Sigma J Eng Nat Sci, Vol. 43, No. 6, pp. 2108–2126, December, 2025

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2025.1907

Research Article

A model to protect disaster recovery centers from cyber threats with multi-layered network security architecture

Aykut YILMAZ[1,*], Ali GÜNEŞ[2]

[1]Department of Computer Engineering, Faculty of Engineering, Istanbul Aydin University, Istanbul, 34295,Türkiye
[2]Department of Software Development, Faculty of Applied Sciences, Istanbul Aydin University, Istanbul, 34295, Türkiye

ARTICLE INFO

Article history
Received: 14 May 2024
Revised: 02 July 2024
Accepted: 10 September 2024

Keywords:
Application Vulnerabilities; Cyber Security; Ddos And Botnet&Malware Attack; Disaster Recovery Center; Network Security

ABSTRACT

Services and applications open to the internet are the target of advanced cyber-attacks. Disaster Recovery Centers are one of the most important infrastructures where systems storing critical data operate with active backup mechanisms. As Disaster Recovery Centers systems are critical infrastructures for business continuity, cyber-attacks can cause valuable corporate and personal data to be seized by cyber attackers. This, in return, results in material and moral damages to institutions, individuals and states. An architecture has been developed to meet the security needs against cyber-attacks by utilizing new and emerging technological infrastructures on Disaster Recovery Centers (DRC). The flowchart and pseudocode structure of the architecture have been presented. Additionally, the scientific distinction lies in the success rates demonstrated by the architecture through the combined use of professional applications and framework systems. This architectural infrastructure has been simulated in the application environment and subjected to performance tests with accessible professional applications and real-world cyber-attack vectors. The novelty of this work is that it leverages all of the globally used and accessible EVE-NG, Nessus, OpenVAS, Kali, Parrot, Enterprise Attacker Tactics Techniques and Common Knowledge (MITRE ATT&CK), National Institute of Standards and Technology (NIST) v2 professional applications and framework systems, which are used and accessible worldwide, were used. A comprehensive application was carried out in a simulation environment with 99 different real-world systems, 14 virtual networks, 10 attack vectors, 10 internet protocols, and 150 different attack scenarios. The simulation was conducted in three phases: the first phase involved attacks aimed at partially or completely disrupting internet access, while the second and third phases involved attacks aimed at rendering the Application Service Servers (DMZ) and local network servers unavailable to the internet. As a result of attacks using various techniques on this network, attempts were made to damage target servers and devices. At the time of the attack, the network traffic between the attacker and the target device was examined using Wireshark and Forti Analyzer software. The developed Disaster Recovery Centers architecture ensured the protection of critical infrastructure and systems against cyber-attacks.

Cite this article as: Yılmaz A, Güneş A. A model to protect disaster recovery centers from cyber threats with multi-layered network security architecture. Sigma J Eng Nat Sci 2025;43(6):2108–2126.

***Corresponding author.**
*E-mail address: aykutyilmaz3@stu.aydin.edu.tr

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

INTRODUCTION

The importance of protecting critical and valuable data has increased with the development of technology. Network security infrastructure and components have become critical due to the constant availability of data and the need to protect it. The value of data has led to an increase in cyber-attacks on critical systems where data is stored and protected.

Disaster Recovery Centers (DRC) consists of a combination of infrastructure systems built on critical systems. DRC systems are also vulnerable to cyber-attacks from the outside world because they work within their own cloud systems. Cyber-attacks target critical data and information held in DRC systems. Additionally, cyber criminals attempt to exploit vulnerabilities in DRC systems using a wide range of real-world or zero-day tactics and matrix exploitation methods.

DRC are of critical importance due to the sensitive data they contain. They are also among the infrastructure systems that are most intensely targeted by cyber-attacks. To ensure their effectiveness, DRCs must be designed and maintained with the utmost care and diligence.

Critical infrastructure systems in the DRC are at risk of cyber-attacks. These systems hold valuable data and connect sectors such as transportation, retail, communication, energy, water, and finance to internet networks [1]. To develop functional protection mechanisms for DRC infrastructure systems, Cyber Security and Network Security managers must be open to information sharing. These teams undertake the task of creating systems to detect and prevent cyber-attack vectors, prevent techniques and tactics that may come from internal or external space, whether targeted or untargeted [2].

Infrastructure systems serving the internet may be exposed to the threat of all kinds of cyber-attack vectors. While the current and modern security model to be applied in infrastructure systems prevents the structure from being vulnerable to attacks, the slightest mistake in architectural design will result in the collapse of the designed structure [3]. At this juncture, the main purpose of Cyber Security and Network Security is to ensure the highest level of protection for existing valuable and critical information. Information security encompasses valuable data belonging to individuals and consists of confidentiality, integrity, accessibility, and account authorization [4].

While the risk rate of vulnerability of DRC systems to cyber threats increases in proportion to the value of the data it contains, the DRC infrastructure consists of structures in which the data belonging to the center are used as active-active or active-passive [5]. The cyber world includes definitions that cover information system infrastructures and affect networks [6]. In addition, Cyber Security and Network Security units, infrastructure systems, information technology teams, institutions, states, private sector, and individuals are working to protect and maintain the cycle of valuable data [7]. The protection of data, which is the most fundamental task of security teams, also applies to DRC infrastructure systems. Failure to consider DRC systems as part of security can result in the snowball effect at the slightest vulnerability in the systems infecting the subcomponent systems and resulting in malicious individuals obtaining data [8]. Research has shown that cyber-attacks, tactics, techniques, and vector tools pose a significant threat to modern systems in a variety of ways. [9].

In critical infrastructure systems, emergency management, management of security policies, improvement of protection systems, dependency model of the data infrastructure, backup equipment and management system components should be easily accessible by critical system administrators in the event of an extraordinary situation [10]. DRC systems, which store critical and valuable information, are vulnerable to cyber-attack threats to the extent that they cannot fulfill their functions, allowing information security to be compromised and data to be stolen. When this situation occurs, the systems and infrastructures that interact with the valuable information obtained by individuals or groups that have malicious purposes, are seriously damaged and affected by the vulnerability [11].

Researchers have previously conducted similar studies [12]. The scientific articles written were mainly based on topics such as cyber security threats [13], various artificial intelligence software [14], MATLAB, Python supported machine learning modeling [15], history of cyber-attacks, blockchain technology, SCADA systems, IoT Technology [16-18].

The basic approaches of Cyber Security and Network Security include methods that aim to protect user computers, servers, mobile systems, electronic infrastructures, and prevent access and vulnerability methods, while ensuring that the data transferred between infrastructure systems is transmitted confidentially in whole [19,20]. The solution to structural security problems is the development of new and modern architectures for DRC systems [21]. Analysis of the impact of any vulnerability that may occur in critical infrastructures and risky anomaly operations on the systems is one of the important points for DRC components [22, 23].

Some of the studies in the literature used limited domain attack datasets such as CICDoS2017, CICDDoS2019, CICIoT2023, CIC-MalMem-2022, CICEV2023 and CICIoV2024. These datasets contain only attack vector data such as Distributed Denial of Service (DDoS), Brute Force, spoofing attack, IDS-DoS, Recon, Browser based attacks, Mirai, etc. within a limited and unchangeable area [24-27].

Akbaş discusses local networks and security modeling, network architectures, enterprise OPNET and Virtual private network (VPN-Virtual private network) as well as traditional network model architecture contents [28]. On the other hand, Kör proposes a real-time network security architecture to prevent Web Server and Domain Name System (DNS) attacks, using EKA and SPSS (Statistical Package for the Social Sciences) simulation

environment [29] and Büyükkılıç proposes a cyber security model for Small and Medium Enterprises (SME) systems. National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization (ISO), Control Objectives for Information and Related Technology (COBIT) standards are covered while addressing the basic cyber security practices required for SMEs to cope with cyber security threats [30]. Herrmann and Pridöhl studied cyber security and network security issues, Database Attacks (SQL Injection), DOS, Network Intrusion Detection System (NIDS) systems, Nessus and Metasploit attacks and vulnerability detection [31].

Çinar and Yildirim examined traditional modeling methods by drawing attention to network security and performance problems in large corporate structures and presented network management system architecture design. During modeling, the Open Systems Interconnection (OSI-Open Systems Interconnection) reference model, ISO standards and FCAPS model were used to determine the requirements for the cyber network security model [32]. AVCI, Cyber network, and security architecture developed on SCADA systems against cyber-attacks, is a study on smart natural gas systems. Analytic Hierarchy Process (AHP), Key Performance Indicators (KPI) determination processes were mentioned with the study on cyber-attacks, their effects, consequences, and protection methods [33].

Xiong et al. mapped cyber-attacks using the Enterprise Attacker Tactics Techniques and Common Knowledge (MITRE ATT&CK) matrix and examined the behavior and profile of the attacker from a technical perspective. With the use of matrix, prevention mechanisms for security vulnerabilities were also examined. They proposed a model and conducted test studies [34]. Frayssinet et al. proposes a methodology for cybersecurity management for government organizations. In the article, a cyber security method is proposed for government institutions using the NIST Cybersecurity Framework (CSF) [35]. Özarpa et al. studied cyber-attacks on autonomous vehicles and detection of attacks. They used ten different attack techniques in attack modeling and developed an architecture to prevent system vulnerabilities. They developed simulations on wireless networks and worked on reducing system vulnerabilities by closing direct access to the single processor of the system [36].

Güneş et al. conducted a study on cyber-attacks, attacks and methods on ports and port facilities and developed a model against cyber-attacks on SCADA infrastructures in port and container systems. While the model includes tactical mechanisms and protection methods against cyber-attacks, they simulated different scenarios. They utilized standards such as NIST, ISO 31000, ISO 27001 [37]. Kara et al. created a software tool to identify security vulnerabilities and detect cyber-attacks. They also simulated cyber-attacks [38]. Artificial networks, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have been used in studies for anomaly detection. Attack scenarios were performed on the CSE-CIC-IDS2018 dataset, and the performance outputs of different artificial networks were compared [39].

There are different studies on artificial networks with ready-made data sets. These include machine learning algorithms such as Support Vector Machine (SVM), Naïve Bayes (NB), Artificial Neural Network (ANN), K-Nearest Neighbor (KNN-K-Nearest Neighbor) and Gated Recurrent Units (GRU) [40,41].

Numerous studies on the IoT ecosystem have focused on DDoS, malware, worms [42], data theft, trojans [43], rootkits, botnet infrastructures [44], backdoors, viruses, application vulnerabilities and communication protocols [45]. They conducted a study on IoT architecture targeted by various attack methods and compared the systems threatened by attacks on infrastructures and categorized the attacks [46,47]. Karaman et al. discuss diverse types of cyber-attacks, including Botnet, BruteForce-Web, BruteForce-XSS, FTP-BruteForce, BruteForceSSH, DDoS, Slowris, DoSattacks-GoldenEye, DoSattacks-Hulk, and DoSattacks-SlowHTTPTest. They used the CSE-CIC-IDS2018 dataset and artificial intelligence models to detect anomalies and analyze the damage caused by these attacks. The authors employed several machine learning methods, such as ANN, KNN, Naive Bayes, and SVM. They proposed a flowchart model to illustrate their findings. [48,49]. Erdem, developed a new firewall architecture different from traditional firewall models with Dynamic Intelligent Firewall Architect (DIFA). In accordance with this architecture, DIFA has developed and simulated a network security architecture that can manage itself and creates access rules by analyzing anomalies and malware through passing traffic data [50]. While there are numerous studies in literature, none have focused on modelling the architectural infrastructure of DRC. The aim of this study is to contribute to academic literature by addressing this gap.

MATERIALS AND METHODS

Malicious attacks and threats present a variety of risks, including those posed by malware, DDoS, botnets, code blocks, viruses, trojans, phishing attacks, and worms. [51]. Detecting and preventing these attacks in advance can be insured by systems with effective architectural design [52-55]. Cybercriminals have been attempting to exploit vulnerabilities in DRC systems with large scale and diverse attack vectors using real world zero-day tactics and matrix exploitation methods.

DRC critical systems vulnerabilities are large scale and operate by stealing valuable information, disrupting critical systems and services, and demanding ransom. Preventing cyber attackers is possible with a well-designed cyber network security architecture. Many advantages for safeguarding critical systems are offered by this study's design of the architecture model, which will be built using

next-generation architecture, layers, frameworks, and processes in accordance with the standard DRC modeling specified for the pertinent structures.

In this study, while developing the infrastructure architecture, frameworks such as EVE-NG simulator application, MITRE ATT&CK Enterprise, NIST were used. The simulation environment aims to create the functioning mechanism of living structures by processing scenarios in the real world.

While the attacks were conducted on an attacker profile sample in the internet environment, DDoS (Distributed Denial of Service), Zombie Computers (Botnet), Malware, browser service HTTP/HTTPS attacks, Application Vulnerabilities were implemented. The contribution of the multi layered and complex structure of the DRC architecture to the cyber network security factor has played an active role in preventing cyber threats, protection, and resistance against attacks.

Architectural Model Scenario and Roadmap

Traditional DRC systems are created to ensure business continuity, consisting of switches, routers, firewalls, server systems and data backup units with simple and limited features. Next-generation DRC architectures include more complex, flexible structures and generally have more features. It consists of switches with advanced features, routers, firewalls, threat detection and prevention systems, sandbox devices with malicious file and email scanning systems, data encryption and authentication systems, and load balancers systems. Next-generation network architectures are designed to be more flexible, secure, performance-driven and meet modern business needs such as digital transformation and cloud computing, such as large data centers and the Internet of Things (IoT). Infrastructure modeling enables the examination and construction of real-world simulations of critical systems using these structures. Infrastructure architectures that emerge through architectural maturity modeling protect systems against unforeseen attacks by analyzing vulnerabilities and weak points on critical systems.

In this study, cyber network and security DRC architectural model design was realized within the framework of confidentiality, integrity and accessibility concepts for critical infrastructure services where information and data flow take place. MITRE ATT&CK Enterprise and NIST v2 framework standards were used to design the architecture. MITRE ATT&CK Enterprise is a knowledge base and contains tactics, techniques and general knowledge that cyber attackers can use. The goal here is to help cybersecurity experts better understand the activities of attackers and create a matrix to develop defense strategies against these activities. [56,57]. The purpose of using NIST v2 in the study is to help in the management of the cyber risk map, prioritization, and measurement of improvements [58]. These framework standards have been reviewed, utilized and incorporated in the study. The framework is designed in accordance with the Multi-tier Model.

Definition of the Problem of DRC Infrastructure

DRC systems are the infrastructure containing the most critical data and components of a structure. These infrastructures are designed to ensure that the valuable data flowing in the live environment continues uninterrupted. As seen in literature review, architectural studies on DRC infrastructures in the academic field are quite insufficient. The studies that have been conducted are combined with various network topologies of insufficient maturity and reveal cyber network security models. In this study and to contribute to this academic gap, a cyber network security model has been developed for the DRC system and infrastructures architecture with scientific observation and perspective. The modern infrastructure architecture, which will be designed in accordance with the DRC infrastructure, will be developed in line with the data from the DRC system administrators, aiming to increase the maturity level of critical infrastructures, while reducing anomaly possibilities and risk map.

Architectural Simulation Scenario

To demonstrate the DRC architecture infrastructure, a real-world infrastructure, a simulation environment will be created. A fictitious multinational Company A is a retail center with more than 10,000 employees and 300 locations in and out of the country. The company generates annual revenues of $2 billion and allocates 2% ($40 million) of its revenues each year to the Infrastructure and Systems Department. The company wants to separate the traditional network infrastructure from the DRC infrastructure. The DRC architecture consists of specially designed, complex security systems against cyber-attacks. In this structure;

1. The connection line with three different Internet Service Providers (ISPs) has been redundantly established via Radio Link (RL) and Fiber Lines (MPLS). The inter-branch connection operates over Software-Defined Networks (SD-WAN). The infrastructure functions in an Active-Active configuration, providing real-time data synchronization. In the event of a failure at the data center located at the headquarters, it performs load balancing and takes over the traffic.
2. A DWDM (Dense Wavelength Division Multiplexing) redundant optical line will be used between the headquarters data center and the DRC. With this line, data will be synchronized instantaneously in a fast and secure manner. In this way, the traffic in between is encrypted.
3. The local DDoS protection system will redundantly block or accept unwanted accesses, ports, and services by filtering against requests from the outside world. Protection will be at layer 3,4,7 level.
4. Intrusion Prevention System & Intrusion Detection System (IPS&IDS) Firewall will protect the signature-based vulnerability and attack vectors in the legal

traffic passing through the DDoS device in the architecture with the most advanced signature database and will be capable of clearing zero-day anomaly attacks with artificial intelligence, machine learning and deep learning algorithms.

5. Packets that pass through the DDoS and IPS&IDS protection systems, which are built redundantly, will pass through the internet firewall and access the Application Layer Firewall (WAF-Web Application Firewall) for Web applications and use Load Balancing (LB-Load Balancer) and Global Server Load Balancing (GSLB-Global Server Load Balancing).
6. The DRC Fabric will be capable of distinguishing traffic from the Internet, Application Service Servers (DMZ), VPN or Campus environments. Traffic can be scanned in DMZ traffic and in the Sandbox product.
7. Incoming and outgoing traffic will pass through the Firewall installed in a redundant structure. The Firewall will create a socket to the address that the packet will try to access locally and send packets to the central router.
8. The central router will be built on a system that transfers data between layers 2 and 3 and at the same time achieves scalable 40GB/100GB port transfer speeds that are capable, flexible, and performant in accordance with the data center architecture. The data will pass through the central application architecture and protect the structure at layer 2 and 3 levels. Thus, it will establish an integrated structure in the architecture by providing integration with critical infrastructure systems.
9. Incoming traffic reaches the center through an IPsec tunnel using the SD-WAN architecture and secured with MPLS. The architecture can block local traffic between networks in the L2 and L3 layers. Certificate-based authentication systems prevent malicious network movement horizontally or vertically within the architecture.
10. In the subsections of the architecture, products that follow cyber-attack prevention tactics and mechanisms should be able to use advanced antivirus systems, classification products, attacker deception systems, network listening and anomaly detection software, vulnerability scanning and log reporting systems.

Similar simulations [59-62], [63-66] and scenario approaches are available in literature [67-70].

Architecture Model

To protect DRC systems from cyber-attack vectors, infrastructure design should be developed for the worst-case scenario. The architecture aims to prevent attacks from the internet environment at a high rate. To protect infrastructure systems from cyber-attacks and other forms of attack, it is designed in three phases.

In phase one of the DRC architecture depicted in Figure 1, the architecture is divided into different layers to separate the systems by design and to reduce the attack area to a micro level. Furthermore, the layering method allows different services to be provided and operated at the same time. Due to the structure of the three-layer architecture, traffic flow within the structure takes the form of a transfer to a lower layer and onward.

The architecture, internet and campus structure are designed to be redundant with three different internet providers. Cyber threats and possible access interruptions will continue to operate with high availability. DDOS devices prevent low-credibility access from the outside, while a wide variety of flood and port scanning operations used by attackers are blocked at the access layer. These devices

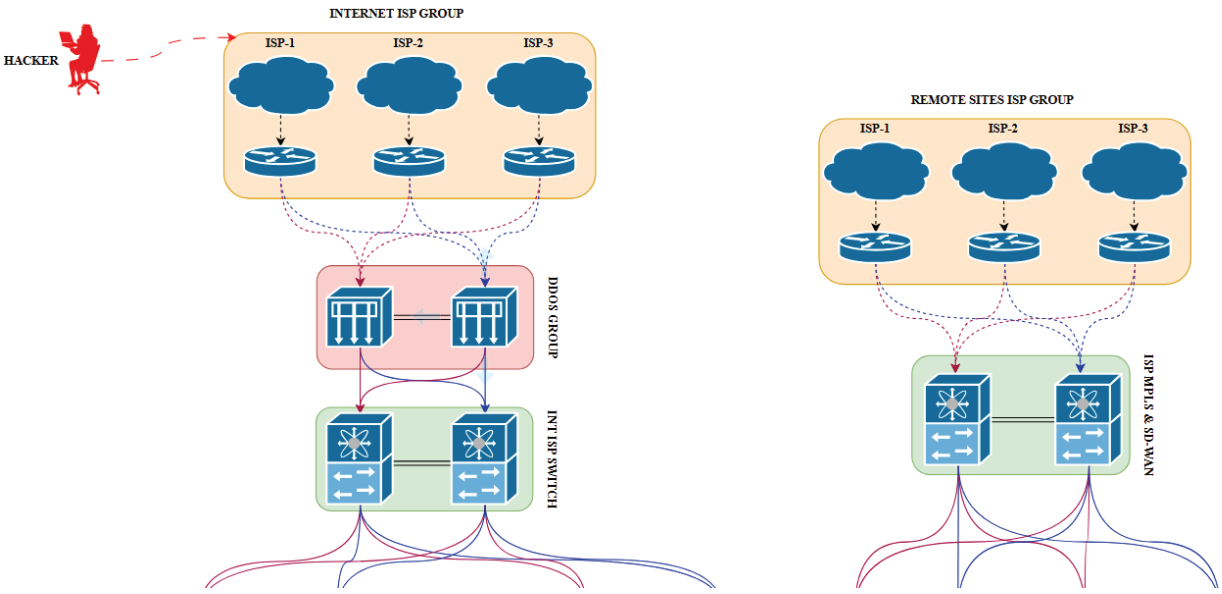

Figure 1. Tier-1 ISP, DDoS, SD-WAN MPLS architecture.

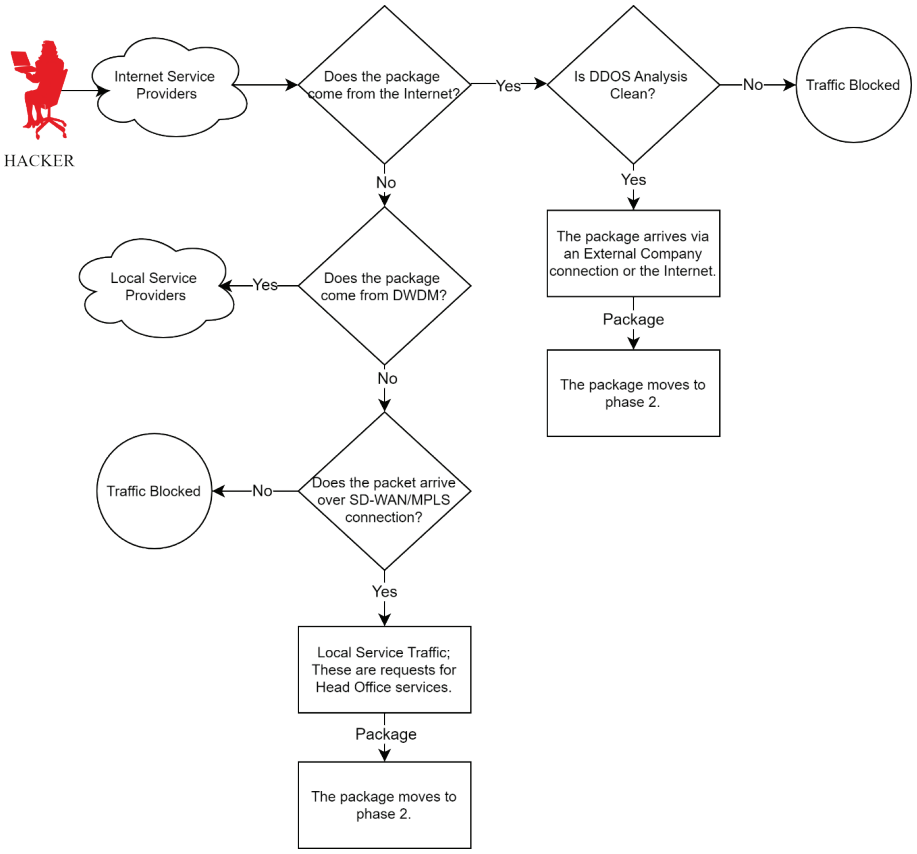

Figure 2. Tier-1 ISP, DDoS, SD-WAN MPLS flowchart.

will prevent BOTNET and DDOS attacks that may come from the volumetric and application layer or from different sources. Two DDOS and four internet provider equipment are located in the building with redundancy. As the campuses are part of the local network traffic, DDOS equipment is not located.

In the flowchart in Figure 2, it can be seen that, as a result of the inspection of the traffic over the internet, if it contains malicious packets, it is blocked, and if it is a clean packet, it is allowed to pass to the second stage. In the case of a local DWDM, SD-WAN, MPLS traffic, it is allowed to pass through the same query mechanisms.

```
Pseudocode Algorithm-1
1. Start;
2. Input: Malicious Data Traffic by the Attacker
3.   ISP1 Traffic
4.   ISP2 Traffic
5.   ISP3 Traffic
6.      If Packet Traffic is via the Internet?
7.           Answer > YES
8.              If Is DDoS Analysis Clean?
9.                 Answer > YES
10.                   go to Forward Package (Package comes via External Company connection or Internet)
11.                      go to Package moves to stage 2
12.                If Answer > NO
13.                   Launch and Block DDoS Protection System
14.          Answer > NO
15.             If Traffic Is DWDN Fiber?
16.                Answer > NO
17.                   If Does the If Package arrive via SD-WAN or MPLS connection?
18.                      go to Forward Package (Local Service Traffic; Requests for Headquarters services)
19.                         go to Package moves to stage 2
20. End
```

Figure 3. Tier-1 ISP, DDoS, SD-WAN MPLS pseudocode.

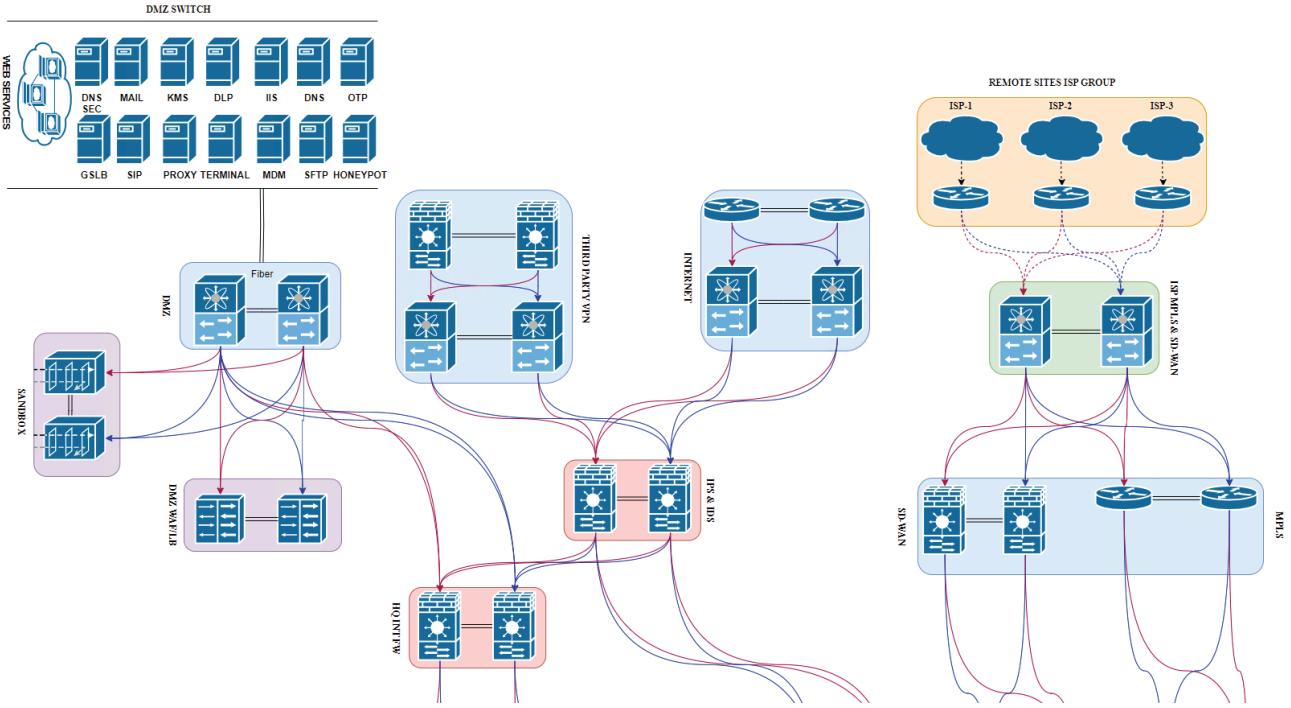

Figure 4. Tier-2 Internet, security systems, web services and remote site architecture.

Figure 3 shows the pseudocode structure of the first stage.

The traffic, which proceeds in accordance with the structure of the cyber network security architectural design with the second stage seen in Figure 4, is analyzed and controlled by passing through various control systems at each stage. By passing through the WAF/LB device, it is cleaned from any attack vectors that may be in HTTP or HTTPS traffic and the load is transferred to the upper layers in a balanced manner. If there is any attached file during data exchange through e-mail or file sharing systems, the Sandbox product scans it and the harmful file is blocked. Traffic coming from the internet and traffic from SD-WAN and MPLS campuses are separated and backed up in this layer.

While the rule sets in the architecture provide access to the traffic by macro and micro segmentation, IPS&IDS forces various malicious web traffic, potentially infected documents to pass through the controls on the systems and ensures that the traffic continues by cleaning and stopping possible threat vectors.

The architecture is based on four different structures: DMZ (Web Services), External Company VPN Lines, Internet Line and Campus area. The basic components of the architecture are designed by preserving the redundancy requirements of the active devices within the structure. In the second phase of the architecture, six fiber switches, two IPS&IDS firewalls, two internet firewalls, two remote site firewalls (SD-WAN firewall), four routers, two web application firewall (WAF), two sandboxes were configured. Redundancy and load distribution integrations between the devices were added to the design.

In the graph shown in Figure 5, detailed analysis of the incoming data packet continues to be performed. Due to the architecture layers, at each stage, it is checked whether the incoming traffic is a cyber-attack or a reliable traffic. At this stage, algorithms such as deep learning, artificial intelligence, machine learning used in systems can work. In Phase 2, each packet is scanned by DDoS, IPS&IDS, WAF/LB and firewall devices. Denial of service attacks attempted by cyber attackers are prevented by these protection walls. In the architecture, incoming traffic is evenly distributed to the subsystems through load balancing systems. SD-WAN and MPLS traffic, which are local traffic, can be transmitted as secure traffic with this infrastructure.

Figure 6 shows the pseudocode structure of stage 2.

The infrastructure equipment, which is the third stage of the architecture is shown in Figure 7. In the architecture, local network infrastructures rise on two different structures: local network infrastructure systems and service systems architecture zone. The basic components of the architecture were designed by preserving the redundancy requirements of the active devices within the structure. In the third phase of the architecture, twelve fiber switches, two wireless network controllers (WLC), two local firewalls, two remote site firewalls (SD-WAN firewalls), four routers and DWDM fiber, it is configured as tow web applications firewall (WAF) equipment. Redundancy and load distribution integration between the devices are shown in detail in the design.

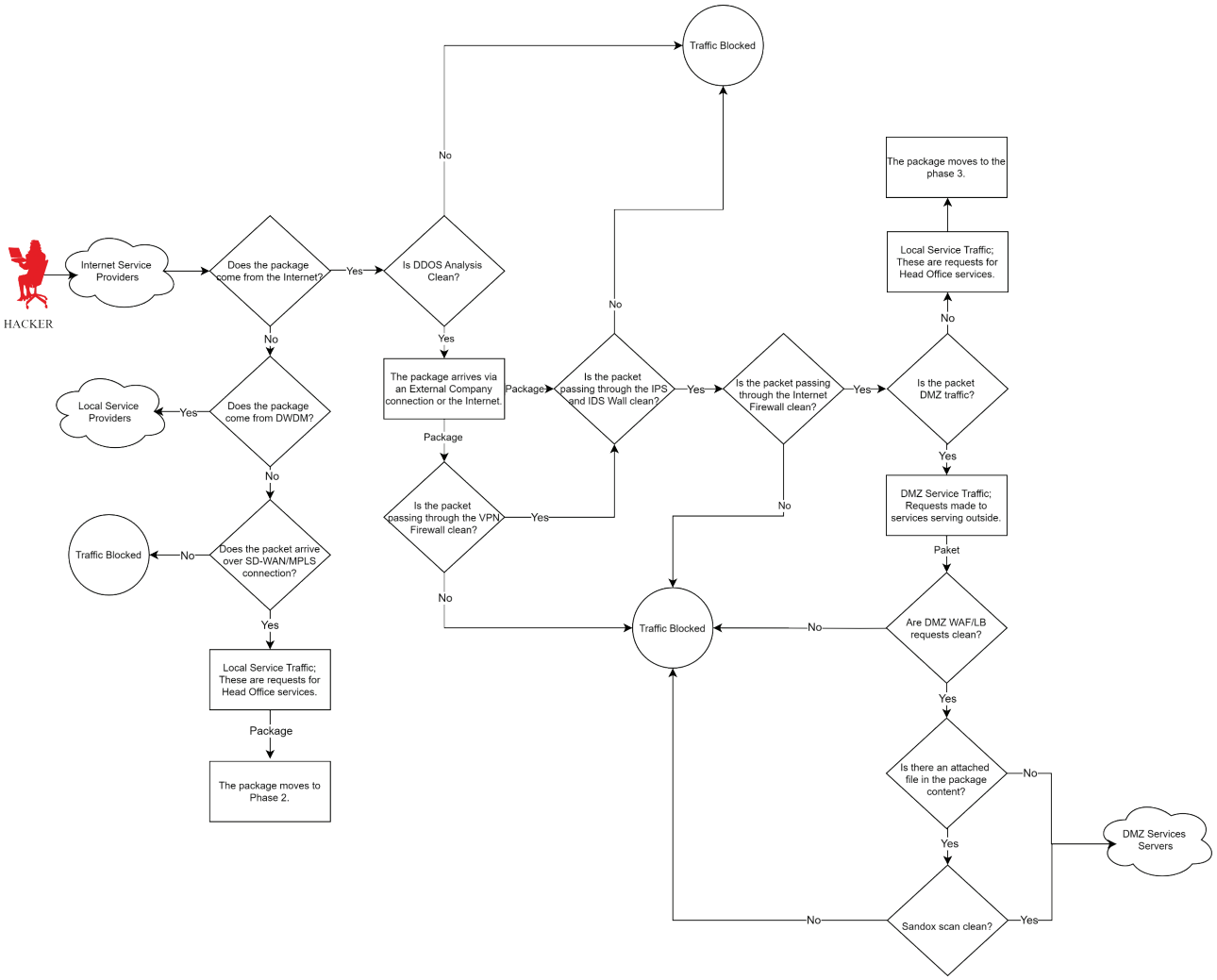

Figure 5. Tier-2 Internet, security systems, web services and remote site flowchart.

The local infrastructure, which is the last stage of the architecture, is shown in Figure 7. In the architecture, the packets that pass through different protection services until they access the local infrastructure are cleaned from DDoS, Botnet, Malware, Application vulnerability and other attacks until they reach the third stage.

The design of the DRC model architecture aims to avoid the slightest design weakness that may occur in the prevention of cyber threats. With the three-layer structure existing in the relevant architectural design, each layer has been developed as a redundant structure within itself. In architectural design, the level of breakdown between layers has been in micro and macro dimensions.

The flowchart in Figure 8 shows that the three-layer structure and the traffic circulating between the layers are in communication by passing through security transitions, devices that can be built with different algorithms and logic. Thus, the DRC architecture can ensure that the traffic generated by applying strict security rules in the transportation of critical data between layers is capable of ensuring that the traffic progresses within the desired security regulations.

Cyber Threats and Attack Vectors

With the DRC architecture developed in Figure 9, an important level of protection from cyber threats and attack vectors that may come from the internet environment is provided. Cyber threats are constantly researched academically and scientifically, and various methods are proposed to prevent attacks. The DRC architecture developed in Figure 9 is one of these architectural methods. Cyber threats and attacks, security gaps and risks, vulnerabilities and other pests, attempt to make systems inaccessible by using a variety of methods and techniques [71,72]. Some of the methods used by cyber attackers are viruses [73], worms [74], trojan horses [75], hackers [76], rootkits [77], spyware [78], ransomware [79], command injection [80], DDoS [81], software, firewall [82,83], TCP/IP, wireless [84], operating system, web servers and many other infrastructure vulnerabilities [85,86].

```
Pseudocode Algorithm-2
1.Start;
2. Input: Malicious Data Traffic by the Attacker
3.   ISP1 Traffic
4.   ISP2 Traffic
5.   ISP3 Traffic
6.      If Packet Traffic Is Via the Internet?
7.            Answer> YES
8.               If is DDoS Analysis Clean?
9.                  Answer > YES
10.                    go to Forward Package (Package comes via External Company connection or Internet)
11.                       If is IPS and IDS Analysis Clean?
12.                          Answer > YES
13.                             If is Internet Firewall Analysis Clean?
14.                             Answer > YES
15.                                   If Forward If Packet (Is the packet DMZ traffic?)
16.                                      If >YES (DMZ Service Traffic; Requests made to services serving outside.)
17.                                         If DMZ WAF/LB requests are clear?
18.                                            Answer > YES
19.                                               If is there any attached file in the package content?
20.                                                  Answer> YES
21.                                                     If Sandbox scan is clean?
22.                                                        Answer > YES
23.                                                           DMZ Services Servers
24.                                                        Answer > NO
25.                                                           Launch and Block Sandbox Protection System
26.                                                  Answer> NO
27.                                                        DMZ Services Servers
28.                                            Answer > NO
29.                                               Launch and Block WAF/LB Protection System
30.                                      Answer > NO (Local Service Traffic; Requests for Headquarters services.)
31.                                         go to Package moves to stage 3
32.                             Answer> NO
33.                                Launch and Block Internet Firewall Protection System
34.                          Answer> NO
35.                             Launch and Block IPS and IDS Protection System
36.                    Answer> NO
37.                       Launch and Block DDoS Protection System
38.               Answer> NO
39.                  If Traffic Is DWDM Fiber?
40.                     Answer> YES
41.                        go to Package moves to stage 3
42.                     Answer> NO
43.                        If Does the Package arrive via SD-WAN or MPLS connection?
44                            go to Forward Package (Local Service Traffic; Requests for Head Office services)
45.                           go to Package moves to stage 3
46.
47.   End
```

Figure 6. Tier-2 Internet, security systems, web services and remote site pseudocode.

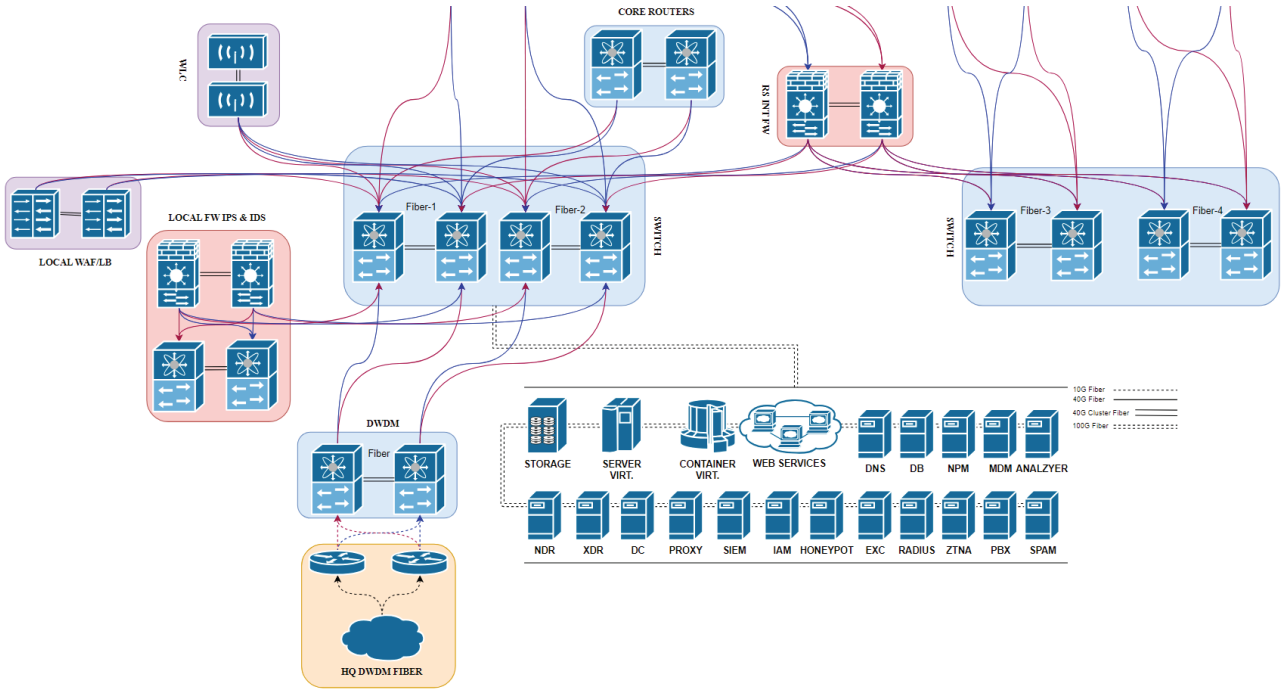

Figure 7. Tier-3 Local Infrastructure, services systems architecture.

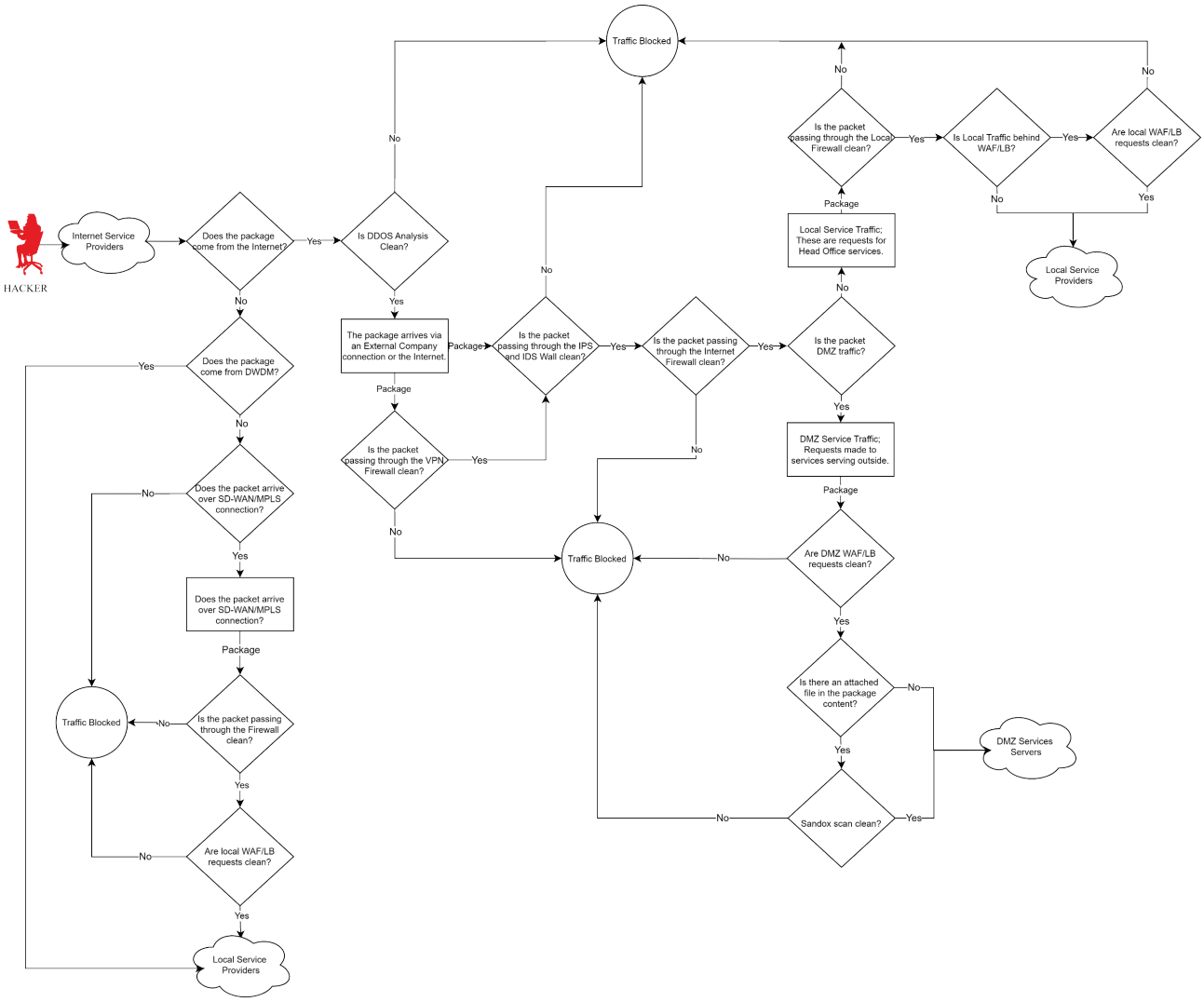

Figure 8. Tier-3 Local infrastructure, services systems flowchart.

MODEL TEST AND PERFORMANCE

The architectural model setup and roadmap, problem definition, simulation scenario, model architecture structure was developed with the cyber network and security architecture on the DRC infrastructure in Figure 9. Its infrastructure and component stages and detailed information of the developed architecture are given in Figures 1-9.

To prove the accuracy of the data obtained in the simulation environment, 150 different test operations were repeated in the simulation environment. For the simulation environment, open access, globally recognized professional infrastructure products were used. Simulation infrastructure and component systems can use algorithms and methods such as machine learning and artificial intelligence. The infrastructure components used in the simulation environment are given in Table 1.

A DRC infrastructure with a three-tier architecture was developed with the required systems. Cyber-attacks were

Table 1. DRC simulation software and hardware list

Pieces	Systems
1	Intel i7 12th Gen, 32GB RAM, 500GB M2 SSD
1	VMware® Workstation 17 Pro
1	EVE-NG 5.0.1 network and security simulator
1	Linux Kali, Parrot systems
1	OpenVas, Nessus10 attack simulators
1	Fortinet Analzyer 7.4.1
1	Wireshark 4.0.10
2	Fortinet Sandbox 4.4.4
2	Fortinet wireless controller 7.4.1
7	Internet service provider
14	VLAN
18	Fortinet Firewall,IPS&IDS, DDOS, WAF/LB 7.4.1
21	Windows server 2022 and Linux servers
28	Cisco Router, Switch L2&L3

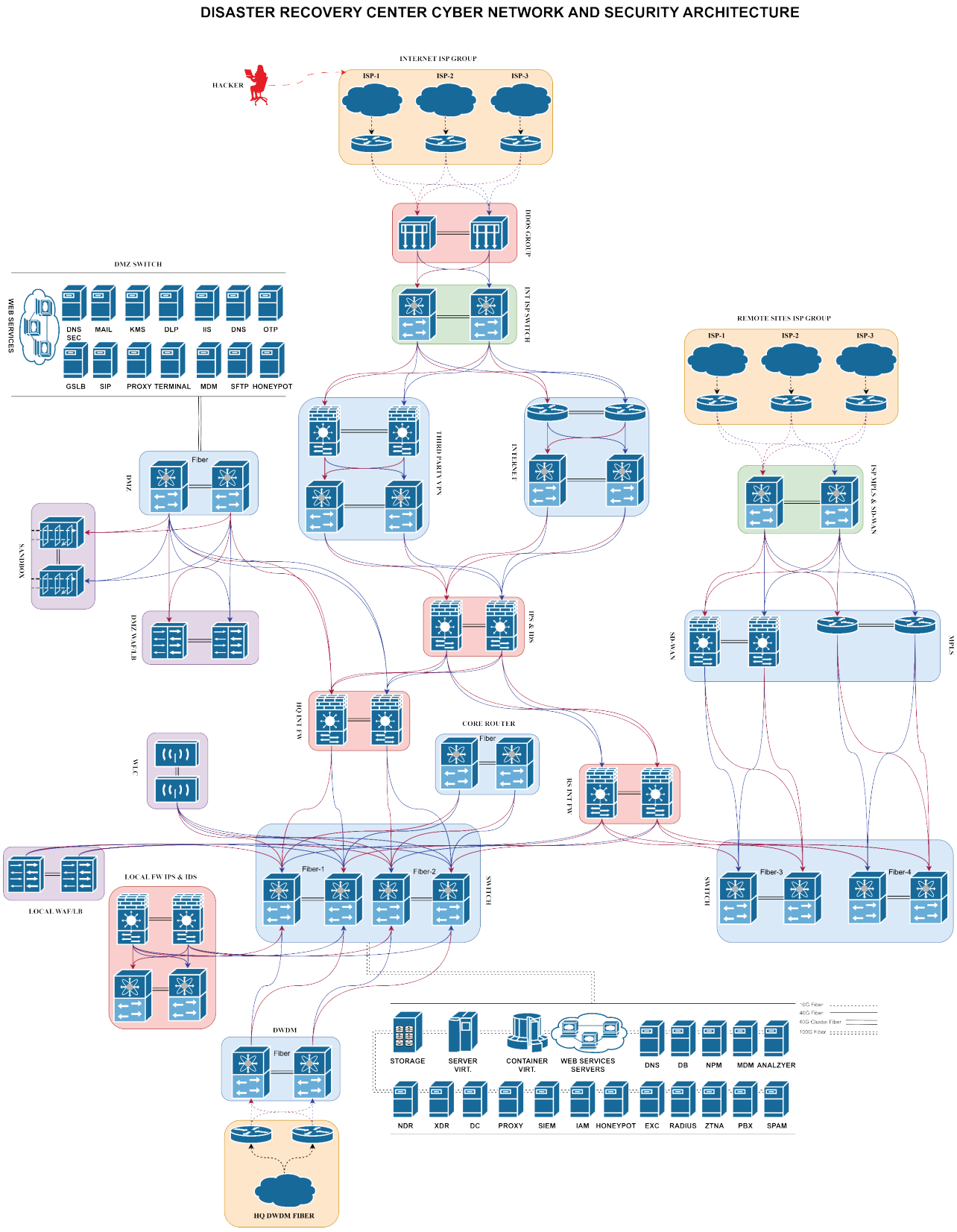

Figure 9. Disaster recovery center (DRC) cyberspace network security architecture.

made on the architecture and the effects of the system as a result of these attacks were observed with professional analysis software. The attacks generated by the attack simulators on the servers, software and hardware in the system infrastructure were designed and created to be similar to the attacks that can come from the internet environment.

In phase 1, the following results were obtained as a result of cyber-attacks on DDoS, SD-WAN and MPLS architecture with packets coming from the internet environment. During this phase, repetitive attacks were conducted, and random service servers that may be open to the internet within the infrastructure were selected and attacks were conducted to disable the service.

Table 2. DDoS, SD-WAN and MPLS attacks

Attack vector	Service	Number of attack	Protection %
tcp_syn_flood	http-https ssh-ftp-smb	101,938,66	99,99
udp_flood	dns-smb snmp-ntp	214,468,22	99,99
port_scanning	1-65535	995,941,89	99,99
land_attack	http-https icmp	221,040	99,99
smurf_attack	icmp	285,234,41	99,99
random_source attack	http-https	2,382,038,154	99,99
slowloris	http-https	31,680	99,99
rstfin_flood	ssh-https	1,546,702,37	99,99
syn_ack_flood	ssh-https	1,356,082,319	99,99
icmp_sweep	icmp	239,598,935	99,99
Total blocked attack numbers		3,977,719,408	

Table 3. Botnet& Malware attack vectors

Attack Vector	Malware	Victim	Source	Count	Total
“Gh0st.Rat	Botnet C&C	53	13	134	92.326
“Mirai.Botnet	Botnet C&C	8	33	52	13.728
“Xtreme.RAT	Botnet C&C	11	2	25	550
“Bladabindi	Botnet C&C	8	11	22	1.936
“JS/TiMove	Virus	1	2	27	54
“ASP/WebSh	Virus	1	2	18	36

Table 4. Application vulnerability attack vectors

Attack vector	Victim	Source	Count	Total
Zyxel.zhttpd.Webserver.Command	51	313	461	7,358,943
ThinkPHP.Controller.Parameter.RCE	4	85	150	51,000
Bash.Function.Definitions.RCE	8	6	282	14,100
Apache.Log4j.Error.Log.RCE	7	8	174	9,744
Remote.CMD.Shell	2	4	396	3,168
vBulletin.tabbedcontainer.Template	4	6	96	2,304
Citrix.Application.Delivery.Control	3	5	102	1,530
Netcore.Netis.Devices.Hardcoded	2	7	72	1,008
vBulletin.Routestring.widgetConfi	4	6	41	984
F5.BIG.IP.Traffic.Management.Us	2	4	97	776
MS.IE.XSS.Filter.Error.Handler	2	4	68	544
Ivanti.Avalanche.ImageFilePath	1	4	57	228
Oracle. WebLogic. Fusion. Middle	1	3	55	165

In Table 2, it is observed that with various attacks made with Hping3, LOIC, Hydra and Nmap applications, the infrastructure of the first stage security system, attack vectors are successfully blocked by 99.99% in the simulation environment. No interruption was observed in the internet services provided during the attack and the system continued to operate.

Similar architectural infrastructure tests were conducted in the second and third stages, and denial of service and application vulnerability attacks were made against security systems (IPS & IDS, firewall, WAF, Sandbox) and web services through which traffic from the internet passes.

For the purpose of denial of service for DRC architecture, attack simulation tools (Nessus, OpenVAS, Parrot) were used to simulate Botnet and Malware attacks from multiple sources simultaneously, and Table 3 shows the total number of attacks of Botnet & Malware attack vectors.

Vulnerability tests were conducted on many applications that run on the services and that may have a weak point in terms of vulnerability of infrastructure systems. As a result of the application vulnerability tests shown in Table 4, there are more than twenty application vulnerability attacks detected, out of which thirteen vulnerabilities are

Table 5. HTTP / HTTPS protocol attacks

Attack vector	Number of attack
SQL injection	9.661
XSS	8.763
Cross.Site.Scripting	8.537
HTTP.URI.SQL.Injection	2.577
TCP.Data.On.SYN	2.507
HTTP.Request.URI.Directory.Traversal	1.434
Nmap.Script.Scanner	1.349
Web.Server.Password.File.Access	1.062
Zyxel.zhttpd.Webserver.Command.Injection	461
Remote.CMD.Shell	396
Code Injection	305
Linux.Kernel.TCP.SACK.Panic.DoS	222
ZGrab.Scanner	204

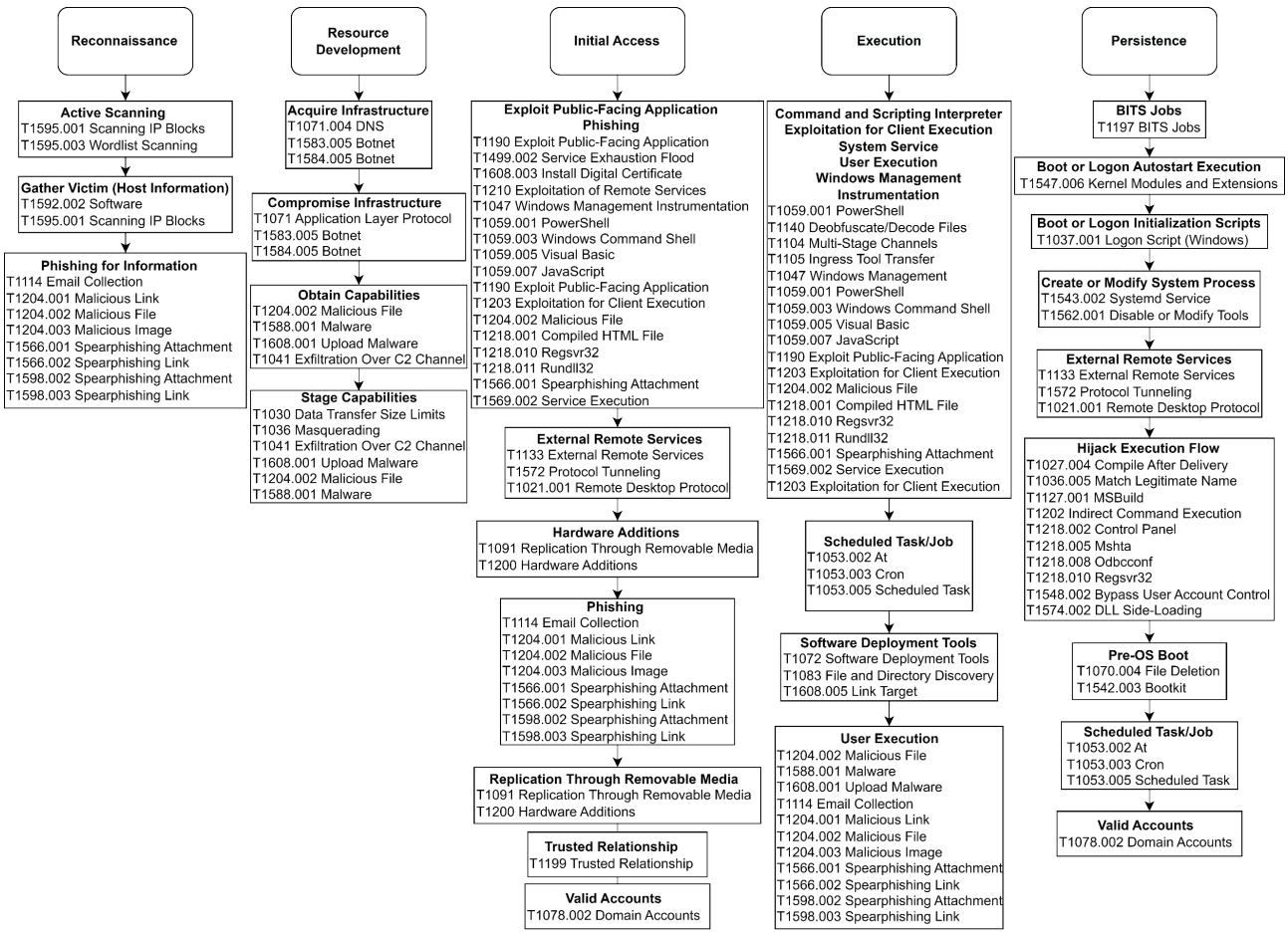

Figure 10. MITRE ATT&CK threat modeling and defense methodology map-1.

shown for illustration. The architectural infrastructure system can detect more than 29,462 application vulnerabilities with the signature database and countermeasures can be taken. Table 4 shows the most vulnerable application layer vulnerabilities of the systems in the attack area.

HTTP/HTTPS protocol attacks were performed using cyber-attack simulation tools (Nessus, OpenVAS, Parrot) in order to block services running in the DMZ infrastructure. While web services are invoked through HTTP/HTTPS protocols, these protocols have many security vulnerabilities due to their nature. The vulnerability attacks detected and blocked by the WAF system are shown in Table 5. It was observed that these attacks were blocked by the DRC architecture.

MITRE ATT&CK is used to classify cyber threat vectors, create attacker profiles and take precautions. This

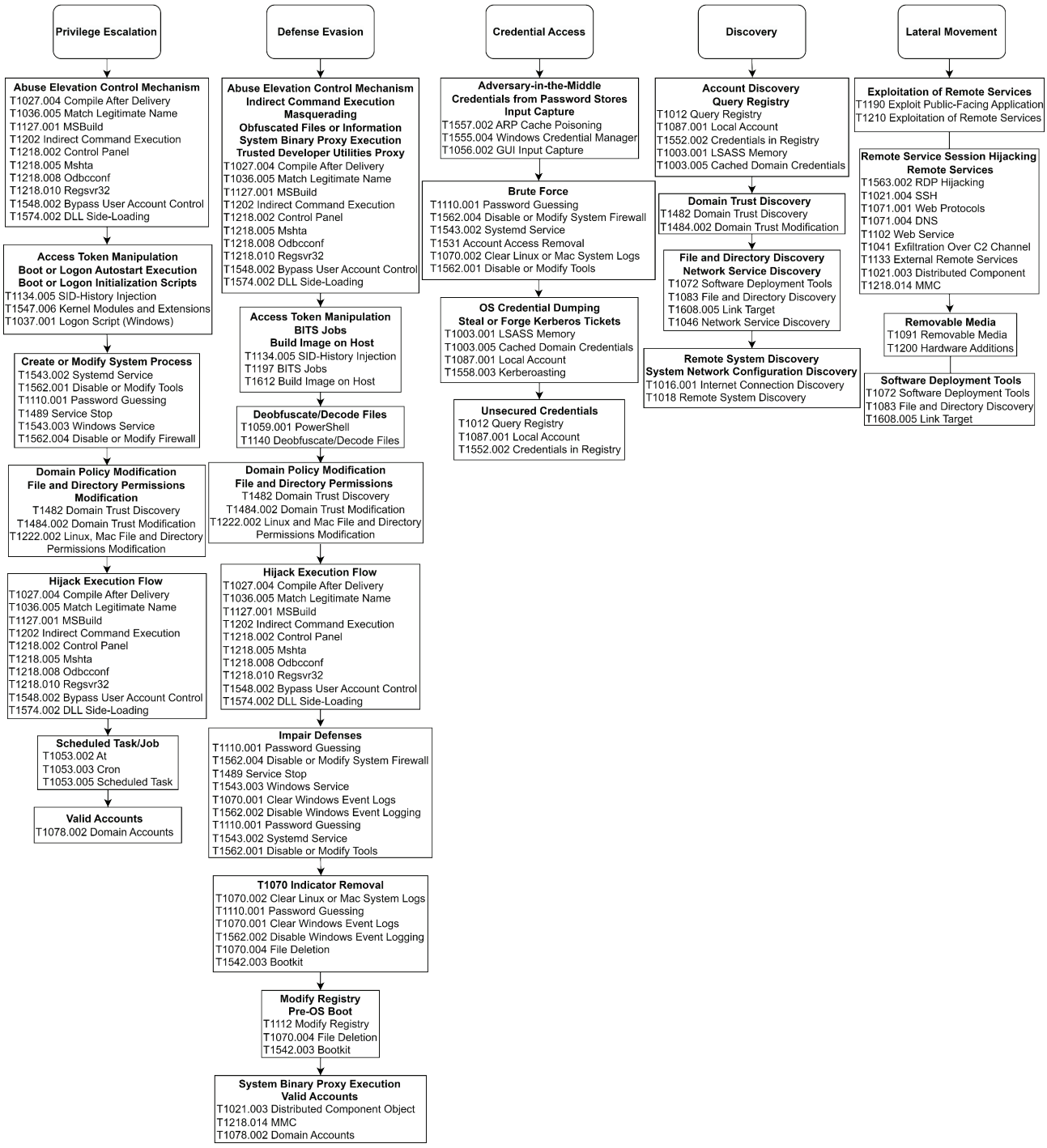

Figure 11. MITRE ATT&CK threat modeling and defense methodology map-2.

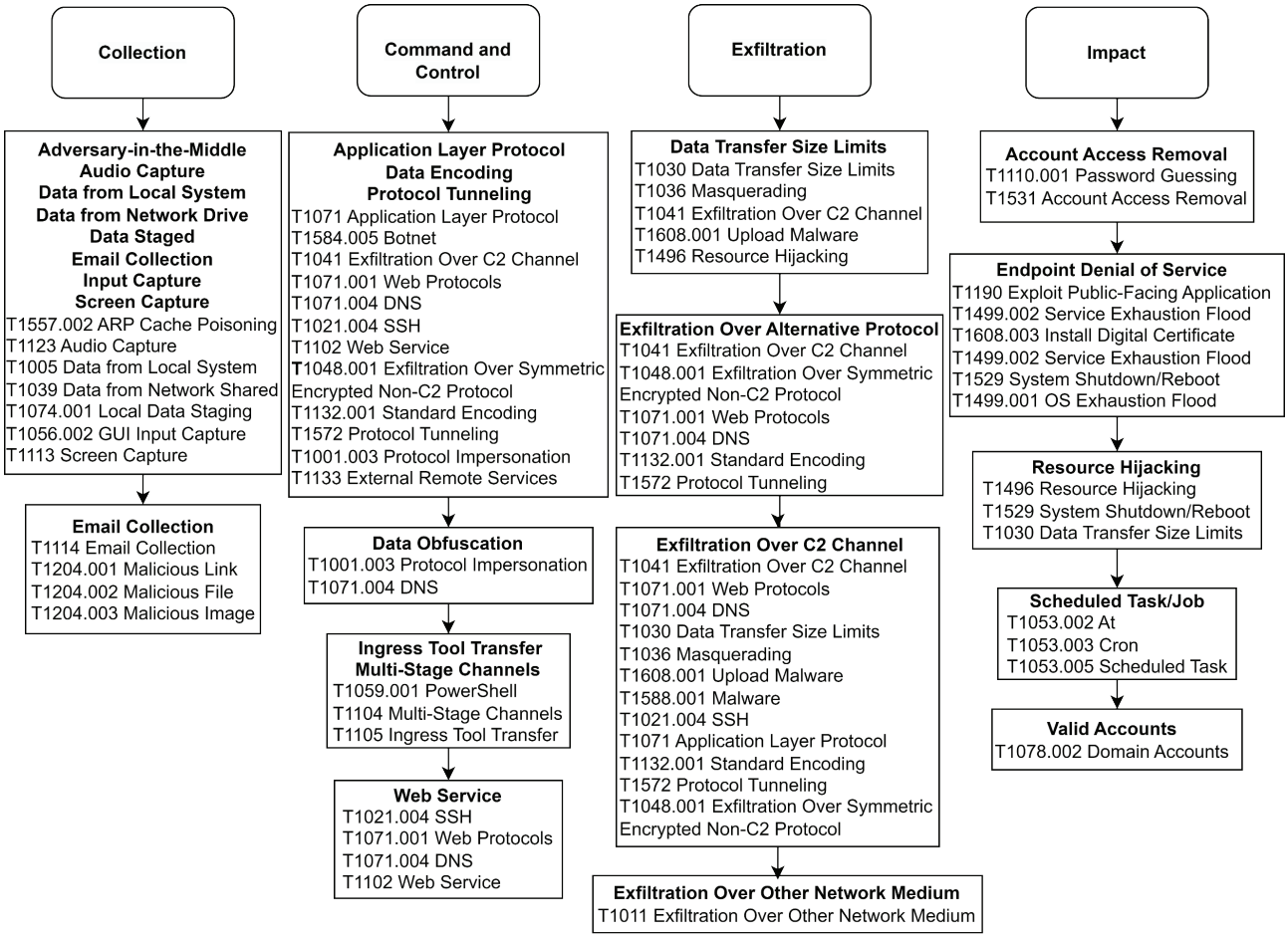

Figure 12. MITRE ATT&CK threat modeling and defense methodology map-3.

framework can be used to create an attack map of the attacker, which is used to gain a better understanding of the vulnerabilities of the system [87,88]. The maps in Figure 10 and Figure 11 help to understand the attacker's steps and improve cyber defense systems.

With the attack maps, future studies on cyber-attack protection and digital maturity will have a more scientific basis. As cyber-attacks continue to evolve and change, the need to systematically categorize the attacker profile and behavior map has led to the emergence of the MITRE ATT&CK and NIST v2 framework. When the results in Figure 12 are combined with the data obtained from Figure 10 and Figure 11, it is seen in the tests and performance evaluations conducted in the simulation environment that the architecture designed for the DRC infrastructure, which houses critical systems, has superior attack and threat prevention mechanisms.

CONCLUSION

Research and technological advancements have shown that cyber-attacks are increasing day by day. This increase underscores the critical need for robust cybersecurity measures to address the ever-evolving threats in the digital landscape. Academic studies in the field of cybersecurity and network security are making significant contributions, and these contributions are becoming more pronounced each year. The referenced studies highlight various types of threats that cyber attackers can deploy, and the findings obtained through studies on various available databases have added valuable insights to the literature.

The novelty of this study to the literature is the development of an architecture that leverages new and emerging technological infrastructures to address the security needs against cyber-attacks on DRC centers. The flowchart and pseudocode structure of this architecture have been detailed comprehensively. Additionally, the scientific novelty of this study lies in the successful integration of professional applications and frameworks such as EVE-NG, Nessus, OpenVAS, Kali, Parrot, MITRE ATT&CK Enterprise, and NIST v2. This integration has enabled the determination of the success limits of the architecture. The architectural infrastructure was simulated in the application environment, and real-world cyber-attack vectors were used to

conduct performance tests through accessible professional applications. This practical validation underscores the effectiveness and reliability of the architecture.

A significant challenge in cybersecurity are unknown zero-day attacks those that have not been previously identified and are not present in databases. These attacks remain a critical problem for existing infrastructure and systems. The developed architecture aims to provide effective protection against such attacks. In the first phase of the architecture, attacks were conducted on DDoS, SD-WAN, and MPLS systems using 10 different attack vectors and 10 different internet protocols. The behavior of these attacks was analyzed in detail using Wireshark packet analysis and Forti Analyzer software. The tests demonstrated that the protection layers could detect and block 99.99% of current and known attack vectors. The 0.01% error margin is anticipated to be due to the simulations conducted in a virtual environment.

In the second and third phases, attacks were conducted on DMZ web services and local network servers. These attacks, generated by attack simulators, were conducted using 57 different attack categories, 89.000 CVEs (Common Vulnerabilities and Exposures) and 219,000 different attack methods on IPS&IDS , layered firewalls, WAF structures, and sandbox products. The servers within the attack area did not exhibit any vulnerabilities, indicating the effectiveness of the developed architecture.

Global cybersecurity frameworks have facilitated the mapping of risks against the actions attackers may take to achieve their goals. Necessary improvements and plans have been implemented, and the ability to control and intervene in the accuracy of security measures has been enhanced, thereby preventing data loss. The real-time network traffic data obtained from the systems showed that malicious attacks designed to cause service interruptions failed. This finding confirms the success of the DRC architecture and infrastructure equipment.

The unique contribution of this research to science is the development of a cybersecurity architecture for DRC systems, an area not previously explored in such scope and detail by any academic author. The use of professional systems and advanced cyber-attack simulations has enabled the prevention of threats, and the data obtained has facilitated the development of a distinctive DRC architecture for distributed infrastructures that can be tiered. This model can be used by institutions and organizations to enhance the maturity level of their cybersecurity and network security, thus preventing potential economic losses.

Future recommendations for further development of this study include the integration of infrastructure systems such as Data Diodes (DataflowX), Secure Access Service Edge (SASE), and software and application-based data centers into the DRC infrastructure. These recommendations aim to further strengthen the current architecture and create a more effective defense mechanism against new cyber threats. Data diodes can minimize security vulnerabilities by making data flow unidirectional, preventing external access to critical systems. Secure Access Service Edge can play a crucial role in securing network access for users and devices, thereby preventing cyber-attacks. Software and application-based data centers can ensure the dynamic and flexible implementation of cybersecurity policies.

In conclusion, this study represents a significant advancement in the field of cybersecurity and network security. The developed DRC architecture has provided effective protection against various cyber-attacks, yielding findings that will inform future research in this field. As a valuable reference for both academic and professional communities, this study demonstrates the applicability of new technological developments and methodologies in cybersecurity. Consequently, it serves as an essential resource for researchers and experts working in the cybersecurity domain.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] AFAD. 2014–2023 Critical Infrastructure Protection Roadmap Document. Ankara: Prime Ministry Disaster Emergency Management Presidency; 2014.

[2] Aslay F. Cyber attack methods and current situation analysis of Türkiye's cyber safety. Int J Multidiscip Stud Innov Technol 2017;1:24–28.

[3] Çölkesen TR. Network TCP/IP UNIX standard network information and internet backbone infrastructure. Istanbul: Papatya Yayıncılık; 2018.

[4] Baykara M, Daş R, Karadoğan İ. 1st International Symposium on Digital Forensics and Security (ISDFS'13); 2013; Elazığ, Türkiye.

[5] Svantesson D, Clarke R. A best practice model for e-consumer protection. Comput Law Secur Rev 2010;26:31–37. [CrossRef]

[6] Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur 2013;38:97–102. [CrossRef]

[7] Craigen D, Diakun-Thibault N, Purse R. Defining cyber security. Technol Innov Manag Rev 2014;4:13–21. [CrossRef]

[8] Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. Comput Netw 2013;57:1344–1371. [CrossRef]

[9] Papp D, Ma Z, Buttyan L. Embedded systems security: threats, vulnerabilities, and attack taxonomy. In: 2015 IEEE 13th Annual Conf Privacy Secur Trust; 2015 Sep; Izmir, Türkiye. p. 145–152. [CrossRef]

[10] Luiijf E, Klaver M. Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. Int J Crit Infrastruct Prot 2021;35. [CrossRef]

[11] Setola R, De Porcellinis S, Sforna M. Critical infrastructure dependency assessment using the input–output inoperability model. Int J Crit Infrastruct Prot 2009;2:170–178. [CrossRef]

[12] Yaacoub JPA, Noura HN, Salman O, Chehab A. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int J Inf Secur 2021;21:115–158. [CrossRef]

[13] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR. A systematic literature review of blockchain cyber security. Digit Commun Netw 2020;6:147–156. [CrossRef]

[14] Kaur J, Ramkumar KR. The recent trends in cyber security: a review. J King Saud Univ Comput Inf Sci 2022;34:5766–5781. [CrossRef]

[15] Maglaras LA, Kim KH, Janicke H, Ferrag MA, Rallis S, Fragkou P, Maglaras A, Cruz TJ. Cyber security of critical infrastructures. ICT Express 2018;4:42–45. [CrossRef]

[16] Waseem M, Khan MA, Goudarzi A, Fahad S, Sajjad IA, Siano P. Incorporation of blockchain technology for different smart grid applications: architecture, prospects, and challenges. Energies 2023;16:820. [CrossRef]

[17] Khan MA, Saleh AM, Waseem M, Sajjad IA. Artificial intelligence enabled demand response: prospects and challenges in smart grid environment. IEEE Access 2022;11:1477–1505. [CrossRef]

[18] Dasgupta D, Akhtar Z, Sen S. Machine learning in cyber security: a comprehensive survey. J Def Model Simul 2020;19:57–106. [CrossRef]

[19] Cole E. Network security bible. Hoboken (NJ): John Wiley & Sons; 2011. p. 768.

[20] Aslan O, Yilmaz AA. A new malware classification framework based on deep learning algorithms. IEEE Access 2021;9:87936–87951. [CrossRef]

[21] Ouyang M, Hong L, Mao ZJ, Yu MH, Qi F. A methodological approach to analyze vulnerability of interdependent infrastructures. Simul Model Pract Theory 2009;17:817–828. [CrossRef]

[22] Wang S, Hong L, Ouyang M, Zhang J, Chen X. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. Saf Sci 2013;51:328–337. [CrossRef]

[23] Wang S, Hong L, Chen X. Vulnerability analysis of interdependent infrastructure systems: a methodological framework. Phys A 2012;391:3323–3335. [CrossRef]

[24] Yungaicela-Naula NM, Vargas-Rosales C, Perez-Diaz JA. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access 2021;9:108495–108512. [CrossRef]

[25] Elubeyd H, Yiltas KD. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Appl Sci 2023;13:3828. [CrossRef]

[26] Kim Y, Hakak S, Ghorbani A. DDoS attack dataset (CICEV2023) against EV authentication in charging infrastructure. In: 2023 20th Annual International Conference on Privacy, Security and Trust (PST); 2023. p. 1–9. [CrossRef]

[27] Carrier T, Victor P, Tekeoglu A, Lashkari HA. Detecting obfuscated malware using memory feature engineering. In: 8th International Conference on Information Systems Security and Privacy (ICISSP); 2022.

[28] Akbaş D. Modeling and analysis of an enterprise network and its security structures. TMMOB Elektrik Mühendisleri Odası Derg 2010. [CrossRef]

[29] Kör A. A dynamic solution model for cyber attacks. [Master's thesis]. Gazi University; 2015.

[30] Büyükkılıç M. Cybersecurity framework for small and medium size enterprises. [Master's thesis]. Bahçeşehir University Institute of Science; 2018.

[31] Herrmann D, Pridöhl H. Basic concepts and models of cybersecurity. In: The ethics of cybersecurity. Int Libr Ethics Law Technol 2020;21. Springer, Cham. [CrossRef]

[32] Çınar MS, Yıldırım A. Efficient management of an enterprise-wide area network with network management systems. NOHU J Eng Sci 2020;9:9–22.

[33] Avcı İ. Investigation of cyber security vulnerabilities and development of maturity model in smart natural gas networks. [PhD thesis]. Istanbul University; 2021.

[34] Xiong W, Legrand E, Aberg O, Lagerstorm R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix. Softw Syst Model 2021;21:157–177. [CrossRef]

[35] Frayssinet F, Esennarro M, Regalado FFJ, Reategui DM. Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3C TIC 2021;10:123–141. [CrossRef]

[36] Özarpa C, Avcı İ, Kara AS. Survey of cyber security risks and defense methods for autonomous vehicles. Eur J Sci Technol 2021;31:242–255.

[37] Güneş B, Kayışoğlu G, Bolat P. Cyber security risk assessment for seaports: a case study of a container port. Comput Secur 2021;103. [CrossRef]
[38] Kara Ş, Zengin A, Hizal S. Discrete event system identification based modeling and simulation of cyber attacks for the security of network systems. J Eng Sci Res 2022;5:186–202.
[39] Ruiz L, Chamon L, Ribeiro A. Graphon neural networks and the transferability of graph neural networks. Adv Neural Inf Process Syst 2020;33:1702–1712.
[40] Polat H, Polat O, Cetin A. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability 2020;12:1035. [CrossRef]
[41] Assis MV, Carvalho LF, Lloret J, Proença ML Jr. A GRU deep learning system against attacks in software defined networks. J Netw Comput Appl 2021;177:102942. [CrossRef]
[42] De Donno M, Dragoni N, Giaretta A, Spognardi A. Analysis of DDoS-capable IoT malwares. In: 2017 Federated Conference on Computer Science and Information Systems (FedCSIS); 2017. p. 807–816. [CrossRef]
[43] Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J. Ioddos – the internet of distributed denial of service attacks. In: 2nd International Conference on Internet of Things, Big Data and Security; 2017. p. 47–58. [CrossRef]
[44] Specht S, Lee R. Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. CEL2003-03, Princeton University, Princeton, NJ, USA; 2003.
[45] Vignau B, Khoury R, Hallé S. 10 years of IoT malware: a feature-based taxonomy. In: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C); 2019. p. 458–465. [CrossRef]
[46] Vignau B, Khoury R, Hallé S, Hamou-Lhadj A. The evolution of IoT malwares, from 2008 to 2019: survey, taxonomy, process simulator and perspectives. J Syst Archit 2021;116. [CrossRef]
[47] Bütün İ. Security implications of underlying network technologies on industrial internet of things. J Polytech 2022;25:223–229. [CrossRef]
[48] Karaman MS, Turan M, Aydin MA. Model application of anomaly based intrusion detection using artificial neural network. Eur J Sci Technol 2021;(Spec Issue):10–17.
[49] Çalkavur S, Guzeltepe M. Secure encryption from cyclic codes. Sigma J Eng Nat Sci 2022;40:380–389. [CrossRef]
[50] Erdem A, Kocaoğlu R. A new approach for network security: dynamic intelligent firewall architecture. J Fac Eng Archit Gazi Univ 2014;29:707–715. [CrossRef]
[51] Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci 2014;80:973–993. [CrossRef]
[52] Or-Meir O, Nissim N, Elovici Y, Rokach L. Dynamic malware analysis in the modern era—a state of the art survey. ACM Comput Surv 2019;52:1–48. [CrossRef]
[53] Rabbani M, Wang YL, Khoshkangini R, Jelodar H, Zhao R, Hu P. A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. J Netw Comput Appl 2020;151:102507. [CrossRef]
[54] Seo SH, Gupta A, Sallam AM, Bertino E, Yim K. Detecting mobile malware threats to homeland security through static analysis. J Netw Comput Appl 2014;38:43–53. [CrossRef]
[55] Utku A, Doğru İA. Permission based detection system for android malware. J Fac Eng Archit Gazi Univ 2017;32:1015–1024. [CrossRef]
[56] The MITRE Corporation. Enterprise Techniques. https://attack.mitre.org/techniques/enterprise/. Release date October 31, 2023. Accessed January 16, 2024.
[57] Bagui SS, Mink D, Bagui SC, Plain M, Hill J, Elam M. Using a graph engine to visualize the reconnaissance tactic of the MITRE ATT&CK framework from UWF-ZeekData22. Future Internet 2023;15:236. [CrossRef]
[58] National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf. Release date August 8, 2023. Accessed on Jan 16, 2024.
[59] Aslan Ö, Aktuğ SS, Ozkan OM, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics 2023;12:1333. [CrossRef]
[60] Victor P, Lashkari AH, Lu R. IoT malware: an attribute-based taxonomy, detection mechanisms and challenges. Peer Peer Netw Appl 2023;16:1380–1431. [CrossRef]
[61] Tripathi D, Biswas A, Tripathi AK. An integrated approach of designing functionality with security for distributed cyber-physical systems. J Supercomput 2022;78:14813–14845. [CrossRef]
[62] Gaur A, Scotney B, Parr G, McClean S. Smart city architecture and its applications based on IoT. Procedia Comput Sci 2015;52:1089–1094. [CrossRef]
[63] GJ M, Kunte RS. A conceptual architecture design – building cyber security architecture for industrial control systems networks and for critical infrastructures. Int Res J Eng Technol 2024;6:1.
[64] Lu X, Dong R, Wang Q, Zhang L. Information security architecture design for cyber-physical integration system of air traffic management. Electronics 2023;12:1665. [CrossRef]

[65] Yousefnezhad N, Malhi A, Keyriläinen T, Främling K. A comprehensive security architecture for information management throughout the lifecycle of IoT products. Sensors 2023;23:3236. [CrossRef]
[66] Vijayakumaran C, Muthusenthil B, Manickavasagam B. A reliable next generation cyber security architecture for industrial internet of things environment. Int J Electr Comput Eng 2019;10:387–395. [CrossRef]
[67] Jalali R, El-Khatib K, McGregor C. Smart city architecture for community level services through the internet of things. In: 2015 18th International Conference on Intelligence in Next Generation Networks. IEEE; 2015. p. 108–113. [CrossRef]
[68] Jiang JR. An improved cyber-physical systems architecture for industry 4.0 smart factories. Adv Mech Eng 2018. [CrossRef]
[69] Lee J, Bagheri B, Kao HA. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 2015;3:18–23. [CrossRef]
[70] Kırışoğlu S, Kara R, Özçelik İ. A new SNMP-based algorithm for network traffic balancing in virtual local area networks. J Fac Eng Archit Gazi Univ 2018;34:365–380. [CrossRef]
[71] Daş R, Bitikçi B. Analysis of different types of network attacks on the GNS3 platform. J Comput Inf Sci 2020;3:3. [CrossRef]
[72] Abomhara M, Koien MG. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur 2015;4:65–88. [CrossRef]
[73] Jouini M, Rabai ABL, Aissa BA. Classification of security threats in information systems. Procedia Comput Sci 2014;32:489–496. [CrossRef]
[74] Khan I. An introduction to computer viruses: problems and solutions. Libr Hi Tech News 2012;29:8–12. [CrossRef]
[75] Rajesh B, Reddy YJ, Reddy BDK. A survey paper on malicious computer worms. Int J Adv Res Comput Sci Technol 2015;3:161–167.
[76] Jaiswal M. Computer viruses: principles of exertion, occurrence, and awareness. Int J Creat Res Thoughts 2017;5:648–651.
[77] Bickford J, Hare R, Baliga A, Ganapathy V, Iftode L. Rootkits on smartphones: attacks, implications, and opportunities. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications; 2010 Feb 22–23; Annapolis, MD, USA. p. 49–54. [CrossRef]
[78] Javaheri D, Hosseinzadeh M, Rahmani AM. Detection and elimination of spyware and ransomware by intercepting kernel-level system routines. IEEE Access 2018;6:78321–78332. [CrossRef]
[79] Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. Ethical hacking: the need for cyber security. In: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering; 2017 Sep 21–22; Chennai, India. p. 1602–1606. [CrossRef]
[80] AlRimy BAS, Maarof MA, Shaid SZM. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput Secur 2018;74:144–166. [CrossRef]
[81] CSO. DDoS attacks: definition, examples, and techniques. https://www.csoonline.com/article/571981/ddos-attacks-definition-examples-and-techniques.html. Release date January 31, 2022. Accessed January 16, 2024.
[82] Baysal K, Taşkın D. Blocking harmful images with a deep learning based next generation firewall. Sigma J Eng Nat Sci 2024;42:1133–1147. [CrossRef]
[83] Yılmaz A, Aslan Z. The impact of the COVID-19 pandemic on data usage rate in enterprise networks. J Anadolu Bil Vocat High Educ 2022;17:95–115. [CrossRef]
[84] Yılmaz A, Aslan Z. The role and future of 802.11ax technology in wireless network infrastructures: performance, security and innovation. J Anadolu Bil Vocat High Educ 2024;19:1–29. [CrossRef]
[85] Zolanvari M, Teixeira MA, Jain R. Effect of imbalanced datasets on security of industrial IoT using machine learning. In: 2018 IEEE International Conference on Intelligence and Security Informatics (ISI); 2018. p. 112–117. [CrossRef]
[86] Humayun M, Niazi M, Jhanjhi N, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. Arab J Sci Eng 2020;45:3171–3189. [CrossRef]
[87] Yamaguchi S, Leelaprute P. Hajime worm with lifespan and its mitigation evaluation against Mirai malware based on agent-oriented Petri net pn 2. In: 2019 IEEE International Conference on Consumer Electronics (ICCE); 2019. p. 1–4. [CrossRef]
[88] Shin Y, Kim K, Lee JJ, Lee K. Focusing on the weakest link: a similarity analysis on phishing campaigns based on the ATT&CK matrix. Secur Commun Netw 2022;2022. [CrossRef]