CLASSIFICATION OF DARKNET ACTIVITIES USING NEURAL NETWORKS

Büşra AKTAN TEN

MARCH 2023

ÇANKAYA UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER ENGINEERING
M.Sc. Thesis in
COMPUTER ENGINEERING

CLASSIFICATION OF DARKNET ACTIVITIES USING NEURAL NETWORKS

Büşra AKTAN TEN

MARCH 2023

ABSTRACT

CLASSIFICATION OF DARKNET ACTIVITIES USING NEURAL NETWORKS

AKTAN TEN, Büşra
M.Sc. in Computer Engineering

Supervisor: Asst. Prof. Dr. Serdar ARSLAN
Co-Supervisor: Assoc. Prof. Dr. Aydın KAYA
March 2023, 140 pages

It is very important to characterize and analyze the network before being exposed to threats. In this study, darknet network traffic analysis was carried out and the darknet network was determined and characterized by examining the 2 layer artificial neural network models. In the first layer, it distinguishes whether the data is benign or darknet traffic, and in the second layer, it is determined which of the categories of Browsing, P2P, Chat, Email, Transfer, Audio/Video Stream and VOIP generated by the traffic. Experiments were made with RNN, LSTM and MLP algorithm models. New data sets were produced with GAN and used as training data. LSTM and MLP algorithms are reconstructed as both multi category and binary category. The feature selection algorithm has been applied in the MLP model. CICDarknet2020 dataset was used. According to the model accuracy values, RNN, 0.98 success was achieved in the detection of darknet traffic, and 0.86 in the second layer. In the LSTM model, values of 0.99 and 0.71 were obtained. Separately modeled categories were obtained as 0.92. In the MLP model, accuracy values of 0.99 and 0.78 were observed. The close outputs were obtained with the feature selection algorithm model. In the binary category model, 96% accuracy was achieved.

Keywords: Darknet, VPN, Tor, Classification, MLP, RNN, LSTM

ÖZET

SİNİR AĞLARI İLE DARKET AKTİVİLERİNİN SINIFLANDIRILMASI

AKTAN TEN, Büşra
Bilgisayar Mühendisliği Yüksek Lisans

Danışman: Dr. Ögr. Üyesi Serdar ARSLAN
Ortak Danışman: Doç. Dr. Aydın KAYA
Mart 2023, 140 sayfa

Tehditlere maruz kalmadan önce ağı karakterize ederek analiz yapmak oldukça önemlidir. Bu çalışmada darknet ağ trafiği analizi yapılarak darknet ağı 2 katmanlı yapay sinir ağı modellerinde inceleme gerçekleştirilerek tespit ve karekterize edilmiştir. İlk katmanda verinin iyi huylu mu yoksa darknet verisi trafiğimi ayırt edilmekte, ikinci katmanda ise trafiğin oluşturduğu Browsing, P2P, Chat, Email, Transfer, Audio Stream, Video Stream ve VOIP kategorilerinden hangisine ait olduğu tespiti yapılmaktadır. RNN, LSTM ve MLP veri algoritma modelleri ile deneyler yapılmıştır. GAN ile yeni veri setleri üretilerek diğer yöntemlerin eğitim verisi olarak kullanılmıştır. LSTM ve MLP algoritmaları ikinci katmanda hem çoklu kategori hem de ikili kategorili olarak tekrar kurgulanmıştır. MLP model de özellik seçimi algoritması uygulanmıştır. CICDarknet2020 veri seti kullanılmıştır. Model doğruluk değerlerine göre RNN darknet trafiği tespitinde 0.98, ikinci katmanda ise 0.86 oranında başarı elde edilmiştir. LSTM modelinde sırasıyla 0.99 ve 0.71 doğruluk değerleri elde edilmiştir. Ayrı ayrı modellenen kategorilerin ortalama doğruluk değerleri 0.92 olarak elde edilmiştir. MLP modelinde, sırasıyla 0.99 ve 0.78 değerleri gözlemlenmiştir. Özellik seçimi algoritma modeli ile aynı çıktılar elde edilmiştir. ikili kategori modelinde ortalama olarak %96 doğruluk değerleri sağlanmıştır.

Anahtar Kelimeler: Darknet, VPN, Tor, Classification, MLP, RNN, LSTM

ACKNOWLEGEMENT

I would like to express my sincere and most special gratitude to my husband Orçun Ten for his support, encouragement, insightful and sacrifice to me. I would like to thank my brother Gökhan Aktan for his unwavering support. Finally, thanks to my Supervisor Asst. Prof. Dr. Serdar Arslan for the guidance to conduct this research.

TABLE OF CONTENTS

STATEMENT OF NONPLAGIARISM .ERROR! BOOKMARK NOT DEFINED.
ABSTRACT...IV
ÖZET... V
ACKNOWLEGEMENT...VI
LIST OF TABLES XI
LIST OF FIGURES XII
LIST OF SYMBOLS AND ABBREVIATIONS XV
CHAPTER I INTRODUCTION... 1
CHAPTER II THE INTERNET 4
2.1. THE CONCEPT OF THE INTERNET.. 4
2.2. STRUCTURE OF THE INTERNET 5
2.3. INTERNET ACCESS 6
CHAPTER III DEEP WEB.. 9
3.1. DEEP WEB DESCRIPTION 9
3.2. DIMENSIONS OF THE DEEP WEB... 10
3.3. POSITIVES AND NEGATIVES OF DEEP WEB... 11
3.4. DIFFERENCES BETWEEN DEEP WEB AND DARK WEB........................ 12
CHAPTER IV DARK WEB 13
4.1. DARK WEB DESCRIPTION.. 13
4.2. DARK WEB STATISTICS.. 15
4.3. DARK WEB BENEFITS AND HARMS 16
4.4. EXISTING DARK WEB NETWORKS AND DARK WEB ACCESS 18
4.4.1. FreeNet 18
4.4.2. SubGraph OS.. 19
4.4.3. Whonix 20
4.4.4. TAILS (The Amnesic Incognito Live System) 20
4.4.5. I2P (Invisible Internet Project) 20
4.4.6. Alternative Domain Roots.. 22
4.5. ROLE OF GOVERNMENT 22

4.6. CYBER ATTACK AND DEFENSE AGAINST CYBER ATTACK 24
4.6.1. Traffic Fingerprinting Attacks 25
4.6.2. Traffic and Timing Correlation Attacks 25
4.6.3. Credential reuse 25
4.6.4. Cross Site Scripting (XSS) Attacks 26
4.6.5. Unpopular Port Attacks 26
4.6.6. Low Resource Routing Attacks 26
4.6.7. Session Hijacking and Man-In-The-Middle Attacks 27
4.6.8. Eclipse Attacks 27
4.6.9. Cell Counter Based Attacks 28
4.6.10. Distributed Denial of Service (DDoS) Attacks 28
4.6.11. Sybil Attacks 28
4.6.12. Correlation Attacks 28
4.6.13. Relay Early Traffic Confirmation Attack 29
4.6.14. Congestion Attacks 29
4.6.15. SQL Injection (SQLI) Attacks 29
4.6.16. Botnets 30
4.6.17. Raptor Attacks 30
4.7. DARK WEB TRAFFIC DETECTION 30
4.7.1. DarkOwl Vision 31
4.7.2. Alert Logic Dark Web Scanning 31
4.7.3. ACID Cyber Intelligence 32
4.8. THE DARK WEB AND MALWARE 34
4.8.1. Data Stealing Trojans 34
4.8.2. Ransomware 35
4.8.3. Remote Access Trojans (RATs) 35
4.8.4. Botnet Malware 36
4.8.5. ATM Malware 36
4.8.6. Phishing 36
4.9. DARK WEB CRIMES 37
4.9.1. Drug Trafficking 37
4.9.2. Human Trafficking 38
4.9.3. Information Leakage 38
4.9.4. Proxing 38

4.9.5. Bitcoin Scam 39
4.9.6. Arms Trafficking 39
CHAPTER V THE ONION ROUTING 40
5.1. TOR DESCRIPTION 40
5.2. TOR PROTOCOL 44
5.3. HIDDEN SERVICES 45
CHAPTER VI VIRTUAL PIRAVATE NETWORK 48
6.1. WHAT IS VIRTUAL PRIVATE NETWORK 48
6.2. HOW VPN WORKS 49
6.3. DATA PROTECTION WITH VPN 50
6.3.1. Encapsulation (Tunneling) 50
6.3.2. Authentication 50
6.3.3. Data Encryption 51
6.4. TYPES OF VPN 51
6.4.1. Site-to-Site VPN 51
6.4.2. Remote Access VPN 51
6.4.3. Firewall VPN 52
6.4.4. User-to-User VPN 52
6.5. VPN PROTOCOLS 52
6.5.1. OpenVPN 52
6.5.2. Point-to-Point Tunneling Protocol (PPTP) 52
6.5.3. IKEv2 53
6.5.4. Secure Socket Tunneling Protocol (SSTP) 53
6.5.5. Layer 2 Tunneling Protocol (L2TP) 53
6.6. VPN AND DARK WEB 54
CHAPTER VII RELATED WORKS 55
7.1. LITERATURE REVIEW 55
7.1.1. Darknet Traffic Detection 55
7.1.2. Vpn Traffic Detection 60
7.1.3. Tor Traffic Detection 63
CHAPTER VIII METHODOLOGY 66
8.1. CLASSIFICATION 66
8.1.1. Classification Terminology 67
8.2. NEURAL NETWORK 68

8.2.1. Artificial Neural Network (ANN) 69

8.2.2. Multilayer Perceptron (MLP) 70

8.2.3. Convolutional Neural Network (CNN) 70

8.2.4. Generative Adversarial Networks (GANs) 70

8.2.5. Recurrent Neural Network (RNN) 71

8.2.6. Long short-term memory (LSTM) 71

8.3. DATASET 71

8.4. PREPROCESSING DATA 75

8.4.1. Data Cleaning 75

8.4.2. Normalizing 76

8.4.3. Feature Selection 76

8.4.3.1. How to Choose Feature Selection 76

8.4.3.2. Select K-Best 77

8.4.4. Eveluation Metrics 78

8.5. IMPLEMENTATION 78

8.5.1. RNN Model 79

8.5.2. LSTM Model 81

8.5.3. MLP Model 87

CHAPTER IX RESULTS AND DISCUSSION 89

9.1. RNN Layer1 Model 89

9.2. RNN Layer2 Model 91

9.3. LSTM Layer1 Model 92

9.4. LSTM- GAN Layer1 Model 93

9.5. LSTM Layer2 Model 94

9.6. LSTM-GAN Layer2 Model 95

9.7. LSTM-Binary Layer2 Model 95

9.8. MLP Layer1 Model 100

9.9. MLP Layer2 Model 101

9.10. MLP-Binary Layer2 Model 102

CHAPTER X CONCLUSION AND FUTURE WORK 110

REFERENCES 112

LIST OF TABLES

Table 3.1: Deep Web Versus Dark Web 12
Table 4.1: Dark Web Monitoring Tools Information.. 33
Table 6.1: Advantages and Disadvantages of VPN Types.. 53
Table 6.2: VPN and Tor Access Comparison 54
Table 8.1: Features Details in Dataset.. 74
Table 8.2: Table of Clean Values 75
Table 8.3: Select K-Best Algorithm Pseudocode.. 77
Table 8.4: Size of Training and Test Data 79
Table 8.5: RNN Model Architecture.. 79
Table 8.6: LSTM Model Architecture 82
Table 8.7: GAN Generator Model Architecture.. 84
Table 8.8: GAN Discriminator Model Architecture 84
Table 8.9: LSTM-Binary Layer2 Model Architecture 86
Table 9.1: RNN Layer1 Model Evaluation Metrics Results 89
Table 9.2: RNN Layer2 Model Evaluation Metrics Results 91
Table 9.3: LSTM Model Layer1 Evaluation Metrics Results................................... 92
Table 9.4: Accuracy Values of Category Models 95
Table 9.5: MLP Layer1 Model Evaluation Metrics Results 100
Table 9.6: MLP Layer1 Model Selected Features 100
Table 9.7: Accuracy Values of Category Models 102
Table 9.8: Summary of Models.. 107

LIST OF FIGURES

Figure 4.1: Tor Transmission Network 15
Figure 4.2: File Request Protocol in Freenet 19
Figure 4.3: I2P Communication Protocol 21
Figure 4.4: DarkOwl Vision Dashboard 31
Figure 4.5: Alert Logic Topology Example 32
Figure 5.1: The Message Traffic on The Onion Routing 42
Figure 5.2: Tor Architecture 45
Figure 5.3: Hidden Service Protocol 46
Figure 5.4: Hidden Services on the Darknet 47
Figure 6.1: Masquereading Attack 49
Figure 6.2: Eavesdropping Attack 49
Figure 6.3: VPN Working Schema 50
Figure 6.4: Site-to-Site VPN Schema 51
Figure 8.1: Parsing Spam Mails With Classification Algorithm 67
Figure 8.2: Activation Function 69
Figure 8.3: Artificial Neural Network 70
Figure 8.4: Darknet and Benign Data Rates 72
Figure 8.5: Application Rates 73
Figure 8.6: RNN Layer1 Model Architecture Diagram 80
Figure 8.7: RNN Layer2 Model Architecture Diagram 81
Figure 8.8: LSTM Layer1 Model Architecture Diagram 82
Figure 8.9: LSTM Layer2 Model Architecture Diagram 83
Figure 8.10: LSTM-GAN Layer1 Model Architecture Diagram 84
Figure 8.11: LSTM-GAN Layer2 Model Architecture Diagram 85
Figure 8.12: MLP Layer1 Model Architecture Diagram 87
Figure 8.13: MLP Layer2 Model Architecture Diagram 87
Figure 8.14: MLP Layer1 Model Architecture Diagram with Feature Selection 88
Figure 8.15: MLP Layer2 Model Architecture Diagram with Feature Selection 88

Figure 8.16: MLP-Binary Layer2 Model Architecture Diagram 88

Figure 9.1: RNN Layer1 Accuracy Graphic 90

Figure 9.2: RNN Layer1 Mean Squared Error Graphic 90

Figure 9.3: RNN Layer2 Accuracy Graphic 91

Figure 9.4: RNN Layer2 Mean Squared Error Graphic 92

Figure 9.5: LSTM Layer1 Model Accuracy Graphic 93

Figure 9.6: LSTM Layer1 Model Confusion Matrix 93

Figure 9.7: LSTM- GAN Layer1 Model Confusion Matrix 94

Figure 9.8: LSTM Layer2 Model Accuracy Graphic 94

Figure 9.9: LSTM Layer2 Model Confusion Matrix 95

Figure 9.10: Accuracy Values According to Epochs in LSTM Binary Algorithm for Audio-Streaming Category 96

Figure 9.11: Accuracy Values According to Epochs in LSTM Binary Algorithm for Browsing Category 96

Figure 9.12: Accuracy Values According to Epochs in LSTM Binary Algorithm for Chat Category 97

Figure 9.13: Accuracy Values According to Epochs in LSTM Binary Algorithm for Email Category 97

Figure 9.14: Accuracy Values According to Epochs in LSTM Binary Algorithm for File-Transfer Category 98

Figure 9.15: Accuracy Values According to Epochs in LSTM Binary Algorithm for P2P Category 98

Figure 9.16: Accuracy Values According to Epochs in LSTM Binary Algorithm for Video Streaming Category 99

Figure 9.17: Accuracy Values According to Epochs in LSTM Binary Algorithm for VOIP Category 99

Figure 9.18: MLP Layer1 Model Confusion Matrix 100

Figure 9.19: MLP Layer1 Feature Selection Model Confusion Matrix 101

Figure 9.20: MLP Layer2 Model Confusion Matrix 102

Figure 9.21: Confusion Matrix According to the MLP Binary Algorithm for the Audio-Streaming Category 103

Figure 9.22: Confusion Matrix According to the MLP Binary Algorithm for the Browsing Category 103

Figure 9.23: Confusion Matrix According to the MLP Binary Algorithm for the Chat Category 104

Figure 9.24: Confusion Matrix According to the MLP Binary Algorithm for the Email Category 104

Figure 9.25: Confusion Matrix According to the MLP Binary Algorithm for the File-Transfer Category.. 105

Figure 9.26: Confusion Matrix According to the MLP Binary Algorithm for the P2P Category 105

Figure 9.27: Confusion Matrix According to the MLP Binary Algorithm for the Video-Streaming Category... 106

Figure 9.28: Confusion Matrix According to the MLP Binary Algorithm for the VOIP Category 106

LIST OF SYMBOLS AND ABBREVIATIONS

ABBREVIATIONS

VPN	: Virtual Private Network
TOR	: The Onion Router
SSL	: Security Socket Layer
SSH	: Secure Shell
CNN	: Convolutional Neural Network
MLP	: Multi Layer Perceptron
URL	: Universal Resource Locator
DNS	: Domain Name System
FTP	: File Transfer Protocol
CSHS	: Closed Shell System
I2P	: Invisible Internet Project
TAILS	: The Amnesic Incognito Live System
ICANN	: The Internet Corporation for Assigned Names and Numbers
TLD	: Top Level Domain
CIPAV	: Computer and Internet Protocol Address Verifier
DARPA	: The Defense Advanced Research Projects Agency
CAUSE	: Cyber Attack Automated Unconventional Sensor Environment
IDG	: Research Service Survey
SOCKS	: Socket Secure
RAT	: Remote Access Trojans
OONI	: Open Ovservatory of Network Interface
FNR	: False negative Rate
SVN	: Support Vector Machine
TF-IDF	: Term Frequency-Inverse Document Frequency
SGD	: Stochastic Gradient Descent

PCA	: Principle Component Analysis
CNN-LSTM	: Convolution-Long Short Term Memory
CNN-GRU	: Convolution-Gated Recurrent Unit
XGB	: Extreme Gradient Boosting
RFR	: Random Forest Regressor
SFFS	: Sequential Floating Forward Selection
Forward-SFS	: Forward-Sequential Feature Selection
KNN	: K-Nearest Neighbor
FGSM	: Fast Gradient Sign Method
BIM	: Basic Iterative method
AC-GAN	: Auxiliary Classifier Generative Adversarial Networks
SMOTE	: Syntetic Mimority Oversampling Technique
MIM	: Micro Independent Metering
CFS	: Correlation-based Feauture Selection
CIC	: Canadian Institute for Cybersecurity
AGMV	: Accumulated Generalized Mean Value
CAE	: Convolutional Auto-Encoding
DSRR	: Differentiation of Sliding Rescaled Ranges
GAN	: Genarative Adversarial Network
CW	: Clarke Wright
SGD	: Stochastic Gradient Descent
TLS	: Transport Layer Security
DC	: Decision Tree

CHAPTER I
INTRODUCTION

Information systems perform a continuous and large-scale data exchange. In these processes, the data takes place one after the other frequently and it becomes difficult to process due to its large proportions. Therefore, even if these large data are processed, they are either deleted or archived. For all these reasons, analysis, monitoring and classification of internet network traffic will be a step towards preventing crimes.

Data flow is provided in packets in the network. These packet formats can be requests, responses or control data. Since this data is divided into multiple interconnected packets, it becomes very difficult to interpret the data. For this reason, it is important to enrich the number of such network analysis studies and to develop them.

Organizations collect excess traffic data and analyze it in conjunction with unit services to improve their security processes. In this way, safer conclusions can be made. Network security and traffic analysis can be applied to security services, making it possible to model traffic. These can be achieved by customizing and optimizing intrusion prevention and detection solutions, ensuring that critical data does not leak out. In this way, cybercriminals can be identified and forensic data can be verified.

Traffic packet analysis may not always be an adequate solution. For example; Special analyzes should be performed for security measures against zero-day attacks. Therefore, with the ever-changing attack types, there is an increasing need for the management of security environments [1]. With this study, it is aimed to provide a solution to this need.

Various encryption protocols are in use today. The common ones are the security Socket Layer (SSL), Virtual Private Network (VPN), Secure Shell (SSH), and The Onion Router (Tor). This security is available to everyone, as well as providing privacy for hackers to hide their actions. For this reason, it is essential to identify encrypted traffic in a timely manner in order to detect attacks on the network, to prevent attacks before they occur, and to reduce damage [2].

Dark web access is one of the effects that creates this increasing security problem. People trying to access the dark web environment are very likely to fall into a dangerous trap and are in danger of spreading from one device to another. Darknet represents a virtual network area that provides anonymous access and has a hidden layer structure. It is also known as the dark side of the deep web and is one of its layers. Illegal onion nets are a place where political protests, drug trafficking, supply of forged documents and all other illegal activities take place. Deep Web consists of 8 layers. The dark web is the most dangerous layer of these layers, although the ways of accessing these layers vary, the most tried and used ways are to change proxy, vpn connection and tor browser. Darknet, on the other hand, creates the dark web with the hidden services network hosted by the websites. Considering the free roaming, information that can be obtained and the actions to be taken, the dark web puts people in an unknown danger because it is dark from where and from whom. 60% of the information on the dark web can be used to harm businesses. In addition, hackers attack an average of 2,244 times a day every 39 seconds. Again, a ransom attack is planned to occur every 11 seconds [3]. Since the identity of the other person is protected by many secret services, we can say that it is very difficult to access the sources of the data packets. Therefore, it is difficult to counter these threats. The work done in countering these threats is very valuable.

Cyber attackers try quite different methods to stay undetected. While reaching their goals through reliable methods in the network environment, on the other hand, organizations cannot fully determine the security risks. Network traffic analysis applications have emerged in order to respond to these attitudes of attackers and there is hope that there may be a way to combat it.

In summary, it is necessary to provide a security environment with automated solutions. These solutions can be grouped as follows; real-time incident handling, analysis, and other security information to identify known and unknown threats and reduce the risk for the critical data through a scalable troubleshooting and logging approach [4].

In this thesis, it is aimed to categorize the dark network traffic analysis and which services it reaches through to automate the detection process of malicious data with RNN, LSTM and MLP methods. In this way, the desired goal is to be able to detect and monitor a malicious software early before an attack, and to have early knowledge of the intended malicious activities. It is intended to contribute in a necessary field with the study.

In this article, there is the layer1 model, which can distinguish between darknet and benign data, and the layer2 model, which allows us to determine from which application the darknet data is provided. This two-layer study was carried out with artificial neural networks RNN, LSTM and MLP algorithm models. In the LSTM model, a second model test was applied by including the GAN algorithm on both layers. In addition, the binary method and the model improvement method in categories were tested in the LSTM model second layer. MLP was compared with LSTM by using binary method for model improvement in the second layer model. Model improvement was also observed by applying feature selection in the MLP model.

In general, in the rest of this thesis, Chapter 2 discusses the basic internet structure and web layers required to understand the Darknet. In Chapter 3, what the Deep Web is, how it emerged, its good and bad aspects and its difference from the dark web are mentioned. Dark Web statistics, benefits and harms, existing dark web networks and providing access, the role of the government in this sense while discussing the good and bad aspects of the dark web, cyber attacks and detection methods, preferred dark web monitoring tools, malware attack encountered in the dark web and dark web crimes are included in Chapter 4. Chapter 5 explains where Tor came from, how it developed, how it works and its services. In Chapter 6, VPN working principle, types, protocol structure and dark web relationship are mentioned. In Chapter 7 there are literature surveys of Darknet Traffic Classification. Chapter 8 describes the experimental infrastructure models of the thesis. Chapter 9 discusses the results and analyzes of the experiments mentioned in the previous chapter. Finally, in Chapter 10, determinations according to the results of the experiment, the importance of this study and future studies to shed light on future studies are mentioned.

CHAPTER II
THE INTERNET

2.1. THE CONCEPT OF THE INTERNET

The fact that we come across words such as electronic life (e-life), electronic world (e-world), electronic mail (e-mail), electronic commerce (e-trade) and electronic advertising (e-ad) are the most common terms in our lives. While there are big factors, technology inside gives rise to the fact that we have to use the internet in this way. The Internet can be expressed in many ways and differently for everyone. Some use the internet; While using and characterizing information technology in subjects such as ease of access, culture, opportunity and health, some may consider it as the most favorable environment for crimes, danger for children, misdirection, and a factor in reducing social communication. At the same time, there is a section that thinks it causes social deviations. “The Internet is simply an international, dynamic and vibrant large library, parts of which are scattered all over the world. Moreover, it is a communication, solidarity and sharing environment in which millions of people participate” [5]. “It is clear that in a country where there is no internet and access opportunities, cultural activities and cultural structure will remain closed in itself and cultural interaction will be at a minimum level” [6].

Internet when defined to cover every thought; It is an electronic system and a cultural phenomenon that can be described as the highest point where limits can be exceeded in information and communication. It is the leading role of communication and access to information individually and socially. While the terms Agricultural and Industrial society appear in the definitions of society that have survived until today, information society and information society have taken their place in our age. In this rapid change, the easy and quick access capability of the internet cannot be ignored.

The internet, which is defined as communication, speed and sharing, was actually born with the idea of storing and transmitting information. However, the idea of spreading the produced information and making it available to people was not the purpose of the internet. It was formed from military needs during the cold war period. The Internet was a system created to communicate against the Soviet Union as a result of the emergence of many damaged devices, as the American government sought a nuclear attack.

The Internet was originally intended to be used only for military applications. It cannot be said that it is predicted that the internet will become so widespread in other areas, even until recently. Bill Gates, the founder of Microsoft, said that the internet is a relatively useless and ephemeral environment, and some management consultants and respected academics stated that the internet has no commercial value. In 1966, Lawrence G. Roberts develops the ARPANET project at the Darpa agency, where he works in the United States, and demonstrates the feasibility of the network between remote buildings in a large area [7]. This system was expanded and divided into two. In addition to ARPANET, the other network environment is also called MİL-NET. Communication between these two networks is provided by internet protocols. The term IP emerged when it was desired to establish a connection between a computer and another computer [8].

In addition to the presence of 5.1 billion people using the internet as of January 2022, there are more than 1.9 billion websites as of December 2021 in the part called surface internet [9]. In summary, billions of people are on the network, national and international companies, organizations, countries and states are looking for a place for themselves in this environment where all the dynamics of the society have not yet been drawn.

2.2. STRUCTURE OF THE INTERNET

With the software that started to develop in the early 1990s and other reasons affecting it, the internet became commercialized and its use began to become widespread. Over time, the internet has turned into a network structure that individuals or businesses can connect to whenever they want, without being connected to any institution. The most important trend in information technology today is the easy connection of corporate networks and personal devices to the internet. For this reason, we can observe that the internet has begun to affect all aspects of life today. Many of the activities of daily life are included within their virtual boundaries. However, what is the size of the internet and what are its limits leads to questions.

The main issue on networks is data exchange between computers. Sites visited on the Internet are the screens that people share via URL (Universal Resource Locator) web servers, coded in computer languages and named in a standard way, in order to present their online documents or their own sites that they want to share with each other. This standard has been accepted all over the world and is used with a protocol we call the world wide web. The World Wide Web is divided into three: Surface web, deep web and dark web. Surface web includes public websites and is easy to access by search engines. When describing the web, it can be seen as consisting of websites that can only be accessed by a search engine such as Google. However, this content, known as the "Surface Web", covers a portion of the web. Only 0.03% of results are retrieved via surface web search engines. Experts interpret as follows." Measuring the size of the Deep Web is nearly impossible. With some early estimates 4,000–5,000 times larger than the Surface network, the changing dynamics of how information is accessed and presented means that the Deep Web is growing at an exponential and quantitatively defying rate" [10]. Beyond the Internet, accessible to most people, lies a large layer that has traditionally been inaccessible. As the researchers point out, "Searching the Internet today can be likened to dragging a web across the surface of the ocean. Although much of it is caught in the net, there is still a lot of deep and thus missed information." [11]. The deep web is called the invisible, hidden network. While 9% of the internet is deep web, 4% is the dark web that can be accessed with special access. It is possible to access the dark web through a method that can be accessed through servers that provide special permissions called VPN (Virtual Private Network) and through some browsers such as TOR.

2.3. INTERNET ACCESS

The internet has 8 layers. Each one is different in terms of access and requires competencies. Details of the layers;

Layer 1 (Commen Web): It is the daily used internet access.

Layer 2 (Surface Web): It is the internet that can be accessed with some simple queries and browsers in daily use. Services such as temp mail services and DNS querying are accessible at this layer.

Layer 2 (Bergie Web): In this layer, there is internet access locked by search results. FTP servers with file sharing, adult movies that are not indexed are accessible in this layer. Requires detailed query for transportation. Many sites in this tier are usually included in recent search results. This level is the last layer that can be accessed by conventional means.

Layer 3 (Deep Web): It is the initial Deep Web level. It is divided into proxy-level access and Tor-level access.

Proxy Level: There are sites that are not indexed, usually made with php coding. They are illegal sites. Hacker groups, viruses, VIP gossip, assassination videos, etc. content is accessible via the network at this layer.

Tor Level: .onion sites are included in this layer. Most of the sites are on personal servers. When the accessible areas in this layer are sampled; Data traders, some government documents, terrorist organization information, bomb and weapon training, illegal scientific research are included in this layer.

Layer 4 (Charter Web): It is referred to as the privileged Deep Web level. Requires Tor level access or special access. It is a dangerous level.

Tor Level: Accessible only using the Tor browser. Confidential company and market information, predetermined million betting results, billion-dollar sales, world famous arms smugglers, banned movies, videos, books, music, important audio recordings, detailed confidential wiki encyclopedias, drug trade, trade in banned chemicals and drugs, trade in blood smuggled from blood banks, information such as the search for human subjects for illegal experiments can be accessed.

Special Access Level: The most dangerous level ever achieved. There is a special access method called "Closed Shell System". At this level; Artificial intelligence processors, GGGEQP processors, secret HAARP projects, plans for special production engines can be accessed. This layer can be accessed using the Closed Shell System (CSHS). CSHS creates a network within itself. There is an intranet within the internet and neither the intranet can access the internet nor the intranet can be joined from the internet. Domain names here are .clos. .clos sites check for header and key. It cannot be accessed without the necessary verifications of its own. In order to access, a proxy that can take control mechanism must be written. By analogy, it can be thought of as if you don't have a key, you can't enter the house. There is no known application for accessing sites with the .clos extension. While the Tor browser may be sufficient to access some layers of the deep web, the software must be written by the person who wants to access the .clos. Even if the sites published in this network structure can be accessed, if the network access is not fully achieved, a blank page or meaningless characters will be encountered. Example domain names on sites with .clos extension are gir4roia5yeik9.clos.

The part up to this layer constitutes 80% of the Deep Web. From here on, devices working with Quantum technology and the necessity of internet are mentioned.

Layer 5 (Marianas Web): There is no information that this level has been reached yet. Today's technology is insufficient for this level of access. It takes its name from the Mariana Trench, the deepest trench in the world. Its boundaries are uncertain, but it is clear that it has an end. For this level, it was said, “If it is reached one day, the war on the internet will end that day”. It is said that many scientists in high-tech R&D laboratories have reached this level and shared information.

Level 6 : It is the most dangerous level known. There is no information about it. Its borders are uncertain and its end is uncertain. It has not been reached even with the most advanced technology.

Level 7 (The Fog/Virus Soup): Level 7 is called the war zone. It is said that if one day it can be reached, everyone will fight for himself. The goal is to prevent other people from reaching level 8.

Level 8 (The Primarch System): Level 8 is not open to direct access. It is controlled by a Primarch System that neither a government or organization nor anyone knows for sure. This system was first discovered by chance in the 2000s. The system is unresponsive and sends random commands to the entire internet that cannot be changed. Level 8 uses "level 17 quantum t.r.001 level function lock", a huge processing power that today's computers cannot cope with. Level 8 is referred to as “The Latest Boss of the Internet” [12] [13].

CHAPTER III
DEEP WEB

3.1. DEEP WEB DESCRIPTION

Micheal Bergman, an academic and entrepreneur, is the first person to coin the word "Deep Web" and is the person who conducts scale research on its depth. Bergman said that the deep web has a fast-growing structure in his studies and emphasized that in his last measurement, it was two or three times larger than the surface internet in the 90s [14].

It is a matter of curiosity whether the sites that have been blocked or closed have disappeared completely. These sites are removed from DNS servers, that is, they are closed only to browser searches used in daily life. It started with the search for ways to access these sites, developed and the deep web was born. In short, basic access can be achieved by opening proxy servers and adjusting various browsers such as tor accordingly. Deep web has the largest library in the world, according to the thoughts of what will provide access to these sites, deep web data as bad content.

Conceptually, the Deep Web is often represented by an iceberg. In addition, mining operations can also be used to exemplify the Deep Web. While everything on the ground that is easy to find represents the surface internet, everything below the surface is likened to the hidden structure of the Deep Web, which is not easily accessible [15]. In a company, a private network that is not indexed by search engines and a structure that can only be accessed by an employee account can be called Deep Web [16].

Deep Web, which is used to symbolize the network that traditional search engines cannot reach, specifically:

For dynamically created pages in HTTP request, for sites whose content is prohibited from direct access or blocked, such as CAPTCHAs, pragma no-cache HTTP headers, or ROBOTS.TXT entries,

- For pages that are not linked to any page, where a web page does not have access to other pages,
- For private sites that require registration and login,
- For content with a different encoding structure or depending on a specific IP range or browsing history,
- It has started to be used for content that cannot be accessed with a standard internet infrastructure [17].

As Bergman stated; Deep Web has many content such as content databases, publications, internal libraries, message and chat services, postings, auctions and shopping [11].

3.2. DIMENSIONS OF THE DEEP WEB

The BrightPlanet team conducted a study between 13 and 30 March 2000. Micheal K. Bergman, the founder of the Deep Web at that time, was the chairman and vice chairman of this company. In this study, the size and importance of the Deep Web were tried to be measured, its content quality and suitability for information seekers were characterized, search sites were tried to be determined and automated tools were discovered to direct queries to these sites. For this study; Analysis of the largest deep web sites and surface web sites, estimation of the total number of sites, size analysis, content coverage and type analysis, site page images and link references, growth analysis, quality analysis, analysis of the largest web sites have obtained the results of the study. After the data in this study, no current data has been included in the sources yet. According to these data;

- The data in the world wide web is 400 to 500 times smaller than the deep web.
- There is an estimated 19TB of data on the Internet. In the Deep Web, only the size of publicly available data is 7500 TB, which is data from the 60 largest publicly available sites.
- While the internet has 1 billion documents, the deep web has 550 billion documents.
- There are more than 200,000 Deep Web web pages.

- Network traffic is 50% higher on deep web pages than surface web pages. However, Deep websites that are open to the public are not well known by the people searching the internet.
- Deep Web is the category of information that is showing the greatest growth on the Internet.
- Deep Web sites have the structure of being deeper but narrower than surface sites.
- Deep Web's quality page and document content is 1000 to 2000 times higher than surface web.
- More than half of Deep Web content is kept in separate topic-specific databases.
- 95% of the Deep Web is public information. It is therefore not subject to fees or subscriptions [18].

3.3. POSITIVES AND NEGATIVES OF DEEP WEB

Deep Web access is not separated by a clear line, whether it is legal or illegal. It is a wrong statement to talk about the fact that the use of the Deep Web, which is considered as a more advanced form of the classical surface internet, as the exchange of information that many people try to obtain by avoiding some parameters, is completely illegal. Many political thinkers, journalists, scientists, academics and even ordinary citizens who care about their privacy use the Deep Web. It can even change depending on the process or a downloaded content. The answer to the question under which evaluation criteria are the data collected for the benefit of humanity and society and the people who have access to the studies done in this field, may not be certain. For example; If a scientist who has access to a stolen study data from the deep web area, which is not open to the surface internet, has made a discovery with the knowledge he gained from this study, is he still an information thief? This assessment will actually differ according to everyone's assessment requirements.

Despite the prohibition of internet use by the current governments during the Arab Spring process, it is known that the masses who organized demonstrations on Twitter and Facebook actively use the Deep Web together with Tor, as well as VPN. Many IT companies in the West, especially in the USA, provide services in this direction regarding the safe use of the Deep Web.

In addition to this, we can consider the fact that the area that pushes people to do illegal work is the deep web, as it is anonymous. The fact that the principle of confidentiality can be ensured even in commercial transactions also makes the deep web more attractive [19].

3.4. DIFFERENCES BETWEEN DEEP WEB AND DARK WEB

Deep web and Dark web are different terms from each other. The dark web is located in the Deep Web and is known as the layer where all illegal transactions are carried out. The Deep Web, on the other hand, consists of more layers and in fact, it cannot be said that only legal proceedings are carried out. In the table below, a comparison of Deep web and Dark web has been made. **Table 3.1** below shows the differences between dark web and deep web.

Table 3.1: Deep Web Versus Dark Web

	Deep Web	**Dark Web**
Level Access	Requires login authorization. Accessible via a direct url or IP Access.	It is encrypted and anonymous. Requires access with specialized tools and software.
Data Content	Contains unindexed data. Therefore, it cannot be found in any search engine. It has dynamically generated data content.	It contains intentionally hidden data. It is difficult to watch.
Data Storage	There are databases specific to content topics.	There are often customized or custom databases.
Legality	It is possible to access both legal data and illegal content.	It is the area where illegal transactions are usually carried out.

CHAPTER IV
DARK WEB

4.1. DARK WEB DESCRIPTION

The Dark Web qualifies as a cave for access to illegal business. The basic components of the Dark Web are browsers, data encryption technique, virtual private networks and routing algorithms.

It is not easy to access the desired data on the Dark Web. There are Dark Web search engines, but it is difficult to keep up with the changing environment. Even the best search engines can return repetitive or irrelevant results. Hidden wiki links are also a method of accessing data, but it is possible to encounter expired links here as well.

It is important to remain anonymous, to maintain anonymity. Proxy is one of the basic techniques on which the Dark Web is based for anonymous and privacy. In proxy access, requests are collected from clients. After receiving a response from the relevant service, the proxy is sent back to the information requester. It acts as a message between sender and receiver. Proxies are also used to filter and display users' access to some websites. Another key factor is virtual private networks (VPN). This method, known as network tunneling, is the most common method. It is a private network that exchanges information between devices and servers. In addition to bypassing Internet censorship, it is also an effective and secure method of accessing the corporate network from an outside network in corporate environments. It is more preferable because it uses protocol security and secure socket layer. In the TOR browser, which is another access method, privacy can be achieved by using more than one complex password layer. It is a network mechanism that allows access by ensuring that the contents are encrypted during transmission. This access mechanism takes place through 3 routers. For example, As can be seen in **Figure 4.1** when a search request is thrown, the client will have three encryption keys.

The encrypted message goes to router 1. Router 1 contains the address of router 2 and switch 1. Using key 1, it decrypts the message and forwards it to router 2. Router 2 knows key 2 and the address of router 3. Router 2 decrypts it with key 2 and forwards it to the final router.

The final referrer finds the get request for search and passes to the target server. To respond to this request, the server re-performs all layers up to this stage in reverse, with private keys. And the person searching in the browser reaches the page he is looking for in this way. Finally, access can be achieved with the Domain Name System Based bypassing method. When we send an access request from our browser, the relevant domain name forwards this request to the server that translates the ip addresses of the domain names called dns, and if the dns servers know the ip address in return for this request, it returns us. Using DNS, access to internet resources can be forced and censorship can be circumvented.

Dark Web sites are the same as surface web, but there are differences in their extensions. Dark Web sites end with .onion. That's “a special-use top level domain suffix designating an anonymous hidden service reachable via the Tor Network,” according to Wikipedia [20]. Apart from the extension being different, an encrypted URL naming is also unique to the Darknet. For example, instead of abc market, it can be accessed as “horwn3pgnz49ngp3.onion”.

There are some points to consider in order to browse the Dark Web safely. Disabling Java from the current network settings, logging into the dark web with a non-administrator local account and logging into the dark web with this user account, avoiding downloading documents on the dark web, restricting tor access on that device if it is a family device, real attention should be paid to points such as not using e-mail accounts, identity information and passwords in daily use, using accounts or prepaid bank accounts to hide identity during a purchase on the Dark Web.

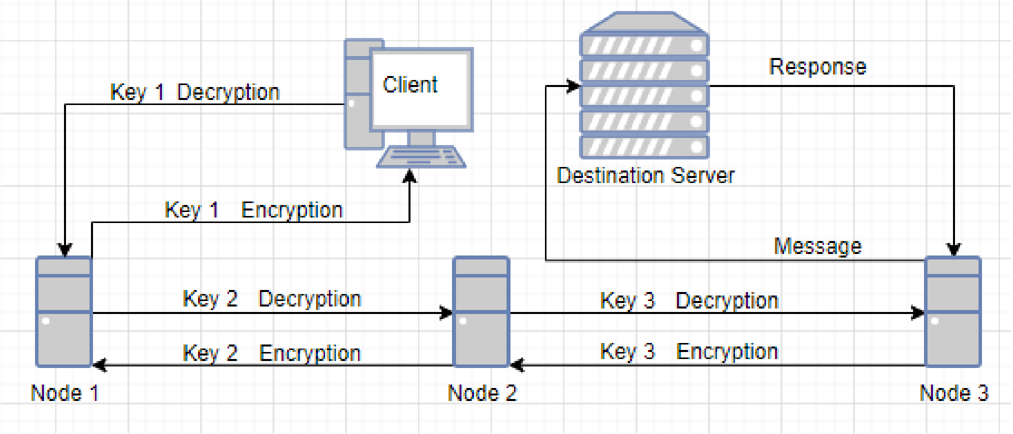


Figure 4.1: Tor Transmission Network

In 2021, a hacker posted 700 million LinkedIn member profiles on the Dark Web. As a result of this data breach, the profiles of 92% of users were accessed. In this attack, users' profile url information, phone numbers, email addresses, other social media accounts and even geolocation information were captured. These records were put up for sale, and examples were published about being serious. The hackers obtained 230,487 files belonging to the personnel of an International union. This action, which took place at the beginning of 2022, shows that social security numbers, name, surname and address information were seized. If the union personnel whose data are stolen are business lines; It is reported that there are school bus employees, window cleaners, maintenance and food teams [21]. According to The Hacker News report published in August 2021, operators change their obfuscation and encryption mechanisms every 37 days to cover their tracks and secretly collect users' credentials [22].

4.2. DARK WEB STATISTICS

According to the research data of 2022;

The largest rate in the use of darknet platforms belongs to India. It accounts for 26% of all countries.

In terms of male and female usage rates, 29.4% of dark web users are female and 70.6% are male users.

70% of Dark Web users are between the ages of 18 and 35. 35.9% of them have usage rates between the ages of 18-25 and 34.8% of them between the ages of 26-35.

While those between the ages of 36-45 have 16.8% usage rates, this rate is 3.1% for those between the ages of 56-65 and 0.6% for those over 65 years old.

Darknet covers roughly 48% of the internet.

Terrorism statistics on the darknet show that there are 50,000 pro-groups. After the Paris attacks in 2015, they turned to the dark web with the decision to remain anonymous.

There are 8 categories in Dark Web marketplaces.

Weapons and drugs top the list, followed by hacking and malware. Then there are Fraud and forgery, guide and other categories.

59% of listings on darknet markets reveal that they are for drugs. After the Silk Road, its most famous market, was closed in 2013, the drug trade in the names Empire and Nightmare continues.

They are the most frequently listed pistols on the Darknet, accounting for 84% of category listings. In addition, firearms make up only 1% of the lists.

In the remaining 40% area, the rates according to the market categories; hacking 2%, guides 11%, fraud 17%, drugs 3% and other 7%.

Darknet market share is around 6%.

Illegal financing such as phishing, malware covers 6.3% of the entire darknet market.

The list of Darknet Illegal and unknown category corresponds to 22.6% of the total area. These aforementioned areas usually contain websites that contain policies and are used for information storage. 1.5% of Tor browser traffic visits the Dark Web. As understood from this data, Tor is not only preferred for Dark Web access.According to studies, stolen credit card numbers can be bought for $9, $2 is enough to get a scanned copy of a passport [21].

4.3. DARK WEB BENEFITS AND HARMS

Due to the fact that user data is encrypted, it is one of the main reasons why the user prefers the dark web. Due to political reasons, people cannot freely express themselves in the digital environment. At this point, the dark web provides a convenience because it is difficult to follow. In this way, people will be able to express their opinions in any way they want, be it political or any other issue. Since it is a structure that is difficult to follow in encrypted form, it provides convenience for people to move freely, and therefore it provides people to trust this environment. In addition, having their own search engines and secure e-mail browsers makes the Dark Web preferable in terms of personal information security.

Law enforcement officers can use confidentiality to create an anonymous call line and carry out clandestine operations. People can use private messaging lines, journalists can access some sites through the dark web to convey their important articles. The Dark Web can also be effective in blogging anonymously.

On the dark web, some legal products can be accessed cheaper on the sales pages. There may be products that are not available in the country or on the market. Gehl & McKelvey stated that the adjective "dark" in the name Dark Web may suggest that moral or illegal activities are being carried out [23]. The disadvantage of the Dark Web is that certain people abuse their access power in this area. Because it promises privacy, some people can use this power to disclose other people's privacy. They can access and threaten people's personal information such as identity theft, private photos, financial information. In addition, fraud, malicious software, narcotic sales, money laundering, political, religious, ethnic blog content, unauthorized access of copyrighted books, passport, counterfeit money sales, gambling promotion, gun sales, pornography are the main topics of abuse.

When caught in one of the attacks carried out by some malicious software on the dark web, keyloggers can record keystrokes and calls, showing the attacker the navigational path. In addition, access to files may result in encryption. They can also have financial information with follow-up. For example, if data locked for ransom is recovered, there is no guarantee that the attacker will release the data after payment. In addition, there is no guarantee that you will not use or sell them. The attacker cannot be traced as the payment is usually made in virtual currency such as bitcoin. Another type of attack that can be encountered is to try to commit fraud by redirecting to another page. Another threat is that some sites accessed with Tor are known to be tracked by governments. When you come across one of these sites, you may encounter being a government target.

4.4. EXISTING DARK WEB NETWORKS AND DARK WEB ACCESS

In the Dark Web, anonymous and confidentiality can be accessed with the VPN network that creates a tunnel between devices and the internet, with a proxy change that functions as filtering and bypass, and with browsers. The browser most used for Dark Web access is known as Tor. In addition to Tor, FreeNet, Whonix, I2P (Invisible Internet Project), TAILS (The Amnesic Incognito Live System), Sub graph OS browsers are intermediary tools used for Dark Web access. Detailed information about VPN and TOR is covered as another topic.

4.4.1. FreeNet

As with the Tor browser, access to data is provided by communication between nodes. All nodes work in conjunction with each other. Each node is responsible for its own child nodes. They also maintain lists of neighboring nodes for security purposes. This is called the "small world principle". The request key visits the nodes closest to the source key. It finds it through keys defined by hash value. It offers little flexibility in terms of hosting service. Therefore, it is more suitable for serving static content. Although the range of services seems narrow in this sense, it does not mean that malicious activities cannot be done on this platform [17]. FreeNet is known to perform better with Bit Torrent. It takes care of maintaining the browser speed and is effective in fast downloading of large files. In addition to these positive aspects, FreeNet does not have a fixed storage size, so it cannot be certain about the permanent storage of the file. Therefore, it uses decentralized distributed data stores to hold and transmit data. It does not have its own search system.

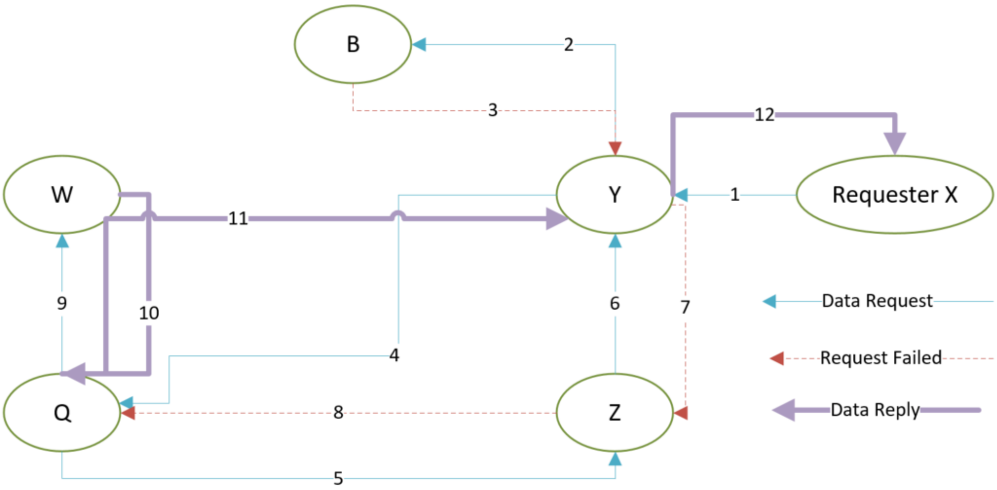


Figure 4.2: File Request Protocol in Freenet

Nodes connected to each other ask the request to all nodes they are connected to until the data is returned. If no other node is found in the chain, a fail report is returned. And an alternative node is sought. The steps in **Figure 4.2** are followed.

1. The user initiates a file search request on node X. The request is forwarded to Y and B.

2. Node B has no other node connections, so it returns Request Failed to Y.

3. Y will forward the request to its neighbors Z and Q. Since it has no neighborhood to Z, it asks Q to transmit it.

4. Since Z must receive the request and forward it to another node, which cannot return a response, it sends it to Y and enters a loop. Therefore, it returns as Y Request Failed. In Z, the message returns to Q as Request Failed.

5. This time Q forwards the request to its neighbor W.

6. W finds the file and sends the request to the user by following the path Q, Y, X respectively.

4.4.2. SubGraph OS

It was created to reduce the attack rates of the operating system. Prevents user manual configurations. Because it's OS content, it's also easy to run malicious code and bypass the firewall. Encryption on the file system is mandatory when installing. It is resistant to Cold Boot Attack. In order to connect to Tor's proxies, the application requires changing the built-in proxy settings [24].

4.4.3. Whonix

This scanner provides software flexibility. It is protected against location and IP address detection. It is effective in providing automatic routing of all applications. However, it is more difficult to install than the Tor browser. The maintenance requirement is high. The hardware requirement is obvious. Therefore, it needs a virtual machine or backup hardware. Provides user privacy for application access such as IRC, chat and email. Its security is ensured by isolation. Protocol leak and fingerprint protection are also among the features of the browser [25].

4.4.4. TAILS (The Amnesic Incognito Live System)

It encrypts mails, messages and files with cryptographic tools in making encryption. The best part is that it does not need to be installed in the system. It can be run virtually on platforms such as Virtual Box. It is insufficient in firmware attacks. It has multi-language support and makes it easy to customize [26].

4.4.5. I2P (Invisible Internet Project)

It has a message-based network structure. It hosts encrypted identifiers, thus hiding the visibility of IP addresses. Garlic has a structure called routing. In this structure, in many layers; Encryption takes place between the sender and the destination, between routers in the network, and end-to-end access in tunnels. This is more difficult than Onion routing. It has ease of file sharing. With all these features, it only works efficiently on Linux. It differs from other browsers in accessing content. The user is required to log in. There is a messaging service called I2P Bote and it provides anonymity while sending and receiving messages. Setting up I2P is easy compared to Whonix. P2P was created as a distributed communication layer. It was developed to serve users to host services such as web access and mail. In Tor, there are clusters of randomly encrypted nodes, while in I2P there are virtual tunnels and each node acts as a router. It operates by routing traffic flowing through virtual paths to a pool. For example, while sending data from point x to point y, it also sends the routes of virtual tunnels to y, and this information is kept in a decentralized database. A node in an I2P network can be a server that hosts the darknet service, or it can be a client that accesses servers and services using other nodes. In I2P, every client or server is an automatic relay node. In I2P, the network consists of its own anonymous and private sites called eepsites. I2P can be used by installing a routing service on a client's device. A temporary one-sided encrypted connection is established with the I2P router on the target devices. Four tunnels are needed to provide a single round trip. Data is output over outgoing tunnels and received from incoming tunnels of other devices. A two-way data flow is not provided in the same tunnel. Tunnels are not built for a long time. It is constantly updated for security [17].

Figure 4.3 below shows the operation of the I2P communication protocol. Here is the functioning protocol for I2P communication:

- Routers F and B are the endpoints of the outgoing tunnel.
- Application B uses router C as incoming tunnel and E router as outgoing tunnel.
- Application A's I2P gateway is Router F, Application B's is Router C.

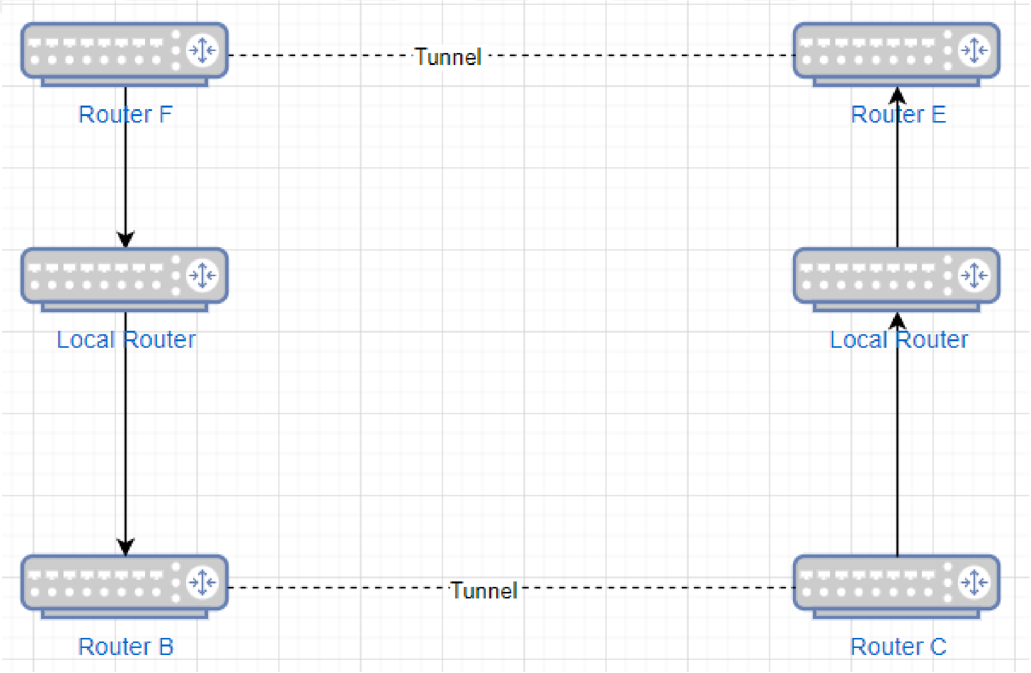


Figure 4.3: I2P Communication Protocol

4.4.6. Alternative Domain Roots

.dot , .net , .org are known DNS entities under the control of ICANN. These domains, referred to as rogue TLD's, belong to a class of networks not under ICANN's control. Therefore, it requires the use of a dedicated name server. In this scenario, since there is no common control mechanism, they communicate to be aware of each other when a new record is entered in the network consisting of .bit DNS servers. Alternate DNS domains do not provide anonymity like Tor does. However, if a domain crash is encountered, the protection provides flexible domain management.

DNS roots in use:

- *Namecoin:* To access the domain, connection to online dns servers must be made. .bit is known as TLD and has the same logic as bitcoins.
- *Cesidian Root:* It is an Italian operator DNS containing TLDs .5w, .ispsp, .cw, .6w. It has a network structure consisting of more than 30 dns servers all over the world.
- *Namespace.us :* It has 482 alternative TLDs such as .big, .manifesto, .academy. It has been in use since 1996. As an alternative domain name provider, it has its own DNS servers that resolve both its own and ICANN servers.
- *OpenNIC:* Consists of a DNS server network run by volunteers. It maintains a strict policy for security, anonymity and performance [17].

4.5. ROLE OF GOVERNMENT

The increasing use and crime rates in the Dark Web have also prompted the government to take part in this island. It is known that the FBI uses an application called computer and internet protocol address verifier (CIPAV) to monitor malicious activities to identify suspicious individuals using proxy servers and anonymous services such as tor. Thanks to this anonymous and secure network, opportunities have arisen for law enforcement, such as online surveillance and conducting covert operations.

The balance of the Dark Web on the side of governments should be maintained at a near-perfect level. Because we are faced with a multifaceted dilemma. On the one hand, there is the segment that wants to express their opinions freely and to have the right to share what they want. Governments need to ensure that democratic values are protected. On the other hand, they have to deal with an unidentified new tech-savvy and uncontrollable criminal.

The negative effects of the Dark Web in the field of cyber security at the national and international level are great. Tactics must be devised by governments to streamline the Dark Web. With these regulations, it should be ensured that criminal web activities are restrained and that the innocent can be distinguished from the criminal. For the control policy of this anonymous and confidential network, governments can benefit from the capabilities of some relevant government agencies. For example, Computer and Internet Protocol Address Verifier (CIPAV) is used to identify suspicious people's addresses by separating normal internet traffic from TOR traffic. It helps narrow down the research. The Defense Advanced Research Projects Agency (DARPA) of the Ministry of Defense plays an active role in the detection of illegal activities with the "Memex" application. It is used to identify criminals in certain patterns. In addition, it is known that the FBI seized the hacking application and used this application to determine IP addresses [12]. The Cyber Attack Automated Unconventional Sensor Environment (CAUSE) program is another method used by the authorities for early detection of cyber attacks [27]. In some cases, without the need for another application, the TOR browser can also be used directly. Tor's online surveillance feature allows authorities to access questionable websites and services without leaving a trace. It is an effective way of conducting covert operations with its anonymity. Anonymous hotlines are also one of the most popular methods.
Monitoring some areas helps to make the Dark Web manageable.

- *Mapping the hidden services directory:* Database tables are not kept in a regular structure, they are in a distributed structure. Monitoring can be achieved by following the tables in the distributed structure.
- *Customer Data Monitoring:* Web request targets need to be monitored. Although it has a secure structure, e-mail and electronic communication channels can be tracked with some special tools.
- *Monitoring of Social Sites:* Popular sites are followed for access to hidden services so that any data can be captured with a redirect other than the multitude of usage rates.
- *Monitoring of Hidden Services:* Captured services should be checked quickly. It is possible to change the name. Or it may be inactive.

- *Semantic Analysis:* Maintaining a database of activity and history of hidden sites.
- *Marketplace Profiling:* It is necessary to follow up the users, whose illegal actions are detected, to learn about their other actions or to follow up other data that can be learned [12].

However, in order to continue all these studies and efforts, permission must be given within the legal framework.

4.6. CYBER ATTACK AND DEFENSE AGAINST CYBER ATTACK

The downside to the potential of technology is the misuse of the internet. Pointing out the Dark web as the interference of media objects, Gehl & McKelvey also stated that anonymous networks attack themselves and then reconfigure their infrastructure [28].

The attackers trying to stay one step ahead and working on new attack methods on the victims they choose make it very difficult to provide cyber security. 2020 can be said to be the year that broke the record in the number of data records breached. In April 2020, half a million Zoom user accounts were stolen and sold on the dark web. According to the FBI, there has been a fourfold increase in cybersecurity complaints this year. The number of identity theft reports in 2020 was reported as 1.4 million by the US Federal Trade Commission. And this figure is double the number reported in 2019.

In 2021, Yahoo Finance 2020 stated that despite increasing IT security investments, 78% of top IT security leading organizations were inadequate in protecting against cyber attacks, and this result was obtained as a result of the IDG Research Service survey [22].

The reason for choosing an attack over the Dark Web is actually due to the fact that anonymity gives the attacker great confidence. The Sybil attack, in which a system can impersonate multiple identities, is among the most notable attacks. With this attack, users can be directed to the desired hidden sites.

The types of attacks on the dark web are evaluated in two categories. It can observe with passive attack or manipulate with active attack. It tries to make changes in the network by following the input and output nodes with single-end or end-to-end attacks [29]. It is discussed in 4 group titles. Client-based attacks aiming to harm the Tor user, server attacks trying to obtain IP information with hidden services, network attacks to interfere with the entire network, and generic attacks with multiple targets are grouped.

4.6.1. Traffic Fingerprinting Attacks

Single-ended client is a passive type of attack that allows traffic flow to be monitored without removing encryption. In this attack type, traffic can be accessed in two ways. The first is performed using the input node. However, certainty cannot be obtained as the victim does not need to connect to this node of the attacker. The other method is a more robust method. In this way, the attacker can intercept the node between the victim and Tor access and listen to the traffic. There are variety of defense mechanisms accessible for this sort of attack specifically hypertext transfer protocol with Obfuscation (HTTPOS), pipeline randomisation and Guard node adaptative artifact and Traffic Morphing and so on [12] [30] .

4.6.2. Traffic and Timing Correlation Attacks

In this attack type, end-to-end client is an active type. Attackers try to reach the target server's information by monitoring the flows of the input and output nodes. When the number of clients in Tor is relatively small, traffic and timing attack are easier to implement. Tor provides this attack measure with methods such as packet buffering, scrambling and delaying [12] [30].

4.6.3. Credential reuse

Client is the active attack type. There is always a saying that the password you set does not comply with the password rules. This is taken care of in applications, websites and corporate accounts. Because it is obvious that simple defined passwords and passwords containing personal information (name, date of birth, etc.) are constantly tried and detected by attacks. In fact, attackers obtain collections of usernames and passwords from the black market on the Dark Web. It is being tested whether this data is still in use. In order not to be exposed to this attack; The same passwords should not be used in every application that requires a password. Care should be taken to configure the password in accordance with the standard password policy (at least 8 characters, one uppercase letter, one lowercase letter, one number and/or one special character). Help can be obtained from password manager applications [30].

4.6.4. Cross Site Scripting (XSS) Attacks

In this attack type, it targets users of the target website. Client is an active attack type. In this attack, the web page is not under any attack. The malware is expected to run in the user's browser. However, since user information is at risk, the reputation of the relevant web page will be damaged. There are three types as Refected XSS, Persistent XSS and DOM-based XSS. Generates a url in Rejected XSS. By clicking this url, the script is transmitted to the browser on the user's side and executed by the browser. In Persistent XSS attack, a post message containing script execution command line rules is left on one of the form pages of the web page. When the user clicks on this address, the malware is run by the user's browser. In DOM-based XSS attack, it happens when there is a user-side vulnerability. Malware hosted by the user is sent to the target browser. With this attack, accounts can be hijacked, malware can be installed or websites can be redirected to different locations. To prevent this type of attack, browsers must be configured to prevent automatic loading. Content security policy can be exploited as XSS attacks provide additional levels of protection [12] [30].

4.6.5. Unpopular Port Attacks

This type of attack is known as client passive. Attackers introduce multiple TOR nodes and expect users to choose one of them as innocent. However, Tor consists of 700 routers, which reduces the selection rate of attackers' routers. Some Tor nodes allow customized ports. Therefore, Sulaiman and Zhioua proposed a type of attack. They suggested that using these customized ports and using a Tor router that prefers customized ports, they can make their own redirects to the relevant page request after the user's preference for using this network [12] [31]. With this attack, which is planned with a secret service script running on this redirected server, the attackers will be successful if the user accepts access over this network.

4.6.6. Low Resource Routing Attacks

The client is a passive attack. In this type of attack, a study is carried out to reduce the correct selection rates of access protections. Valid login protections can also be changed as the attacker wishes. It is a bandwidth and uptime attack. In the attack, the payload data entry can be detected by following the Tor circuit structure algorithm [30].

4.6.7. Session Hijacking and Man-In-The-Middle Attacks

When a user makes a request on a web page, it goes to the relevant server and the server sends the information it has to the user. This communication is provided with the session ID. In this type of attack, attackers can gain access to both user information and target server information by obtaining the session ID. By intervening, it can take over the session by appearing to both parties like the other party. For this reason, this type of attack is called man in the middle. There are ARP Spoofing, Rogue Access Point, mDNS Spoofing and DNS Spoofing attack types. In a Rogue Access Point attack, attackers create wireless access points and trick nearby devices into joining this network. When a computer wants to communicate with a computer, it uses the ARP cache, which resolves the IP address to the MAC address. Wireless cards try to connect to the access point automatically. This attack is based on exploiting this and collecting data from the attackers' own access points. In an mDNS Spoofing attack, an application needs the information of the device to which it will be connected. In DNS Spoofing, the attacker gives the server its own server dns information, so the server that is trying to retrieve data sends the data to the attacker's server. In the prevention of this attack; It is important to update the default user information of wireless network devices. VPN use can be preferred as it provides a secure network environment. HTTPS connections with a security certificate can be used for communication. The accuracy of the place to be communicated can be checked with RSA (Public Key Pair Based Authentication) [12] [30].

4.6.8. Eclipse Attacks

It is a server-based active attack type. The Eclipse attack tries to obscure the client's view of the network. A single node is targeted. For this reason, Sybil differs from the attack at this point. It allows the creation of an artificial environment between the node and the user. The affected node is isolated from neighboring nodes [12] [30].

4.6.9. Cell Counter Based Attacks

This attack is a passive server-based attack type. Allows signal addition to input and output relays. The relays at the ends recognize the signal to verify that the client and server are communicating. The traffic is transported by cells, held in a queue temporarily, and sent to an output buffer before passing to the network. A signal can be generated in traffic by taking control of the number of exit cells. It is necessary to set the signal sending time well. Short time shipping will have to wait for other relays. Waiting for a long time will make you think that there is a suspicious situation [12] [30].

4.6.10. Distributed Denial of Service (DDoS) Attacks

Network active attacks. The purpose of this type of attack is to block the victim's access and slow down the connection. To accomplish this, a lot of requests are sent to the destination. Multi-variate threat detection can be used to detect DDoS attacks. It also has the feature of preventing other routers from being selected by doing package spinning. However, in doing so, it risks compromising anonymity. Proxy routing in its own environment is more likely to be selected as other routers will appear busy as it slows down the network. Thus, more attacks can be carried out [12] [30].

4.6.11. Sybil Attacks

It is one of the network active attacks. The offensive use of Tor relays is called a sybil attack. An attack by a malicious node requesting fake identities or generating new identities. It sabotages the network by creating multiple identities. Accounts that appear to be more than one are actually managed by a single entity. It directs the probability of preference to the nearest node and drives away honest nodes. The only way to prevent this attack is to increase the cost of identity [12] [30].

4.6.12. Correlation Attacks

In this attack type, the first and last routers are checked to correlate timing and data properties, and data anonymity is attempted to be bypassed. It is tried to provide flow through these controlled routers. End-to-end networking is a type of attack known as passive. Since it is a complex type of attack, there is no established method to prevent it. A student sent fake bomb threat emails to his school to avoid the exam. The FBI found that the student made this submission with an app that creates temporary emails. The identity of the student was determined with the help of correlation [12] [30].

4.6.13. Relay Early Traffic Confirmation Attack

This attack is a combination of correlation and sybil attack. In this attack, the attacker must have secret service management and authority on the access node. When the client sends the secret service connection request, the secret service entry point information is transmitted with relay-early cells and hidden circuit. The input node resolves the name of the hidden service over the traffic and associates it with the client [12] [30].

4.6.14. Congestion Attacks

This type of attack represents an end-to-end server active attack. The connection between the nodes is monitored and at the same time, if there is a blocked node, it can interfere with the connection speed of the person attacked by the attacker. This type of attack is also known as a clogging attack. Murdoch and Danezis performed a combination of timing analysis and congestion attack to detect routers. This attack method can also be applied on routers with different bandwidths. This type of attack can be solved by disabling JavaScript [12] [30].

4.6.15. SQL Injection (SQLI) Attacks

It is a generic attack type. In this attack type, the attacker's target is directly in line with the website. SQL (Structured Query Language) is used to manage data. These servers are targeted in this attack. The data to be attacked can be critical such as bank account information, credit card passwords. There are three attack types as Sanitized Input, Blind SQL Injection and Out of-Band Injection. Out-of-Band attack is the most complex attack type among them. It is used when the other two types do not work. The attacker creates a sql statement, and when this action is triggered, this server is made to establish a connection with an outside server and delegate control authority to the outside server. In a blind SQL attack, it is also known as inferential SQL injection. With this attack, as soon as the data is revealed directly, the behavior is carried out by examining the data in line with the data that the attacker wants to capture. In Unsanitized Input attack, the user is faced with unverifiable input. To be protected from this type of attack; dynamic sql should be used or stored procedures should be preferred. Limitation of database traces should be ensured. Care should be taken to use parameterized queries, it should be noted that data used as plain text will make it easier for attackers to access open data. Sensitive data can be encrypted. Information can also be obtained from error messages, so care should be taken when sharing this information with other users. Web Application Firewall (WAF) should be used in web applications that have access to the database. Databases should be kept up to date [12] [30].

4.6.16. Botnets

It is a generic attack type. Users can download malware when they enter a web page, and once the malware enters the device, it starts its activities. It can give illegal orders to botnets to do identity theft, to spam found accounts, like bitcoin mining. Bots are controlled by botmaster. And they all connect to a central server called C&C. The botnet architecture continues to be developed, as this is at a high risk of being caught in a single server architecture. Central architectural security is tried to be provided by methods such as fast transfer of data from one C&C server to another, and DGA (domain creation algorithms) [12] [30].

4.6.17. Raptor Attacks

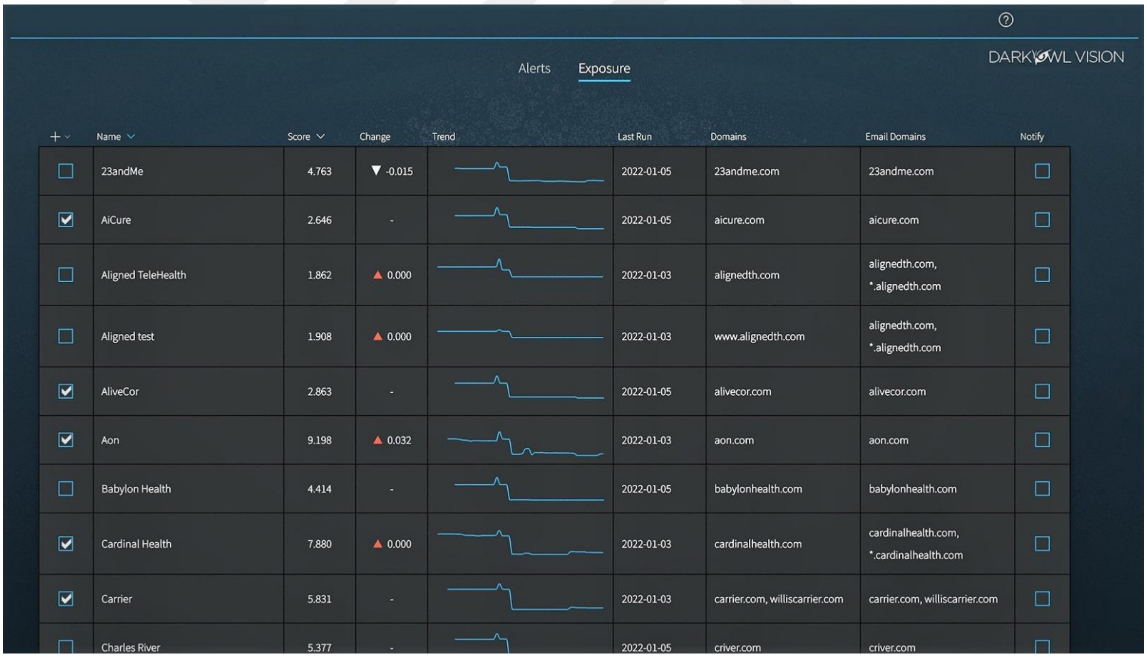
It is a type of attack that can monitor the traffic between the client and the input relay, and between the output relay and the destination server, and analyze the packet in the traffic. Sun at all. They stated that Raptor, a correlation attack, left Tor vulnerable [32].

4.7. DARK WEB TRAFFIC DETECTION

There are some software and tools to protect from various damages and attacks on the Dark Web. Dark Web monitoring platforms are effective in searching and tracking whether the information of individuals or organizations is under threat. These apps provide proactive protection. They act by monitoring their offensive activities. Echosec Beacon, Spycloud Ato Prevention, Digital Shadow SearchLight, DigitalStakeout Scout, Dashlane Business, ZeroFox, DarkOwl Vision, Acid Cyber Intelligence, Alert LogicDark Web Scanning and Cybersprint are the most well-known ones.

4.7.1. DarkOwl Vision

It is a platform application that started collecting data in 2015. It provides the user with a secure and comprehensive search for darknet data. It provides a way to efficiently extract data from leaked data. DarkOwl continuously collects and indexes darknet data. It can perform extensive searches within daily large data entry rates. Search can customize. Using Boolean and Regex search logic, searches can be automated and give search results by sending notifications. It allows searching in 47 languages [33]. It is integrated into an intelligence service package called the Darkint Suite. Data streams of Darkint Suite can be integrated into applications via an API. Dark owl vision can be thought of as the ears and eyes on the Dark Web. It is a powerful research tool that allows analysts to search. It is an application that appeals not only to analysts, but also to penetration testers, law enforcement and incident responders. It can provide support to law enforcement in the investigation of cyber crimes. In **Figure 4.4**, dashboard view of the DarkOwl Vision application is shown.



+	Name	Score	Change	Trend	Last Run	Domains	Email Domains	Notify
□	23andMe	4.763	▼ -0.015		2022-01-05	23andme.com	23andme.com	□
☑	AiCure	2.646	-		2022-01-05	aicure.com	aicure.com	□
□	Aligned TeleHealth	1.862	▲ 0.000		2022-01-03	alignedth.com	alignedth.com, *.alignedth.com	□
□	Aligned test	1.908	▲ 0.000		2022-01-03	www.alignedth.com	alignedth.com, *.alignedth.com	□
☑	AliveCor	2.863	-		2022-01-05	alivecor.com	alivecor.com	□
☑	Aon	9.198	▲ 0.032		2022-01-03	aon.com	aon.com	□
□	Babylon Health	4.414	-		2022-01-05	babylonhealth.com	babylonhealth.com	□
☑	Cardinal Health	7.880	▲ 0.000		2022-01-03	cardinalhealth.com	cardinalhealth.com, *.cardinalhealth.com	□
☑	Carrier	5.831	-		2022-01-03	carrier.com, williscarrier.com	carrier.com, williscarrier.com	□
□	Charles River	5.377	-		2022-01-05	criver.com	criver.com	□

Figure 4.4: DarkOwl Vision Dashboard

4.7.2. Alert Logic Dark Web Scanning

It is an application that scans the domain and checks the possibility that your credentials have been accessed, and tests sensitive data for a security breach. It is an application of Alert Logic, which was established in 2002. It regularly scans and checks whether identity data and password data have been stolen, and provides notification by sending a notification in case of detection. It is one of the applications used in the fight against fraud. It has essentials, professional and enterprise support. The features it offers vary according to the type of application. For example; In the Enterprise model, the web protection service offers protection against waf, sql injection and DoS attacks [34]. **Figure 4.5**, there is a topology sample screen of the Alert Logic application.

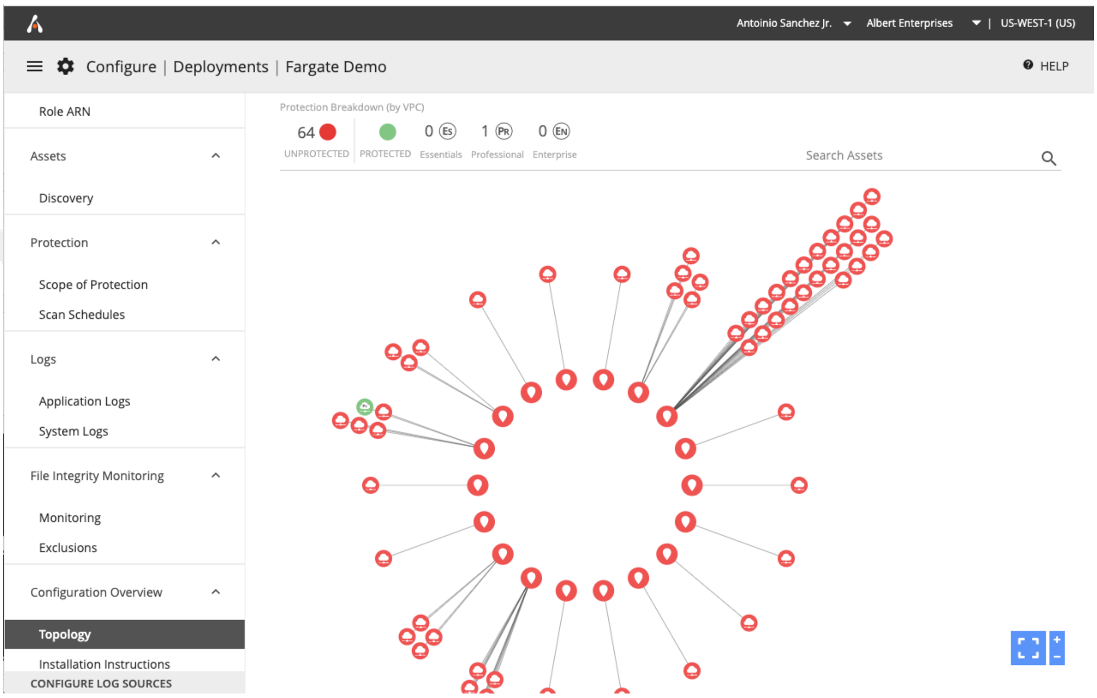


Figure 4.5: Alert Logic Topology Example

4.7.3. ACID Cyber Intelligence

It is a platform created for monitoring in areas where cybercriminals operate. It sends its agents for field detection with advanced AI algorithms. It is effective in continuous monitoring of various sources. It covers leak sites, social media, IRC chats, and criminal sites tracking. By defining key words (emails, domain names, credit card information, etc.), it is effective in detecting threats before they follow an approaching attack situation. It also mimics regular user activity [22]. **Table 4.1** also includes other well-known dark web monitoring tools. The usage areas, publication years and features of the tools are included.

Table 4.1: Dark Web Monitoring Tools Information

Applications	Usage Area	Year	Features
Cobwebs Technolohies	Large organizations in government sectors that want AI and ML-based monitoring	2015	Threat identification Real-time alert Streamlined artificial intelligence Improve response times
Digital Stakeout Scout	Medium-sized institutions in all industries.	2010	Automatic data labeling Boolean and linked data search Dashboard and analytics Mitigating digital risk and increasing resilience Intellectual property and brand protection
Echoses System Platforms	All sectors	2013	Advanced SaaS based solution Monitoring digital assets Enhanced access to social data
SpyCloud ATO Prevention	Medium businesses	2016	Resetting hacked passwords Early violation notification workflows and data flows It monitors Active Directory and sets strong password policies such as mandatory password complexity.
ZeroFox	Enterprise-sized organizations	2013	Attack Blocking Artificial Intelligence powered threat analysis Domain protection

In 2019, Alkhatib and Basheer developed an application that categorizes dark market products with a python library known [35]. They did an analysis that produced lists of sites on the dark web [36].

Although there are some application-specific capabilities, in general, the promised features are very close to each other. Being able to scan with very large data in a large network like Cloud Darknet and staying safe while doing this shows that successful works have been achieved.

However, despite all these working and safety practices, the last action comes from human hands. Martin Rösler summed it up in his article Below the Surface:

> *“If you go to the doctor and undergo surgery and you wake up in your hospital room and violate all the hygiene rules, you will die even if you have the best surgeons, the best tools, the best hospital. Same thing with anonymity, if you are behaving in an unwise manner, even the best tool can't protect you.”* [16].

4.8. THE DARK WEB AND MALWARE

It enjoys a privileged environment by malware authors and botnet administrators. Scammers have gotten themselves a good gathering place to buy malware.

In the Dark Web Price Index values for September 9, 2021, the pricing of goods and services sold on the Dark Web in USD is as follows.

- Copied credit card $30
- Banking account login information is 120$
- Bitcoins account 350$
- Facebook account, whose password was compromised, $65
- Netflix account $44
- Fake US green card $150
- Fake EU passport 4000$
- Website DDoS attack $15 [37]
- paypall account information $30
- Walmart account $14
- Instagram account with hacked password 45$
- Twitter account with hacked password 35$ • Gmail account with compromised password $80
- Instagram followers x1000 2$
- Adult site accounts $5
- Fake driver's license $20-80 [38]

These data vary according to the applications, whether there is money in the accounts, according to the number of followers, according to the region or state. Darknet is used as a trading platform by offering different types of malware for sale, each with different costs. Some of these software are:

4.8.1. Data Stealing Trojans

This software is capable of stealing passwords, blocking keystrokes, disabling antivirus software.

4.8.2. Ransomware

Ransomware locks files and for this, attackers demand a ransom to gain access to the data again. By seizing control, it prevents access to its user. Ransomware usage growth accelerated in 2017 with the WannaCry attack. With this attack being considered profitable, ransomware applications have diversified. With the impact of COVID-19, security vulnerabilities occurred in cyber defense lines during the periods when organizations switched to working from home. In 2020, ransomware attacks increased by 50%. Ransomware variants that have made a name for themselves as successful: Ryuk, Maze, Revil (Sodinokidi), Lockbit, DearCry, Lapsus. The attack is provided by violating the corporate user user information using the remote desktop protocol (RDP) in Ryuk. Maze software is a type of ransomware that performs file encryption and data theft. They sell this data to others, threatening to make the data public if their aggressive ransom demands are not met. It is a software that uses Double Extortion technique to steal data and encrypt files. It is a type of attack targeting large companies. It competes with Ryuk in terms of ransom amounts. Lockbit has been active since 2019. It was developed to encrypt large company data by bypassing security devices and IT teams. DearCry is software designed to attack by exploiting 4 vulnerabilities detected in Microsoft's Exchange servers in March 2021. lapsus; A South American ransomware gang known for accessing data from companies like Nvidia, Samsung, and Ubisoft. It shows malware applications as trustworthy through source codes [12] [30].

4.8.3. Remote Access Trojans (RATs)

This software connects to the hacker-controlled command and control server, compromising an open TCP port on the user's device. The attacker who will make a rat attack creates a special port on his internet access device. He creates a server environment by using the RAT management program. Sets the IP address to fixed. The device infected by the trojan establishes a connection with the server opened by the attacker with a p2p connection, and the administration is transferred to the attacker's side [39]. It allows attackers to monitor user activities, execute files and commands on user devices, format drives, take screenshots, access webcam and microphone and download internet documents, delete and modify file systems, keyboard and mouse functions. Popular RATs are: DarkComet, ProRAT, Back Orifice, Turkojan, CyberGate, Cerberus and Spy-Net.

4.8.4. Botnet Malware

In the botnet, the attacker can simultaneously order the devices under his control to commit a crime. These devices can receive an instant update and change their actions immediately. Common botnet actions are Email spam, DDoS, financial breach and intrusion. Emails are exposed to spam emails from botnets every day. For example, the Cutwail botnet can send up to 74 billion messages per day. It covers the efforts of people who view these e-mails and click on the relevant fields to seize device controls. Botnets created for financial breaches are designed to directly steal credit card information. DDoS causes crashes by making constant requests to the target server. They are botnets designed to gain unauthorized access to areas with high-value data [12].

4.8.5. ATM Malware

As the name suggests, this software was created for ATM piracy. It is prepared for all platforms. Tyupkin virus is a type of ATM malware. By gaining physical access to the ATM, attackers install their bootable applications and take control. The ATM enters a pending loop. In order to make it difficult to detect, they continue normal use and can steal money from the device by sending commands at certain days and times of the week when the usage is low. In this attack, the principle works as follows; Atm creates a session from its own random numbers in each session. The attacker generates this session number as the session key in the algorithm. When he uses this key, he can access the ATM money information. Depending on which one has more, the attacker can steer there and steal up to 40 banknotes at once [12] [40].

4.8.6. Phishing

The phishing tactic requires acting someone else to obtain data. It may be aimed to install malicious software or to obtain private information about the user. The tactics used for this are applied by sending fake e-mails to the user and directing them to the link they want. If the email contains an attachment or a link, it can direct you to another link and collect data, or it can have a malware installed directly on your device with a click. There are three types of phishing: Spear Phishing, Whaling and Clone Phishing. Spear says phishing has been used, especially when targeting an organization. In this attack type, access to more data is aimed by targeting the multitude of people. The Whaling attack targets the senior authorized segment of the organizations. Trying to be deceived by focused messaging. In Clone Phising, a copy of a message taken from people's data is sent, and the user is simply tried to deceive from a point known to them. To avoid this attack; malicious urls can be checked with character recognition filtering. Before clicking on the link or attachment sent while trying to deceive using an image, it can be checked whether it is a known address by hovering over the url data and the suspicious addresses can be quarantined. Since it can be easy to capture passwords in this way, two-step-protected security measures can be taken in applications. From time to time, devices can be checked for malware detection by performing a security scan with various tools. WAWTRACK malware is a banking trojan spread by phishing.

Using VPN, taking regular backups, benefiting from reputable virus protection programs, raising user awareness in organizations, receiving and giving trainings are among the measures that can be taken to protect against malware. Cyber attack training should be given importance due to the prevalence of attacks carried out by the user clicking on a malicious link. Data backups with automatic protection can ensure that the attack can be exited with minimal loss. It is important to keep the applications used up to date. It would be wise to follow the patches released in certain periods and update them, considering that organizations that have not applied this are the target of attackers. Considering that the stealing technique of RDP user information is a common type of attack, care should be taken to ensure that user password information is secure and in compliance with standards [12].

4.9. DARK WEB CRIMES

Darknet's privacy criminology provides an advantage to crimes. Due to the low detection risk of crimes, the Dark Web is one of the crime platform points.

4.9.1. Drug Trafficking

It is one of the distribution centers of illegal drugs and unlicensed drugs. When it comes to drugs, silk road comes to mind in the Dark Web. However, it was detected and closed down by law enforcement in 2013. Ross William Ulbricht, known as "Terrible Pirate Roberts", was arrested on charges of drug trafficking, computer hacking and money laundering. It is also in the criminal files that someone who threatened that the site's user information was in his hands had him killed with a hired killer. is located. 3.6 million bitcoins were seized by the FBI. Atlantis emerged as Silk Road's biggest competitor, but it was also shut down on September 20, 2012 [17]. The applications that were closed were replaced by Alpha Bay [41]. Also known drug markets on the Dark Web include Dream Market, Valhalla and Wall Street Market, Mr. Nice Guy.

4.9.2. Human Trafficking

In the Dark Web, people are trafficked on a site called Black Death. The model named Chloe Ayling is one of the victims of this application. This application is used by constantly updating URLs [12]. It facilitates the spread of darknet technology as it is easier to communicate with customers in the digital environment. There are multiple categories of human trafficking. Like child trafficking, organ trafficking. The abduction and adoption of babies has become an industry, and the use of women in the production of babies for sale at some points under the name of “baby factories” has also been turned into an industry [42].

4.9.3. Information Leakage

It is a supportive platform for law enforcement and whistleblowers, and a convenient platform for attackers to leak personal data. Information Leakage can be considered in two categories, hacking and stolen data. Hackers can target companies, celebrities and the public [30]. The best example is Wikileaks. It is possible to see newly leaked information on this page [13].

4.9.4. Proxing

Tor web page URLs do not appear as HTTPS secure websites as they do on the surface Web. You need to bookmark them to make sure they are legit sites. If it is not added and when the attack is taken, the attackers manipulate the proxy settings and show their victims as if they are the page they want to connect to, and actually redirect them to the page they want, and the fraudster is paid with the entered payment information [12].

4.9.5. Bitcoin Scam

The preferred currency on the Dark Web is bitcoin. Even though Bitcoin is considered anonymous, credentials must be added to crypto wallets. Bitcoin transactions are public. For these reasons, it is actually easy to track bitcoin. Services are added to the system in order to reduce the tracking of the crypto currency. Bitcoin is mixed with the micro-transaction network and delivered to the owner with a fee deduction [43]. This structure is called laundry services. Some of the services that provide anonymity to crypto money; ACH, PayPal and Western Union [44].

4.9.6. Arms Trafficking

The volume of arms smuggling on the dark web is less than other crimes. However, in terms of security, its impact is quite high worldwide. Europe, Germany and Denmark are the leading countries in the dark web arms sales market [43]. Terrorist organizations in the Dark Web pose great threats to world security. They use the Dark Web to distribute information among members, recruit members, purchase weapons, and plan terrorist activities [30].

CHAPTER V
THE ONION ROUTING

5.1. TOR DESCRIPTION

It forms the basis of Onion Routing Tor. It developed over time and took its final form. The foundations of Onion Routing were laid in 2002. The Tor structure, which started with the use of the army, was set out with the idea that it should not remain with limited use. This necessitated the development of anonymous methods for identification. It was created at the Naval Research Lab with the support of Roger Dingledine, Nick Mathewson, and others. It has developed with the contributions of the software team consisting of volunteers. The relay network reached 160 nodes in 2005. It was difficult to use as it relies on multiple tools working together. Tor browser emerged in 2008 under the leadership of Steven Murdoch. All components are collected in one place and installed as downloadable from the website. The biggest contribution to the development of Tor design has been with the development of Onion Service. The architect of this service is Roger Dingledine. Initially, he started to develop this service as a hobby. Onion Routing was born with the philosophy of hiding high-risk users among daily internet users. Onion Routing studies were initiated in the US Naval Research Laboratory under the leadership of David Goldschlag, Michael Reed and Paul Syverson in 1995. In 1996, an article called Hiding Routing for Onion Routing was published based on these studies [45].

The main purpose of Onion Routing is to wrap the routing information required for internet access in internet traffic packets in the form of encryption layers and send them to the onion router.

Tor is the largest anonymous communication network worldwide with quite a large number of different server nodes. It provides anonymous communication services to hundreds of thousands of users and carries terabytes of traffic every day. TOR, which aims to ensure the privacy and security of users and was inspired by a project belonging to the United States Navy, was launched in 2003 for non-profit use [46].

Tor developers aimed to build a stable and reliable structure rather than disrupting the technology or using it for other purposes. The design and software balance was evaluated under the titles of privacy, flexibility, reliability and usability [45]. It is an application developed using the Tor tails operating system. Although there are many applications that provide privacy on the Internet, Tor is the most widely used. It offers the client to use without packet delay and size problem. Offering low latency is also one of the important reasons for preference.

Tor design has been shaped by the applicability of 3 basic features. The network is not centralized. The core team that designed Tor has minimal control. It is this structure that was created to prevent surveillance. However, it also complicates the intervention in case of malicious use. The second is low latency. The third is speed. However, while providing this, the time calculations of the signals sent from the Tor network can be taken and abuse can be caused.

Tor secures our connection with three layers of encryption and passes it through servers that run voluntarily around the world. In this way, it provides anonymous browsing on the internet. The more users connect to Tor, the harder it is to spy on users. Analyzing and tracking a mass of anonymous users makes things difficult. As long as the user does not share their information, connections provided through tor are not known from where in the world they are connected. Tor's working logic is as follows; When a user connects to tor, it passes through routers on 3 nodes before reaching its destination. Servers and relays located all over the world manage the traffic between them. When one of the nodes is reached, it has information to show the other destination, but no node can see all the traffic. The network layer consists of the input node, the middle transition nodes, and the output node. It is the entry node that receives the traffic and encrypts the communication between the traffic source and the entry relay nodes. The IP addresses of users connected to the Tor network are recorded in the list of protection nodes. In this way, the user IP addresses can follow the input relay nodes. The first node knows the client ID but does not know where the request is going. The middle node acts as a bridge to send traffic to the exit node. It only knows the address to which it will forward to next. The IP address information of the output relay is known as the source of Tor traffic [47]. The output relay has a key for encrypted data. It has information about where the request arrived, but not the client.

In the **Figure 5.1** in order to get the information about where the relevant Router data comes from and where it will go, in each layer, they decrypt the passwords and transmit the data to the next router. A learns the place to be transmitted by decrypting it, then B and finally C receives the message and forwards it to the destination.

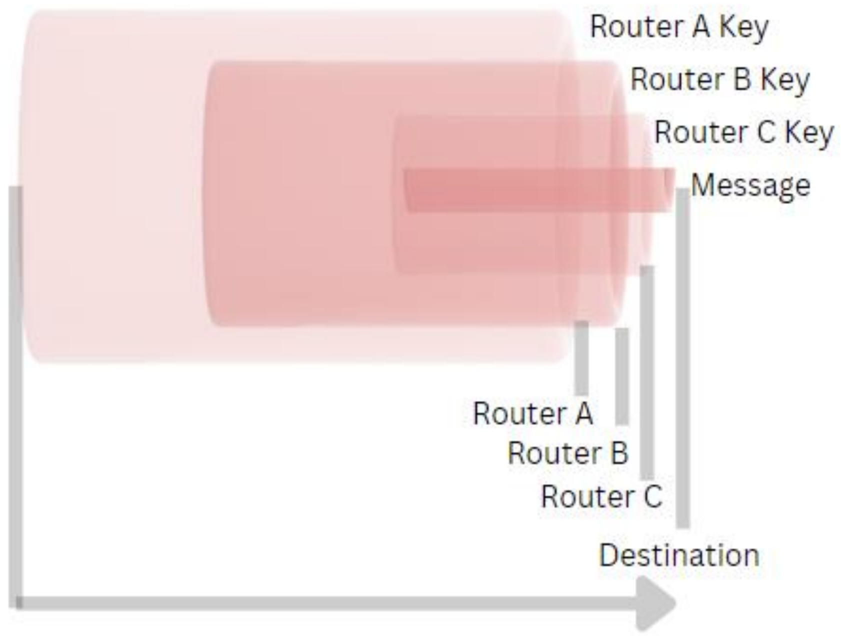


Figure 5.1: The Message Traffic on The Onion Routing

Global address extensions com,org etc. instead of Tor browser, as the name suggests (The onion router), there are onion extension web pages such as “bo862ghoc31.onion”. Since the sites here do not use DNS, the extensions appear in this way. In addition, these address links are changed daily, except for some up-to-date sites through hidden services. Apart from this, it is possible to encounter extensions such as bitnet, i2p, exit and freenet. These domain names that are not in a global form are called “Pseudo Top Level Domains” (Pesudo-TLD) [48]. Something that will not be encountered in Tor browser are cookies. After all the searches we make on our browsers in our daily lives, we come across recommendation cookie links and advertisements in certain parts of the web pages. This is not the case in Tor browser.

Although Tor works at the Transport Layer (Level 4) layer of OSI protocols, Users display the Socket Secure (SOCKS) interface on the Onion proxy software

Session layer. In addition, request redirection is made between the sender and the receiver in the transmission nodes. Thus, it becomes impossible to decipher the passwords during the transmission and to determine the transmission starting points.

We can see that the Tor network provides the HTTPS (Hypertext Transfer Protocol Secure) protocol as well as providing an encrypted connection. It mimics this protocol, making it difficult to identify Tor channels. Therefore, trying to detect the tor network with only the port will be a wrong method and will not give reliable results [1].

Although we talk about the difficulties of Tor traffic detection due to its secrecy, detection is not impossible. At the beginning of the applied methods are the statistical differences in the SSL protocol. SSL carries out the messaging between client and server until handshake occurs. The handshake occurs when the server transmits its public key to the user, followed by the server and user jointly creating a symmetric key for encryption and decryption. Tor clients also use a self-signed SSL using a domain with a random algorithm that changes every 3 minutes. In line with this information, TOR sessions combined with HTTPS traffic can be detected with Network traffic analysis [49].

Other projects under the Tor umbrella are worth examining. The OONI (Open Ovservatory of Network Interface) project is one of them. As in Tor, it develops with the infrastructure of people working on a voluntary basis and collecting devices. The aim of this project is to provide free internet use by collecting all data about internet censorship. The application, which has an interface that those who want to support can install on their devices, provides information flow to Tor developers about which surveillance and censorship practices are in effect. Within the Tor team, developers using Tor in their own technology, information security experts trying to break it, research academics, public relations experts, politicians. There are journalists, experts in the fundraising business. A community is formed within itself. When Tor was first created, the team was a community that came together to develop software and encryption. With the support of Tor's technological design and the increase in the number of interested, it has enabled the growth of the Tor project and the formation of a full-time staff. Tor development efforts are driven by the social world [45].

There are two ways to get into Tor traffic. It is compromising relays or manipulating ISPs (Internet Service Providers). Tor architecture consists of onion proxy (OP), onion router (OR), and directory server (DS). The client can choose any

OP. Each relay communicates via TLS (Transport Layer Security) connection. Creates a random path with OR and forwards the packet to DS. DS has all active OR information. The fastest of the medium relays is chosen. The output relay is usually chosen randomly. If the Tor relays are under attack, a bridge is formed from the triple relays to the target server. In this case, the Onion relays only carry out emergency relay operations [30].

The management of the Tor network is actively involved in many countries. Being over a single country makes it traceable. Tor servers don't just show country diversity. It works on different types of computers, with different operating systems. In this way, Tor infrastructure can be protected.

At each layer, the relevant Router transmits the data to the next router by decrypting the passwords in order to get information about where the data comes from and where it will go. A learns the place to be transmitted by decrypting it, then B and finally C receives the message and forwards it to the destination.

5.2. TOR PROTOCOL

Communication between client and server in Tor. It is shown in **Figure 5.2**. According to this;

- The client sends an HTTP request to the target server for Onion Router information.
- Onion processor determines suitable guard, middle and exit relays according to Tor selection algorithm.
- Onion Proccessor issues the create cell request command to the guard node that responds with the Key1 hash.
- Onion Processor cell request is sent to the input relay with the encryption key.
- The partner role receives the request. It gives the “create cell and hash of the negotiated key” feedback. The process ends with the output relay saying “created cell and hash of the key 3”.
- The Onion Processor then has an encryption key that encrypts the message 3 times in 3 layers.
- Onion Processor creates a package containing source and destination information with this information.
- Destination Server encrypts the package with key3. This package contains middle and exit role information and target server information.

- Client source and destination information is encrypted with Key2.
- With Key1, the packet, Onion Processor source-destination address and input relay are encrypted.
- The encrypted message is sent to the input relay. Since the input relay knows the key1 password, it decrypts it and transmits it to the middle relay.
- Decrypts the middle relay with key2 and transmits it to the output relay.
- The exit node decrypts the password with key3 and transmits it to the target server.
- This path continues in the opposite direction when sending the message back to the client.
- In this circuit, the target cannot know the source, only the output relay. Thus, anonymity is ensured [30].

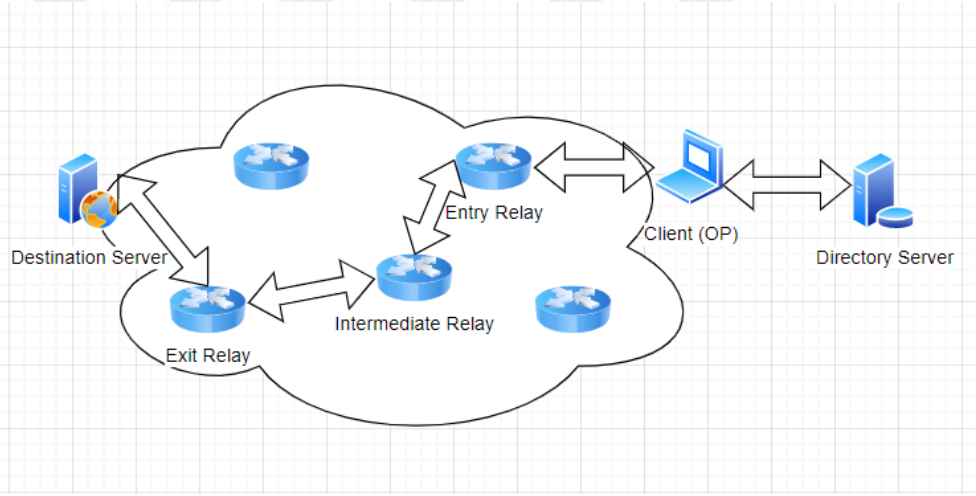


Figure 5.2: Tor Architecture

5.3. HIDDEN SERVICES

Hidden Services help maintain anonymity on Tor. By establishing a connection with the client, the onion provides access to the address via the hidden service. H.S is a server that hosts hidden services. Directory Server (DS) has all relay information.

The Hidden Service protocol is shown in the **Figure 5.3** according to this;

- Client selects RPO (Rendezvous Point) and sends data to remote server.
- I.P. (Introductory Point) It is the Tor relay used in the client connection selected by H.S.

- Some relays in H.S operate as I.P.
- This protocol is a public key and I.P. in the Distributed Hash Table. Defines
- The defined address (eg aa.onion) communicates with the client.
- The client obtains the address using an identifier to create a circuit in a random relay. The client becomes the meeting point.
- The client informs the secret service about the meeting point using the I.P.
- H.S generates a communication circuit to the meeting point.
- In-circuit special relays randomly select guard nodes for security [30].

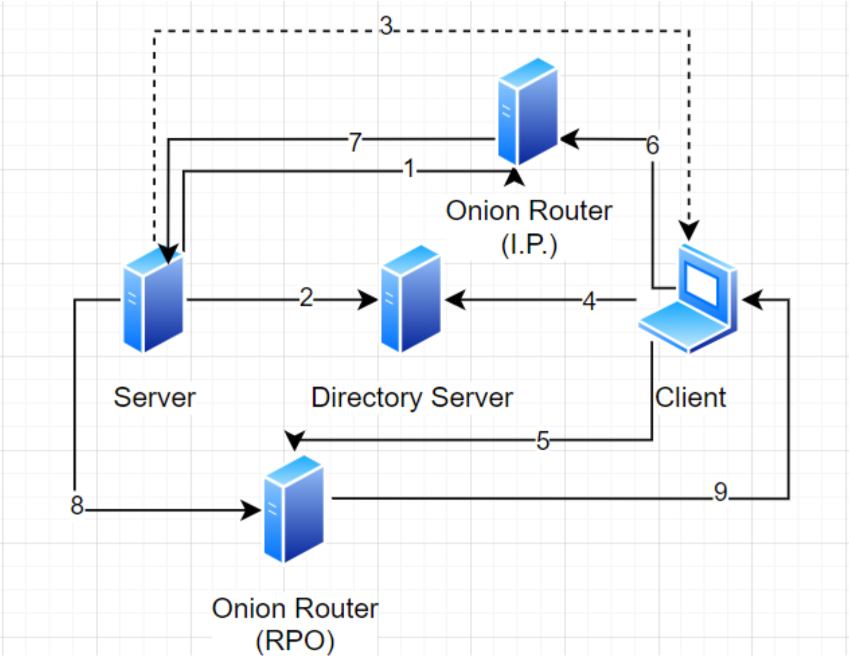


Figure 5.3: Hidden Service Protocol

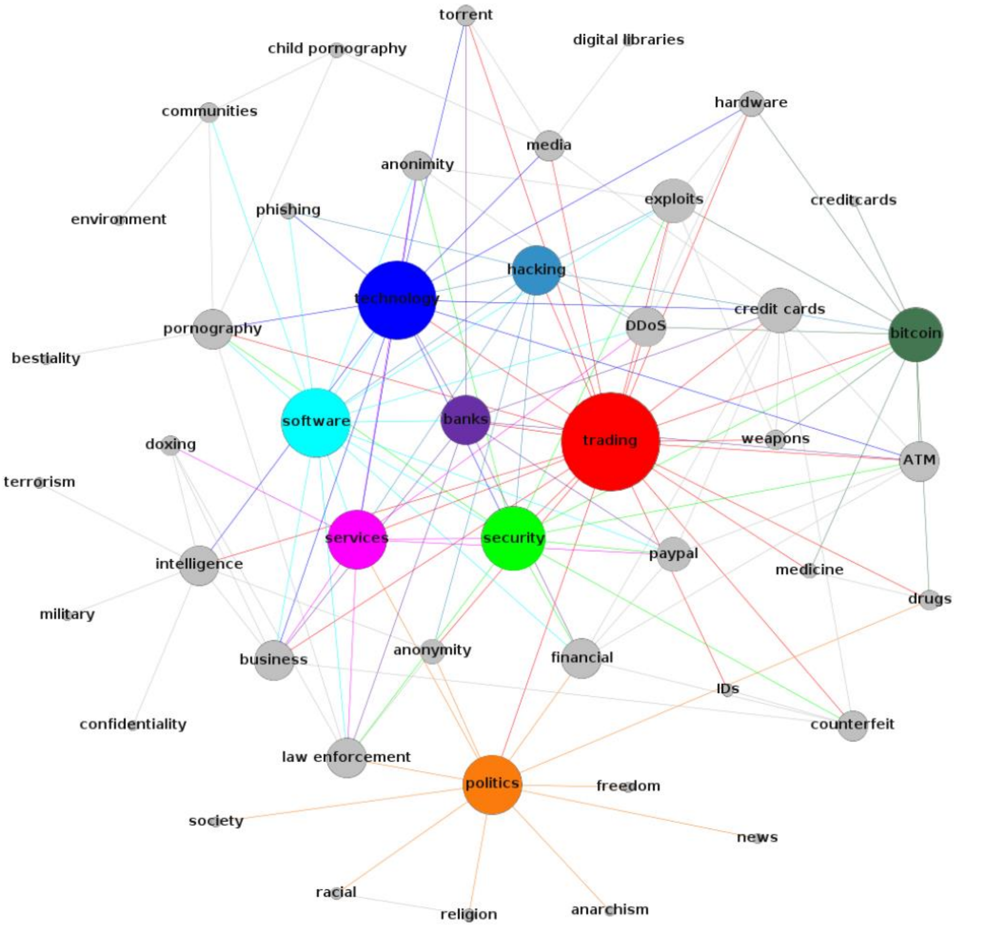


Figure 5.4: Hidden Services on the Darknet

The Darknet network of hidden services makes up the Dark Web. Hidden Services are anonymized through peer to peer services with Onion Routing. **Figure 5.4** shows the hidden services in the Darknet environment and the relationships between them [50].

CHAPTER VI
VIRTUAL PIRAVATE NETWORK

6.1. WHAT IS VIRTUAL PRIVATE NETWORK

Vpn can be briefly summarized as a virtual private network. It is a system that does not use your real IP address to connect to the place to be connected or to be sent using a different IP address. The VPN system has developed due to the need to prevent the data flow provided by companies over a certain communication network from being misused by third parties. It creates a tunnel between communication and another communication point and hides the information with its unique encryption system. In this way, third parties who want to access this data can only see the encrypted data and cannot analyze the data, so the data is protected. The deeper and stronger the degree of encryption in VPN, the more secure the information. Vpn system provides a secure communication network without any security vulnerability over the communication network. Unencrypted data exchange between two communication points can be easily detected by any third user. The vulnerability in this testing can cause harm to companies, the public, or individuals. Attacks are divided into Eavesdropping and masquerading. In the Eavesdropping method as shown in **Figure 6.2**, third parties can listen to the data exchange between two computers without any indication and can receive important and private information such as passwords, and credit cards. Harm may be done to the public or individuals. In the Masquerading system as shown in **Figure 6.1**, on the other hand, a user can access the user's information by appearing as a client or server they want to reach. He can give the fishing technique as the most common example of a masquerading system. The attacker can access your username and password by sending you his site, which looks like a real site, via mail and allowing you to log in [51] .

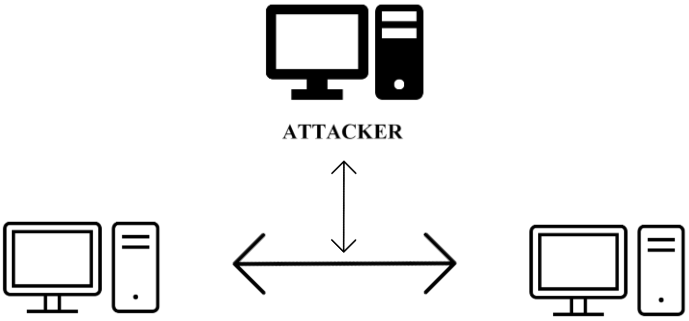


Figure 6.1: Masquereading Attack

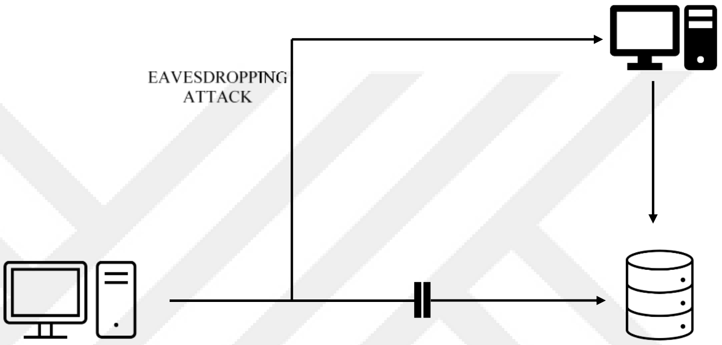


Figure 6.2: Eavesdropping Attack

6.2. HOW VPN WORKS

The VPN hides real IP through the server by connecting with the VPN's remote server. Surfing the internet via VPN ensures that internet service provider (ISP) and malicious attackers cannot access the data. Vpn encrypts online data with its unique cryptosystem. It works as a converter that turns data into meaningless things. For this reason, even if any third party gets their hands on data, it will not mean anything because it is encrypted. VPN creates an encrypted tunnel between network and the network are tried to reach. With the help of a VPN, the computer will appear where the VPN server is. When VPN is connected to the internet with any device, it connects it to a different location virtually. The VPN scheme is shown in **Figure 6.3**. According to this the data goes to the VPN server first. VPN protocols make data pointless and complex. In this way, the data becomes unreadable by third parties. It then connects it to a virtual IP address from the desired network. It is possible to browse the internet over the connected IP [51].

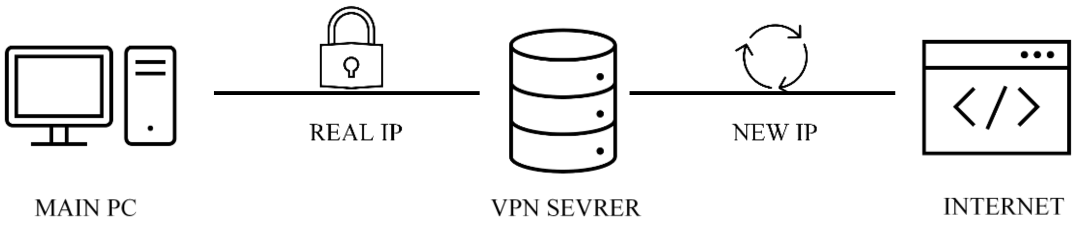


Figure 6.3: VPN Working Schema

6.3. DATA PROTECTION WITH VPN

We can examine the data protection of VPN connections under 3 headings as encapsulation, authentication, and data encryption [52].

6.3.1. Encapsulation (Tunneling)

Billings entering the VPN network are encapsulated as headers. The encapsulated data in this header contains information that will allow them to pass through diagonally during migration. It adds other names on top of the packet's name, allowing it to be hidden by other observers during transit. During tunneling, it allows the capsules reaching the server to pass by reading their original names, and the data transfer process is realized [53].

6.3.2. Authentication

It checks whether the IP trying to access a network is authorized to access this data. It performs this control process using the HTTPS protocol and no outside interference can be made during this control. People who are not authorized to connect to the network cannot connect. There are 3 different authentication methods. These; Point-to-point (PPP), Internet key exchange (IKE), and Data integrity. PPP implements a user-level authentication method and if an authorized person is trying to gain access, it authenticates and allows it to connect to the network. IKE is a computer-level authentication method. This method makes use of the computer certificate protocol. It checks the certificate of the computer trying to log in and allows it to connect to the network if it is authorized. Finally, the data source method uses a special encryption method between the sender and receiver of the data. This encryption method checks whether the information has changed during the transfer phase and ensures that it does not change [54] [52].

6.3.3. Data Encryption

It modifies and confuses data in a way that cannot be understood by third parties monitoring the network. In this way, it encrypts the data and ensures that the people who access this data cannot analyze the data. This decryption process is provided by the key between the sender and the receiver of the data. Only the sender and receiver can decrypt the encrypted data. Encryption methods range from 128, 256, 512, or 1028 bits. While higher bits provide higher data protection, this can cause a slowdown on the network. accesss reason, the fastest encryption method in general, namely 128 bits, is used. There are two types of encryption methods; is software and hardware. The software encryption method access slower than the hardware [54] [52].

6.4. TYPES OF VPN

We can divide Vpn types into 4 titles in general; Site-to-site VPN is Remote Access VPN, Firewall VPN, and User to User VPN.

6.4.1. Site-to-Site VPN

Compared to other VPN types, site-to-site VPN does not provide data communication over a common network. VPN connection access is just like a WAN (Wide Area Network). Intercity and inter-country communication in remote areas access with WAN connection. Networks send data from one connection to the other with the help of a VPN tunnel. As shown in **Figure 6.4** site-to-site VPN connection creates a tunnel between 2 servers that want to provide data flow and connects the two. This connection takes place by providing authentication between 2 servers [51].

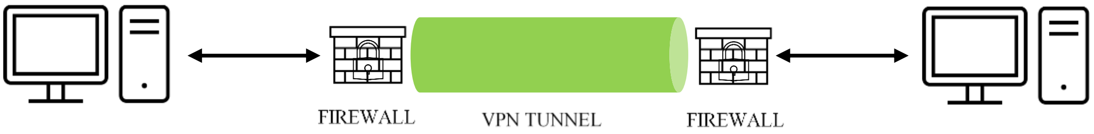


Figure 6.4: Site-to-Site VPN Schema

6.4.2. Remote Access VPN

Users who do not have a computer with access to the public network can access the server on a private network from a distance with this method. A connection is established between the client and the server. A Point to Point connection occurs. The data sent or received is sent over a private network, so the infrastructure of the public network does not affect the speed of this data transfer [51].

6.4.3. Firewall VPN

This type of VPN can be thought of as the use of a firewall in addition to VPNs connected with a tunneling system. This type of VPN generally has an additional firewall due to the security policy of the server. During data communication, 2 firewalls mutually approve each other and the pass is confirmed [51].

6.4.4. User-to-User VPN

Provides user-to-user VPN type data flow with transport mode method [51].

6.5. VPN PROTOCOLS

Every VPN has a VPN protocol running in its background. VPN protocols can be summarized as the case of deciding how to encrypt data. It determines how the VPN forwards data from the computer to the VPN server. Most important of vpn protocols are; OpenVPN, L2TP/IPsec, SSTP, IKEv2, and PPTP [52] [53].

6.5.1. OpenVPN

OpenVPN is an open-source protocol. Since OpenVPN is one of the first used protocols, it is found in almost all VPN brands. OpenVPN's key encryption standard is AES-256 bit. OpenVPN is one of the most secure VPN protocols because it also uses other security protocols. One of the biggest advantages of OpenVPN is that it is used as both UDP and TCP. UDP prioritizes speed while TCP is a more secure protocol [55] [56].

6.5.2. Point-to-Point Tunneling Protocol (PPTP)

The point-to-point tunneling protocol creates a VPN network and provides a seamless transfer of data from a remote client to a corporate server. PPTP creates a private virtual network over multi-protocol networks such as the Internet. PPTP is a network protocol that enables transmission by encapsulating PPP packets [52] [53] [55].

6.5.3. IKEv2

It stands for internet key exchange. It works as a tunneling protocol without privacy and security considerations. Therefore, it takes advantage of the IPsec protocol, which makes use of the AES-253-bit encryption method. IKEv2 is a fast protocol among other protocols. It has mobility and multi-target protocol because it takes advantage of the IPsec package. The multi-destination protocol ensures that traffic is secure even when switching networks. It is the most used protocol in mobile devices due to its mobility and stable speed [52] [53] [55].

6.5.4. Secure Socket Tunneling Protocol (SSTP)

One of the biggest VPN protocols is the sstp protocol. Microsoft and many large companies have this protocol. SSTP is a very secure protocol when compared to other protocols. It takes advantage of the AES-256 encryption protocol, which is one of the popular protocols for encryption [52] [53] [55].

6.5.5. Layer 2 Tunneling Protocol (L2TP)

The L2TP protocol is just a tunneling protocol. It is assisted by the IPsec packet, which uses the AES-253-bit encryption method. From a security point of view, it is not as secure as OpenVPN. It provides the UDP protocol, but the fact that it provides it on connection 500 makes it insecure. One of its biggest advantages is stable broadband support [52] [53] [55].

Table 6.1: Advantages and Disadvantages of VPN Types

VPN TYPES	ADVANTAGES	DISADVANTAGES
OpenVPN	Open Source Strongest Encryption Versatile Use	Sometimes Slow
SSTP	High Security Hard to Block	Only Windows Compatible
PPTP	High Speed Wide Support	Security Gap Web-only
IKEv2	High Speed Numerous Open Source Applications	Limited Platform Support
L2TP	Common Use High Speed	Easy to Block

6.6. VPN AND DARK WEB

Darkweb is a sensitive issue where privacy and anonymity should be given importance. Since the data to be shared when entering the dark web is important, it should be given equal importance to its encryption. Tor, VPNs and pgp methods are actively used as dark web access methods to meet the need for anonymity. There are many intermediary applications that are used to enter the dark web and to surf and use it effectively. There are 3 main elements of the dark web; The browser to be used to enter the dark web, the data encryption technique to be used to prevent the data to be transmitted from being understandable, and the transmission path to transmit the encrypted data in a secure way. Anonymity is a very important element in order to be protected from the dangers and negative elements of the dark web. The browser used to access the dark web, for example tor, is not a sufficient method to remain anonymous on its own. Using the Tor browser also requires assistance from the virtual private network. For this purpose, Nord VPN and Phantom VPN, which are the most used and most reliable VPNs, can be used. The Tor browser uses multi-layered encryption and provides some security by using random routing technique. But using only this method should warn not to share data that should not be shared. Since it does not provide sufficient anonymity and protection, the data wanted to transmit may be in the hands of third parties and pose a danger. Encrypting data like VPN and providing it through a secure way, of course, greatly increases anonymity. A special method designed for dark web login and tor use plays a very important role in meeting this anonymity sensitivity. This method is the Pretty Good Privacy (PGP) method. The working principle of PGP is based on asymmetric encryption. In this encryption method, there are two different keys to decrypt the data, one is a private key and the other is a public key. If the data is encrypted with your public key, person who encrypts the data is the only person who can read that data [57] [58]. In the

Table 6.2 below, vpn and tor comparison according to some categories is shown.

Table 6.2: VPN and Tor Access Comparison

Category	VPN	TOR
Access to censored websites	No	No
Encrypts traffic	Yes	Yes
Hides IP address	Yes	Yes
Protects traffic outside browser	Yes	No
Supports torrents	Yes	Yes, but not recommended
Costs Money	Yes	No

CHAPTER VII
RELATED WORKS

7.1. LITERATURE REVIEW

Various methods have been discussed in darknet traffic detection and categorization.

The main ones are:

- Package and port-based feature extraction
- Graph theory to distinguish between Darknet and Normal traffic
- CNN, RNN and LSTM learning methods
- GAN-based defense mechanisms

Missing detections in Current Methods:

- In package or port studies, obstacles are encountered due to reasons such as hiding or routing the port, assigning a random port, and placing a protocol. Machine learning models achieve high accuracy, but the improvement in F1 score poses a problem.
- FNR (False negative Rate) rate is high in graph theory models [59].

7.1.1. Darknet Traffic Detection

The studies in this section cover the studies that were modeled using the CICDarknet2020 dataset. In studies that did not benefit from this dataset, the data set information they used was shared.

[60] scanned the onion network with the Scrapy Crawler tool. They collected the datasets themselves by developing this tool. They listed 130K onion addresses. They conducted the Naive Bayes classification experiment with TF-IDF (Term Frequency-Inverse Document Frequency) feature extraction.

When a study was done under 300 features, a decrease in accuracy values of the entire algorithm was observed, so they experimented with 300 features. NB test results were compared with SGD (Stochastic Gradient Descent) and SVM (Support Vector Machine). They obtained an accuracy value of 0.935 in the results of the Experiment with Naive Bayes [61] proposed to classify darknet traffic with a two-dimensional convolutional neural network. In layer 1, benign traffic was separated from anonymous traffic, and in the second layer, they created an approach called DeepImage for their method. They carried out a study to classify large datasets. They developed the DeepImage approach using a two-dimensional convolutional neural network, which is a deep learning method. They used the CICDarknet2020 dataset. They calculated the importance values of the features with the CICFlow Meter. The maximum idle value time was listed as the most important feature in traffic detection, and forward packets per second was listed as the most important feature in traffic categorization. 22 features were listed and it was observed that 15 of them were common in both lists. In the DeepImage study, these selected features are used to create images. Multi-Class classification was made. According to the values, the accuracy rate of the model was 95% in the first layer and 92% in the 2nd layer. It included 86% overall accuracy rates in the common performance evaluation.

[62] compared the results of machine learning approach methods and deep learning approach methods . It is aimed to detect and classify dark network traffic. This study started by removing the null values that will increase the performance of deep learning classification. Principle Component Analysis (PCA), DT, and XGB algorithms were used for feature selection. Experiments were performed by selecting 20 important features. The authors experimented on Convolution-Long Short Term Memory (CNN-LSTM) and Convolution-Gated Recurrent Unit (CNN-GRU) deep learning methods to determine traffic type. Machine learning methods are determined as GB(Gradient Boosting), DT(Desicion Tree), RFR(Random Forest Regressor), and XGB(Extreme Gradient Boosting). XGB, which is one of the preferred machine learning classifiers for feature selection, gave the best score compared to other machine learning classifiers with a result of 85%. However, it was observed that deep learning methods gave better results than machine learning methods. As a matter of fact, according to the results, CNN-LSTM was the algorithm that gave the highest success. According to the results, using XGB for feature selection, it gave 96% success

in traffic detection and 89% performance in traffic categorization in CNN-LSTM classification algorithm.

[63] converted the features into a three-dimensional image and made a time-based feature selection. Using the method called DeepInsight, numerical data was converted into image data. A study was conducted on 10 pre-trained models. These algorithms are: Alexnet, ResNet18, ResNet50, ResNet101, DenseNet, GoogleNet, VGG16, VGG19, Inception3, SqueezeNet, Support Vector Machine, Decision Tree and Random forest. Random forest, Desicion Tree and SVM models are trained with these 10 pre-trained algorithm values. The study was conducted to detect malicious activity and traffic type. In the model results, VGG19 gave 96% successful results in traffic data. This rate was given by Random Forest algorithm. AlexNet, which was trained beforehand in Desicion Tree, and VGG19 again in SVM gave the best model performances.

[2] propose Encrypted Two-Label Classification using CNN architecture, which is called ETCC method. CICDarknet2020 dataset is used. 41 features are determined using SFFS (Sequential Floating Forward Selection) feature selection algorithm. CNN algorithm and LSTM algorithm values are compared. In the models, categorical crossentropy is used as loss function, Relu is used as activation function, batch size is 32 and epoch number is 15. While SGD is used in CNN for optimizer, Adam is preferred in LSTM. In this sense, CNN performed better due to intermediate computation processes. 97.65% accuracy rate was obtained.

[64] experimented with ML algorithms using several evaluation metrics. Feature selection has been made using PCA (Principal Component Analysis). It is one of the metrics applied to algorithms in SMOTE. Overfitting was mostly observed before PCA and SMOTE. However, only two algorithms were overfitted after applying PCA and SMOTE. The Extra Tree and Decision Tree network gave 100% accuracy in classification.

[65] experimented with ensemble methods. They tested that they were more successful in classification. The algorithms they used in the models they created were Random Forest, AdaBoost and Gradient Boosted Tree. Boosting is the idea of empowering weak learners. They started with the same weight values in AdaBoost and made weight changes at the points depending on the performances. In Gradient Boosting, they worked by fitting simple parameters. They also modeled with Artifical Neural Network. However, they argued that ensemble models will outperform

artificial neural network models. Among the 3 ensemble models tested, Adaboost gave the best value with a rate of 98%. In the category layer, it gave a 97% success result.

[66] advocated modeling with the Weight Agnostic Neural Network methodology. With the Weight Agnostic Neural Network methodology, darknet traffic analysis was performed to automate the malicious intent detection process with machine learning algorithms. The reason for choosing this methodology is to measure whether it is possible to categorize the potential problem with good performance even when random weights are given. XGBoost gave the highest value with a rate of 90%.

[67] made feature selection by using Chi -Squared statistical score in their models. They handled the instances of classes using the Conditional Generative Adversarial network to balance them. Efforts have been made to improve the precision and recall of classification by creating virtual samples. They modeled multi-class classification with Random Forest algorithm. They observed that the use of GAN had an effect on performance improvement with synthetic sampling. They found the F1 score value as 97.87%.

[68] They used various machine learning methods. Roc analysis is a technique to visualize, organize and select classifiers according to their performance. They performed ROC analysis for good performance values. In the Random Forest algorithm model, the maxium dept was determined as 16 and the estimators were 50. It gave the best results with 8 estimators in KNN. MLP has been successful with 100 hidden layers. In Gradient Boosting classification, they achieved successful results with 100 estimators. They achieved 98% success with Random Forest in classification and traffic detection categories.

[59] proposed the Stacking Ensemble (SE) model. They used Forward-Sequential Feature Selection (Forward-SFS). They have done their work in 3 models using Random Forest, K-Nearest Neighbors. They used the CIC Darknet 2020 dataset. Model Fast Gradient Sign Method (FGSM), Basic Iterative method (BIM), DeepFool and Boundary attack were evaluated as the strongest competitors of this model and the model was tested against them. The accuracy rate was 98.89% in the SE model, and 97.88% in the categorization.

[69] worked on the Gradient Boosting algorithm model with the CICDarknet2020 data set. 70% was reserved for training and 30% for testing. An accuracy rate of 99.8% was obtained. The Boosting number was given as 100, the learning rate was determined as 0.1 and the maxium dept 3, and a high accuracy rate

was obtained. They also modeled with 6 other machine learning methods. 87% success rates in K Neighbors Algorithm, 78% in Logistic Regression, 98% in Random Forest, 82% in Support Vector Machine, 70% in Linear Discriminant Analysis, %96 in Extra Tree Classifier has been obtained.

[70] performed validation, integration and analysis using CICFlowMeter. 33 features with information gain values above 0.3 were selected. The test data was set as 0.8 training 0.2 tests. K-Neigbors Network algorithm model was created. By repeating k values from 1-55 for the best k value, the best k=1 96.17 accuracy value, 92.21% precision value, 92.39% recall value and a recall value become 1. f-value of 1 point is 92.30%.

[71] applied both classical machine learning techniques and deep learning architectures with SVM (Support Vector Machines), RF (Random Forest), CNN (Convolutional Neural Network), AC-GAN (Auxiliary Classifier Generative Adversarial Networks) models. Using SMOTE (Syntetic Mimority Oversampling Technique) in their classification model, they found that Random Forest is the most effective algorithm for traffic detection and classification of application types. RF gives the highest value by providing the SMOTE balance. This rate was 99.9% in traffic detection and 92.3% in classification. If the SMOTE balance is not used, the RF’s success rate declining to 80%.

[72] developed declarectinal Long Short Term Memory (Bi-LSTM) models using a one-dimensional convolutional neural network in their study. They identified two types of feature selection as content features and side channel features. Side channel feature was applied for selection of the most important feature content. They used the MLP (Multi Layer Perceptron) algorithm to determine the side channel features. They achieved a multi-class accuracy of 92%.

IoT networks are subject to various cyber attacks. [73] studied the performances of Darknet traffic detection systems in IOT networks. They used supervised machine learning technique. These; DT (Desicion Tree), BAG-DT (Bagging Desicion Tree Ensembles), ADA-DT (AdaBoost Desicion Tree Ensembles), RUS-DT (RusBoosted Desicion Tree Ensembles), O-DT (Optimizable Desicion Tree), O-KNN (Optimizable K-Nearest Neighbor), O-DSC (Optimizable Discriminant). In BAG-DT, an accuracy of 99.50% was obtained compared to other techniques.

[74] They proposed a deep neural network system called Tor-VPN detector with 79 input artificial neurons and 6 hidden layers. They worked on their models

without using preprocessing technique and feature extraction technique. They argued that it was solvable through high-class imbalance. They used activation function relu in the hidden layer and softmax in the output layer. They achieved a high success rate by using Sparse categorical cross entropy as the loss function, using adam as the optimizer, choosing 100 as the epoch number, setting the batch size as 64 and setting the validation split to 33%. Model values showed a success of 96%.

7.1.2. Vpn Traffic Detection

The studies in this section cover the studies that were modeled using the ISCXVPN2016 dataset. In studies that did not benefit from this dataset, the data set information they used was shared.

It is aimed to analyze the encrypted traffic passing through the virtual private network. MLP (Multi Layer Perceptron), RFT (Random Forest Tree) and KNN (K-Nearet Neighbor) algorithm models are proposed by [75]. The MLP model consists of two hidden layers. There are 30 neurons in the first layer and 15 neurons in the second layer. The activation function is hyperbolic tangent. Conjugate gradient was used as the learning algorithm. Test-trained with the epoch 5000. In the KNN algorithm model, the neighbor number parameter is set to 50. In the Random Tree method, classifier type Bag is used and the training cycle is 150. They obtained very close values in all their experiments. In their experiments, they found that the classifiers work better when using short values of time parameters. Random Forest model gave the best value.

[76] proposed the K-RUSboost algorithm model and the AdaBoost model. First, they trained the model with Adaboost to improve the detection effect. Then, they analyzed the abnormal traffic detection with the K-RUSboost algorithm. They combined these two algorithms and applied them in a single method. As a result of these experiments, they observed that the changes made to increase the recall rate also increased the false positive rate.

In this research, [77] aimed to classify VPN network traffic flow by designing ANN model on Apache Spark. In the research, VPN and non-VPN data are first classified and then categorical classification is made. It achieved 96.76% VPN classification success.

[78] modeled using CAE (Convolutional Auto-Encoding) and CNN (Convolutional Neural Network) to achieve the experimental objectives. In CNN model, image size was studied with 39x39 matrix. SGD was preferred for weight

adjustment. Batch size is set as 50, and the number of epochs is given as 20,000. In the CAE based method, the batch size was determined as 100 and the number of epochs was determined as 200. Adam was used as an optimizer. In the two-category definition, CAE gave the best performance value with a rate of 98.77%. In the 6-category measurement, CNN gave the best results with 92.92% values.

[79] proposed an approach called DSRR (Differentiation of Sliding Rescaled Ranges). They obtained a precision of 0.97 with DSRR and Random Forest in the model they used to characterize traffic and separate VPN-non-VPN data. With 2D CNN, they obtained a precision of 0.93.

In this study, [80] analyzed SSL VPN encrypted traffic. A neural network called CaspsNet (Capsule Neural Network) is used to recognize SSL VPN. CapsNet replaces the sampling layer with two new layers. The first layer is the convolutional layer, the second layer is the basic capsule layer, and the third layer is the digital capsule layer. They used the squashing function as the activation function. They observed that their proposed model achieved 99.98% success when compared with RF (Random Forest), C4.5, CNN (Convolutional Neural Network) and SVM (Support Vector Machine) algorithms.

[81] proposed the Accumulated Generalized Mean Value (AGMV) method. They observed that the combination of AGMV and Random Forest gave much better results. Therefore, they found that good results can be obtained when AGMV is combined with complex classifiers with flow-based parameters. They detected encrypted and unencrypted traffic, then classified the traffic categories separately. At the same time, they combined the AGMV algorithm models with the random forest algorithm they used together and got the best results compared to their other scenarios.

[82] suggested the PCNN (pruning convolution neural network) method. With the rapidly developing technology, they developed this method, thinking that the original traffic classification methods were not sufficient. Extract feature is not done manually, they argued that high-level features can be extracted together with CNN. They suggested that with pruning technology, the model would be simplified and important features could be determined. Thus, they argued that this method would reduce the model size and computations. They achieved better performance when pruned with a larger weight value in the model. They stated that this model showed an improvement of 94%.

Machine Learning based network traffic classification method is the most common method in traffic classification studies. [83] offer GAN (Genarative Adversarial Network) architecture, which argues that the approach to achieve high accuracy that does not take into account the zero imbalance of ML algorithms and the unequal distribution of internet traffic can cause performance degradation. They proposed the ITCGAN method, which they aim to create an adaptable, stable model. The model framework consists of 3 parts. These are Traffic Vectorization, Pre-Training and Formal Training.

[84] proposed the Graph Neural Network (GNN) model. The reasons for choosing GNN are as follows: since it accepts stream data containing an arbitrary number of packets, because it allows network traffic flows to be easily converted to a non-Euclidean space in GNN, it allows for global attribute increments such as packet length and duration values. All these preferences have revealed that they can preserve data accuracy, prevent data loss, and preserve the original properties of streams. They used SplitCap in data segmentation in their models. They benefited from dropout regularization and used cross entropy as a loss function, they used adam as an optimizer, they set the batch size as 128 and they benefited from 500 epochs. According to the recall, precision and f1 score results in the detection values of each category, they achieved performance results with values over 90%.

[85] proposed a classifier for encrypted network traffic based on prototypical networks and taking advantage of distances to class prototypes. They used the Mahalanobis distance. They used a mix of wavelet transform coefficients as input in addition to data from the dataset for segment and class estimates of bidirectional network flows. The model is structured as fully connected hidden layers, each 64 neurons, relu activation, 25% dropout between 2-3 and 3-4 layers in weights. They were 98% successful in predicting the most likely categories of traffic.

[86] suggested the surge period-based feature extraction method. In this preference, they made a choice in order to get as many traffic flow features as possible. In order to solve the problem of not being able to influence the identification of unknown traffic in their model, they preferred JigClu with a self-supervised learning approach. It is aimed to use Self-Supervised learning in the training phase in unstable traffic. The study showed a success rate of more than 74% in the classification of unknown traffic.

[87] conducted experiments with algorithm models of k-Nearest Neighbors (KNN), Artificial Neural Network (ANN), and Random Forest (RF) to classify network data streams. They distinguished VPN and non-VPN data in all model scenarios and then looked at the correct detection rates of application data categories in 7 categories. Among them, the RF (Random Forest) model gave the most refiend result with a rate of 85%.

[88] offer RF (Random Forest) model with 4 categories of traffic characteristics based on TPC (tunneling protocol characteristics). TPC features; Cummulative Sums (pk_cnt, pad_bytes) is the total number of packets, the total payload bytes, and the ratio of the maximum payload bytes in the forward and reverse stream to the total payload bytes; second is payload size (max_pad_size,Mean and min pad size) is the maximum value, average and minimum value; Packet Inter-Arrival Time(max_pk_iat,Mean and min ph_iat) are packet interval time, maximum, average and minimum values; Standard Entropy (pad_size_ep, pk_iat_ep) is standard entropy of packet payload size, and standard entropy of inter-arrival time. They achieved an accuracy rate of 95.3% in the modeling using TPC.

7.1.3. Tor Traffic Detection

The studies in this section cover the studies that were modeled using the ISCXTor2016 dataset. In studies that did not benefit from this dataset, the data set information they used was shared.

[61] preferred CfsSubsetEval + BestFirst (SE + BF) and Infogain+ Ranker(IG + RK) algorithms for feature selection in separating Tor and NonTor data. They did time-based modeling, so they worked with time-dependent features in feature selection. They worked with ZeroR, C4.5 and KNN algorithm models to separate these two classes. Random Forest, C4.5 and KNN algorithms were used to classify traffic data in 8 categories. It was successful in TOR data detection with a C4.5 accuracy rate of 94.8%. Zero R recorded low data in all experiments compared to other algorithms. In classification, more successful results were obtained in the experiment with the Random Forest algorithm model.

[89] used CFS feature selection and modeled on 28 features. Artifical neural Network (ANN) and Support vector Machine (SVN) algorithm models are presented. Levenberg-Marquardt training function (trainlm) is used in the ANN model. The results were higher with the selected feature selection algorithm. An accuracy

performance of 99.8% was obtained in the ANN model. In SVM, this result was observed as 88.1%.

Considering that packet length is effective in detecting traffic, [90] proposed a signature extraction based approach based on packet length. They carried out their work on 9 features. Considering that the network can change easily, they avoided time-based feature selections. They developed the J48 desicion tree algorithm model to determine the network traffic classes. They reached a balanced and effective modeling result with the accuracy value of 91%.

[91] worked with ML models. Analysis was performed using IBMAutoAI to determine the best values among these algorithms. With AutoAI, the dataset is split into 2 datasets and selects the 2 best ML algorithms and creates a pipeline. Performance, accuracy, sensitivity are measured using the ROC curve. The best performance values were observed in Extra Trees and Random Forest algorithm models.

[92] have been modeling tests with ML algorithms. Decision Tree gave the best results among them. Models achieved better results with increasing timeout values. ZeroR showed the highest change in tests with balanced and unbalanced dataset. With its balanced dataset, it showed a great loss of performance. In classification scenarios, on the other hand, as timeouts increased, performance values decreased. Rates decreased in all models except DNN. The best performing was the Random Forest algorithm model.

[93] proposed a deep learning architecture called Servername Protocol Packet Network (SPPNet) for the classification of real-time network flow. They created a convolutional architecture with the ResNet18 algorithm. In their experiments, they first identified the immutable features of a package, then measured the relevance of the reference model results with deep learning approaches. GradCAM was applied to test data in bit format in seven packages in two-dimensional representation. According to the obtained values, it was observed that the best hypothesis evaluation was 0.84 with the combination of packet, port, protocol and server name.

[94] proposed a Convolutional Neural Network (CNN) model. Relu and Sorftmax are used in the fully connected layer as the activation function. Adam was preferred for optimization. In the test results, they achieved 99.9% success in distinguishing traffic and 97.2% in classification.

[95] proposed a two-dimensional CNN model. They preferred to use the sigmoid activation function in the model. Cross entropy loss function and RMSProp (Root Mean Square Prop)to update weight and bias were preferred for optimization. They achieved a success rate of 95.47%.

[96] applied random oversampling and random undersampling in their models to avoid data imbalance. To increase efficiency, they used k-fold cross-validation and Grid Search algorithms for hyperparameter tuning. After data processing, the model was studied with 7 machine learning algorithms. Success performance values of over 90% were obtained in machine learning models created by considering these values. The algorithm model that gave the best results was Random Forest (RF) in undersamling F1 score analysis with 98.6% and oversampling F1 score analysis with 99.7%. It was followed by Desicion Tree, K Nearest Neighbor, Adaboost, SVM and Logistic Regression, respectively.

[97] worked with models of deep learning algorithms and intrusion detection prevention algorithms. While they preferred DNN, CNN and LSTM in deep learning, they performed their experiments with FGSM (Fast Gradient Sign Method), BIM (Building Information Modelling), MIM (Micro Independent Metering) and CW (Clarke Wright) in intrusion detection algorithms. These preferred attack algorithms are white-box attack algorithm based on fuzzy strategy and a black-box attack algorithm based on smooth data enhancement. Among the intrusion detection algorithms, MIM had the best performance in white box attacks. DNN and LSTM achieved an obfuscation rate of 90%. In black box attack, LSTM again showed the best performance in obfuscation success rate. It is concluded that CNN has stronger robustness.

[98] proposed a two-dimensional convolutional neural network model called DOC-IDS. Three different loss functions are used in the model. In addition to regular traffic data, they also included multi-class labeled traffic data in their study for feature extraction. Variance minimization was applied to distinguish between normal and abnormal data. With this study, they achieved high performance value in detecting high anomaly. They worked with USTC-TFC2016, ISCXTor2016, ISCXVPN2016, Bos 2018 and CIC-IDS2017 input and target datasets. In their work with BOS 2018 dataset data, they obtained higher accuracy values with DOC-IDS.

CHAPTER VIII
METHODOLOGY

8.1. CLASSIFICATION

The most important feature of machine learning is discrimination. The most used algorithm types of supervised algorithms are Regression and Classification. Regression Problems are used to generate real-valued real output. Classification algorithms are used for discrete output. It can be performed on structured and unstructured data. The type of data to be predicted can be label or category. Classification algorithms ensure the best separation of labeled products. The main purpose of the classification algorithms is to categorize the new incoming data in the best way with the experience gained from the previous data. It is necessary to choose the best algorithm according to the data types contained in the dataset. The algorithm that works best in one dataset may not work best in another dataset. Good or bad results can be obtained according to the application forms of the algorithms applied on the dataset. Algorithm and algorithm features should be tested with trial and error methods. Thus, the algorithm that gives the best result is used. In order for the algorithms to work correctly, the Dataset must be pre-cleaned. Empty or undefined data should be replaced with values (median) similar to the meaningful data in the dataset. A clean and concise dataset is created by unifying the repetitive inputs with the same feature. In this way, classification algorithms draw polynomials that more sharply separate the labels to be classified. Label names are given to define the type of data on the dataset. It is used to classify data during Training or Testing. As an example of classification algorithms, it is ensured that our inbox remains clean through algorithms that detect whether the messages in our mailbox are spam or not. If we categorize the e-mails received in our e-mail correctly, for example, if we mark an unsolicited message as spam, the classification algorithms of the e-mail service providers improve themselves in line with this information. Taking this into account in the next incoming messages, it moves the messages that we do not want to receive to the spam box.

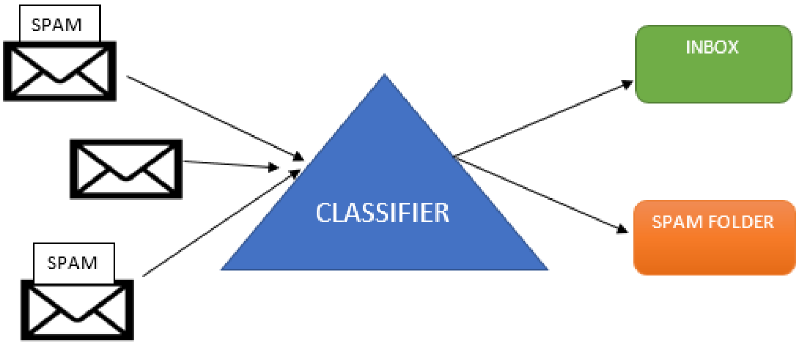


Figure 8.1: Parsing Spam Mails with Classification Algorithm

In **Figure 8.1**, parsing spam mails with classification algorithms is shown. The way of learning in ML takes historical data as input. It trains itself with these inputs. As a result, if the evaluation achieves an output above the score threshold, it is used. Otherwise, training is strengthened by providing more data. If the results still do not pass the evaluation threshold, the data is preprocessed or a new algorithm is preferred [99].

8.1.1. Classification Terminology

- *Classifier:* An algorithm that maps inputs to class. Example: Random Forest, K Nearest Neigbor
- *Classification Model:* It is the model created to predict the class of the inputs. Predicts class labels for new data.
- *Features :* It is the data containing scalable data in the data set we are analyzing. It is displayed as a column.
- *Binary Classification:* It is a classification with two outputs. Example: [Yes, No], [Good, Bad]
- *Multi-class Classification:* Classifications made according to more than one output. Example: [Good, Bad, Normal]
- *Multi-label Classification:* Outputs based on more than one label. Example: A news article can be about sports, a person, and location at the same time.
- *Train-Set:* It is the dataset created to train the model.
- *Test-Set:* It is the dataset created to test the Trained Model.
- *Evaluation:* These are the methods used to analyze the test result [100] [99].

8.2. NEURAL NETWORK

Artificial neural network algorithms are inspired by the human brain. Artificial Intelligence Algorithms are expected to show features such as learning and discovering, which are the characteristics of the human brain [101]. Artificial neural networks are a mathematical modeling inspired by neurons in the human brain. Learning processes in artificial neural networks are provided by giving sample data. Neurons that make up artificial neural networks perform complex operations. They have learning abilities. They can produce results for unseen outputs. They can make pattern identification and classification. They can complete the missing pieces. They can process real-time information. Artificial neural networks can be mainly used in areas such as classification, diagnosis, predictive control and interpretation. Usage Areas of Artificial Neural Networks; Computational Biology Tumor detection, DNA sequencing Energy Production Price and load forecasting Natural Language Processing: Voice assistant.

The creation of similar artificial models by examining the behavior of living things and modeling them mathematically is called cybernetics. What is desired to be obtained from these models is to create models that imitate the human brain with trainable, self-learning and evaluation neural networks.

Parts of artificial nerve cells

1. Inputs: Inputs are the information coming to neurons.

2. Weights: The inputs to the artificial nerve cells are multiplied by the weight of the connections. It provides an effect on the outputs to be produced from the inputs.

3. Addition Function: The additive function is the function that we obtain the net input of that cell by taking the sum of the product of the inputs to the artificial neuron with the weights.

4. Activation Function: It is the function that takes the weighted sum of all the inputs in the previous layer and produces the output value and passes it to the next layer. **Figure 8.2** includes Activation Function graphics and formulas.

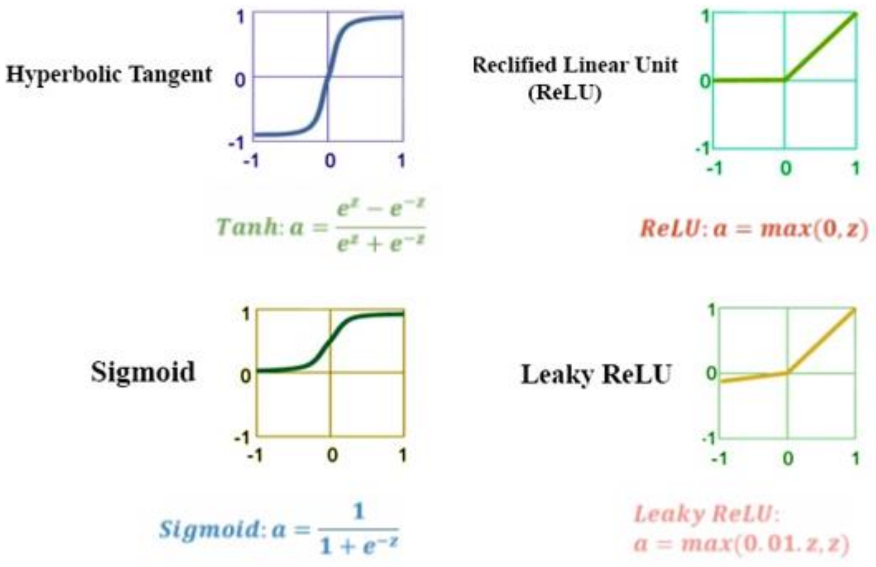


Figure 8.2: Activation Function

5. Outputs: The outputs from the activation function are the output values. Cells can have multiple inputs but only one output. These outputs can be linked to another cell as input.

The artificial neural network model consists of 3 main layers. These are Input Layer, Middle Layer and Output Layer. The middleware can be duplicated. Neural networks consisting of many neurons and hidden layers are called Multilayer Neural Networks. If it consists of a single layer, it is called a Single Layer Neural Network [102]. In the following sections, information will be given about the algorithm methods used primarily and included in the model. Afterwards, the details of each model and the results of the application will be given.

8.2.1. Artificial Neural Network (ANN)

It consists of neurons. Each neuron takes input and generates output by adding certain weighting values. The outputs of each Neuron until the last layer enters the next neurons as inputs. During the training period, the weight values try to be adjusted.

When the inputs to be estimated are sent to the adjusted weight values, it is ensured that it does not classify according to the training result [103]. The ANN model is shown in **Figure 8.3.**

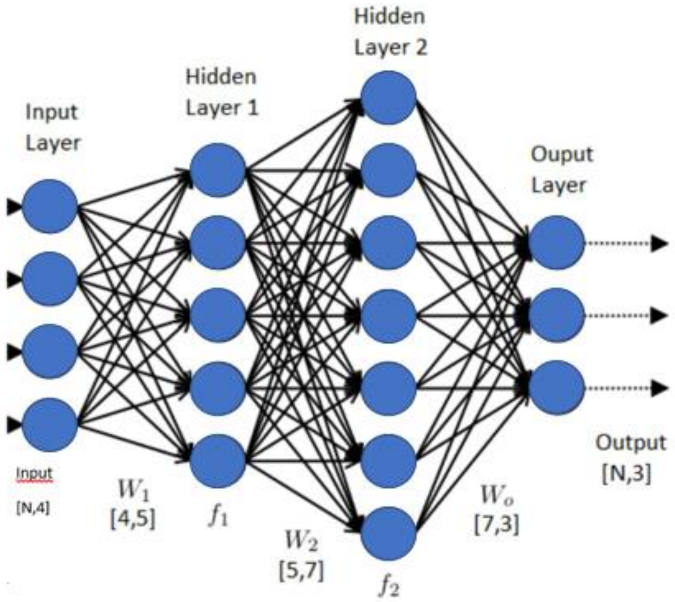


Figure 8.3: Artificial Neural Network

8.2.2. Multilayer Perceptron (MLP)

MLP is a fully connected feed-forward artificial neural network (ANN) class. An MLP consists of at least three node layers: an input layer, a hidden layer, and an output layer. Except for the input nodes, every node is a neuron using a nonlinear activation function. MLP uses a supervised learning technique called back propagation for training.

8.2.3. Convolutional Neural Network (CNN)

It is the most mature algorithm used in deep neural networks to produce better results in computer vision than human. It consists of Convolution layers created by scanning each pixel in a dataset. These objects can be used for identification, classification, etc. It can be used for things. As examples of CNN, we can give Google Translator and Google Lens. CNN can also be used for problems not related to vision [101].

8.2.4. Generative Adversarial Networks (GANs)

The GAN method was developed by Ian et al. in 2014 [104]. GAN uses unsupervised learning to increase model accuracy and efficiency. Creates new data samples that resemble training data. It is a generative deep learning algorithm. GAN has 2 components. It is a generator that produces fake data and a discriminator that learns from misinformation. Among the usage areas of GAN; video game resolution development, improvements to astronomical images, creating cartoon characters, creating 3D objects. In Gan modeling, fake data is generated during initial training. The discriminator learns to distinguish between real data and fake data. The GAN sends the results to the generator and discriminator to update the model [101].

8.2.5. Recurrent Neural Network (RNN)

RNN records the output of a layer and feeds back the output to the input to predict the output of the layer with feedback. RNN has a memory that remembers the output values. It uses the same parameters in each input, as it does the same task in all layers to produce output. This reduces the complexity of the parameters [105].

8.2.6. Long short-term memory (LSTM)

LSTM models were proposed by Hochreiter and Schmidhuber in 1997. In the training phase of RNN models, the results of the previous step are also used to calculate a current value. Therefore, there is a short-term memory in RNN models. Basically, in LSTM, an input is combined with the previous step results. It is then filtered from a forget layer and taken as an input to the training model. With this structure, it has a longer-term memory than RNN and therefore generally gives better results in the analysis of data containing dependency structure [106].

8.3. DATASET

The dataset used in this study has been publicly shared by the University of New Brunswick's Canadian Institute for Cybersecurity. The dataset used in this research is the dataset obtained by the Canadian Cyber Security Institute by listening to real darknet traffic.

It is a dataset created by combining ISCXTor2016 and ISCXVPN 2016 datasets for the examination and characterization of darknet traffic. TOR and VPN traffic data are discussed together. There is a two-layer structure in the CICDarknet2020 dataset, and in the first layer, there is data suitable for a modeling that generates benign and darknet traffic, and in the second layer, deduces which applications the detected darknet data represent. The original data consists of 85 columns and 141,530 rows.

The scopes of traffic types as follows:

- *Browsing:* HTTP and HTTPS traffic generated by users while browsing,
- *Email:* Traffic samples generated using IMAP, POP3 and SMTP protocols,
- *Chat:* identifies Instant messaging applications,
- *Audio-Streaming:* Require a continuous and steady stream of data,
- *Video-Streaming:* Identifiessteady stream video applications,
- *File Transfer:* FTP over SSH (SFTP) and FTP over SSL (FTPS) traffic sessions,
- *VoIP:* The Voice over IP label groups all traffic generated by voice applications,
- *P2P:* downloaded .torrent files from the Kali linux distribution.

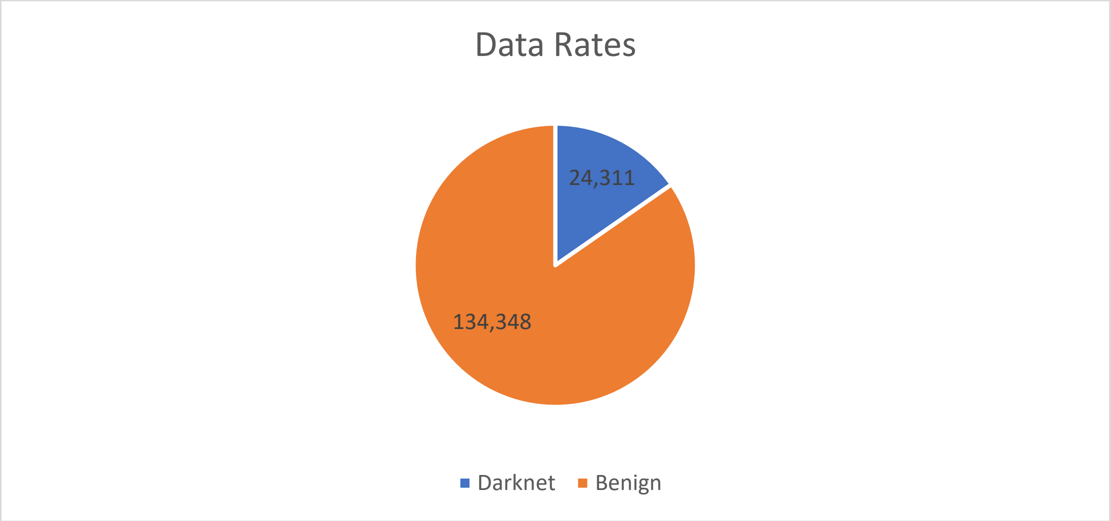


Figure 8.4: Darknet and Benign Data Rates

In **Figure 8.4 ,** the total numbers of darknet and benign data in the dataset are given. **Figure 8.5** shows the application rates obtained as a result of listening to darknet traffic.

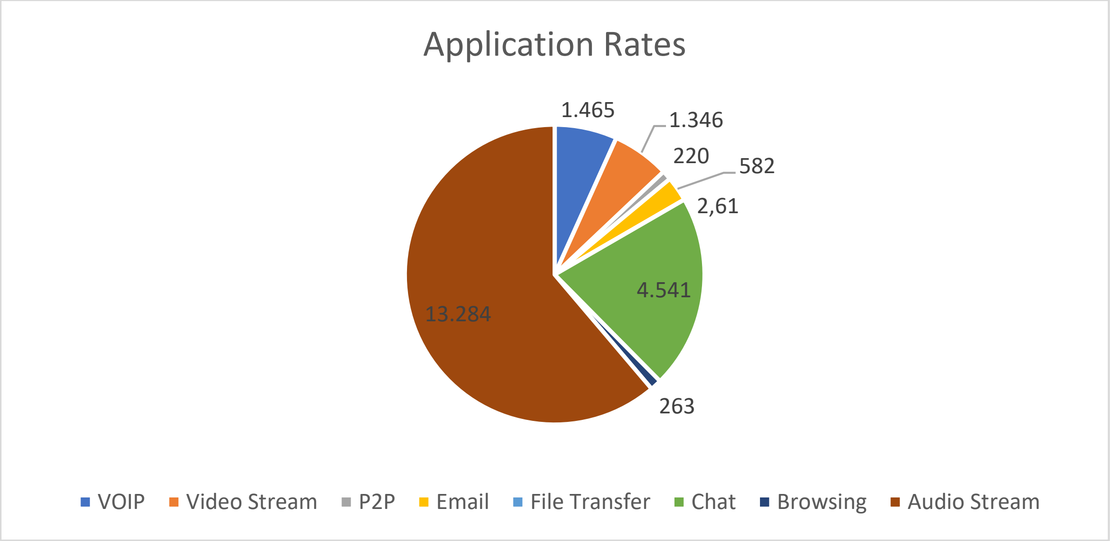


Figure 8.5: Application Rates

The dataset contains 81 features for traffic network detection and categorization. **Table 8.1** lists these features and their descriptions. The fields specified in parentheses in this are included as separate features in the dataset.

CIC developers have categorically stated that Source IP, Destination IP, Source Port, Destination Port and Protocol resources are not suitable for classification, and that the variability of the data will cause difficulty in obtaining accurate results. For this reason, Source IP, Destination IP, Source Port, Destination Port and Protocol fields are not taken into account in this study as they may vary.

Table 8.1: Features Details in Dataset

Feature	Description
Idle Time	(Mean, max, min, std) The amount of time the flow was idle before it was activated
Active Time	(Mean, max, min, std) The amount of time the flow was active before it was idle
Forward seg size min	Minimum segment size in the forward direction
Forward Act Data pkts	Number of packets with TCP payload
Init win bytes	(Forward and Backward) Number of bytes sent
Subflow bytes	(Forward and Backward) Average number of bytes of subflow
Subflow packets	(Forward and Backward) Average number of packets in a subflow
Bulk rate avg	(Forward and Backward) Average number of bulk rate
Packet/Bulk avg	(Forward and Backward) Average number of packets bulk rate
Bytes/Bulk avg	(Forward and Backward) Average number of bytes bulk rate
Segment size avg	(Forward ,Backward and Flow) Average size
Average packet size	Average size of packet
Ratio	Down and up Ratio
Header length	(Forward and Backward) Total bytes used for headers
Flag count	FIN, SYN, RST, PSH, ACK, URG, CWE, ECE packet counts
Flags	(Forward and Backward) PSH, URG times
Backward IAT	(Total,max,min,mean,std) Time between two packets sent in the backward direction
Forward IAT	(Total,max,min,mean,std) Time between two packets sent in the forward direction
Flow IAT	(Total,max,min,mean,std) Time between two flows
Packets/s	(Forward and Backward) Packet for second
Flow packets/s	Packets transferred per second
Flow bytes/s	Bytes transferred per second
Flow packet length	(Variance,max,min,mean,std) Length of a flow
Length of packet	(Forward and Backward) (Total,max,min,mean,std) Size of packet
Packet	(Forward and Backward) Total packets
Flow duration	The duration of the flow
Protocol	The protocol of the flow
Port	Source and Destination
IP	Source and Destination

8.4. PREPROCESSING DATA

If there are outliers in the dataset, scalable data or transformable data, a reaction should be taken accordingly. Considering that it can make a huge difference in the model effect, one or more of these processes can be applied.

8.4.1. Data Cleaning

In the research application, the data preprocessing step was carried out first. This step includes checking and removing inconsistent data, removing duplicate data, and updating what needs to be corrected with correct data. Cleaning up empty and missing data allows to obtain efficient values in data training estimation results. These missing and empty data may have been interrupted during data transfers or experienced errors for other reasons. In order for the analysis process to be efficient, these values should be compared to middle values even if they are not removed. With this method, the amount of data, deviation rate, average values and the lowest value, which is our main goal, can be displayed proportionally. Nan Infinity and object values are determined. After these determinations, the values that would not affect the analysis process positively were removed or replaced with mean values. As a result of data preprocessing, the number of columns in the new data set was 74 and the number of variables was 117,073.

Table 8.2: Table of Clean Values

Traffic Category	Application	Benign Data	Tor Data	VPN Data	Total
Audio-Stream	Vimeo and Youtube	4780	121	13060	17961
VOIP	Facebook,Hangouts,Voice calls and Skype	2101	298	1167	3566
Browsing	Chrome and Firefox	32451	263	0	32714
Video-Stream	Youtube and Vimeo	8421	202	1144	9767
Chat	Skype,Hangouts,Facebook,AIM and ICQ	6937	65	4476	11478
P2P	BitTorrent and uTorrent	24150	110	0	24260
Email	IMAPS,POP3,SMTP	5563	13	569	6145
File Transfer	Skype,SFTP	8572	107	2503	11182
Total		92975	1179	22919	117073

8.4.2. Normalizing

Normalization allows dataset values to be smaller without changing their essence. It is among the basic steps to increase model accuracy. At this stage, the most preferred normalization methods are Feature Scaling, Z Score, RobustScaler, StandardScaler. The Min Max Scaler scales all values in the data. The Standard Scaler is normalized by taking the average of each value and dividing it by the standard deviation. In Robust Scaler, it should be used if there are outliers in the data. In this research application, StandardScaler normalization and Min Max Scaler were performed to ensure that the data values do not remain in large scales and conform to the real values.

8.4.3. Feature Selection

The feature selection technique is applied by reducing the number of input variables and eliminating unnecessary or irrelevant data. After this process, the related processes with the model are narrowed down and the useful model is created. With proper application of feature selection, overfitting is reduced, accuracy is increased, and training time is reduced. Various feature selection methods are available. By using statistics with these methods, by comparing the relations between the input variables and the target variable, it is ensured that the input variables with a strong relationship are determined. For these reasons, care should be taken in choosing the right feature [107].

8.4.3.1. How to Choose Feature Selection

One of the issues that should be preferred is which of the supervised or unsupervised feature selection methods will be selected. Unsupervised feature selection ignores the target variable, while supervised feature selection does. The area to be determined in feature selection with supervised modeling is wrapper, filter or Intrinsic feature selection methods. In Wrapper feature selection methods, many models are created with input features and feature selection is made according to the model values that give the best result according to a performance criterion value. In the filter method, it evaluates the relevance between each input and target variable and models predictors that fit the criteria. Another controlled feature selection method is the intrinsic methods. With this method, it is possible to make automatic feature selection during training. Neither the best set of input variables nor the best machine learning algorithm can be selected, nor can the best feature selection method be chosen. According to the data studied, the best experiments should be done statistically. Examples of feature selection algorithms encountered in the literature review are mentioned below [107].

8.4.3.2. Select K-Best

In this study, select K-Best feature selection is applied. In order to run the algorithms with less variables in the dataset, the K-highest score (SelectKBest) of the feature selection algorithms was applied. The K-highest score algorithm is also among the supervised algorithms. In this method, a score is calculated to measure the explanatory ability of the explanatory variables on the explained variable, and k of them are added to the final model, starting from the variable with the highest score to the lowest.

In this study, the mutual_info_regression method under the Python Scikit library was used to measure the annotation ability of the variables. According to this method, the amount of mutual information between two random variables takes non-negative values. This value is equal to zero if and only if two random variables are independent and grows as the dependency between the variables increases.
The feature selection algorithm was applied in this study as follows:

Table 8.3: Select K-Best Algorithm Pseudocode

Algorithm : Select K-Best

```
all_dataset = Read Dataset ;
best_accuracy = mlp_model(all_dataset) ;
k= MIN_FEATURE ;
While k<MAX_FEATURE
    d= The set of variables specified for k ;
    res = mlp_model (d) ;
    if(res> best_accuracy)
        best_accuracy = res;
    End
    k++;
end
```

8.4.4. Eveluation Metrics

Accuracy and F1 score measurements are used for the performance values of the classifiers. Accuracy includes the sum of correct prediction values. F1 score is the weighted average value of precision average and recall metrics. They give the scoring results with 1 being the best for these two values. Precision measures the proportion of correctly classified samples for the positive class, and recall measures the total number of positive class values classified [71].

$$Accuracy = \frac{Correct\ Classification}{All\ Classification}$$

$$F1\ Score = 2x\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

$$Recall = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

8.5. IMPLEMENTATION

The first modeling studied is RNN (Recurrent Neural Network). LSTM (Long-Short Term Memory) method, one of the machine learning algorithms, is used in the categorization of the data for second model . The third model study is with the MLP method. In the categorization of the data, new data sets were produced with GAN (Generative Adversarial Networks) in LSTM (Long-Short Term Memory) and MLP (Multi-layer Perceptron) methods, which are machine learning algorithms, and used as training data for other methods. In order to further improve the model results, the LSTM and MLP algorithms were reconfigured for the second layer as both multi-category and two-category. In addition, the Feature Selection algorithm has been applied to remove the variables with low explanatory ability from the model. By making 3 model studies, it was observed with which algorithms and features the best values were obtained.

8.5.1. RNN Model

First model classifies the traffic analysis data set as benign or darknet traffic. This model is Layer 1 of classifying the Dataset. At layer 1, the RNN model is trained to predict the outcome of benign and darknet traffic. The data given to train the model has been pre-cleaned. Overfitting is prevented by removing duplicate lines from the dataset. The test and training set for the model are set to 20 and random state 40 using the train test split algorithm. It has been observed that if these ratios are changed, it affects the educational success negatively. The best test separation ratio was determined as 0.20. The total data sizes allocated for Testing and Training are given in the following **Table 8.4**.

Table 8.4: Size of Training and Test Data

Data Type	Boyut
Train Data Frame	93638
Test Data Frame	23410

StandardScaler was used to scale the dataset. In the first layer, we have 2 types of output as Benign and Darknet. The type of output data set was determined as category.

Table 8.5: RNN Model Architecture

Layer (type)	Output Shape	Param
gru_1 (GRU)	(None, 64)	12864
batch_normalization_2 (BatchNormalization)	(None, 64)	256
dense_3 (Dense)	(None, 1024)	66560
batch_normalization_3 (BatchNormalization)	(None, 1024)	4096
dense_4 (Dense)	(None, 16)	16400
dense_5 (Dense)	(None, 2)	34
Total params: 100,210 Trainable params: 98,034 Non-trainable params: 2,176		

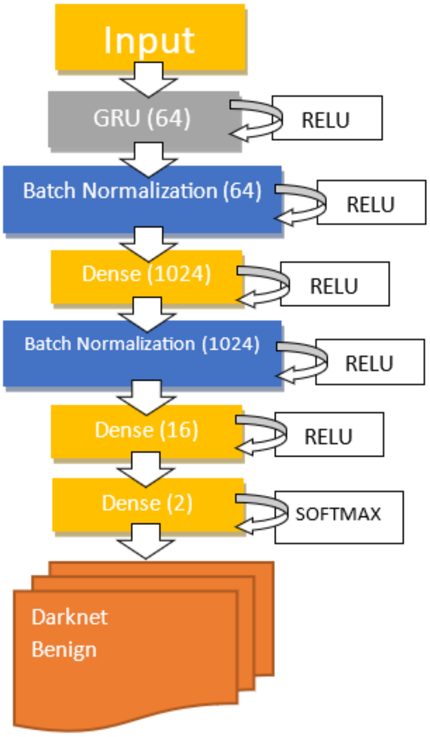


Figure 8.6: RNN Layer1 Model Architecture Diagram

Model architecture is shown in **Table 8.5** and model diagram is shown in **Figure 8.6**. In the model, relu is preferred as the Activation function, and sigmoid is preferred in the last layer. Calculated with the loss function binary crossentropy. Batch Normalization was used in the model to reduce the covariance. After the data pre-cleaning, the remaining 73 columns were given to the model as input. Dense layer with 2 units is defined for the output. In the model fitting process, the batch size was given as 64 and the model was trained with 10 epochs.

In Layer 2, the RNN model is trained to predict category outcomes. Categories are given in detail in **8.3** heading section. As in the first model, the data has been pre-cleaned. Again, the test separation ratio was determined as 0.20. The total data sizes allocated for Testing and Training are given in the following **Table 8.4**. Model diagram is shown in **Figure 8.7**. In the second layer we have 8 types of output. The type of the output data set was determined as the category.

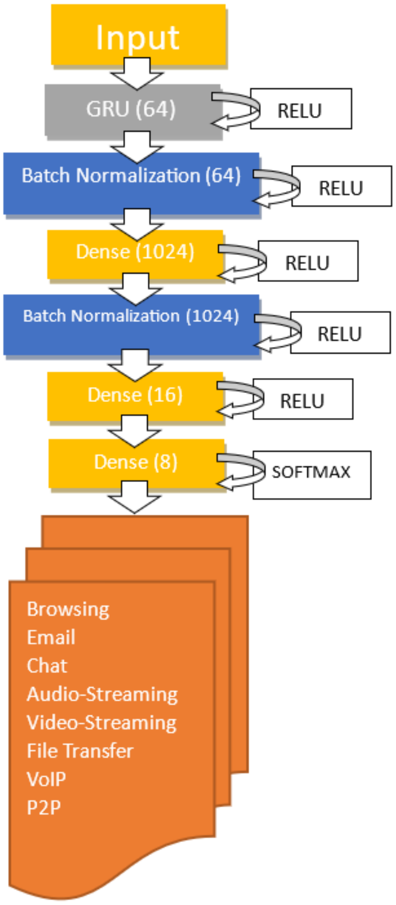


Figure 8.7: RNN Layer2 Model Architecture Diagram

The remaining model structure is the same as the first model. Model hyper parameters are set the same as the values in the first layer. After the data pre-cleaning, the remaining 73 columns were given to the model as input. Dense layer with 8 units is defined for output. Since there are 8 output shapes in the last dense layer, there are 136 parameter values. In the model fitting process, the batch size was given as 64 and the model was trained with 10 epochs.

8.5.2. LSTM Model

In the RNN model, the values were quite high. Since the LSTM algorithm model has a longer-term memory than RNN, it is preferred to compare whether the second model will obtain good results compared to RNN. In order to apply LSTM to the studied problem, first of all, the data were normalized. For this purpose, the value of each data was taken as the difference from the mean of the relevant column and proportioned to the standard deviation of that column. The standardized data was then divided into training and test data. LSTM 4-layer model is established. The layer structure in the model is as follows:

Table 8.6: LSTM Model Architecture

Layer (type)	**Output Shape**	**Param**
lstm_2 (LSTM)	128	66560
batch_normalization_8 (BatchNormalization)	128	512
dense_8 (Dense)	64	8256
batch_normalization_9 (BatchNormalization)	64	256
dense_9 (Dense)	16	1040
batch_normalization_10 (BatchNormalization)	16	64
dense_10 (Dense)	16	272
batch_normalization_11 (BatchNormalization)	16	64
dense_11 (Dense)	2	34

The model structure in **Table 8.6** is used. Model diagram is shown in **Figure 8.8.** There are 77.58 parameters in the model. ReLU (Rectified Linear Unit) function was used as the activation function of the layers except the last layer in the model, and softmax was used in the last layer. In the first layer of the LSTM model, since the outputs have two categories, the parameters are optimized over the binary crossentropy loss function.

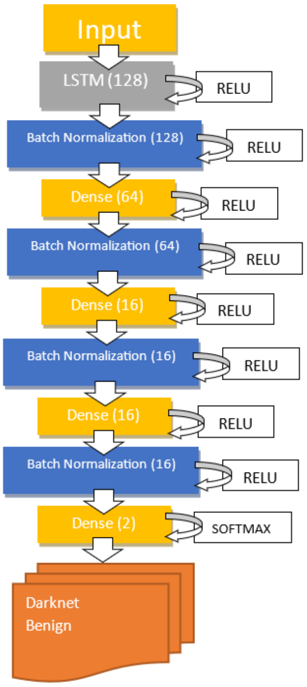


Figure 8.8: LSTM Layer1 Model Architecture Diagram

In second layer model, the dense layer, there are 8 units and changes in the number of parameters in the last. The loss function is used as categorical crossentropy in this model since there are multiple outputs. This is used as categorical-cross entropy in the second layer. Another difference between the two layers is the scaler preferences. Standard scaler was preferred in the first model and min-max scaler was preferred in the second model. Model diagram for layer2 is shown in **Figure 8.9.**

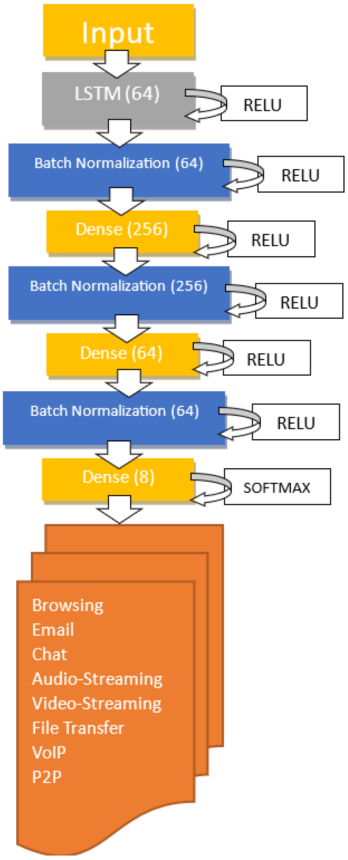


Figure 8.9: LSTM Layer2 Model Architecture Diagram

In addition, new data were produced with GAN (Generative Adversarial Networks) and used as training data for other methods. By generating data with GAN, training was carried out with LSTM model. By using the model structures in **Table 8.7** and **Table 8.8**.

Table 8.7: GAN Generator Model Architecture

Layer	Output Shape
Dense	128,input_dim=32
Dropout	0.2
LeakyRelu	Alpha=0.2
BatchNormalizaton	Momentum=0.8
Dense	256
LeakyRelu	Alpha=0.2
BatchNormalization	Momentum=0.8
Dense	512
Dropout	0.2
LeakyRelu	Alpha=0.2
BatchNormalization	Momentum=0.8
Dense	73

Table 8.8: GAN Discriminator Model Architecture

Layer	Output Shape
Dense	512, input_dim=32
LeakyRelu	Alpha=0.2
Dense	256
LeakyRelu	Alpha=0.2
Dropout	0.4
Dense	128
LeakyRelu	Alpha=0.2
Dropout	0.4
Dense	1

The aim of this model is whether more new datasets that will be formed by changing the dataset will make successful predictions in this model. With the GAN model, examples were produced with the same data type as the data set. In this model, GAN learned how darknet data is and how clean data is, and created data according to which features get values in the new data.

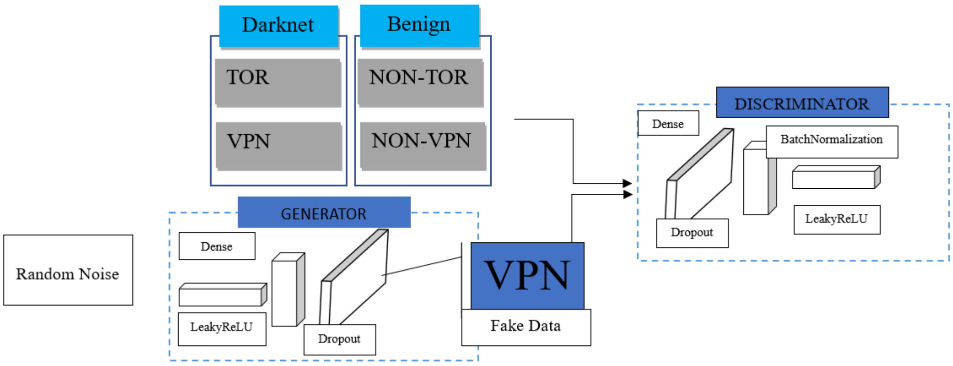


Figure 8.10: LSTM-GAN Layer1 Model Architecture Diagram

Model diagram is shown in **Figure 8.10**. At this stage, discriminator starts to distinguish real data by trying to understand fake and real data. As the generator gets better at discriminating, it starts to produce more realistic data. In the first model of GAN, binary cross-entropy is used in both generator and discriminator. Because, every discriminator output vector component is not affected by other component values and it is independent for each vector component (class).

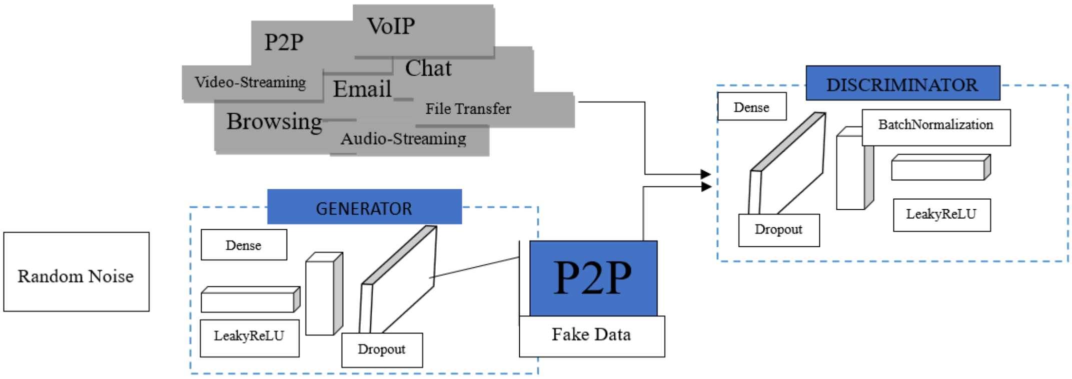


Figure 8.11: LSTM-GAN Layer2 Model Architecture Diagram

Generator is also modeled as categorical cross-entropy, since data needs to be generated for Gan second model categories. Activation function tanh is used in the last layer of the generator model in first model. Using tanh in the generator is for duplicating data in a wide range. In the discriminator model, it was determined as sigmoid. The use of sigmoid in discriminator has been used since it is thought that it will give more accurate and faster results in determining whether the data is real or not. Softmax is used in both the generator and the discriminator as well as in the first and second models. Since it has to process more than one class, it was preferred to increase categorical data and make predictions. LSTM-GAN Layer2 Model Architecture Diagram is shown in **Figure 8.11**. In both models, a higher standard deviation ratio was determined in the generator. 0.02 is preferred and a wide range of standard deviation distribution was targeted. The discriminator was set to 0.01. This determination was made because it is closer to the mean value at a low standard deviation rate. Leaky Relu activation function is used in hidden layers by choosing tanh in generator. It is preferred because it enables back propagation for negative input values. Dropout is used in the model to prevent overfitting, as our training data expands and a long-term training is required. Optimizer is adam and batch normalization momentum parameter were modeled as 0.8. In the model training set, the batch size is trained as 128. The number of epochs is 500.

In the second layer of the LSTM model, experiments were carried out as multiple categories. Two category modeling methods were used to improve the values. In this model, Browsing, P2P, Chat, Email, Transfer, Audio Stream, Video Stream and VOIP categories are modeled separately. Since layer 2 model results are generally observed lower, they were modeled by considering separate categories. Each category was trained and tested separately with the model diagram in **Figure 8.9**. The model created for each category was based on whether the compared category was predicted correctly. For example, the output of this model created for P2P is either P2P or not. The results of 8 different models created to predict the categories of the data are examined and the category of the model with the best ratio is determined. In this model, relu (Rectified Linear Unit) function was used as the activation function of the layers except the last layer in the model, and softmax was used in the last layer. In the second layer of the LSTM-binary model, since the outputs have eight categories, the parameters are optimized over the binary crossentropy loss function, adam gradient-based optimization algorithm was utilized to update the weights of the network during the training phase. Layers in the network do not have to wait for the previous layer to learn. It provides as simultaneous learning and accelerates education. Since this speed will be advantageous in large data sets, batch normalization has been applied in this model. The model structure in **Table 8.9** is used.

Table 8.9: LSTM-Binary Layer2 Model Architecture

Layers	**Output Shape**	**Param**
lstm_1 (LSTM)	(None, 512)	1052672
batch_normalization_3 (BatchNormalization)	(None, 512)	2048
dense_3 (Dense)	(None, 256)	131328
batch_normalization_4 (BatchNormalization)	(None, 256)	1024
dense_4 (Dense)	(None, 64)	16448
batch_normalization_5 (BatchNormalization)	(None, 64)	256
dense_5 (Dense)	(None, 2)	130

8.5.3. MLP Model

MinMaxScaler normalization was used in the MLP model. Model diagram is shown in **Figure 8.12.** The Layer 2 model diagram for category classification is shown in **Figure 8.13.** The maximum iteration value is given as 5. The activation function decides how the weighted sum of input to a perceptron forms its output and eventually the network’s output. The activation function used for hidden layers in this model is ReLU. While adam was used for optimization to update the weights of the network during the training phase.

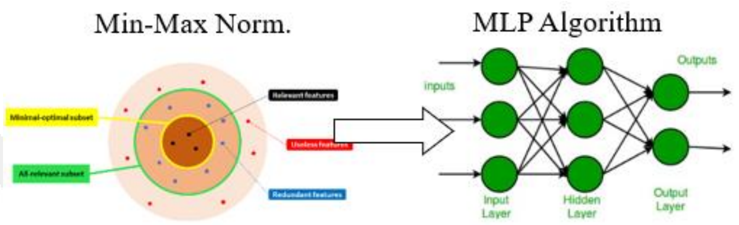


Figure 8.12: MLP Layer1 Model Architecture Diagram

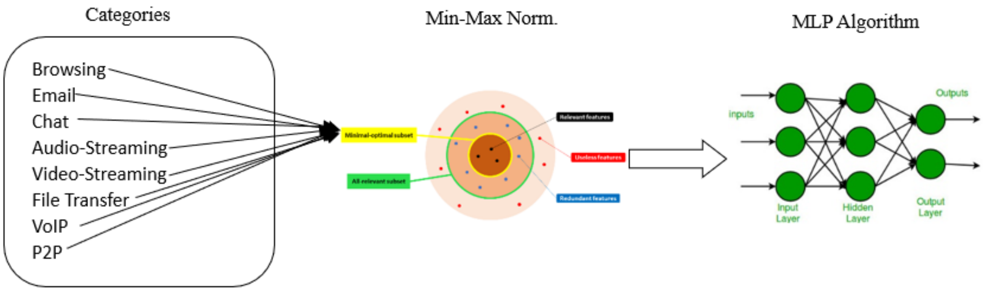


Figure 8.13: MLP Layer2 Model Architecture Diagram

Min-Max Scaler normalization is used. Min-max scaling is used that when is need values in a bounded interval. In the MLP model, model tests were also carried out with SelectKBest and feature selection. Model diagram for Layer 1 and Layer 2 is shown in **Figure 8.14** and **Figure 8.15 .** This feature selection algorithm is preferred because it is an algorithm model that excludes less important data categories from evaluation. Information about this feature selection algorithm is given in **Table 8.3**. A feature selection ratio of 2-50 is given. The same model hyper parameters are valid in the MLP model second layer.

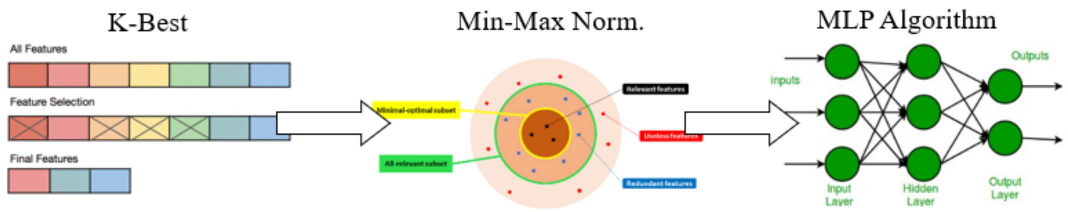


Figure 8.14: MLP Layer1 Model Architecture Diagram with Feature Selection

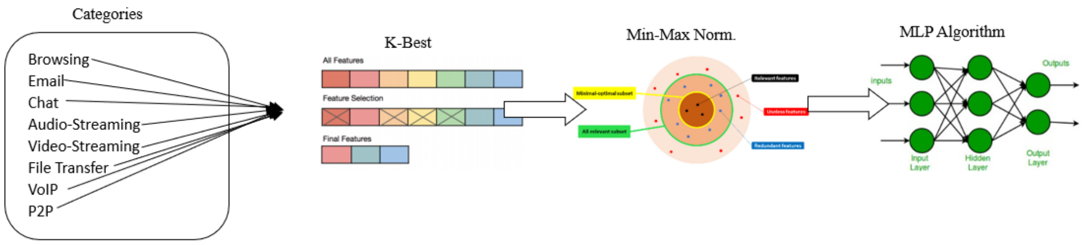


Figure 8.15: MLP Layer2 Model Architecture Diagram with Feature Selection

The MLP model was also modeled separately for each category in the second layer and output was produced. Model diagram is shown in **Figure 8.16.** In the binary model, the maximum iteration is set to 50. The binary application model, which was tried in the LSTM model, was also tested with the MLP algorithm. It was tested whether 8 different model categories were predicted correctly for 8 categories so that the model structure was the same.

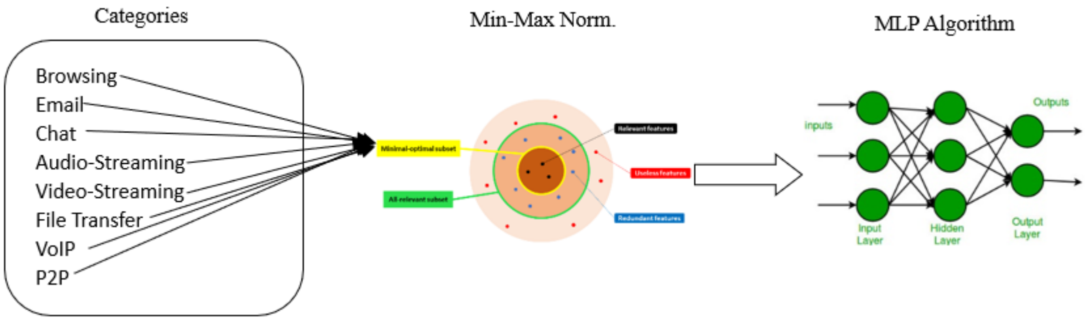


Figure 8.16: MLP-Binary Layer2 Model Architecture Diagram

CHAPTER IX
RESULTS AND DISCUSSION

9.1. RNN Layer1 Model

The evaluation metric values obtained for layer 1 as a result of the experiments performed on the RNN model are given in **Table 9.1**. According to these values; In detecting benign data lines, the Precission ratio in detecting Darknet data lines gave a result of 0.9684. Accuracy value of 0.9845 indicates that the data model is well trained. F score and Recall measurement metric rates are also included in the table. The model classified 18,591 as benign data and 4819 as darknet data out of the 23,410 line test set.

Table 9.1: RNN Layer1 Model Evaluation Metrics Results

Output	**F1-Score**	**Recall**	**Precision**
0 (Benign)	0,9912	0,9867	0,9923
1 (Darknet)	0,9623	0,9924	0,9446

The graph of the training accuracy rate and test accuracy rate calculated for each epoch during model training is shown in **Table 9.1**. According to this graph, it was observed that the accuracy rates of the dataset reserved for training increased without jumping throughout the epoch. It was observed that the accuracy rates of the test set caught the accuracy rate of the training set after epoch 4.

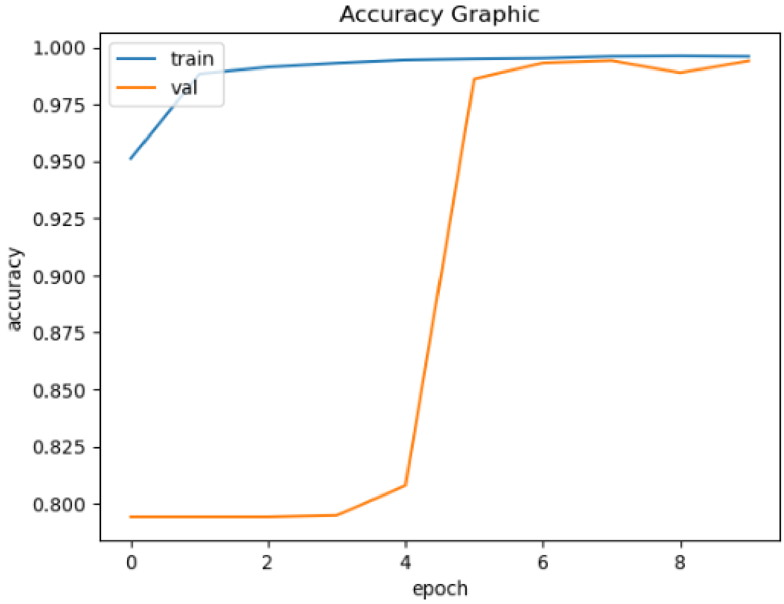


Figure 9.1: RNN Layer1 Accuracy Graphic

The graph of the rate of change of Mean Squared Error rates over the epoch is shown in **Figure 9.2**. According to this graph, it was observed that the error rates allocated for training decreased throughout the epoch and decreased to 0.0230. It was observed that the error rates of the test set were refracted during epoch 2 and decreased to 0.0242.

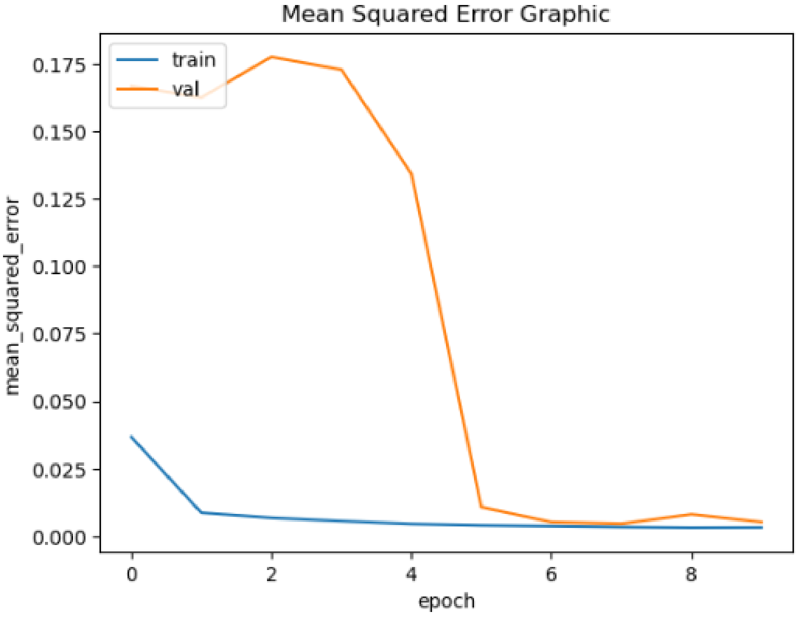


Figure 9.2: RNN Layer1 Mean Squared Error Graphic

9.2. RNN Layer2 Model

The evaluation metric values obtained for layer 2 as a result of the experiments performed on the RNN model are given in figure 1. According to these values; traffic categories gave the best results in detecting data rows with the P2P category with a rate of 0,9935. The lowest estimation was realized in the Email and Video Streaming categories with a rate of 0,6142. It was seen that the Accuracy value gave a result of 0,8614. F1 score result was 0,7909. Estimated rates by categories are given in the Support column of reference **Table 9.2**.

Table 9.2: RNN Layer2 Model Evaluation Metrics Results

Category	F1 Score	Recall	Presicion
Audio-Streaming	0,8873	0,8734	0,8853
Browsing	0,9315	0,9767	0,9067
Chat	0,7046	0,6989	0,7220
Email	0,6532	0,6142	0,6919
File-Transfer	0,7967	0,7520	0,8325
P2P	0,9912	0,9935	0,9887
Video-Streaming	0,6142	0,6116	0,7236
VOIP	0,7489	0,8810	0,6342

In the Accuracy analysis of traffic connection types, it was observed that the test and training rates converged towards the end of the epoch according to **Figure 9.3**.

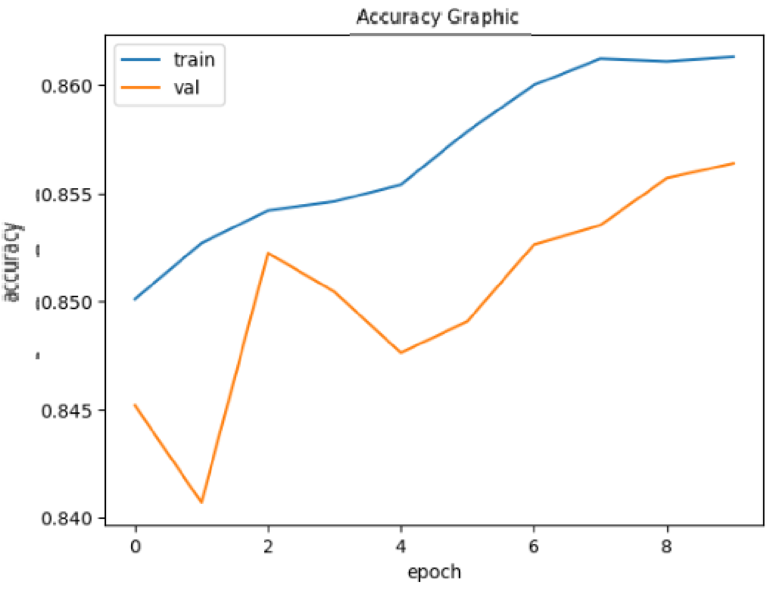


Figure 9.3: RNN Layer2 Accuracy Graphic

In **Figure 9.4** it is seen that the training error rates show a slope close to linear. It has been observed that the test data drops by making jumps.

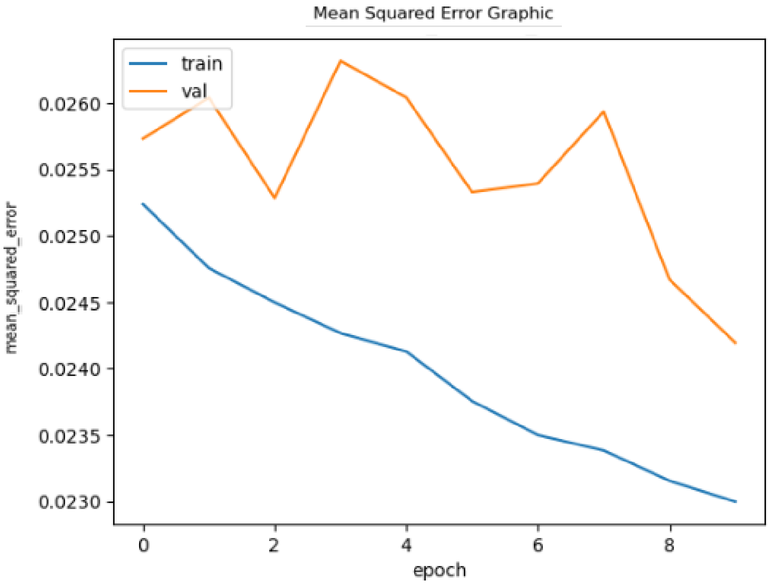


Figure 9.4: RNN Layer2 Mean Squared Error Graphic

9.3. LSTM Layer1 Model

According to LSTM model results, as a result of iterations, the accuracy rate was 0,9961, the loss value was 0,0151 and f1 score was 0,9856 at the first layer. Other metric rates are also included in the table in **Table 9.3**. The graphs of training and test phase loss and accuracy values by epochs are presented in **Figure 9.5** and te confusion matrix of the model is given in **Figure 9.6**.

Table 9.3: LSTM Model Layer1 Evaluation Metrics Results

Output	F1-Score	Recall	Precision
0 (Benign)	0,9976	0,9812	0,9867
1 (Darknet)	0,9736	0,9845	0,9532

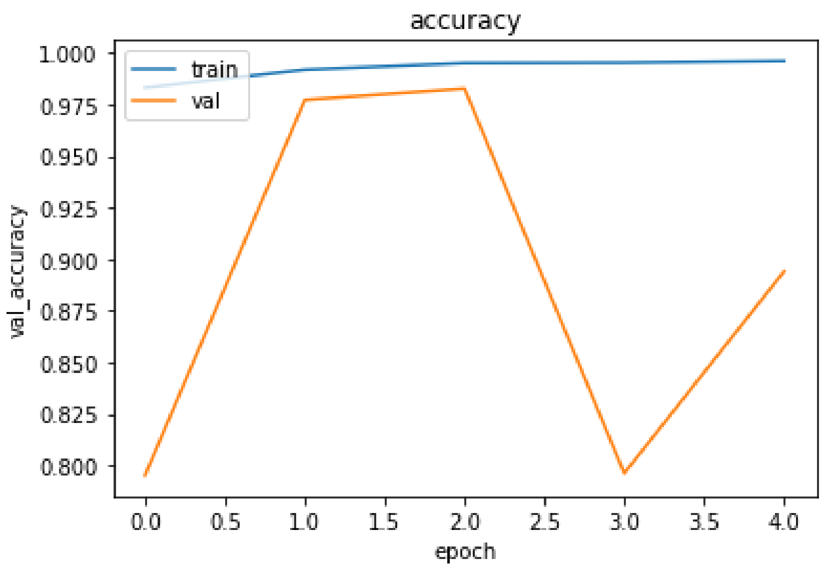


Figure 9.5: LSTM Layer1 Model Accuracy Graphic

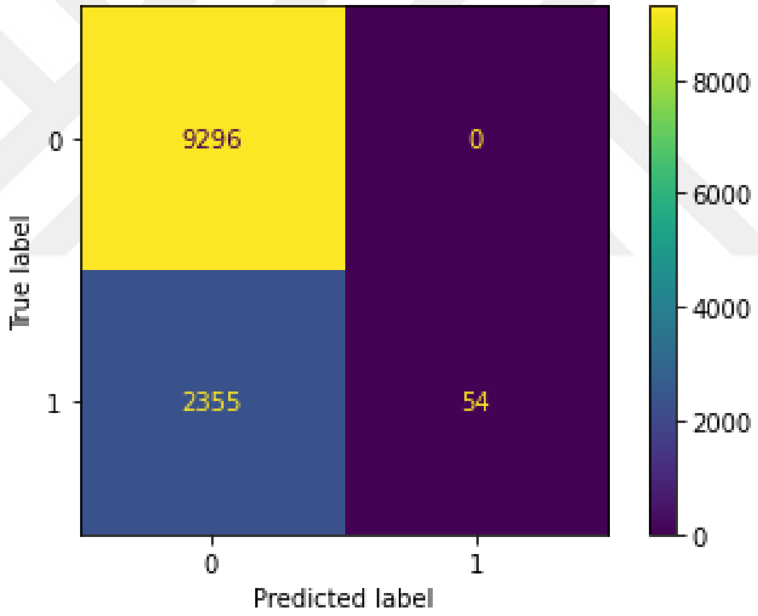


Figure 9.6: LSTM Layer1 Model Confusion Matrix

9.4. LSTM- GAN Layer1 Model

After the first stage training process of the GAN model was completed, new data were also produced and the first stage classification process was reconsidered. The accuracy value obtained with this method was obtained as 0,9590. F1 score result was 0,9445. The confusion matrix of the model is shown in **Figure 9.7**.

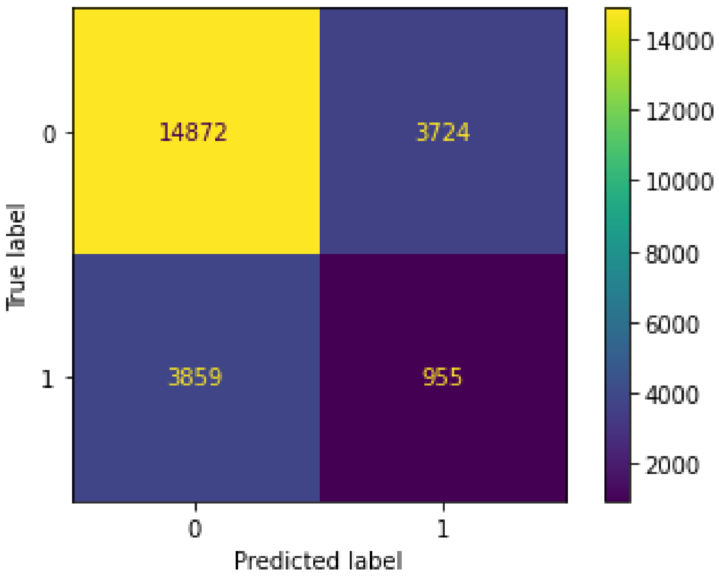


Figure 9.7: LSTM- GAN Layer1 Model Confusion Matrix

As a result of the results obtained, it was observed that the GAN application decreased the values in this model.

9.5. LSTM Layer2 Model

According to LSTM model second layer results, the accuracy value was 0,7154 and the F1 score value was realized as 0,7542. The graphs of loss and accuracy values according to the steps are presented in **Figure 9.8**.

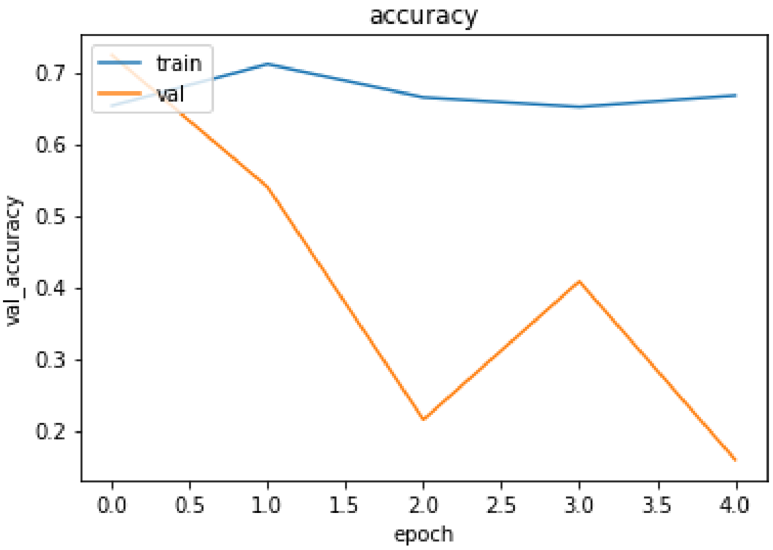


Figure 9.8: LSTM Layer2 Model Accuracy Graphic

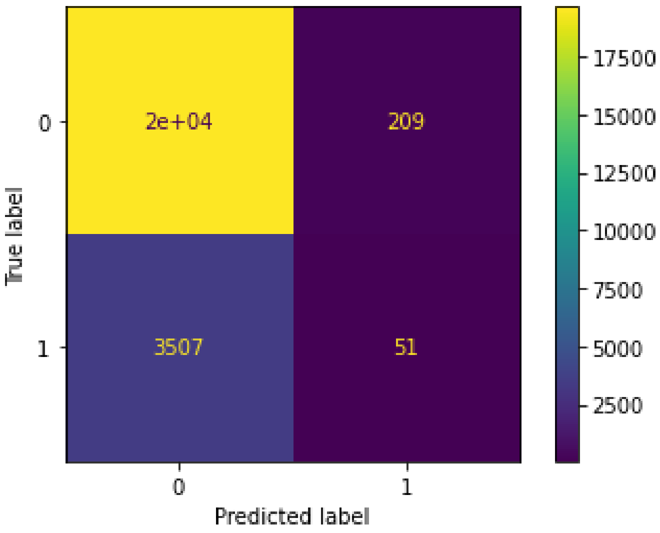


Figure 9.9: LSTM Layer2 Model Confusion Matrix

9.6. LSTM-GAN Layer2 Model

After the second layer training process of the GAN model was completed, new data were also produced and the second layer classification process was reconsidered. The accuracy value obtained with this method was obtained as 0,6680. F1 score result was 0,6489.

9.7. LSTM-Binary Layer2 Model

In order to improve the values obtained in the LSTM second model, the categories were set up as binary and run separately for 8 categories. The accuracy values, evaluation metrics and confusion matrixes of the models are listed below.

Table 9.4: Accuracy Values of Category Models

Category	Accuracy	F1 Score	Recall	Presicion
Audio-Streaming	0,9503	0,8480	0,8345	0,8403
Browsing	0,9584	0,7194	0,7532	0,7045
Chat	0,9324	0,9038	0,8950	0,8938
Email	0,9273	0,9477	0,9820	0,9652
File-Transfer	0,9375	0,9039	0,8698	0,8970
P2P	0,9850	0,7915	0,7915	0,7815
Video-Streaming	0,9258	0,9152	0,9610	0,8845
VOIP	0,9775	0,9704	0,9354	0,9316

Average F1 score was 0,8749 and average accuracy was 0,9492 . The graphic analysis of the accuracy and loss values in each epoch in the training phase for each category of the model is given below.

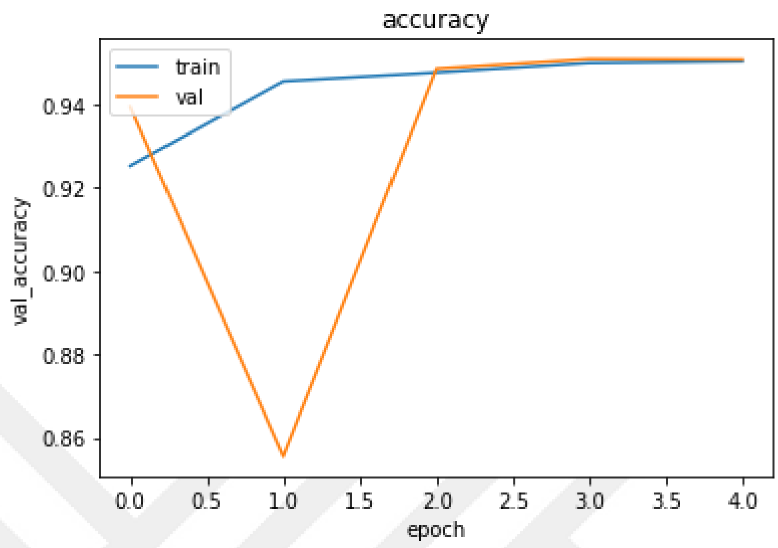


Figure 9.10: Accuracy Values According to Epochs in LSTM Binary Algorithm for Audio-Streaming Category

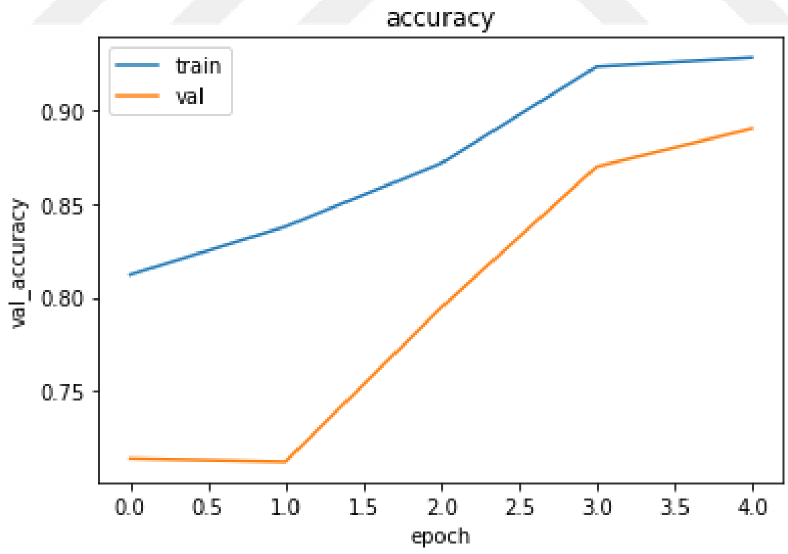


Figure 9.11: Accuracy Values According to Epochs in LSTM Binary Algorithm for Browsing Category

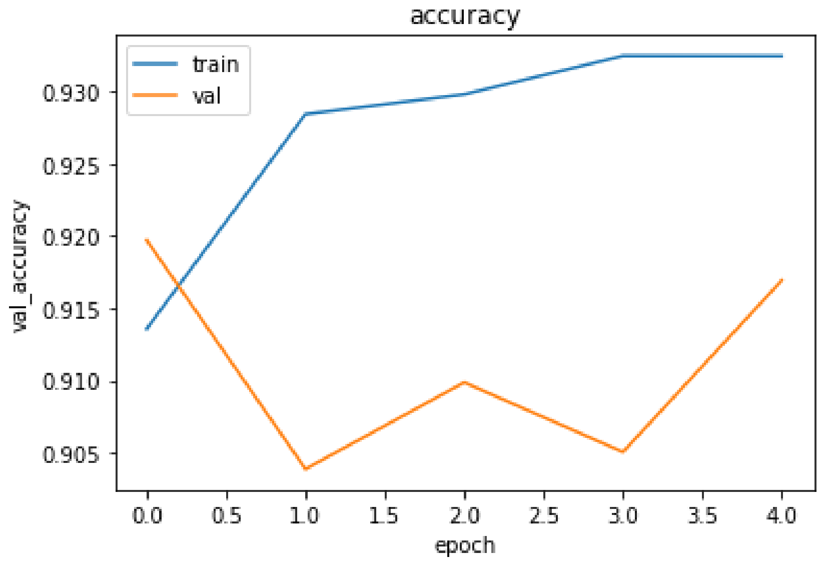


Figure 9.12: Accuracy Values According to Epochs in LSTM Binary Algorithm for Chat Category

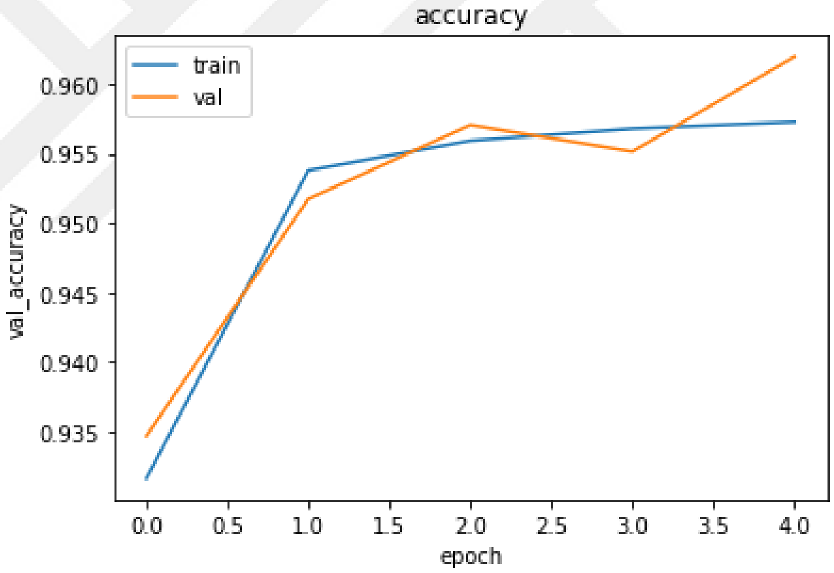


Figure 9.13: Accuracy Values According to Epochs in LSTM Binary Algorithm for Email Category

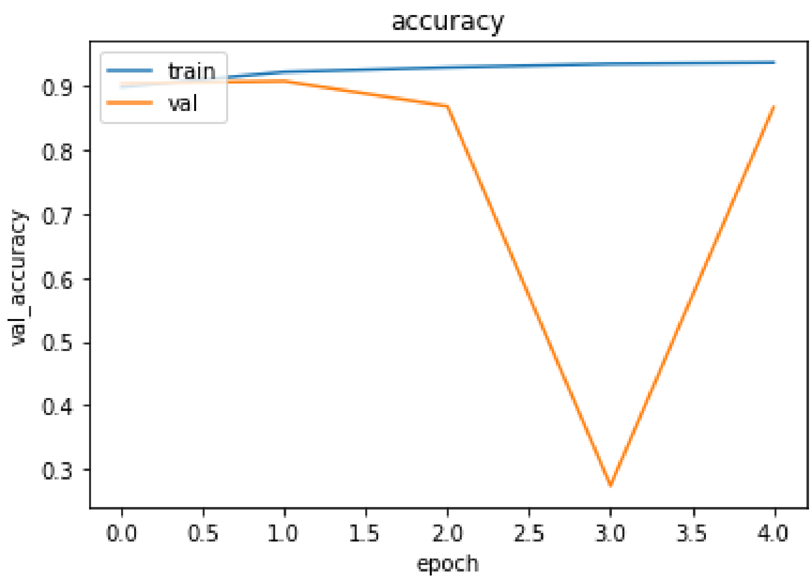


Figure 9.14: Accuracy Values According to Epochs in LSTM Binary Algorithm for File-Transfer Category

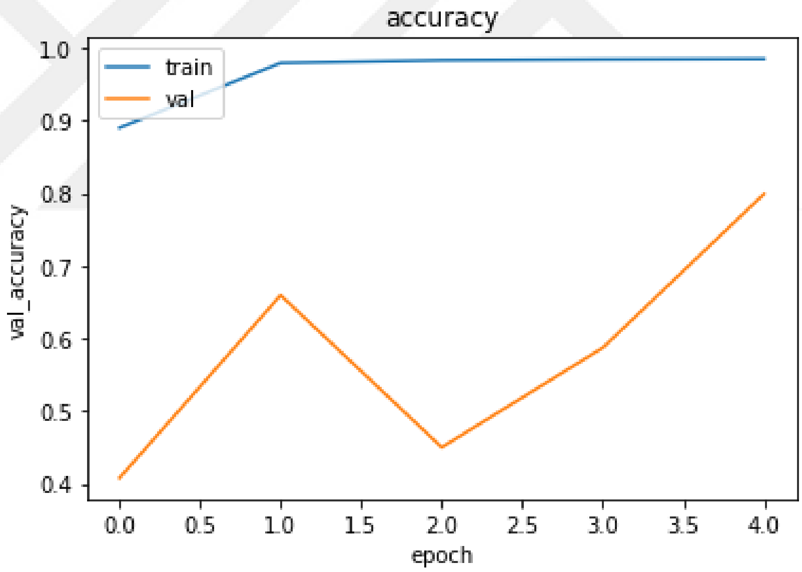


Figure 9.15: Accuracy Values According to Epochs in LSTM Binary Algorithm for P2P Category

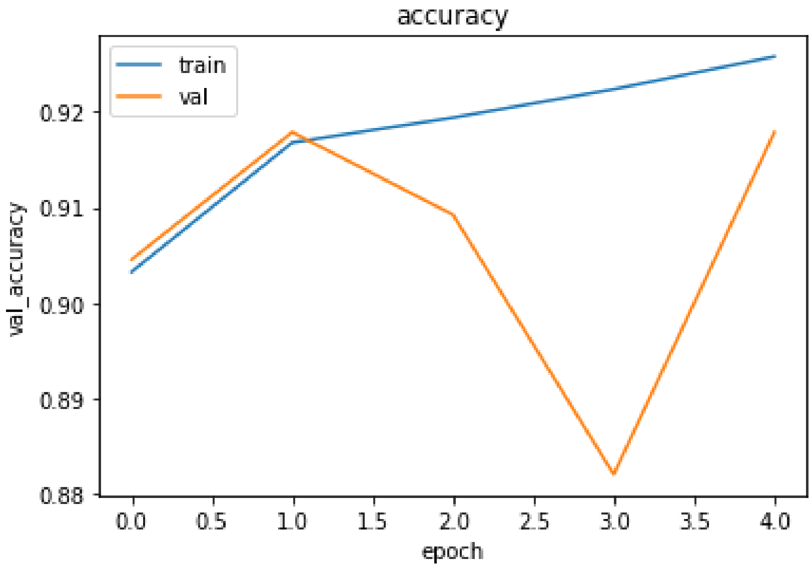


Figure 9.16: Accuracy Values According to Epochs in LSTM Binary Algorithm for Video Streaming Category

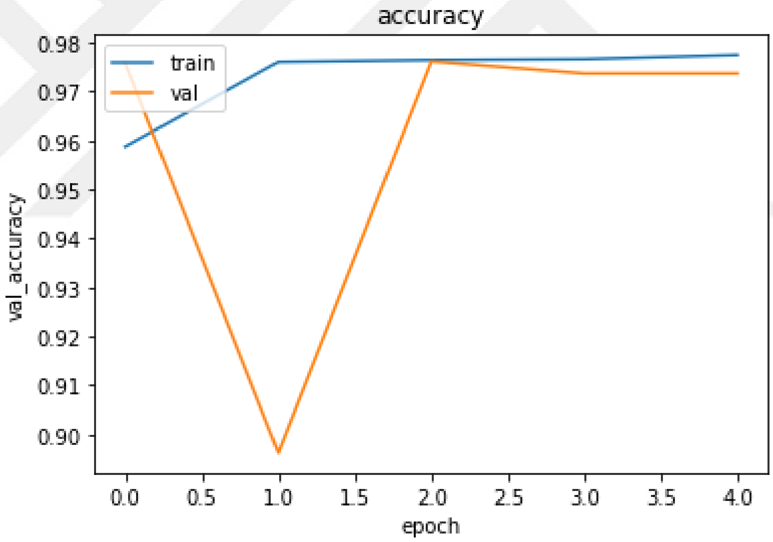


Figure 9.17: Accuracy Values According to Epochs in LSTM Binary Algorithm for VOIP Category

Based on this, the categories were modeled and tested separately, and with this study, it was concluded that the values increased to a large extent than multi category LSTM model.

9.8. MLP Layer1 Model

According to MLP model results, in the modeling for the first layer with MLP, the training stage accuracy was 0,9945. F1 score result was 0,9935. The confusion matrix of the first layer MLP model is shown in **Figure 9.18** .

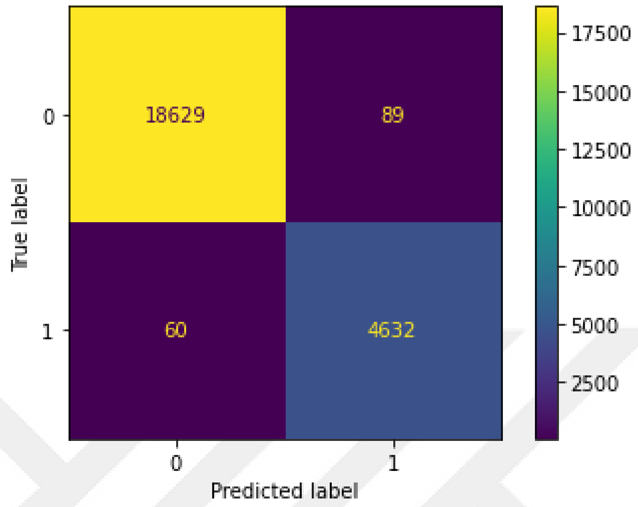


Figure 9.18: MLP Layer1 Model Confusion Matrix

Table 9.5: MLP Layer1 Model Evaluation Metrics Results

Output	**F1-Score**	**Recall**	**Precision**
0 (Benign)	0,9955	0,9910	0,9967
1 (Darknet)	0,9915	0,9924	0,9943

Feature Selection algorithm has been applied to improve the MLP result in first layer model. The columns selected as a result of the algorithm are as follows in **Table 9.6**.

Table 9.6: MLP Layer1 Model Selected Features

Src Port	Dst Port	Flow Duration	Total Length of Fwd Packet	Total Length of Bwd Packet
Fwd Packet Length Max	Fwd Packet Length Mean	Bwd Packet Length Max	Bwd Packet Length Min	Bwd Packet Length Mean
Flow Bytes/s	Flow Packets/s	Flow IAT Mean	Flow IAT Min	Fwd Header Length
Bwd Header Length	Fwd Packets/s	Bwd Packets/s	Packet Length Max	Packet Length Mean
Packet Length Std	Packets Length Variance	Average Packet Size	Fwd Segment Size Avg	Bwd Segment Size Avg
Subflow Bwd Bytes,	FWD Init Win Bytes	Bwd Init Win Bytes	Idle Mean, Idle Max	Idle Min, Subtype
s_ip_1	s_ip_3	s_ip_2	d_ip_0	d_ip_1
d_ip_2	d_ip_3			

Detailed descriptions of selected features are shown in **Table 8.1**. The s and d partitioned fields, which are not included in the table, include the 3-partitioned versions of the source IP and destination IP features. With these columns, After feature selection, MLP reached an accuracy value of 0.9945 during training and testing phases. F1 score result was 0,9932. In this case, the confusion matrix is formed as follows.

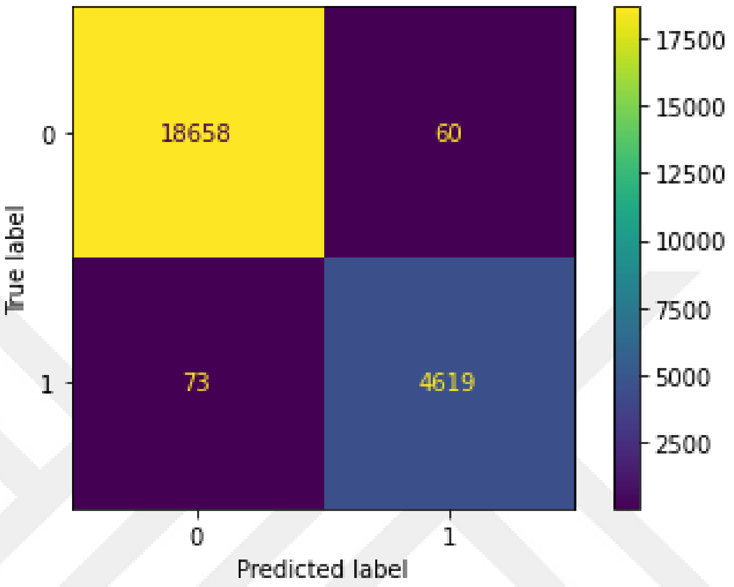


Figure 9.19: MLP Layer1 Feature Selection Model Confusion Matrix

The data were given the same accuracy value as output by selecting the feature and performing the training and testing stages with the same model.

9.9. MLP Layer2 Model

In the modeling for the second layer with MLP, accuracy was 0,7845. F1 score was 0,7756. The confusion matrix of the first stage MLP model is shown in **Figure 9.20**.

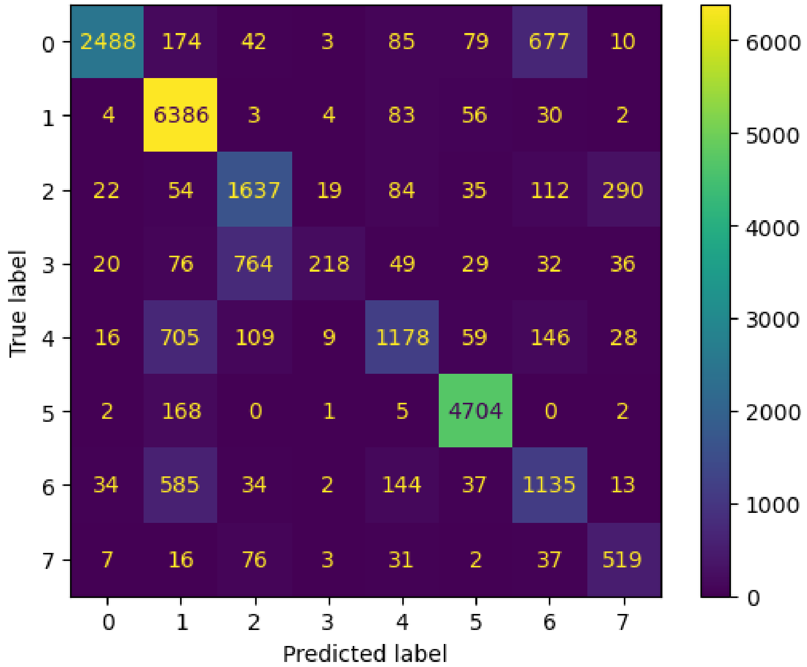


Figure 9.20: MLP Layer2 Model Confusion Matrix

The same feature selection algorithm is modeled in Layer2. The accuracy value of 0,7845, which is the model value performed before the feature selection according to the result values, was obtained at the same rates in this model.

9.10. MLP-Binary Layer2 Model

Accuracy values for MLP binary categories are given in **Table 9.7**. According to table average F1 score was 0,9616 and average accuracy was 0,9643 .

Table 9.7: Accuracy Values of Category Models

Category	Accuracy	F1 Score	Recall	Presicion
Audio-Streaming	0,9623	0,9610	0,9523	0,9256
Browsing	0,9515	0,9511	0,9403	0,9366
Chat	0,9527	0,9428	0,9601	0,9240
Email	0,9639	0,9654	0,9567	0,9632
File-Transfer	0,9642	0,9563	0,9520	0,9445
P2P	0,9956	0,9954	0,9899	0,9723
Video-Streaming	0,9415	0,9387	0,9350	0,9117
VOIP	0,9827	0,9820	0,9442	0,9422

In the matrices below, the total results of the predicted and expected values of each of the categories are plotted.

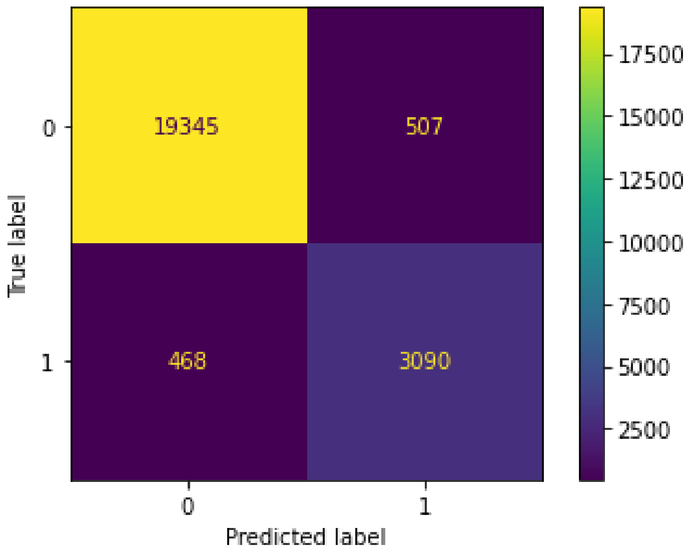


Figure 9.21: Confusion Matrix According to the MLP Binary Algorithm for the Audio-Streaming Category

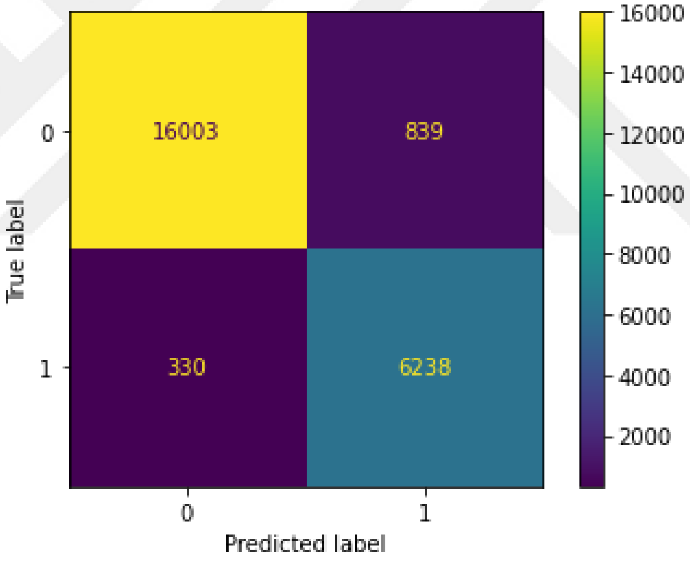


Figure 9.22: Confusion Matrix According to the MLP Binary Algorithm for the Browsing Category

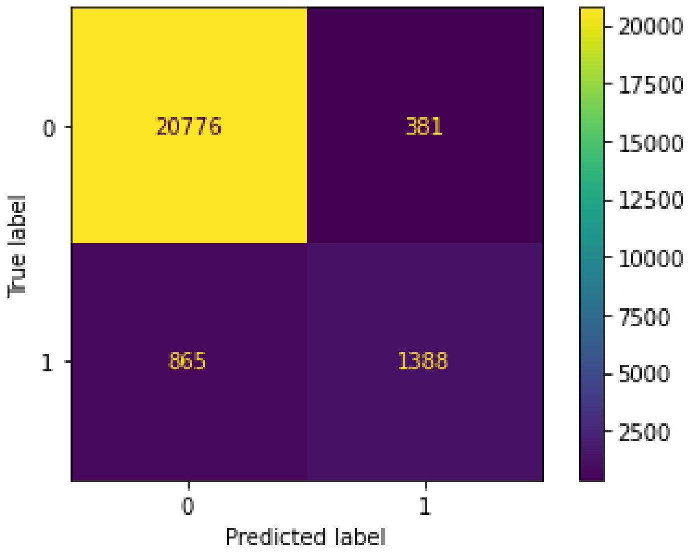


Figure 9.23: Confusion Matrix According to the MLP Binary Algorithm for the Chat Category

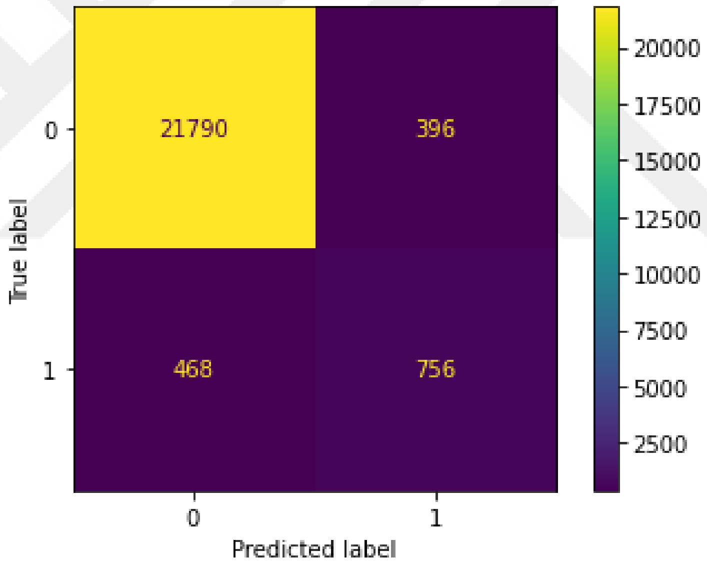


Figure 9.24: Confusion Matrix According to the MLP Binary Algorithm for the Email Category

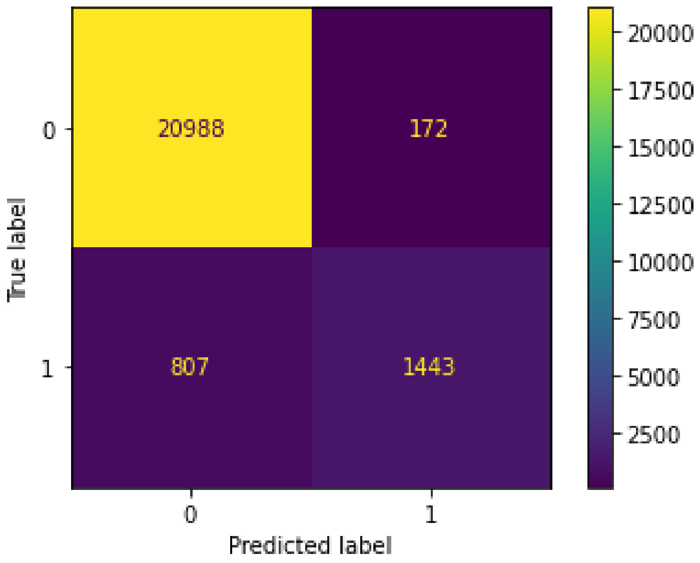


Figure 9.25: Confusion Matrix According to the MLP Binary Algorithm for the File-Transfer Category

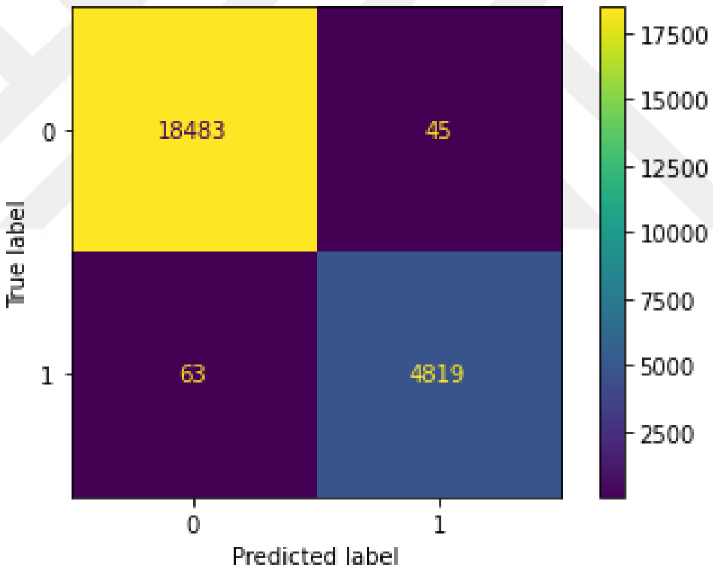


Figure 9.26: Confusion Matrix According to the MLP Binary Algorithm for the P2P Category

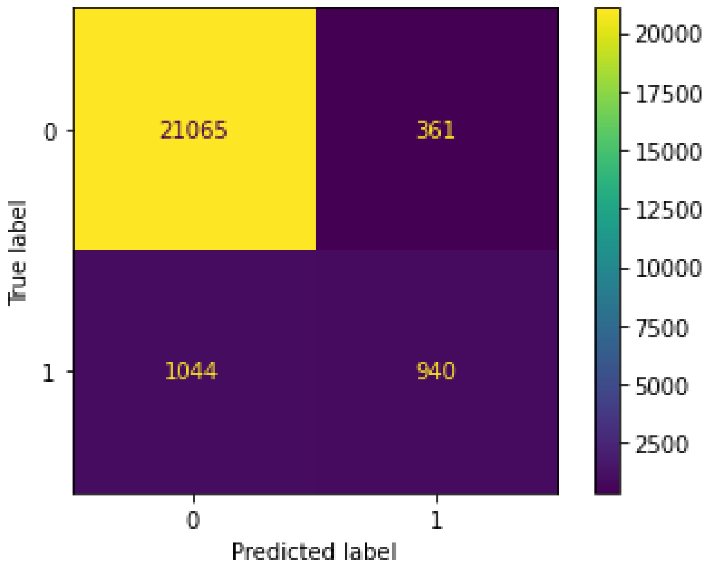


Figure 9.27: Confusion Matrix According to the MLP Binary Algorithm for the Video-Streaming Category

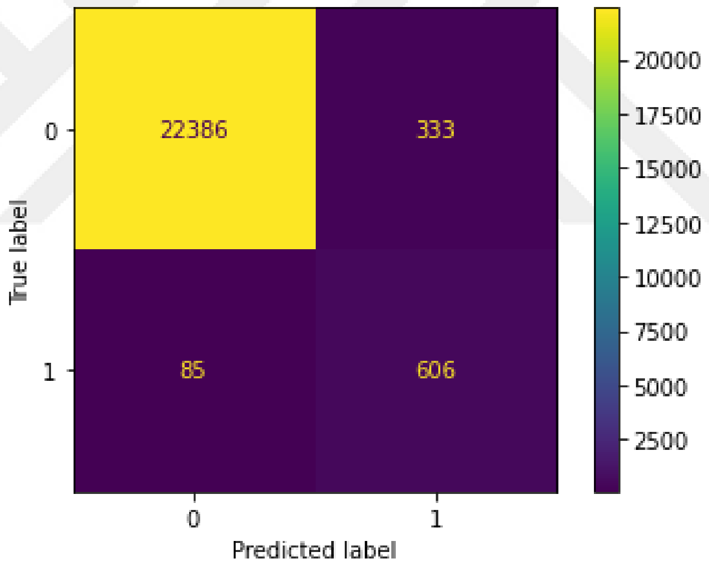


Figure 9.28: Confusion Matrix According to the MLP Binary Algorithm for the VOIP Category

Table 9.8: Summary of Models

Models	F1-Score	Accuracy	Recall	Precision
RNN Layer1	0.9767	0.9845	0.9895	0.9684
RNN Layer2	0.7909	0.8614	0.8001	0.7981
LSTM Layer1	0.9856	0.9961	0.9828	0.9699
LSTM Layer2	0.7542	0.7154	0.7201	0.7435
LSTM Binary Layer2	0.8749	0.9492	0.8778	0.8623
LSTM-GAN Layer1	0.9520	0.9590	0.9610	0.9350
LSTM-GAN Layer2	0.6460	0.6680	0.6830	0.6835
MLP Layer1	0.9935	0.9945	0.9917	0.9955
MLP Layer2	0.7756	0.7845	0.7850	0.7570
MLP Layer1 with Feature Selection	0.9935	0.9945	0.9917	0.9955
MLP Layer2 with Feature Selection	0.7756	0.7845	0.7850	0.7570
MLP Binary Layer2	0.9616	0.9643	0.9538	0.9400

According to **Table 9.8**, accuracy values above 0,9845 were taken in the RNN model applied for layer 1. In terms of categorizing darknet data, the accuracy rates have reached very high values by evaluating the categories separately in the LSTM model, which is one of the artificial neural network models applied for layer 2. It was observed that the LSTM-GAN application caused the values to decrease in the model in both the first layer and the second layer. As a result of feature selection in the MLP model, it was determined that there was no change in the values in both the first layer and the second layer. The RNN model, which gave the best values in the algorithm model structures that were not improved in layer 2, became the model. However, according to the results in LSTM and MLP models with binary application; In the LSTM binary model, lower values were observed in the Chat, Video-Streaming and Email categories compared to the other categories, but in the MLP model, it was concluded that these categories showed an increase in accuracy. The binary experiment applied in the models has been quite successful. As a result of the comparison of the MLP and LSTM binary models, it was observed that the average values were 96% in the MLP model and 92% in the LSTM model. The success of category detection in the MLP model was higher.

In this study, unlike other studies, source and destination ip properties are not removed from the dataset. It has been divided into 3 parts and evaluated. Between the categories that appear as 11, the data division caused by the fact that the same data looks like different data due to small-capital letters was prevented, and the same ones were modeled as 8 categories, and the same ones were combined**.** In [108] study the number of hidden layers is 1, each layer has 128 neurons. The optimization algorithm is rmsprop. In this study, it includes 7 hidden layers. The optimization algorithm is chosen as adam. Only the category model was created. In this study, modeling was performed separately as layer 1 and layer 2, and even each category was modeled separately. The batch size ratios were given equal in both studies. While 90.46% success was achieved in the their study, 94.92% success was achieved in this study thanks to binary modeling. In their study, they created a darknet classification model with the MLP model. According to this model, they achieved 96.27% success by performing binary work with 10 hidden layers and 100 iterations. In this study, a success rate of 96.43% was achieved by modeling with 50 iterations and 4 hidden layers. In addition to this modeling, a second comparison was made by including feature selection. And the same high values were achieved in darknet and category classification. [2] is in their study, the dropout layer is used in the lstm model. There are 2 hidden layers in the model. One of them is droput. In this study, each of them was modeled and tested separately as non-tor, non-vpn, lstm for tor and lstm for vpn. Compared with the average success results, a success of 96.5% was achieved. In addition, it was stated that there was a 91.8% success in tor data detection. In this study, non-vpn and non-tor in the dataset were accepted as benign data and it was ensured that the darknet data were estimated with features that would distinguish them from these data. Lstm model success was 99.61%. Even after data increase with GAN, it is observed that the success is 95.90%. [62] used smote for data balancing. They tested the lstm model with relu in hidden layers, and adam as the optimizer. Experimenting with PCA, DT and XGB from feature selection algorithms, they achieved 81%, 90% and 95% accuracy success rates, respectively. In the category classification model, they achieved a success rate of 89%. The average of the binary evaluation results is lower than the results obtained in this study according to this success evaluation and traffic classification. In this study, while the success rate in binary modeling is 94% on average, the success rate in traffic classification is 99%.In [67] study, they used the random forest algorithm model for darknet traffic classification, but they did data balancing with gan. Gan has an embedding of dimension size 128, a generator network with 2 Residual layers having 256 nodes each and a discriminator with 2 Linear layers having 256 nodes each. GAN network is trained with a batch size of 500 and a learning rate of 0.0002 with Adam Optimizer. In this study, the activation function was determined as tanh in the generator. In Discriminator, the loss function is sigmoid. Leaky relu and dropout are used in hidden layers. This data is used as input in the lstm model. According to the model results obtained, the model of the study achieved 92% success, while this study achieved 95% accuracy. [68] worked with the default hidden layer in the mlp model experiment. In this modeling, it achieved a success rate of 88% in traffic detection and 70% in category classification. In this study, by determining the max iteration of 5 and 50 in the second layer, a success of 99% was achieved in the first model and a success of 78% in the second model.

CHAPTER X
CONCLUSION AND FUTURE WORK

The Darknet is difficult to track due to its size and variety. Despite the difficulty of obtaining information in such a large structure, it can be facilitated by the development of effective classification methods. Darknet traffic classification is of great importance in combating cybercrime and preventing anonymous network interaction.

In this research, by working with a data set obtained from a darknet environment where illegal activities can be created, it can be determined which connection point darknet access is provided, and which application accesses are provided at the same time. With this study, encrypted traffic was detected with a source that obtained data from Tor browsers, which are accessed through encrypted and reliable VPN protocol and darknet by switching between many server connections.

This research has established a system that covers the process of analyzing malware threats in darknet traffic using neural networks methods. By monitoring large numbers of addresses, these systems can significantly increase the likelihood of quickly detecting a new threat as it tries to infect other hosts on the Internet.

Malicious link detection applications are the first step in dealing with attacks. Correct and efficient applications will provide a high level of protection. The importance of such applications, which will distinguish whether the data coming from the traffic is benign or malignant, is increasing day by day. The analysis results that can be obtained with this study will enable organizations to work effectively and to be prepared against attacks that may come from the darknet field in the cyber field.

For darknet classification, RNN, LSTM and MLP models are used. Among the models, according to the validation and test data, the MLP model gave the best performance in both darknet data detection and category classification with an accuracy rate of 99% and an average of 96%.

With this study, it performs well in darknet classification with artificial neural network models. It has been studied with a large dataset. Accordingly, high accuracy rates have been obtained. In general, the model values revealed results that were close to each other. The same ratios were obtained in the MLP model, in which feature selection was applied. In the LSTM-GAN model, which was made to detect the data by multiplying, a decrease in the accuracy rates was observed. It was a successful choice to evaluate it as binary in category classification models.

As a result, it can be said that artificial neural networks can be used in modeling darknet data, producing good results in detecting darknet data, and it can be developed over these model structures. In the categorization of data, more information is needed in the dataset. However, it has been observed that, according to the high success rates obtained as a result of evaluating each category separately rather than multiple categories, it has been observed that these dataset features are sufficient and low results have been obtained due to the differences in the detection features of the categories.

In the future, different feature selection methods can be tried to test whether successful results will be obtained. This way it will affect all the results in the model. In addition, it is planned to increase the number of classifiers and to make tests by grouping these classifiers into a group. The targeted study is to show high performance even with very large data with these working models. GAN pattern detection was performed for this reason, but the model showed a decrease in their performance. In this algorithm, it is possible to develop tests of other neural network models. It is aimed to expand the study with all these items.

REFERENCES

[1] Demertzis K., K. Tsiknas , D. Takezis , Skianis C. and Iliadis L. (2022), "Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework", *Electronics*, Vol. 10, No. 7, pp. 781.

[2] Li Y. and Y. Lu (2021), "ETCC: Encrypted two-label classification using CNN", *Security and Communication Networks*, Vol. 2021, No. 4, pp. 1-11 .

[3] Mercaldo F., F. Martinelli and A. Santone (2019), "Real-Time SCADA Attack Detection by Means of Formal Methods", *IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 231-236, Italy.

[4] SOCRadar (2021), "Under the Spotlight: Most Popular Dark Web Marketplaces (DWMs)", https://socradar.io/under-the-spotlight-most-popular-dark-web-marketplaces-dwms/, DoA. 05.06.2022.

[5] Işık U. (2009), "Medya Bağımlılığı Teorisi Doğrultusunda İnternet Kullanımının Etkileri ve İnternet Bağımlılığı", *Araştırma,* Vol. 76, No. 28, pp. 29-55.

[6] Yılmaz S. (2016), *İnternet ve İnternet Kafelerin İlk ve Orta Öğretim Öğrencilerine Etkileri* (Master Thesis), Sakarya University, Sakarya.

[7] Dede M. B. (2004), *İnternet*, İnsan Publications, Istanbul, pp. 250-278.

[8] Toğuslu D. Ö. (2002), *Halkla Iliskilerin Yeni Macerası:Internet* (Master Thesis), Social Sciences Institute, Istanbul University, Istanbul.

[9] Ahlgren M. (2022), "100+ İnternet İstatistikleri ve 2022 İçin Gerçekler", https://www.websiterating.com/tr/research/internet-statistics-facts/, DoA. 14.03.2022.

[10] Bright Planet (2022), "Deep Web: A Primer", http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/, DoA. 12.03.2022.

[11] Bergman M. K. (2001), "White Paper: The Deep Web: Surfacing Hidden Value", *Journal of Electronic Publishing,* Vol. 7, No. 1, pp. 502-540.

[12] Kaur S. and S. Randhawa (2020), "Dark web: A web of crimes", *Wireless Personal Communications,* Vol. 112, No. 4, pp. 2131-2158.

[13] Finklea K. (2017), "Dark Web Kristin Finklea Specialist in Domestic Security", https://fas.org/sgp/ crs/misc/R44101.pdf, DoA. 12.09.2022.

[14] Çelik E. (2017), "Deep Web ve Dark Web: Internet'in Derin Dünyası", *DergiPark,* Vol. 2, No. 4, pp. 2-15.

[15] Ciancaglini V., M. Balduzzi, R. McArdle ve M. Rösler (2015), "The Deep Web", *Trend Micro,* Vol. 107, No. 6, pp. 20-25.

[16] Ciancaglini V., M. Balduzzi, R. McArdle and M. Rösler (2015), "Below the surface: Exploring the deep web", *Trend Micro,* No. 120, pp. 1-48.

[17] Ciancaglini V., M. Balduzzi, R. McArdle and M. Goncharov (2013), "Deepweb and Cybercrime", *Trend Micro,* No. 9, pp. 5-6.

[18] Bergman M. K. (2001), "Beneath the Surface of the Ocean of Data: The Deep Web", *Electronic Publishing,* Vol. 7, No. 1, pp. 42-78.

[19] Davis S. and B. Arigo (2021), "The Dark Web and anonymizing technologies: legal pitfalls,ethical prospects, and policy directions from radical criminology", *Crime, Law and Social Change,* No. 76, pp. 367-386.

[20] Guccione D. (2021), "What is the dark web? How to access it and what you'll find", https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html/ , DoA. 04.11.2022.

[21] Georgiev D. (2022), "How Much of the Internet is the Dark Web in 2022", https://techjury.net/blog/how-much-of-the-internet-is-the-dark-web/#gref/, DoA. 26.11.2022.

[22] ACID Teknologies (2014), "Threat Intelligence Company: Dark Web Services", https://www.acid-tech.com/, DoA. 18.05.2022.

[23] Sardá T. (2020), *The Dark Side of the Internet: A Study about Representations of the Deep Web and the Tor Network in the British Press* (Dissertation Thesis), Loughborough University, UK.

[24] Subgraph (2020), "Subgraph OS: Adversary resistant computing platform", https://subgraph.com/, DoA. 13.04.2022.

[25] Whonix (2016), "Whonix", https://www.whonix.org/, DoA. 14.04.2022.

[26] Tails (2019), "Tails: Portable Operating System", https://tails.boum.org/, DoA. 14.04.2022.

[27] Finklea K. M. (2015), "Dark web", *CRS Report,Congressional Research Service,* No. 51, pp. 1–16.

[28] Gehl R. and F. Mckelvey (2019), "Bugging out: darknets as parasites of large-scale media objects", *Media,Culture & Society,* Vol. 41, No. 2, pp. 219-235.

[29] Evers B., J. Hols, E. Kula, J. Schouten, J. A. Pouwelse, R. M. Van der Laan and M. den Toom (2016), *Thirteen Years of Tor Attacks* (Master Thesis), Computer Science, Delft University of Technology, The Netherlands.

[30] Saleem J., R. Islam and M. A. Kabilr (2022), "The Anonymity of the Dark Web: A Survey", *IEEE Access,* Vol. 10, pp. 33628-33660.

[31] Sulaiman M. A. and S. Zhioua (2016), "Attacking Tor through Unpopular Ports", *IEEE 33rd International Conference on Distributed Computing Systems Workshops,* pp. 33-38, USA.

[32] Sun Y., A. Edmundson, N. Feamster, M. Chiang and P. Mittal (2017), "Counter-RAPTOR: Safeguarding Tor against active routing attacks", *IEEE Symposium on Security and Privacy,* pp. 977-992, USA.

[33] Rees M. (2022), "The Top 10 Dark Web Monitoring Solutions", https://expertinsights.com/insights/the-top-dark-web-monitoring-solutions/, DoA. 22.04.2022.

[34] Alert Logic (2018), "Alert Logic Managed Detection and Response", https://www.alertlogic.com/, DoA. 05.05.2022.

[35] AlKhatib B. and R. Basheer (2019), "Crawling the dark web: A conceptual perspective, challenges and implementation", *Digital Information Management*, Vol. 45, No. 17, pp. 51.

[36] Ferry N., T. Hackenheimer, F. Herrmann and A. Tourette (2019), "Methodology of dark web monitoring", *11th International Conference on Electronics, Computers and Artificial Intelligence,* pp. 1-7, Romania.

[37] Crowdstrike (2022), "What is Dark Web", https://www.crowdstrike.com/cybersecurity-101/the-dark-web-explained/, DoA. 25.11.2022.

[38] Ignoffo Z. (2021), "Dark Web Price Index 2021”, https://www.privacyaffairs.com/dark-web-price-index-2021/, DoA. 01.11.2022.

[39] Dikmen T. (2020), "Remote access trojan (RAT) nedir", https://www.btkakademi.gov.tr/portal/blog/remote-access-trojan-rat-nedir-1550/, DoA. 04.07.2022.

[40] Kaspersky (2017), "Tyupkin Virus (Malware) | ATM Security", https://www.kaspersky.com/resource-center/threats/tyupkin-malware-atm-security-malware/, DoA. 05.01.2022.

[41] Tzanetakis M. (2018), "Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time", *International Journal of Drug Policy,* Vol. 56, No. 2018, pp. 176-186.

[42] Reid J. and B. Fox (2020), "Human trafficking and the darknet: Technology, innovation, and evolving criminal justice strategies", *Science Informed Policing Conference,* pp. 77–96, Brazil.

[43] Nazah S., J. Abawajy, S. Huda and M. M. Hassan (2020), "Evolution of dark web threat analysis and detection: A systematic approach", *IEEE Access,* Vol. 99, No. 8, pp. 171796–171819.

[44] Saleh S., J. Qadir and M. U. Ilyas (2018), "Shedding light on the dark corners of the internet: A survey of Tor research", *Journal of Network and Computer Applications,* Vol. 120, No. 114, pp. 1–28.

[45] Collier B. J. (2020), *Critical infrastructure: A Social Worlds Study of Values, Design and Resistance in Tor and the Tor Community* (Dissertation Thesis), Edinburg University Research Archive, Scotland.

[46] Vaccari I., L. Patti, M. Aiello and E. Cambiaso (2019), "Darknet Security: A Categorization of Attacks to the Tor Network", *3rd Cyber Security Conference*, pp. 1-12, Pisa, Italy.

[47] Adewopo V., B. Gonen, N. Elsayed, M. Ozer and Z. S. Elsayed (2022), "Deep Learning Algorithm for Threat Detection in Hackers Forum (Deep Web)", https://arxiv.org/pdf/2202.01448.pdf, DoA. 04.08.2022.

[48] Yeşilyurt Z. (2019), “Deep Web, Web'in Karanlık Yüzü”, https://ab.org.tr/ab15/bildiri/249.pdf, DoA. 20.11.2022.

[49] Siswanto A., A. Syukur, E. A. Kadir and E. A. Suratin (2019), "Network Traffic Monitoring and Analysis Using Packet Sniffer", *Advanced Communication Technologies and Networking*, Vol. 12, No. 14, pp. 1–4.

[50] Kaur G., A. Rahali and A. H. Lashkari (2020), "DIDarknet: a contemporary approach to detect and characterize the darknet traffic using deep image learning", *10th International Conference on Communication and Network Security*, pp. 1-13, Japan.

[51] Ferguson P. and G. Huston (1998), "What is a VPN", http://www.123seminarsonly.com/Seminar-Reports/006/48862380- Virtual-Private-Network.pdf, DoA. 03.05.2022.

[52] Abdulazeez A., B. Salim, D. Zeebaree and D. Doghramachi (2020), "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol", *International Association of Online Engineering*, Vol. 2, No. 14, pp. 31-40.

[53] Alshalan A., S. Pisharody and D. Huang (2016), "A Survey of Mobile VPN Technologies", *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 2, pp. 1177–1196.

[54] Böge S. (2018), *Sanal Özel Ağlarda Veri Güvenliği* (Master Thesis), Karatay University, Konya.

[55] Zhang Z., Y. Q. Zhang, X. Chu and B. Li (2004), "An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN", *Photonic Network Communications*, Vol. 7, No. 3, pp. 213–225.

[56] Karaymeh A., M. Ababneh, M. Qasaimeh and M. Al-Fayoumi (2019), "Enhancing data protection provided by vpn connections over open wifi networks", *2nd International Conference on New Trends in Computing Sciences*, pp. 450-490, Amman.

[57] Cole J. (2016), "Dark web 101", *Air & Space Power Journal,* Vol. 1, No. 2, pp. 3-8.

[58] Gulati H., A. Saxena, N. Pawar, P. Tanwar and S. Sharma (2022), "Dark Web in Modern World Theoretical Perspective: A survey", *IEEE 2022 International Conference on Computer Communication and Informatics*, pp. 1-10, India.

[59] Mohanty H., A. H. Roudsari and A. H. Lashkari (2022), "Robust stacking ensemble model for darknet traffic classification under adversarial settings", *Computers & Security*, Vol. 120, No. 45, pp. 98-200.

[60] He H., Y. He and M. Li (2019), "Classification of illegal activities on the dark web", *2nd International Conference on Information Science and Systems,* pp. 73-78, Japan.

[61] Lashkari A. H., G. Draper-Gil, M. S. Mamun and A. A. Ghorbani (2017), "Characterization of tor traffic using time based features", *ICISSP,* Vol. 69, No. 18, pp. 253-262.

[62] Sarwar M. B., M. K. Hanif, R. Talib, M. Younas and M. U. Sarwar (2021), "DarkDetect: Darknet Traffic Detection and Categorization Using Modified Convolution-Long Short-Term Memory", *IEEE Access*, Vol. 5, No. 9, pp. 113705-113713.

[63] Singh D., A. Shukla and M. Sajwan (2021), "Deep transfer learning framework for the identification of malicious activities to combat cyberattack", *Future Generation Computer Systems,* Vol. 125, No. 40, pp. 687-697.

[64] Jadav N., N. Dutta, H. K. Sarma, E. Pricop and S. Tanwar (2021), "A machine learning approach to classify network traffic", *13th International Conference on Electronics, Computers and Artificial Intelligence,* pp. 1-6, Romania.

[65] Hakim S. A., M. Z. Alam and M. Toufikuzzaman (2021), "Application and Interpretation of Ensemble Methods for Darknet Traffic Classification", *Electronics*, Vol. 11, No. 4, pp.556.

[66] Demertzis K., L. Iliadis and V. D. Anezakis (2018), "A Dynamic Ensemble Learning Framework for Data Stream Analysis and RealTime Threat Detection", *Artificial Neural Networks and Machine Learning ICANN Conference*, pp. 669–681, USA.

[67] Sridhar S. and S. Sanagavarapu (2021), "DarkNet Traffic Classification Pipeline with Feature Selection and Conditional GAN-based Class Balancing", *IEEE 20th International Symposium on Network Computing and Applications,* pp. 1-4, USA.

[68] Iliadis L. A. and T. Kaifas (2021), "Darknet traffic classification using machine learning techniques", *IEEE 10th International Conference on Modern Circuits and Systems Technologies,* pp. 1-4, Greece.

[69] Horasan F. and A. H. Yurttakal (2022), "Darknet Web Traffic Classification via Gradient Boosting Algorithm", *International Journal of Engineering Research and Development,* No. 14, Vol. 2, pp. 794-79.

[70] Ramdan A. R., N. Winyasono and H. Mubarok (2022), "Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet", *Jurnal Sistem Cerdas,* Vol. 5, No. 9, pp. 21-35.

[71] Rust-Nguyen N. and M. Stamp (2022), "Darknet Traffic Classification and Adversarial Attacks", https://arxiv.org/abs/2206.06371, DoA. 13.04.2022.

[72] Lan J., X. Liu, B. Li, Y. Li and T. Geng (2022), "DarknetSec: A novel self-attentive Deep Learning Method for Darknet Traffic Classification and Application Identification", *Computers & Security,* Vol. 116, No.14, pp. 86-190.

[73] Abu Al-Haija Q., M. Krichen and W. Abu Elhaija (2022), "Machine-learning-based darknet traffic detection system for IoT applications", *Electronics,* Vol. 11, No. 4, pp. 556.

[74] Alimoradi M., M. Zabihimayvan, A. Daliri, R. Sledzik and R. Sadeghi (2022), "Deep Neural Classification of Darknet Traffic", *In Artificial Intelligence Research and Development,* Vol. 15, No. 8, pp. 105-114.

[75] Battalov R. I., A. V. Nikonov, M. M. Gayanova, V. V. Berkholts and R. C. Gayanov (2019), "Network traffic analyzing algorithms on the basis of machine learning methods", *Information Technology and Nanotechnology,* Vol. 110, No. 14, pp. 710-850.

[76] Huan W., H. Lin, H. Li, Y. Zhou and Y. Wang (2020), "Anomaly detection method based on clustering undersampling and ensemble learning", *IEEE 5th Information Technology and Mechatronics Engineering Conference,* pp. 980-984, China.

[77] Aswad S. A. and E. Sonuç (2020), "Classification of VPN network traffic flow using time related features on Apache Spark", *IEEE 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),* pp. 1-8, Turkey.

[78] Guo L., Q. Wu, S. Liu, M. Duan, H. Li and J. Sun (2020), "Deep learning-based real-time VPN encrypted traffic identification methods", *Journal of Real-Time Image Processing,* Vol. 17, No. 1, pp. 103-114.

[79] Nigmatullin R., A. Ivchenko and S. Dorokhin (2020), "Differentiation of sliding rescaled ranges: New approach to encrypted and VPN traffic detection", *International Conference Engineering and Telecommunication,* pp. 1-5, USA.

[80] Xian K. (2021), "An optimized recognition algorithm for SSL VPN protocol encrypted traffic", *Informatica,* Vol. 45, No. 6, pp. 40-140.

[81] Nigmatullin R., A. Ivchenko and S. Dorokhin (2021), "Accumulated Generalized Mean Value-a New Approach to Flow-Based Feature Generation for Encrypted Traffic Characterization", *IEEE 11th Annual Computing and Communication Workshop and Conference,* pp. 165-169, USA.

[82] Han Z., E. Li, S. Li, X. Li, C. Kang, R. Deng and Y. Gao (2021), "An Effective Encrypted Traffic Classification Method Based on Pruning Convolutional Neural Networks for Cloud Platform", *IEEE 2nd International Conference on Electronics, Communications and Information Technology,* pp. 206-211, Japan.

[83] Guo Y., G. Xiong, Z. Li, J. Shi, M. Cui and G. Gou (2021), "Combating imbalance in network traffic classification using GAN based oversampling", *IEEE IFIP Networking Conference,* pp. 1-9, China.

[84] Huoh T. L., Y. Luo and T. Zhang (2021), "Encrypted Network Traffic Classification Using a Geometric Learning Model", *IFIP/IEEE International Symposium on Integrated Network Management,* pp. 376-383, Germany.

[85] Jorgensen S., J. Holodnak, J. Dempsey, K. De Souza, A. Raghunath, V. Rivet and A. Wollaber (2022), "Extensible Machine Learning for Encrypted Network Traffic Application Labeling via Uncertainty Quantification", https://arxiv.org/pdf/2205.05628.pdf, DoA. 25.06.2022.

[86] Wei D., F. Shi and S. Dhelim (2022), "A Self-Supervised Learning Model for Unknown Internet Traffic Identification Based on Surge Period", *Future Internet*, Vol. 14, No. 10, pp. 289.

[87] Trang K. and A. H. Nguyen (2022), "A Machine Learning-based Approach for Network Traffic Classification", *Knowledge Engineering and Data Science*, Vol. 4, No.2, pp. 58-140.

[88] Li Y., F. Wang and S. Chen (2022), "VPN Traffic Identification Based on Tunneling Protocol Characteristics", *IEEE 5th International Conference on Computer and Communication Engineering Technology*, pp. 150-156, China.

[89] Hodo E., X. Bellekens, E. Iorkyase, A. Hamilton, C. Tachtatzis and R. Atkinson (2017), "Machine learning approach for detection of nontor traffic", *Proceedings of the 12th international conference on availability, reliability and security*, pp. 1-6, India.

[90] Chari M., H. Srinidhi and T. E. Somu (2019), "Network traffic classification by packet length signature extraction", *IEEE International WIE Conference on Electrical and Computer Engineering*, pp. 1-4, India.

[91] Brooks J. A. and Y. M. Banadaki (2021), "Differentiating Potentially Malicious Darknet Traffic from Benign Network Traffic Using Machine Learning", *Research Conference*, pp. 780-950, Louisiana.

[92] Johnson C., B. Khadka, E. Ruiz, J. Halladay, T. Doleck and R. B. Basnet (2021), "Application of deep learning on the characterization of tor traffic using time based features", *Internet Services and Information Security*, Vol. 11, No. 1, pp. 44-63.

[93] Meslet-Millet F., E. Chaput and S. Mouysset (2021), "SPPNet: An Approach For Real-Time Encrypted Traffic Classification Using Deep Learning", *IEEE Global Communications Conference*, pp. 1-6, Spain.

[94] Lim H. and S. Lee (2021), "Classification of Tor network traffic using CNN", *Journal of Convergence Security*, Vol. 21, No. 3, pp. 31-38.

[95] Ma H., J. Cao, B. Mi, D. Huang, Y. Liu and Z. Zhang (2021), "Dark web traffic detection method based on deep learning", *IEEE 10th Data Driven Control and Learning Systems Conference*, pp. 1050-1200, China.

[96] Gurunarayanan A., A. Agrawal, A. Bhatia and D. K. Vishwakarma (2021), "Improving the performance of Machine Learning Algorithms for TOR detection", *International Conference on Information Networking*, pp. 439-444, Korea.

[97] Liu L., H. Yu, S. Yu and X. Yu (2022), "Network Traffic Obfuscation against Traffic Classification", *Security and Communication Networks*, Vol. 19, No. 4, pp. 17-28.

[98] Yoshimura N., H. Kuzuno, Y. Shiraishi and M. Morii (2022), "DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic", *Sensors*, Vol. 22, No.12, pp. 34-56.

[99] Upadhyay A. (2020), "Classification In Machine Learning", https://medium.com/analytics-vidhya/classification-in-machine-learning-ed30753d9461/, DoA. 06.02.2022.

[100] Garg R. (2018), "7 Types of Classification Algorithms", https://analyticsindiamag.com/7-types-classification-algorithms/, DoA. 17.03.2022.

[101] Pedamkar P. (2020), "Classification of Neural Network", https://www.educba.com/classification-of-neural-network/, DoA. 21.10.2022.

[102] Yıldırım E. (2022), "Yapay Sinir Ağı (Artificial Neural Network) Nedir", https://www.veribilimiokulu.com/yapay-sinir-agiartificial-neural-network-nedir/, DoA. 12.05.2022.

[103] Otchere D. A., T. O. Ganat, R. Gholami and S. Ridha (2021), “Application of Supervised Machine Learning Paradigms in the Prediction of Petroleum Reservoir Properties: Comparative analysis of ANN and SVM Models”, *Petroleum Science and Engineering*, No. 200, pp. 145-200.

[104] Ian G., J. Jean, M. Mehdi, X. Bing, W. F. David, O. Sherill and C. Courville Aaron (2019), "Generative adversarial nets", *Proceedings of the 27th international conference on neural information processing systems*, Vol. 2, pp. 2672-2680, France.

[105] Sherstinsky A. (2020), "Fundamentals of Recurrent Neural Network and Long Short-Term Memory Network", *Physica D: Nonlinear Phenomena, Vol. 12, No. 3,* pp. 404.

[106] Hochreiter S. and J. Schmidhuber (1997), "Long Short-Term Memory", *Neural Computation,* Vol. 9, pp. 1735-1780.

[107] Jović A., K. Brkić and N. Bogunović (2015), "A review of feature selection methods with applications", *38th international convention on information and communication technology, electronics and microelectronics,* pp. 1200-1205, Croatia.

[108] Soyman C. (2015), "İnternetin Yeraltı Dünyası Deep Web Nedir? Nasil Girilir?", https://cahitsoyman.blogspot.com/2015/07/internetin-yeralti-dunyas-deep-web.html/, DoA. 01.03.2022.

[109] Hu Y., F. Zou, L. Li and P. Yi (2020), "Traffic Classification of User Behaviors in Tor, I2P,ZeroNet, Freenet", *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* pp. 418-424, Guangzhou, China.