të ulët se teknika SECURE. Tek të dyja teknikat u vu re se sistemi operativ ishte përgjegjës për rrëzimin e paketave në rastin e rritjes së trafikut nga 2 Gbps deri në 10 Gbps. Në këto shpejtësi rrjeti, bufferat e memories okupoheshin plotësisht duke mos realizuar dot leximin e paketave brenda këtyre buferave, si rrjedhojë të dyja teknikat kërkojnë memorje RAM më të madhe në rastin e kapaciteteve të larta të rrjetit që varion nga 2Gbps deri në 10Gbps. Ky fenomen nuk ekziston për shpejtësi të ulta të rrjetit nga 100 Mbps deri në 1 Gbps.

Ambjentin e eksperimentit e kemi ndërtuar në platform virtuale duke përafruar sa më shumë të mundet me një platform cloud publike. Duke mos patur informacion se çfarë versioni SNORT ka pasur teknika SECURE, kemi ndërtuar të njëjtin ambjent eksperimental të bazuar tek aplikacioni SNORT 2.9.17 build 199. Ky version është i pajisur me opsionin shumë-procesues në të njëjtën kohë dhe ofron një performancë më të mirë krahasur me versionet e mëparshme.

Në eksperimentet e realizuara i mëshuam gjithashtu rëndësisë të saktësisë në dedektim për të dyja teknikat. Në rastin kur kishim një injektim të të dy trafiqeve, atij legjitim dhe të dëmshëm mbi teknikat, vumë re se Norma Fals Pozitive (NFP) tek teknika SECURE+ ishte më ulët se ajo e teknikës SECURE. Kjo normë është më e ulët për të pesë llojet e sulmit si dhe vlen të theksohet që ka një trend zbritës në rastin kur kohëzgjatja e eksperimentit rritet. Rezultatet e ekperimenteve treguan që teknika SECURE+ ka një Normë Fals Pozitive rreth 4% më të ulët se teknika SECURE.

Metrika tjetër me shumë rëndësi që studiuam ishte Norma e Dedektimit të Ndërhyrjes, e cila është një metrikë shumë e rëndësishme për shkak se përcakton efikasitetin e një sistemi dedektimi. Nga rezultatet e eksperimetit vumë re se vlera e NDNs u rrit me rritjen e kohës duke arritur vlerën maksimale prej 98.8% gjatë orës së 40. Duke e krahasur me teknikën SECURE edhe ky metrik është përafërsisht 5% më i ulët se teknika SECURE+.

Në këtë punim në propozuam teknikën SECURE+, një teknikë me dedektim automatik të ndërhyrjeve të ligjshme dhe të pa ligjshme dhe vet-mbrojtëse në rast të një sulmi mbi një platform cloud computing. Kjo teknikë synon të ofrojë sigurinë e kërkuar platformave cloud të sotme. Teknika e propozuar mbështetet mbi identifikimin e sulmeve të ndryshme në mënyrë automatike nëpërmjet aplikacionit SNORT dhe algoritmit të përmirësimit të gradientit XGBoost, si dhe për të ndërmarrë veprime përmirësuese ndërmjet algoritmit me mësim automatik dhe vendim-marrje pemë.

Ne mendojmë se kjo teknikë është premtuese për arritjen e rezultateve të dëshirueshme në kohë-reale, me dedektim shumë të saktë dhe tejkalimin nga sulmet e sigurisë të pesë llojeve të ndryshme DoS, DDoS (duke përfshirë UDP Flooding dhe NTP amplification), Probing, U2R, dhe R2L mbi platformat cloud computing.

6.1 PUNËT NË TË ARDHMEN

Duke konsideruar teknikën e propozuar dhe studiuar, realizimin dhe rezultatet e përfituara, dalim në konkluzionin se punët në vazhdim mund të bazohen në:

- Realizimin praktit të teknikës SECURE+ në një mjedis real Cloud.
- Përmirësimi i SECURE+ për identifikimin dhe parandalimin e sulmeve të ditës-zero.
- Përmirësimi i SECURE+ për të evidentuar normën e shkeljes së marreveshjes së nivelit të shërbimit
- Përmirësimi i SECURE+ për të punuar me disa parametra të tjerë si efektivitetin energjetik, përshkallëzueshmërinë, etj.

7 REFERENCAT

[1] Z.R. Alashhab et al., Impact of coronavirus pandemic crisis on technologies and cloud computing applications, Journal of Electronic Science and Technology, https://doi.org/10.1016/j.jnlest.2020.100059, November 2020.

[2] B. Caswell and J. Beale, Snort 2.1 Intrusion Detection, Syngress, 2004.

[3] M. S. Siva Priya, Bipin Kumar Sahu, Badal Kumar, Mayank Yadav "Network Intrusion Detection System using XG Boost", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.

[4] Sukhpreet Singh Dhaliwal , Abdullah-Al Nahid and Robert Abbas "Effective Intrusion Detection System Using XGBoost" MDPI Journal of Information, 9, 149; doi:10.3390/info9070149, 21 June 2018.

[5] S.S. Gill and R. Buyya, "SECURE: Self-ProtectionR. Buyya, "SECURE: Self-ProtectionApproach Approach In Cloud Resource Management", IEEE Cloud Computing, 2018, pp 1-8.

[6] Barrie Sonsisky, " Cloud Computing Bible", Wiley Publishing Inc, 2011, pp 10 - 20.

[7] Burko Furht and Armando Escalante, "Handbook of Cloud Computing", Springer Science+Business Media, LLC 2010, pp 3 – 5.

[8] Thomas Erl, Zaigham Mahmood and Ricardo Puttini, " Cloud Computing, Concepts, Technology and Architecture", Prentice Hall, Service Tech Press, September 2013, pp 33-43.

[9] E. Alite, O. Shurdi, ISTI 2015 "Implementation of Cloud Computing platforms in Albania. Data Security and financial impact for storing them within national boundaries", TIRANA, June, 2015.

[10] E. Alite, J. Imami, ISTI 2014 "Technical Challenges and Economic Opportunities of Cloud Computing Implementations in Albania", TIRANA, June, 2014.

[11] LIGJ, Nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012 "PËR MBROJTJEN E TË DHËNAVE PERSONALE", http://www.inovacioni.gov.al/files/pages_files/ligji_nr_9887_date_10_03_2008_i_ndryshuar_me_nr__48__2012__per_mbrojtjen___.pdf

[12] Thomas Erl, Zaigham Mahmood and Ricardo Puttini, " Cloud Computing, Concepts, Technology and Architecture", Prentice Hall, Service Tech Press, September 2013, pp 117-138.

[13] State of Cloud Adoption And Security. (2017). https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/ (Retrieved 25 May 2017)

[14] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Procedia Computer Science 110, 465–472, 2017, by Elsevier B.V.

[15] Nabeel Khan, Adil Al-Yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework", Procedia Computer Science 94 485 – 490, 2016 by Elsevier B.V.

[16] Josiah Dykstra, Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", Digital Investigation 9 S90–S98, 2012 Dykstra & Sherman. Published by Elsevier Ltd.

[17] Sato H, Kanai A, Tanimoto S. A cloud trust model in a security aware cloud. In: Proceedings of the 2010 10th IEEE/IPSJ international symposium on applications and the Internet. SAINT '10; 2010. p. 121–4.

[18] Karan B. Virupakshar, Manjunath Asundi, Kishor Channal, Pooja Shettar, Somashekar Patil, Narayan D. G. "Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud ", Procedia Computer Science 167, 2297–2307, 2020 by Elsevier B.V.

[19] Bikram Khadka, Chandana Withana, Abeer Alsadoon, Amr Elchouemi, 2015. Distributed Denial of Service attack on Cloud Detection and Prevention. School of Computing and Mathematics, Charles Sturt University, Sydney, Australia Hewlett Packard. 2015 International Conference (pp. 1-5). IEEE.

[20] B. Hari Krishna, Dr.S. Kiran, G. Murali , R. Pradeep Kumar Reddy, "Security Issues In Service Model Of Cloud Computing Environment" Procedia Computer Science 87 246 – 251, 2016 by Elsevier B.V.

[21] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System", TSINGHUA SCIENCE AND TECHNOLOGY, ISSNl l1007-0214l l05/12l lpp40-50, Volume 18, Number 1, February 2013.

[22] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, Monarch: Providing real-time URL spam filtering as a service, in Proc. IEEE Symposium on Security and Privacy, Oakland, California, USA, 2011, pp. 447-462.

[23] Dan Gonzales, Member, IEEE, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 3, JULY-SEPTEMBER 2017.

[24] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Jul.–Dec. 2013.

[25] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Procedia Engineering 15 2852 – 2856, 2011 by Elsevier B.V.

[26] Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan "Study on the security models and strategies of cloud computing", 2011 International Conference on Power Electronics and Engineering Application, Procedia Engineering 23 586 – 593, 2011 by Elsevier B.V.

[27] Farrukh Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14), Procedia Computer Science 37, 357 – 362, 2014 by Elsevier B.V.

[28] Rizwana Shaikh, Dr. M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015), Procedia Computer Science 45 380 – 389, 2015 by Elsevier B.V.

[29] Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad "Multilevel classification of security concerns in cloud computing",

Applied Computing and Informatics, Saudi Computer Society, King Saud University, April 2016

[30] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015), Procedia Computer Science 48, 204 – 209, 2015 by Elsevier B.V.

[31] Issam Kouatli "Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management.", Information Technology and Quantitative Management (ITQM 2016), Procedia Computer Science 91 412 – 421, 2016 by Elsevier B.V.

[32] Hicham Toumi, Fatima Zahra Fagroud, Amiyne Zakouni, Mohamed Talea "Implementing Hy-IDS, Mobiles Agents and Virtual Firewall to Enhance the Security in IaaS Cloud", The International Workshop on Emerging Networks and Communications (IWENC 2019), Procedia Computer Science 160, 819–824, 2019 by Elsevier B.V.

[33] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2003.

[34] W. Stallings and L. Brown, Computer Security Principles and Practice, Pearson, 2012.

[35] M. Goodrich and R. Tamassia, Introduction to Computer Security, Pearson, 2010.

[36] K.J. Houle, G.M. Weaver, N. Long and R. Thomas, Trends in Denial of Service Attack Technology. CERT Coordination Center, Oct. 2001. [Online] Available: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[37] D. Moore, G.M. Voelker and S. Savage, Inferring Internet denial-of-service activity, in: Proceedings of the 10th USENIX Security Symposium, Washington, DC, 2001.

[38] CERT Coordination Center, Overview of attack trends, Feb. 2002. [Online] Available: http://www.cert.org/archive/pdf/attack_trends.pdf.

[39] Cisco Systems, Inc., Characterizing and tracing packet floods using cisco routers, Feb. 2003.

[40] R. Stone, Centertrack: An IP overlay network for tracking DoS floods, in: Proceedings of the 9th USENIX Security Symposium, Denver, CO, 2000.

[41] R.K. Chang, Defending against flooding-based distributed denial-of-service attacks: A tutorial, IEEE Commun. Mag. 40(10) (2002), 42–51.

[42] P. Ferguson and D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, May 2000.

[43] Cisco Systems, Inc., Characterizing and tracing packet floods using cisco routers, Feb. 2003.

[44] B. Guha and B. Mukherjee, Network security via reverse engineering of TCP code: Vulnerability analysis and proposed solutions, IEEE Network 11(4) (1997), 40–48.

[45] V. Paxson, An analysis of using reflectors for distributed denial-of-service attacks, ACM SIGCOMM Computer Communication Review 31(3) (2001).

[46] S. Northcutt and J. Novak, Network Intrusion Detection, 3rd edn, New Riders Publishing, Indiana, IN, 2002.

[47] CERT Coordination Center, Overview of attack trends, Feb. 2002. [Online] Available: http://www.cert.org/archive/pdf/attack_trends.pdf.

[48] S.A. Crosby and D.S. Wallach, Denial of Service via algorithmic complexity attacks, in: Proceedings of the 12th USENIX Security Symposium, Washington, DC, USA, 2003.

[49] SecuriTeam, Kiss of Death – a new Denial of Service attack, 1999.

[50] P. Papadimitratos and Z.J. Haas, Securing the Internet routing infrastructure, IEEE Commun. Mag. 40(10) (2002), 60–68.

[51] D. Moore, C. Shannon and J. Brown, Code-Red: a case study on the spread and victims of an Internet worm, in: Proceedings of the Internet Measurement Workshop, Marseille, France, 2002.

[52] I. Arce and E. Levy, An analysis of the Slapper worm, IEEE Security & Privacy 1(1) (2003), 82–87.

[53] D. Moore, C. Shannon, G.M. Voelker and S. Savage, Internet quarantine: Requirements for containing self-propagating code, in: Proceedings of the IEEE Infocom, 2003.

[54] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N.Weaver, Inside the Slammer worm, IEEE Security & Privacy 1(4) (2003), 33–39.

[55] S. Staniford, V. Paxson and N. Weaver, How to 0wn the Internet in your spare time, in: Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, 2002.

[56] Christos Douligeris, Christos Douligeris, “DDOS Attacks and Defense Mechanisms: a Classification”, DOI: 10.1109/ISSPIT.2003.1341092 · Source: IEEE Xplore, January 2004.

[57] G. Qu, O.A. Rawashdeh, and D. Che, “Self-Protection against Attacks in an Autonomic Computing Environment,” International Journal of Computer Applications (CAINE), vol. 17, no. 4, 2010, pp. 250–256

[58] A. Carpen-Amarie, “Towards a self-adaptive data management system for cloud environments,” IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW 11), 2011, pp. 2077–2080.

[59] A. Wailly, M. Lacoste, and H. Debar, “Vespa: Multi-layered self-protection for cloud resources,” Proceedings of the 9th International Conference on Autonomic Computing (ICAC 12), 2012, pp. 155–160.

[60] A. Sulistio and C. Reich, “Towards a Self-Protecting Cloud,” On the Move to Meaningful Internet Systems: OTM 2013 Conferences., Springer, 2013, pp. 395–402.

[61] E. Benkhelifa and T. Welsh, “Towards Malware Inspired Cloud Self-Protection,” Proceedings of the 2014 International Conference on Cloud and Autonomic Computing (ICCAC 14), 2014, pp. 1–2.

[62] P. Manuel, “A trust model of cloud computing based on Quality of Service,” Annals of Operations Research, vol. 233, no. 1, 2015, pp. 281–292.

[63] R.D. Di Pietro, F. Lombardi, and M. Signorini, “Secure Management of Virtualized Resources,” Security in the Private Cloud, CRC Press, 2016; doi.org/10.1201/9781315372211-14.

[64] A.Y. Sarhan and S. Carr, “A Highly-Secure Self-Protection Data Scheme in Clouds Using Active Data Bundles and Agent-Based Secure Multi-party Computation,” Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud 17), 2017, pp. 228–236.

[65] S. Singh and I. Chana, “QRSF: QoS-aware resource scheduling framework in cloud computing,” The Journal of Supercomputing, vol. 71, no. 1, 2015, pp. 241–292.

[66] Duda R. and Hart P., "Pattern Classification and Scene Analysis", Wiley, New York 1973

[67] Nello Cristianini and John Shawe-Taylor, “An Introduction to Support Vector Machines and Other Kernel-based Learning Methods”, Cambridge University Press, 2000.

[68] A. J. Smola. Regression estimation with support vector learning machines. Master's thesis, Technische Universit¨at M¨unchen, 1996.

[69] M. Salehie and L. Tahvildari. Self-adaptive software: Landscape andresearch challenges. ACM Transactions on Autonomous and AdaptiveSystems (TAAS), 4(2):14, 2009.

[70] A. Computing et al. An architectural blueprint for autonomic comput-ing. IBM White Paper, 2006.

[71] Idziorek, J., and Tannian, M. Security analysis of public cloud computing, International Journal of Communication Networks and Distributed Systems, 9(1&2), 4–20, 2012.

[72] B. Grobauer, T. Walloschek and E. Stocker, Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy, vol. 9, no. 2, pp. 50–57, 2011.

[73] Z. Su and G. Wassermann, The Essence of Command Injection Attacks in Web Applications, ACM SIGPLANSIGACT Symposium on Principles of Programming (POPL), pp. 372–382, 2006.

[74] G. Wassermann and Z. Su, Static Detection of Cross-Site Scripting Vulnerabilities, International Conference on Software Engineering (ICSE), pp. 171–180, 2008.

[75] A. Barth, C. Jackson and J. C. Mitchell, Robust Defenses for Cross-Site Request Forgery, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), 2008.

[76] K.-S. Lhee and S. J. Chapin, Buffer Overflow and Format String Overflow Vulnerabilities, Software−Practice and Experience, vol. 33, no. 5, pp. 423–460, 2003.

[77] A. Kadav and M. M. Swift, Understanding Modern Device Drivers, Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2012.

[78] A. Srivastava and J. Giffin, Efficient Monitoring of Untrusted Kernel-Mode Execution, Network and Distributed System Security Symposium (NDSS), 2011.

[79] X. Xiong, D. Tian and P. Liu, Practical Protection of Kernel Integrity, Network and Distributed System Security Symposium (NDSS), 2011.

[80] D. Oliveira, N. Wetzel, M. Bucci, D. Sullivan and Y. Jin, Hardware-Software Collaboration for Secure Coexistence with Kernel Extensions, ACM Applied Computing Review Journal, vol. 14, no. 3, pp. 22–35, 2014.

[81] K. Hashizume, D. G. Rosado, E. Fernández-Medina and E. B. Fernandez, An Analysis of Security Issues for Cloud Computing, Journal of Internet Services and Applications, vol. 4, pp. 5, 2013.

[82] L. Ertaul, S. Singhal and S. Gökay, Security Challenges in Cloud Computing, Proceedings of the International Conference on Security and Management (SAM), pp. 36–42, 2010.

[83] M. Tehranipoor, H. Salmani and X. Zhang, Integrated Circuit Authentication− Hardware Trojans and Counterfeit Detection, Springer, 2014.

[84] J. Kurose and K. Ross, Computer Networking: A Top-Down Approach, Pearson, 2012.

[85] J. S. Reuben, A Survey on Virtual Machine Security, Helsinki University of Technology, 2007.

[86] Atmel, Bits and Pieces, Symmetric vs. Asymmetric Encryption: Which Way Is Better?, 2013, available at http://blog.atmel.com/2013/03/11/symmetric-vs-asymmetric-encryption-which-way-is-better/.

[87] Microsoft, Microsoft Technet, Encryption, 2015, available at https://technet.microsoft.com/en-us/library/Cc962028.aspx.

[88] T. Erl, R. Puttini and Z. Mahmood, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.

[89] Z. Wang and X. Jiang, HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity, IEEE Symposium on Security and Privacy, pp. 380–395, 2010.

[90] N. Santos, K. Gummadi and R. Rodrigues, Towards Trusted Cloud Computing, Conference on Hot Topics in Cloud Computing, 2009.

[91] F. Zhang, Y. Huang, H. Wang, H. Chen and B. Zang, PALM: Security Preserving VM Live Migration for Systems with VMM-Enforced Protection, Trusted Infrastructure Technologies Conference, pp. 9–18, 2008.

[92] N. Bridge, 2013 Future of Cloud Computing Survey Reveals Business Driving Cloud Adoption in Everything as a Service Era, 2013, available at http://www.northbridge.com/2013-future-cloud-computingsurvey-reveals-business- driving-cloud-adoptioneverything- service-era-it.

[93] A. Cavoukian, Privacy in the Clouds, Identity in the Information Society, vol. 1, no. 1, pp. 89–108, 2008.

[94] R. Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum, 2009.

[95] P. T. Jaeger, J. Lin and J. M. Grimes, Cloud Computing and Information Policy: Computing in a Policy Cloud?, Journal of Information Technology and Politics, vol. 5, no. 3, pp. 269–283, 2009.

[96] S. Pearson and A. Charlesworth, Accountability as a Way Forward for Privacy Protection in the Cloud, Hewlett-Packard Development Company (HPL-2009–178), 2009.

[97] D. Lin and A. Squicciarini, Data Protection Models for Service Provisioning in the Cloud, Proceedings of the 15th ACM Symposium on Access Control Models andTechnologies, pp. 183–192, 2010.

[98] M. Nabeel, E. Bertino, M. Kantarcioglu and B. Thuraisingham, Towards Privacy Preserving Access Control in the Cloud, 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaborate Com), pp. 172–180, 2001.

[99] M. Nabeel, N. Shang and E. Bertino, Privacy Preserving Policy-Based Content Sharing in Public Clouds, IEEE Transaction on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2602–2614, 2013.

[100] N. Shang, M. Nabeel, F. Paci and E. Bertino, A Privacy-Preserving Approach to Policy-Based Content Dissemination, IEEE 26th International Conference on Data Engineering (ICDE), pp. 944–955, 2010.

[101] A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Technique (EUROCRYPT), pp. 457–473, 2005.

[102] S. Sundareswaran, A. Squicciarini, D. Lin and S. Huang, Ensuring Distributed Accountability for Data Sharing in the Cloud, IEEE Transactions on Dependable and Secure Computing (TDSC), vol. 9, no. 4, pp. 556–568, 2012.

[103] M. Bawa, R. J. Bayardo, R. Agrawal and J. Vaidya, Privacy-Preserving Indexing of Documents on the Network, Very Large Data Base Journal, vol. 18, no. 4, pp. 837–856, 2009.

[104] Y.-C. Chang and M. Mitzenmacher, Privacy Preserving Keyword Searches on Remote Encrypted Data, 2004.

[105] Z. Yang and S. Z. N. Wright., Towards Privacy-Preserving Model Selection, PinKDD, pp. 138–152, 2007.

[106] A. Squicciarini, S. Sundareswaran and D. Lin, Preventing Information Leakage from Indexing in the Cloud, IEEE International Conference on Cloud Computing, 2010.

[107] B. Khadka, C. Withana, A. Alsadoon, and A. Elchouemi, "Distributed Denial of Service attack on Cloud : Detection and Prevention," vol. 4, no. September, pp. 210–215, 2015.

[108] J. Buchanan, Bill; Flandrin, Flavien; Macfarlane, Richard;Graves, "A Methodology To Evaluate Rate-Based Intrusion Prevention System Against Distributed Denial of Service," no. August 2016, pp. 17–22, 2010.

[109] S. Singh, and I. Chana, "QRSF: QoS-aware resource scheduling framework in cloud computing," J. Supercomputing, vol. 71, no. 1, pp. 241–292, 2015.

[110] S. Singh, and I. Chana, "Q-aware: Quality of service based cloud resource provisioning," Comput. Electr. Eng., vol. 47, pp. 138–160, 2015.

[111] Gill, S. S., & Buyya, R. (2019). Resource provisioning based scheduling framework for execution of heterogeneous and clustered workloads in Clouds: From fundamental to autonomic offering. Journal of Grid Computing, 17(3), 385–417. doi:10.1007/s10723-017-9424-0

[112] Benkhelifa, E., & Welsh, T. (2014). Towards Malware Inspired Cloud Self-Protection. Proceedings of the IEEE International Conference on Cloud and Autonomic Computing (ICCAC) (pp. 1-2). IEEE Press.

[113] Singh, S., Chana, I., & Buyya, R. (2017). STAR: SLA-aware Autonomic Management of Cloud Resources. IEEE Transactions on Cloud Computing. doi:10.1109/TCC.2017.2648788

[114] Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., & Garraghan, P. et al. (2019). Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges. Internet of Things, 8, 100118. doi:10.1016/j.iot.2019.100118

[115] Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. Annals of Operations Research, 233(1), 281-292.

[116] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30–48. doi:10.1016/j.comcom.2017.03.010

[117] M. N. Banu, “Cloud Computing Simulation Tools - A Study,” vol. 7, no. 1, pp. 13–25, 2015.

[118] Hping3. Available online: http://www.hping.org/hping3.html (accessed on 20 February 2021).

8 SHTOJCA _A

8.1 ALGORITMET E PËRDORUR

8.1.1 Algoritmi 1 Funksioni pikë-më-pikë

L_D ←Lidhu me Nyjen e Dedektimit

M ←Ngarko Modelin e Permiresimit te Gradientit

L_B ←Lista e Zeze

while** Vertete **do

for** D ne L_D **do

L_E ←Terhiq hyrjet e rrjedhes nga D

F ←Krijimi i Karakteristikes (L_E)

DEDEKTIM_SULMI (F)

end for

Prit per pak kohe

end while

***procedure** DEDEKTIM_SULMI (F)*

C ← Klasifiko F duke perdorur M

if** C eshte sulm **then

I ←Merrni identifikuesit e burimit nga F

SHMANGIA E SULMIT(C, I)

end if

end procedure

***procedure** SHMANGIA E SULMIT (C, I)*

if** I nuk eshte ne L_B **then

E ← Krijoni hyrjen e rrjedhes per te bllokuar ose ridrejtuar I

Instalo E ne S

L_B.shto (I)

end if

end procedure

8.1.2 Algoritmi 1 - Kodi Burim (Python)

```
# Algoritmi 1 Funksioni pike-me-pike
#
import time
import numpy

L_D = GetConnectedSDNSwitches()  # Lidhu me Nyjen e Dedektimit
from classifier import RFclassifiermodel #Ngarko Modelin e Permiresimit t
e Gradientit
M = RFclassifiermodel
from blacklist import Lista_e_Zeze
L_B = Lista_e_Zeze

while True:

    for D in L_D:
        L_E = Get.Source.Input(D)
        F = FEATURE_CREATION(LE)
        DEDEKTIM_SULMI(F)

    time.sleep(5)

def DEDEKTIM_SULMI(F):

    C = Klasifiko(F, M)

    if (C == sulm):
        I = Merr_identifikuesit_e_burimit_nga(F)
```

```
        SHMANGIA_E_SULMIT(C, I)


def SHMANGIA_E_SULMIT(C, I):
    if I not in L_B:
        E = CreateFlowEntrytoBlockorRedirect(I)   #Krijon hyrjen e rrjedh
es per te bllokuarose ridrejtuar I
        Instalo(E, S)
        L_B.add(I)
```

8.1.3 Algoritmi 2 Krijimi i Karakteristikave

L_E ← *Hyrjet e Rrjedhes*

F ← *Vektori i Karakteristikes*

C ← *LLOGARIT_PERBASHKET*(L_E)

for all *E ne* L_E ***do***

F.Sbytes ← *E.getByteCount()*

F.Spkts ← *E.getPacketCount()*

F.Dur ← *E.getDuration()*

F.Mean ← *C.mean*

F.Stddev ← *C.stddev*

F.Sum ← *C.sum*

F.TnP_PSrcIP ← *C.TnP_PSrcIP*

F.TnP_PDstIP ← *C.TnP_PDstIP*

F.TnP_Per_Dport ← *C.TnP_Per_Dport*

srcIP ← *E.getSourceIp()*

dstIP ← *E.getDestinationIp()*

proto_number ← *E.getInternetProtocolNumber()*

if *proto_number eshte TCP ose UDP* ***then***

srcPort ← *E.getSourcePort()*

dstPort ← *E.getDestinationPort()*

key ← *dstIP + dstPort + srcIP + srcPort*

F.Dbytes ← *C.hashMap.get(key)*

else if *proto_number is ICMP* ***then***

key ← *dstIP + srcIP*

F.Dbytes ← C.hashMap.get(key)

end if

end for

kthehu F

end procedure

8.1.4 Algoritmi 2 - Kodi Burim (Python)

```
# Algoritmi 2 Krijimi i Karakteristikave

def FEATURE_CREATION(FlowEntries)
L_E = FlowEntries                # Hyrjet e Rrjedhes
F = Vektori i Karakteristikes
C = LLOGARIT_PERBASHKET(L_E)

for E in L_E:
    F.Sbytes = E.getByteCount()
    F.Spkts = E.getPacketCount()
    F.Dur = E.getDuration()
    F.Mean = numpy.mean(C)
    F.Stddev = numpy.stddev(C)
    F.Sum = numpy.sum(C)
    F.TnP_PSrcIP = C.TnP_PSrcIP
    F.TnP_PDstIP = C.TnP_PDstIP
    F.TnP_Per_Dport = C.TnP_Per_Dport
    srcIP = E.getSourceIp()
    dstIP = E.getDestinationIp()
    proto_number = E.getInternetProtocolNumber()

    if proto_number is TCP or UDP:
        srcPort = E.getSourcePort()
        dstPort = E.getDestinationPort()
```

```
        key = dstIP + dstPort + srcIP + srcPort
        F.Dbytes = C.hashMap.get(key)

    elif proto_number is ICMP:
        key = dstIP + srcIP
        F.Dbytes = C.hashMap.get(key)

return F
```

8.1.5 Algoritmi 3 Përllogaritja e Karakteristikave dhe Statistikave të Përbashkëta

procedure *LLOGARIT_PERBASHKET(L_E)*

C ← Statistika te Perbashketa

srcIpSet ← Krijon Grupin Hash te IP te burimit

dstIpSet ← Krijon Grupin Hash te IP te destinacionit

portSet ← Krijon Grupin Hash te portes se destinacionit

L_K ← Krijon Listen e kohezgjatjes

totalPacketCnt ← 0

for all *E ne L_E* ***do***

pkts ← E.getPacketCount()

totalPacketCnt ← totalPacketCnt + pkts

bytes ← E.getByteCount()

L_K.add(E.getDuration())

srcIP ← E.getSourceIp()

srcIpSet.add(srcIP)

dstIP ← E.getDestinationIp()

dstIpSet.add(dstIP)

proto_number ← E.getInternetProtocolNumber()

if *proto_number is TCP or UDP* ***then***

srcPort ← E.getSourcePort()

dstPort ← E.getDestinationPort()

key ← srcIP + srcPort + dstIP + dstPort

C.hashMap.put(key,bytes)

else if *proto_number is ICMP* ***then***

key ← srcIP + dstIP

C.hashMap.put(key,bytes)

end if

end for

C.tnP_PSrcIp ← totalPacketCnt/srcIpSet.size()

C.tnP_PDstIp ← totalPacketCnt/dstIpSet.size()

C.tnP_Per_DPort ← totalPacketCnt/portSet.size()

C.mean ← mesatarja e L_K

C.stddev ← devijimi standart i L_K

C.sum ← shumatorja e L_K

return *C*

end procedure

8.1.6 Algoritmi 3 - Kodi Burim (Python)

```
# Algoritmi 3 Perllogaritja e Karakteristikave dhe Statistikave te Perbas
hketa


def LLOGARIT_PERBASHKET(L_E):


    C = Statistika_te_Perbashketa
    srcIpSet = CreateSourceIPHashSet()
    dstIpSet = CreateDestinationIPHashSet()
    portSet = CreateDestinationPortHashSet()  # Krijon Grupin Hash te por
tes se destinacionit
    L_K = CreateDurationList()  # Krijon_Listen_e_kohezgjatjes
    totalPacketCnt = 0


    for E in L_E:
        pkts = E.getPacketCount()
        totalPacketCnt = totalPacketCnt + pkts
```

```
        bytes = E.getByteCount()
        L_K.add(E.getDuration()
        srcIP = E.getSourceIp()
        srcIpSet.add(srcIP)
        dstIP = E.getDestinationIp()
        dstIpSet.add(dstIP)
        proto_number = E.getInternetProtocolNumber()

        if proto_number is TCP or UDP:
            srcPort = E.getSourcePort()
            dstPort = E.getDestinationPort()
            key = srcIP + srcPort + dstIP + dstPort
            C.hashMap.put(key, bytes)

        elif proto_number is ICMP then
            key = srcIP + dstIP
            C.hashMap.put(key, bytes)

C.tnP_PSrcIp = totalPacketCnt/srcIpSet.size()
C.tnP_PDstIp = totalPacketCnt/dstIpSet.size()
C.tnP_Per_DPort = totalPacketCnt/portSet.size()
C.mean = numpy.mean(L_K)
C.stddev = numpy.stddev(L_K)
C.sum = sum(L_K)

return C
```

9 SHTOJCA _B

9.1 REZULTATET E PËRFITUARA NGA EKSPERIMENTET NË FORMË TABELARE

Tabela 9-1 Përdorimi i CPUs në (%) për teknikat SECURE+ dhe SECURE për shpejtësi të ndryshme të trafikut

	Dita 1				Dita 2			
	Cikli 1		Cikli 2		Cikli 3		Cikli 4	
Shpejtesia e Trafikut	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)
1 Gbps	40	48	38	48	40	47	40	47
2 Gbps	42	49	41	48	42	50	43	48
3 Gbps	44	53	45	51	44	53	45	53
4 Gbps	47	65	44	60	46	66	46	65
5 Gbps	54	56	51	58	55	61	54	59
6 Gbps	52	67	54	60	53	65	54	60
7 Gbps	61	62	58	60	60	63	59	65
8 Gbps	54	68	56	67	53	70	54	68
9 Gbps	62	69	58	64	60	68	60	69
10 Gbps	60	70	55	68	59	71	59	70

Shpejtesia e Trafikut	Dita 3				Dita 4			
	Cikli 5		Cikli 6		Cikli 7		Cikli 8	
	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)
1 Gbps	40	48	41	49	41	50	42	51
2 Gbps	42	50	43	52	44	53	45	54
3 Gbps	44	54	45	56	45	56	46	56
4 Gbps	45	66	46	67	47	67	47	67
5 Gbps	53	60	54	62	54	63	54	64
6 Gbps	52	65	54	67	55	65	55	66
7 Gbps	60	67	61	68	62	69	63	69
8 Gbps	53	69	55	70	55	71	55	71
9 Gbps	62	70	64	72	64	73	65	72
10 Gbps	60	71	62	73	63	74	63	75

Shpejtesia e Trafikut	Dita 5					
	Cikli 9		Cikli 10		Mesatarja	
	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)	SECURE+ (%)	SECURE (%)
1 Gbps	43	51	43	54	40.8	49.3
2 Gbps	45	55	45	58	43.2	51.7
3 Gbps	46	58	46	60	45	55
4 Gbps	47	67	47	68	46.2	65.8
5 Gbps	54	65	54	66	53.7	61.4
6 Gbps	55	67	55	69	53.9	65.1
7 Gbps	64	70	64	71	61.2	66.4
8 Gbps	56	72	56	74	54.7	70
9 Gbps	66	73	66	76	62.7	70.6
10 Gbps	64	76	64	79	60.9	72.7

Tabela 9-2 Përdorimi i memorjes në (Gbps) në të dy teknikat SECURE+ dhe SECURE për shpejtësi trafiku të ndryshme

Shpejtesia e Trafikut	Dita 1				Dita 2				Dita 3			
	Cikli 1		Cikli 2		Cikli 3		Cikli 4		Cikli 5		Cikli 6	
	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE
1 Gbps	40	47	41	48	39	46	40	47	42	49	43	50
2 Gbps	52	59	53	60	51	58	52	59	54	61	55	62
3 Gbps	62	69	63	70	61	68	62	69	64	71	65	72
4 Gbps	70	77	71	78	69	76	70	77	72	79	73	80
5 Gbps	75	82	76	83	74	81	75	82	77	84	78	85
6 Gbps	80	87	81	88	79	86	80	87	82	89	83	90
7 Gbps	85	92	86	93	84	91	85	92	87	94	88	95
8 Gbps	90	97	91	98	89	96	90	97	92	99	93	100
9 Gbps	93	100	94	101	92	99	93	100	95	102	96	103

Shpejtesia e Trafikut	Dita 4				Dita 5				Mesatarja	
	Cikli 7		Cikli 8		Cikli 9		Cikli 10			
	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE
1 Gbps	44.0	51.0	45.0	52.0	46.0	53.0	47.0	54.0	41.5	48.5
2 Gbps	56.0	63.0	57.0	64.0	58.0	65.0	59.0	66.0	53.5	60.5
3 Gbps	66.0	73.0	67.0	74.0	68.0	75.0	69.0	76.0	63.5	70.5
4 Gbps	74.0	81.0	75.0	82.0	76.0	83.0	77.0	84.0	71.5	78.5
5 Gbps	79.0	86.0	80.0	87.0	81.0	88.0	82.0	89.0	76.5	83.5
6 Gbps	84.0	91.0	85.0	92.0	86.0	93.0	87.0	94.0	81.5	88.5
7 Gbps	89.0	96.0	90.0	97.0	91.0	98.0	92.0	99.0	86.5	93.5
8 Gbps	94.0	101.0	95.0	102.0	96.0	103.0	97.0	104.0	91.5	98.5
9 Gbps	97.0	104.0	98.0	105.0	99.0	106.0	100.0	107.0	94.5	101.5
10 Gbps	98.0	105.0	99.0	106.0	100.0	107.0	100.0	107.0	96.2	103.2

Tabela 9-3 Shpejtësia e procesimit të paketave për sekondë në të dy teknikat SECURE+ dhe SECURE për kohë të ndryshme

Koha e Kaluar (sek)	Dita 1				Dita 2				Dita 3			
	Cikli 1		Cikli 2		Cikli 1		Cikli 2		Cikli 1		Cikli 2	
	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE
1800	70,000	40,000	75,000	43,000	73,000	42,000	72,000	40,000	75,000	41,000	74,000	40,000
3600	80,000	50,000	83,000	48,000	81,000	49,000	83,000	50,000	82,000	49,000	81,000	48,000
5400	95,000	65,000	94,000	63,000	93,000	64,000	96,000	67,000	95,000	65,000	94,000	64,000
7200	110,000	80,000	105,000	78,000	105,000	78,000	110,000	78,000	109,000	78,000	108,000	77,000
14400	115,000	80,000	110,000	77,000	113,000	79,000	115,000	80,000	113,000	82,000	112,000	81,000
16200	120,000	85,000	122,000	85,000	118,000	88,000	120,000	85,000	122,000	84,000	121,000	83,000
18000	120,000	82,000	124,000	82,000	122,000	85,000	122,000	84,000	123,000	81,000	122,000	80,000
21600	115,000	85,000	118,000	86,000	117,000	84,000	115,000	86,000	116,000	87,000	115,000	86,000
27000	125,000	82,000	123,000	80,000	122,000	83,000	125,000	81,000	124,000	82,000	123,000	81,000

Koha e Kaluar (sek)	Dita 4				Dita 5				Mesatarja	
	Cikli 1		Cikli 2		Cikli 1		Cikli 2			
	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE
1800	75000	41000	74000	40000	75000	41000	74000	40000	73700	40800
3600	82000	49000	81000	48000	82000	49000	81000	48000	81600	48800
5400	95000	65000	94000	64000	95000	65000	94000	64000	94500	64600
7200	109000	78000	108000	77000	109000	78000	108000	77000	108100	77900
14400	113000	82000	112000	81000	113000	82000	112000	81000	112800	80500
16200	122000	84000	121000	83000	122000	84000	121000	83000	120900	84400
18000	123000	81000	122000	80000	123000	81000	122000	80000	122300	81600
21600	116000	87000	115000	86000	116000	87000	115000	86000	115800	86000
27000	124000	82000	123000	81000	124000	82000	123000	81000	123600	81500
28800	125000	87000	124000	86000	125000	87000	124000	86000	123500	86200

Tabela 9-4 Rrëzimi mesatar i paketave (në përqindje) në shpejtësi të ndryshme rrjeti për të dy teknikat SECURE+ dhe SECURE

Shpejtesia e Rrjetit	Shpejtesia Mesatare e Rrezimit te Paketave					
	Paketat UDP		Paketat TCP		Paketat ICMP	
	SECURE+	SECURE	SECURE+	SECURE	SECURE+	SECURE
1 Gbps	1.8%	2.9%	0.2%	6.0%	5.0%	9.3%
2 Gbps	2.1%	3.8%	0.9%	7.9%	6.3%	10.1%
3 Gbps	2.6%	4.5%	1.7%	9.5%	8.5%	11.0%
4 Gbps	2.9%	6.1%	3.1%	10.3%	9.6%	11.8%
5 Gbps	3.6%	7.3%	3.8%	11.4%	10.6%	12.5%
6 Gbps	4.8%	8.9%	4.9%	12.6%	12.0%	13.2%
7 Gbps	6.1%	10.4%	6.0%	13.8%	13.2%	14.0%
8 Gbps	6.8%	11.5%	7.1%	14.9%	14.4%	14.7%
9 Gbps	7.2%	12.3%	7.8%	15.8%	15.4%	15.4%
10 Gbps	7.7%	13.8%	8.5%	17.0%	16.5%	19.1%

Tabela 9-5 Norma Fals Pozitive për llojet e sulmeve (në përqindje) për të dy teknikat

	Cikli 1		**Cikli 2**		**Cikli 3**		**Cikli 4**		**Cikli 5**	
Tipi i Sulmit	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
DoS	42.0%	47.0%	37.0%	41.0%	29.0%	36.0%	21.0%	28.0%	15.0%	19.0%
L2R	39.0%	42.0%	33.0%	38.0%	28.0%	39.0%	29.0%	35.0%	21.0%	29.0%
R2L	44.0%	42.0%	46.0%	38.0%	38.0%	31.0%	29.0%	25.0%	19.0%	20.0%
Probing	35.0%	40.0%	29.0%	30.0%	18.0%	24.0%	11.0%	16.0%	6.0%	10.0%
DDoS	41.0%	46.0%	43.0%	51.0%	37.0%	39.0%	27.0%	32.0%	18.0%	24.0%

	Cikli 6		**Cikli 7**		**Cikli 8**		**Cikli 9**		**Cikli 10**	
Tipi i Sulmit	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
DoS	10.0%	13.0%	8.0%	12.0%	7.0%	11.0%	6.0%	10.0%	5.0%	9.0%
L2R	15.0%	20.0%	10.0%	18.0%	8.0%	17.0%	7.0%	16.0%	6.0%	16.0%
R2L	10.0%	13.0%	8.0%	9.0%	6.0%	7.0%	4.0%	6.0%	3.0%	5.0%
Probing	6.0%	10.0%	6.0%	9.0%	5.0%	9.0%	5.0%	9.0%	5.0%	9.0%
DDoS	15.0%	19.0%	12.0%	17.0%	9.0%	15.0%	8.0%	14.0%	8.0%	13.0%

Tabela 9-6 Norma Fals Negative për llojet e sulmeve (në përqindje) për të dy teknikat

	Cikli 1		**Cikli 2**		**Cikli 3**		**Cikli 4**		**Cikli 5**	
Tipi i Sulmit	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
DoS	2.0%	5.0%	3.0%	6.0%	3.0%	6.0%	4.0%	6.0%	4.0%	7.0%
L2R	1.0%	2.0%	2.0%	3.0%	2.0%	4.0%	3.0%	5.0%	3.0%	6.0%
R2L	1.0%	3.0%	2.0%	3.0%	2.0%	4.0%	3.0%	5.0%	3.0%	6.0%
Probing	1.0%	3.0%	2.0%	4.0%	2.0%	5.0%	4.0%	6.0%	4.0%	7.0%
DDoS	3.0%	5.0%	4.0%	5.0%	4.0%	6.0%	5.0%	7.0%	5.0%	8.0%

	Cikli 6		**Cikli 7**		**Cikli 8**		**Cikli 9**		**Cikli 10**	
Tipi i Sulmit	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
DoS	5.0%	7.0%	5.0%	8.0%	6.0%	8.0%	6.0%	9.0%	6.0%	9.0%
L2R	4.0%	6.0%	4.0%	7.0%	5.0%	7.0%	5.0%	8.0%	5.0%	8.0%
R2L	4.0%	6.0%	4.0%	7.0%	5.0%	7.0%	5.0%	8.0%	5.0%	8.0%
Probing	5.0%	8.0%	6.0%	9.0%	7.0%	9.0%	8.0%	9.0%	8.0%	10.0%
DDoS	6.0%	9.0%	7.0%	10.0%	8.0%	11.0%	9.0%	11.0%	9.0%	12.0%

Tabella 9-7 Norma e dedektimit të ndërhyrjes në varësi të kohës (në përqindje) për të dy teknikat

	Cikli 1		Cikli 2		Cikli 3		Cikli 4		Cikli 5	
Koha e Kaluar (sek)	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
1800	5.3%	3.2%	19.0%	16.5%	42.5%	37.0%	65.9%	62.1%	86.1%	80.6%
3600	6.7%	4.4%	21.0%	18.3%	44.7%	40.2%	67.2%	63.6%	88.9%	81.8%
5400	7.1%	5.9%	24.2%	20.0%	46.9%	42.3%	69.4%	65.2%	90.2%	84.0%
7200	8.5%	6.2%	25.9%	22.7%	49.0%	44.9%	71.5%	67.9%	92.3%	86.3%
14400	10.0%	8.6%	27.5%	24.4%	52.3%	46.2%	73.6%	69.4%	94.0%	87.2%
16200	12.6%	9.9%	29.0%	26.1%	54.6%	49.1%	75.8%	71.0%	95.1%	89.5%
18000	13.2%	11.3%	31.2%	28.8%	57.5%	53.4%	78.3%	73.8%	96.3%	90.4%
21600	15.0%	12.7%	33.4%	29.4%	59.4%	55.0%	80.0%	75.4%	97.2%	91.1%
27000	17.3%	13.1%	36.3%	32.2%	61.2%	57.1%	82.4%	77.5%	98.0%	92.6%
28800	19.0%	15.2%	39.0%	35.5%	64.1%	60.4%	84.9%	79.8%	98.8%	93.5%

	Cikli 6		Cikli 7		Cikli 8		Cikli 9		Cikli 10	
Koha e Kaluar (sek)	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**	**SECURE+**	**SECURE**
1800	89.7%	82.6%	89.9%	82.8%	90.0%	82.9%	90.2%	83.0%	90.4%	83.2%
3600	91.4%	83.8%	91.8%	84.0%	91.9%	84.2%	92.0%	84.4%	92.2%	84.6%
5400	92.3%	86.0%	92.7%	86.2%	92.8%	86.4%	92.9%	86.6%	93.1%	86.8%
7200	93.7%	87.3%	94.1%	87.5%	94.3%	87.7%	94.5%	87.9%	94.6%	88.1%
14400	96.0%	88.2%	96.8%	88.4%	97.0%	88.6%	97.2%	88.8%	97.4%	88.9%
16200	97.1%	90.5%	97.7%	90.7%	97.8%	90.8%	97.9%	91.0%	98.0%	91.2%
18000	98.3%	91.4%	98.4%	91.6%	98.6%	91.8%	98.8%	91.9%	99.1%	92.0%
21600	98.4%	92.1%	98.5%	92.3%	98.7%	92.5%	98.9%	92.6%	99.2%	92.8%
27000	98.5%	92.8%	98.6%	92.9%	98.8%	93.0%	99.0%	93.2%	99.3%	93.1%
28800	99.1%	93.9%	99.1%	94.0%	99.2%	94.1%	99.3%	94.3%	99.4%	94.4%