Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 2, 116-125 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Analysis of Cyberattacks in Public Organizations in Latin America

Segundo Moisés Toapanta Toapanta[*,1], José David López Cobeña[1], Luis Enrique Mafla Gallegos[2]

[1] *Department of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, 010102, Ecuador*

[2] *Faculty of Systems Engineering, Escuela Politécnica Nacional (EPN), Quito, 17-01-2759, Ecuador*

ARTICLE INFO

Article history:
Received: 21 November, 2019
Accepted: 25 February, 2020
Online: 09 March, 2020

Keywords:
Cybersecurity
Cyberattack
Public Organization
Denial of Service
Minimize he attack

ABSTRACT

It was analyzed certain information about cyberattacks in Latin America and methods to counteract the aggressions that affect services, data and infrastructure. The problem is the cyberattack on information networks where there is interdependence between processes, people and devices within public organizations with the negative consequence of denial of services. The objective is to propose a protection model against cyberattacks in public organizations in Latin America to minimize the denial of public services. It was applied the deductive method and exploration to examine the information of cited articles. It resulted a General Model of Protection against Attacks, a Prototype of a network, a Algorithm in flowchart to minimize the attack arrival and a Formula of probability of attack arrival. It was concluded that in order to maintain the continuity of services and activities of public organizations, secure platforms must be in place to monitor and minimize possible attacks; our proposal has an attack detection accuracy of 87.49%.

1. Introduction

Today national and sectional governments use desktop applications, web applications, mobile applications and social networks to improve public services to citizens; ICT help public and private organizations serve their taxpayers and customers respectively, such as time reduction in processes, zero documentation, reservation of shifts, digital tax returns.

The advancement of technology brings with it threats that materialize in damage to infrastructure and services provided by public organizations; the most common types of attacks are social engineering and network attack. There are specific attacks such as: integrity attacks, sparse sensor attacks, false data injection attacks, fake-acknowledge attack, denial-of-service attacks and replay attacks[1].

The cyberattack maliciously update a system, the attacking software tries to destroy the environment; the antithesis of this is cyber security that is protection of information, hardware, software and services against vandalism[2].

Countries like Ecuador, Chile, Brazil, Colombia and Mexico are updating their laws to guarantee privacy, protect data[3] some countries consider cybercrimes in their laws such as Argentina, Bolivia, Costa Rica, Guatemala, Mexico, Paraguay and Peru; other countries generate specific laws: Brazil, Chile, Colombia and Venezuela; Ecuador uses its civil and commercial law in criminal sanctions; Uruguay has a Law on Protection of Copyright[4]. Countries such as United States, China and Israel are pioneers in the application of technological advances in national defense.

Formulation of the research problem: How cyberattack can be minimized to an information network where there is interdependence between processes, people and devices within public organizations; and there are exposed servers that provide services with the possibility of denial of services. The following hypothesis:

Why is an approach to cyberattacks necessary in public organizations in Latin America?

The objective is to propose a protection model against cyberattacks in public organizations in Latin America to minimize the denial of public services.

This research is motivated by the need to analyze and identify cyberattacks in public organizations in Latin America; review mechanisms that serve to minimize the denial of public services; Obtain a model for the identification of vulnerabilities that threaten the provision of services; propose a mechanism that can be used in

[*] Segundo Moisés Toapanta Toapanta, & Email: stoapanta@ups.edu.ec

https://dx.doi.org/10.25046/aj050215

areas such as: education, aerospace, electricity networks, water services, telephony, financial, transportation, communication, business, attention, risk control or infrastructure; avoid the loss of taxpayers, credibility, time and other resources of a public organization, in addition to certifying the availability of services and keep a critical service located on an application server enabled.

The articles reviewed and related cyberattacks in Latin America are: Are We Ready in Latin America and the Caribbean[5], Cyber Risks and Information Security in Latin America & Caribbean Trends [6], Data Breach Investigations Report[7], A cyber-attack on communication link in distributed systems and detection scheme based on H-infinity filtering [8], Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News [9], A Novel Approach for Classification and Detection of DOS Attacks [10], Analysis of efficient processes for optimization in a distributed database [11], Biometric Systems Approach Applied to a Conceptual Model to Mitigate the Integrity of the Information [12], Cyberattacks on Devices Threaten Data and Patients [13], Assessing Mission Impact of Cyberattacks: Toward a Model-Driven Paradigm [14], A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services [15], Attacklets: Modeling high dimensionality in real world cyberattacks [16], Cyberattack Prediction Through Public Text Analysis and Mini-Theories [17], Deep learning approach for cyberattack detection [18], Cyberattack detection in mobile cloud computing: A deep learning approach [19], Adaptation of the neural network model to the identification of the cyberattacks type ‘denial of service’[20], Cybercriminals, cyberattacks and cybercrime [21], Resource efficiency, privacy and security by design [22], A survey of similarities in banking malware behaviours [23], A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual[24], Evaluating practitioner cyber-security attack graph configuration preferences [25], Correlating human traits and cyber security behavior intentions [26], Record route IP traceback: Combating DoS attacks and the variants [27], Evaluating the applicability of the double system lens model to the analysis of phishing email judgments [28], Enhancing security behaviour by supporting the user [29], An Algorithm for Moderating DoS Attack in Web based Application [30], Impact of a DDoS attack on computer systems [31], How Secure are Web Servers? [32], Detection of DoS/DDoS attack against HTTP servers using naive Bayesian [33], Detection of DoS attack and Zero Day Threat with SIEM [34], A Framework for Making Effective Responses to Cyberattacks [35], Attack detection/prevention system against cyberattack in industrial control systems [36], Is the responsibilization of the cyber security risk reasonable and judicious? [37], A visualization cybersecurity method based on features’ dissimilarity [38], Automatic security policy enforcement in computer systems [39], Defending Against Web Application Attacks: Approaches, Challenges and Implications [40], Statistical Application Fingerprinting for DDoS Attack Mitigation [41], Detecting lateral spear phishing attacks in organisations [42], A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud [43], BWManager: Mitigating Denial of Service Attacks in Software-Defined Networks Through Bandwidth Prediction [44].

It is applied the deductive method and exploration to examine the information of cited articles.

The results are: A General Model of Protection against Attacks, a Prototype of a network, a Algorithm in flowchart to minimize the attack arrival and a Formula of probability of attack arrival.

It is concluded that in order to maintain the continuity of services and activities of public organizations, secure platforms must be in place to monitor and minimize possible attacks; our proposal has an attack detection accuracy of 87.49%.

2. Materials and Methods

In a first instance in Materials, works of attacks carried out in Latin America and global level were reviewed. In the second instance in Methods, elements are presented to put together a proposal to minimize attacks such as Ranking, Types and tendencies of attacks, general steps of attack and scope.

2.1. Materials

In 2016 the Organization of American States and the Inter-American Development Bankproduced a cybersecurity report from 32 countries in Latin America and the Caribbean; for each country they reviewed 5 dimensions such as policies and strategies, culture and society, education, legal framework and technology; 49 indicators distributed in 5 dimensions were applied; 5 maturity levels were also reviewed as initial, format, established, strategic and dynamic; It is reported that Brazil, Colombia, Jamaica, Panama, Trinidad and Uruguay adopted cybersecurity strategies [5]. For 2019, Deloitte Touche Tohmatsu Limited presented a report on cyber risks in Latin America and the Caribbean, the public, financial, manufacturing, communications, services, oil and other areas were reviewed; the results compare Latin America against Colombia; Latin America is 9% more important than Colombia in cyber security; Latin America has 5% more protection than Colombia in security level; Latin America has 9% less protection than Colombia in Denial of Services attacks [6].

For 2019, Verizon presented a report that determined that: victims were from the public, health, financial and business sectors; the tactics used were hacking, social engineering, malware, casual, misuse; the actors of the attacks were foreign, internal actors, partners, third parties, criminal organizations and governments; the main attack was Denial of Services[7]. The authors defined a management architecture in a distributed topology, there are physical areas interconnected through software links and they provide data to each monitoring center; for the detection scheme the input data of the areas are filtered before applying the anomaly detection process; by hiding the attack vector effect and not being a data entry, the attack is detected, the time that intervals are 20 seconds [8].

The authors proposed a model that has three phases: preprocessing, identification and classification; in the first phase the news is filtered to leave simple text to analyze; in the second phase the characteristics of the attack are validated with other investigations and the extracted text is stored in a dictionary; the third phase uses statistics to create a probabilistic model and identify the data; the classification algorithm is under construction [9]. The authors proposed a web application for classification and detection of attacks; they have two classifiers, the first one works with a list of malicious communications and the second one works with a tree decision; they also have a package to analyze user data and warn in case of an attack; in the accuracy tests the minimum was 77.77% and the maximum 93.33% [10].

The authors carried out a descriptive evaluation of works in security and processing of distributed databases; they described fourteen articles on scales of 1 to 5; in addition, they grouped the works in processing, concurrence, consultations, fragmentation, communication, consistency and load[11]. The authors proposed a biometric system model to increase the level of information security, the model manage security by fingerprint access, iris, facial recognition; this data is stored in a database [12].

The authors conducted a questionnaire for three cybersecurity professionals; the questions dealt with threats in the health industry, attacks on medical devices, device certification, laboratory evaluation, advances in research; one researcher concluded that the risks are adherent and real when connecting to a network, you should consider mitigating the risks [13]. The authors described the characteristics of an attack evaluation model; this model has several fronts: organization, processes, motivations of the attacker, individual or group attacks and architectures; they affirm that defense against attacks depends on the systematic and quantitative evaluation of the business [14].

The authors modeled a cyberattack where they identified the attacker, the devices, characteristics of the attack, vulnerabilities of the devices, the connection paths between the devices and the data warehouse; the attack model was applied to company infrastructure, an electric power network, a transport system, a medical system and smart home; they concluded that weaknesses and limitations are characteristic of fragile security [15]. With historical data from 1971 to 2017; the authors modeled a cyberattack that executes several actions, uses several user attributes, several data sets simulating people or groups, several states of actors; one of the objectives is the classification of attacks, which serves to determine securities; Attacks are stored and serve as feedback for self-learning [16].

The authors proposed that unused sources of information can be used for the prediction and preparation of cyberattacks found in extensive texts on the web; ontological knowledge is used about the attacks demonstrated that their technique of event extraction and detection of named entities showed a large scale of cyberattack prediction [17]. To mitigate the cyber security problem in IoT environments by shortening the detection time; The authors proposed a DFEL deep learning framework that reduced detection time by 57.75% over other traditional machine learning algorithms [18].

An important point to exist attacks today are mobile devices; the authors proposed a deep learning framework to detect cyber threats in the mobile cloud; its detection accuracy was 97.11% compared to other machine learning approaches[19]. The authors suggested increasing the coefficient values of a reduced quadratic learning error in a neural network; they improved the accuracy of the deviations of the safety parameters in the area of their minimum values [20].

The massive increase in cyberattacks determines that system security is quite vulnerable; the authors proposed that by hardening security at all levels, these attacks can be prevented and if omitted, critical and non-critical infrastructure would be compromised[21]. The authors proposed a prototype that performs a renewing analysis of the connections associated with the resources, the validity, cybersecurity, data protection and data privacy arguments; the model is a set of policies that seeks to increase storage and data security; in the tests they obtained the 2%, 5%, 8% and 15% reuse rate in first, second, third and fourth scenarios respectively [22].

The authors reviewed the attack by malware in the banking sector, where criminal groups steal information; they used an analysis framework for decomposition, control flow study and instruction review; they concluded that there is a need to understand malware tactics at a high level [23]. The authors carried out a cyberattack evaluation model, based on a normative scheme of the United Nations “force use” letters of 1945; some parameters are difficulty, speed, causes, number of operations, identification of consequences, relations between operations and permitted acts; their strategy is in a new calculation to measure the criteria, where they combined algorithms and new grouping of reasons to obtain a destruction value [24].

The authors proposed a graphic visual syntax configuration to effectively present the attacks; in tests the precondition attribute is 38.5%, the flow of events is 32.6% and exploit is 28.8%; Precondition is more significant, and the exploit attribute is less significant in decision making [25]. The authors related human characteristics to cybersecurity behavior; they conducted a survey of 369 people from a public university; the results were: 5.2% of security intention of the device, 16.8% of security intention of the users, 22.8% of intention of conscience, 12.6% of intention to update; they concluded that their work helps to understand populations in safety behavior [26].

The authors studied the denial of services and their variants, they proposed a probabilistic package marking design to forecast routes from the attacker to the victims, this allows the victim to delegate their protection to the ISP; in the tests they carried out between 100 and 5000 DDoS attacks with averages between 20 and 11 packages respectively, where the design takes 21.42 milliseconds to 18.5 seconds to obtain the route; they concluded that their design requires fewer packages to obtain attack routes and lower bandwidth consumption [27]. The authors designed a double lens model to assess human judgments in the mails; in the tests they obtained performance values 0.923 units indicates that the model has a good work to adjust environment and criteria; the knowledge value was 1 unit, indicates a good level in the fields; Other values found are: lack of details of the signer is 0.542, without logos is 0.400 and URL hyperlinks is 0.349; they concluded that their work is a first step to apply judgments to the phishing environment [28].

The authors studied the maintenance and accompaniment in user safety; the experiment on social networks was with 60 participants in 5 scenarios; the e-commerce experiment evaluated the generation of passwords to classify security elections; password security control is less than 0.01 units; the control in the times of the change of password is 0.11 units; suggestion control is 0.17 units [29].

2.1.1. Related Jobs

The authors proposed an algorithm with monitoring, detection and mitigation; in the first phase the IP addresses are identified against a block list to prevent the message from passing; in the second phase the number of applications is verified; in the third phase a threshold value is used according to a behavior; The algorithm identifies the type of attack, there is no evidence of the algorithm[30]. An attack tree was used to identify actions and tools against threats; review of system security behavior, review of attack indicators, selection of profiles of attackers and victims; the results obtained and evaluated the costs of attacks, benefits, impacts, possibilities and skills [31].

The authors evaluated DoS HTTP vulnerabilities in Apache, IIS, Nginx and Lighttpd through the GET and POST methods; in the POST interval tests it is 88% less likely than GET; in slow message attack POST is 87% lower probability than GET; in real traffic POST is 99% less than GET; they concluded that their proposal has precision to detect attacks [32]. The authors proposed architecture that uses Bayes theorem probability to detect attacks on servers; the central package captures and analyzes network traffic, malicious traffic is stored; in the detection tests the minimum accuracy is 96.61% [33].

To detect DoS attack on the server, the authors proposed to work with the server's Log, network characteristics, connection time, packets and addresses; uses a rule implementation which verifies against the records, alarms are notified to the administrator and saved; this process works permanently [34]. The authors described 2 potential risks, defending themselves with a weak system or defending themselves with greater intensity in direct attacks on the attackers [35].

The authors studied the location of vulnerability and attacks on programmable controllers, they created a set of rules to see the start or stop of attacks; they proposed an algorithm in three phases: attack, observation and detection; the tests were descriptive, there are no numerical data, they concluded that security is not yet a priority in organizations [36]. The authors compared the risks in individual security and government security; at the government level they proposed deterrence, rules, location, recovery, remediation; there is no numerical data in tests; they suggested a hierarchical approach where governments take a more dynamic role, provide resources, have police authority and prevention units [37].

To increase intelligent phishing identification, the authors proposed a technique to detect websites and deliver early alerts; the authors applied a formula to rule out redundant characteristics, the values are global score and average score; they evaluated 30 characteristics and reduced to 6; its accuracy is 93% in the classification [38]. The authors proposed a technique for complying with computer policies through the formal relationship and the assessment of security settings; they proposed a formula with conjunction and disjunction; they implemented a prototype, there are no measurement values in the tests [39].

The authors described the validation problems when entering applications, these are entry doors for attackers with different attack targets; the authors created an exploitation model to understand code injection attacks, the algorithm uses common attack steps to identify exploitation routes [40].

The authors created a model for monitoring and detecting traffic behavior in a network; the package, flow and traffic anomalies are measured, also incorporated flow statistics to compare against real traffic; the model has a flow level and a package level; they use algorithms based on histograms, entropy calculation, normal profiles, flow and attacks; the authors state that their model is accurate between 97% and 100% [41].

The authors adopted a technique to detect false positives and true positives in the arrival of emails, they are given a score to take actions on the mail; in the tests they obtained a false positive rate of 0.88% and a true positive rate of 86.69%; the accuracy of the model was 98.79%; they stated that their research serves as an improvement in identifying a higher rate of true positives and a lower rate of false positives [42].

The authors described the concept of cloud computing, the DDoS attack and how it acts on the application layer, control layer and data layer; they deliver the guidelines to detect the attack through resource sharing accesses, highlighted the reasons, software tools to mitigate the attacks; described the attacks of other investigations [43].

The authors proposed an architecture to mitigate DoS attacks, consisting of six components with their detailed description; it also uses an algorithm as a priority manager, a queue management algorithm and a time algorithm; the tests were carried out in 100s with a speed of 500 packages / s they concluded that the architecture is effective by increasing the attack rate [44].

Related works dealt with cyberattacks and against subtracted through: phases, algorithms, threat reviews, indicators to measure attacks, types of attacks, threat identification; others detect attacks, defined rules or alarms, security risks, forms of deterrence, early warning delivery, redundancy reduction, policy compliance.

2.2. Methods

2.2.1. Ranking

According to Internet Crime Report 2018 [45], it received 351,936 complaints with losses of $2.7 Billion, has a ranking of 20 countries of which: the first place is India with 4556 victims; the seventh place is Brazil with 605 victims; the eighth place is Mexico with 591 victims; the tenth place is Philippines with 511 victims, the twentieth place is Japan with 311 victims. The type of crime Government Impersonation has 10,978 victims and cost $64,211,765; Denial of Service/TDoS has 1,799 victims and cost $2,052,340. In this ranking United States is excluded because the 2018 report has an analysis dedicated to this last country.

Figure 1 shows information obtained from [6] and [7]; according to Deloitte, the public sector in Latin America had 6% attacks and according to Verizon, the public sector worldwide had attacks of 16%; the highest percentages are Financial and Small Business where 44.7% and 43% of Deloitte and Verizon respectively. In the tactics used to the organizations we see that 69% are perpetrated outside the organization according to Verizon and 70% of the organizations affirm that they have no effectiveness in response to these cyberattack events according to Deloitte.

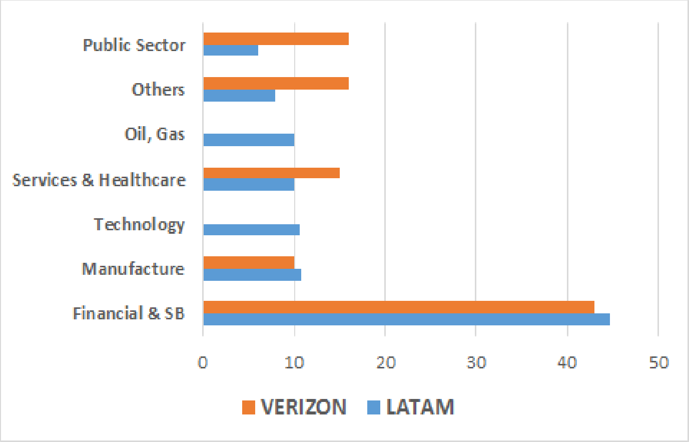

Figure 1 – Victims by sectors.

There are different types of cyberattacks some are: Defacement, Denial of Service, Account Hijacking, Malware and Virus, Phishing, SQL injection, Targeted Attack Unauthorized Access, Unknown Attacks and Zero Day [46].

The trends of cyber-attacks are: Root kit, BotNet, Scareware, SQL Injection, Phishing, Kido, Advanced Persistent Threat, Code Injection, HTML Injection [2].

Reference [30] puts DoS with 37% and Brute Force 25%; there are 2 types of DoS attacks: a) DoS is an attack executed by a single device (multiple requests) to a victim; b) DDoS is an attack executed by many devices distributed to same victim; the victim can be a server, service or infrastructure.

Attacks DoS can be separated into the layers of OSI model: on layer 3 Network that carries Packets there are UDP reflection attacks; on layer 4 Transport that carries Segments are given attacks SYN floods; on layer 6 Presentation that carries data attacks are given SSL abuse; on layer 7 Application that carries data are given attacks HTTP floods, floods of DNS queries.

In [30] 37% of the attacks were due to DoS, it is a type of cyberattack that happens more frequently and causes the interruption of the services offered by public organizations; attacks on the public sector: in [6] it was 6% in Latin America and in [7] it was 16% globally.

2.2.2. *Comparison table of references*

The different proposals reviewed obtained the methods that the authors used to estimate the detection, identification, conduct and analysis of cyber attacks, they propose to protect any of the following resources: information, physical network, infrastructure, applications or computer services.

Table 1 shows the proposals that protect computing resources, according to the information in the references there are a variety of protection methods, each proposal aims to protect only one resource at a time.

Table 1: Comparison of proposal.

Reference	Method	Protect	Accuracy
[1]	Detection estimates	Physical network	Residual evaluation > 0
[2]	Steps to use the internet	Information	Only algorithm
[8]	Filtering H-infinity	Communication links	Residual signal > 0
[9]	Identification of badges	Websites	Only algorithm
[10]	List and decision tree	Web server	77.77%
[12]	Biometric system	Information	Only algorithm
[13]	Cyberattacks	Questionnaire	No evaluation
[15], [16]	Attack models	Information	Descriptive results
[17]	Entity Detection	Information	Only algorithm
[18]	Learning Framework	Hardware connected to IoT	Detection greater than 57.55%
[19]	Learning Framework	Mobile cloud	97.11%
[20]	Cyberattaks identification DoS	Physical network	Only algorithm
[22]	Connection analysis	Data centers	Reuse 15%
[23]	Framework analysis	Bank information	Only algorithm
[24]	Cyberattack evaluation model	Information	Criteria calculation
[25]	Attack tree	Information	Precondition is 38.5%
[26]	Safety behavior	Information	Security intensity 5.2% to 22.8%
[27]	Probabilistic design	Services	Route in 18.5s
[28]	Dual lens model	Mails	Performance 92.3%
[30]	Identification of types of attacks	Web application	Only algorithm
[31]	Impact of attacks	Computer systems	94.80%
[32]	Stopping training and testing	Web server	87.00%
[33]	Odds and capture package	HTTP server	96.61%
[34]	Verification of rules	Web server	Only algorithm
[35]	Risk Classification	Infrastructure	Only Procedure
[36]	Set of rules	Systems	Only algorithm
[37]	Deterrence	Information	Only algorithm
[38]	Phishing identification	User data	93% predictive accuracy
[39]	Security policy framework	Information	Prototype

The information of the materials and of Table 1, was used to propose the scopes and also certain characteristics were adopted from the references to propose results.

2.2.3. *Scope for the proposal*

- Propose a General Model of Protection against Attacks
- Propose general security axes
- Propose a Prototype of a Network to minimize the attack called Denial of Services DoS, the main service of a Public Organization is Service to Citizens
- An algorithm expressed in a flowchart to prevent and minimize attacks that corrupt operations, functions, availability of services that are provided through websites, applications and database; without degrading the functionality of services
- Service servers are inside DMZ
- To access the data services from internet, a 3-layer model is used

- To access the data services from intranet, a 2-layer model is used

2.2.4. Methodology to generate results

General Model: To propose a protection model, the following elements were taken from the references: the qualitative criteria of cyberattack were considered [24]; user behavior was considered for access control [29]; the criteria of levels of responsibility were adopted [37]; the application of security policies was considered [39]; [31] and the [36] use of phases for attack and response detection was considered.

General prototype of a Network: Models, network architecture and services that protect information from the following references [11], [14], [30] and [39] were considered; Server protection was decided as they do in [32], [33] and [34] to continue providing services offered by an organization through its applications.

Algorithm: The Packet Sniffing Sensor[10] was adoptep for unusual traffic analysis; of [36] we adopt the use of phases in the proposed algorithm, the scanning and monitoring of traffic.

Formula: The poisson distribution facilitates the event of occurrence of events that occur in a given interval, this formula was adopted and the number of requests, the time interval in seconds and the attack per unit of time are taken as variables.

3. Results

The information and systems are critical assets, this research tries to minimize cyberattacks and that do not materialize in damages, in addition to increasing the levels of continuity of services and activities of public organization.

The following results were obtained:

- General Model of Protection against Attacks
- Prototype of a network
- Algorithm in flowchart to minimize the attack arrival
- Formula of probability of attack arrival

	IDENTIFY	PROTECT	DETECT	RECOVER AND RESPOND
BASIC	· VULNERABILITIES · ORGANIZATION SERVICES	· ACCESS CONTROL · NETWORKS · CONNECTIONS	MONITORING	· RECOVERY PLAN · EXECUTE CONTINGENCY PLAN
STANDARD	· CERTIFICATION OF HARDWARE AND SOFTWARE · PROCCESS IMPROVEMENT · HUMAN FACTORS · PROTECTION SOFTWARE	· BACKUPS · PRIVACY	· ANOMALIES · LONG PROCESSES	·ORGANIZATION INFORMATION · RECOVERY SCHEDULE · ADMINISTRATION OF THE ACCIDENT · CONTINUITY OF SERVICE
OPTIMIZED	· POLITICS AND PROCEDURES · ROLES AND RESPONSIBILITIES · CRITICAL APPLICATIONS · CRITICAL INFORMATION	· CRITICAL APPLICATIONS · CRITICAL INFORMATION · APPLY AUDITS	· TRAFFIC ANALYSIS · SHARED INFORMATION	· LEGAL ACTIONS · MAINTENANCE PLAN · NEW STRATEGIES · ACCIDENT REPORT

Figure 2: General Model of Protection against Attacks.

3.1. General Model of Protection against Attacks

According to what is specified in the methods section, a protection model was defined to minimize attacks and protect information, it was segmented into three levels; the basic level has the essential measures in to secure the information; the standard level has the measures that every organization must have to increase the level of security of the organization; the optimized level has robust measures against cyberattacks. Figure 2 presents the tasks of each model process.

The model describes vertically the scope of each level that can be applied in a small, medium or large organization in order to prevent or mitigate these attacks; only one level can be applied at a time that allows to control the security of the information in the processes, systems and infrastructure depending on the organization for its economy and development; horizontally there are the phases to identify, protect, detect and recover when there is a threat of attack in the organization; These phases should be applied progressively until reaching the optimum level to ensure the information security of organizations.

3.2. Prototype of a Network

In accordance with what is specified in the methods section, a general prototype of a network was proposed to control the arrival of abnormal requests that are hidden in other legitimate requests and want to reach web servers, applications, mail or transfers; implementing security layers such as ACL that control access to our network allows us to have these levels of greater security; as observed in the following network proposal, it is desired to limit and control access to the network obtaining a high degree of security preventing one of the modalities of denial of service attacks that arrive from the internet or the organization's intranet.

Figure 3 submit the prototype proposal separating in a DMZ the servers that provide services with the local network of the organization, for the security of the database servers a firewall will be used who will control the access by port and IP requirement.

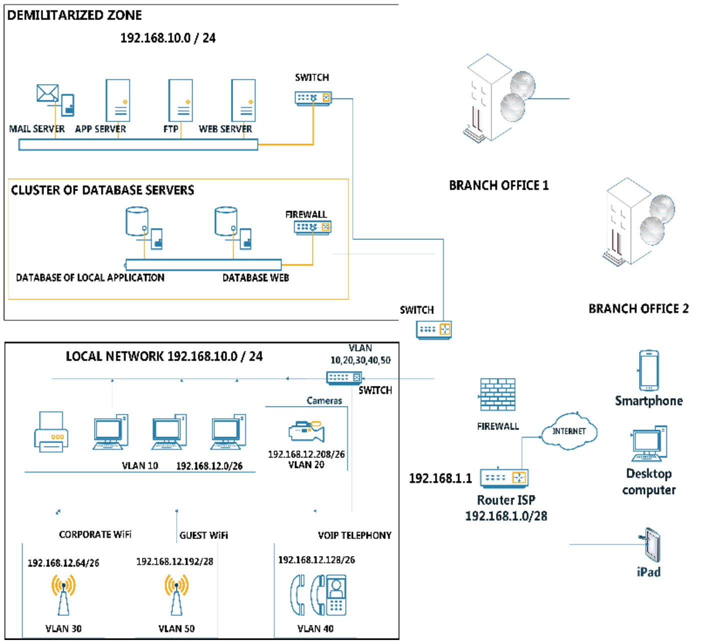

Figure 3: Prototype of a network.

Specifications of proposed network:

Router: 2 WAN interfaces, 2 LAN ports, Link redundancy protocol, Routing protocol

Firewall: UTM policy compliance (Unified Threat Management), 8 LAN ports, 1 WAN port, UTM requirements (statistic, risk threats, security policies by heuristic analysis), manageable by SNMP

Switch: layer 2 manageable by SNMP, with VLAN management, 24 ports, security management MAC

Through the firewall the separation of traffic towards the DMZ and LAN is defined

VLANs are defined in switch, the ports are from the trunk mode to firewall and VLAN is brought to firewall; ports are defined in access mode; VLAN is interconnected in the firewall and security policies are defined by application, port and physical interface or logical interface; each subnet is defined in a different VLAN to separate the traffic flows.

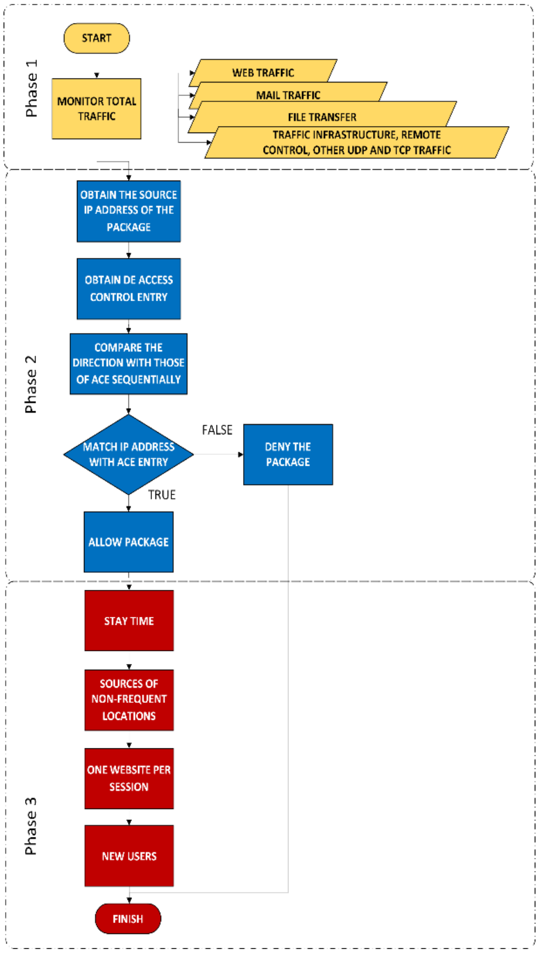
Phase 1
START
MONITOR TOTAL TRAFFIC
WEB TRAFFIC
MAIL TRAFFIC
FILE TRANSFER
TRAFFIC INFRASTRUCTURE, REMOTE CONTROL, OTHER UDP AND TCP TRAFFIC
Phase 2
OBTAIN THE SOURCE IP ADDRESS OF THE PACKAGE
OBTAIN DE ACCESS CONTROL ENTRY
COMPARE THE DIRECTION WITH THOSE OF ACE SEQUENTIALLY
MATCH IP ADDRESS WITH ACE ENTRY
FALSE
DENY THE PACKAGE
TRUE
ALLOW PACKAGE
Phase 3
STAY TIME
SOURCES OF NON-FREQUENT LOCATIONS
ONE WEBSITE PER SESSION
NEW USERS
FINISH

Figure 4: Proposed algorithm expressed in flowchart.

3.3. Algorithm in flowchart to minimize the attack arrival

The sequence of steps that the flowchart technique uses to obtain the algorithm specified in methods is expressed. To help minimize an attack due to the amount of traffic to network, the following algorithm was proposed, which has three phases:

Description of the phases:

Phase 1, Traffic analysis: The analysis was focused on unusual traffic to detect anomalies with adoption of Packet Sniffing Sensor.

Phase 2, Traffic filtering: Packet filtering controls access to network by analyzing incoming, outgoing or transferring packets.

Phase 3, Passage of legitimate traffic: To identify all illegitimate IP packets and pass legitimate IP packets, after phase 2 there may be malicious traffic.

Figure 4 expresses the algorithm in flowchart, then the steps of each phase are recorded.

The algorithm must be applied before entering the DMZ, as a greater protection of services that the organization provides to citizens.

Algorithm:

```
Star
    Phase 1: Traffic analysis
    Monitor total traffic, web traffic, mail traffic, file transfer, traffic infrastructure, remote control, other UDP and TCP traffic.
    Phase 2: Traffic filtering
    Obtain the source IP address of package
    Obtain the Access Control Entry
    Compare the direction with those of ACE sequentially If it matches IP address with ACE  entry then allow the packet else deny the packet
    Phase 3: Passage of legitimate traffic
    About traffic, check the characteristics of:
    Time of permanence
    Sources of non-frequent locations
    One website per session
    New users
End
```

3.4. Formula of probability of attack arrival

To obtain a formula of probability and arrival of the attack it was proposed to adopt the Poisson Distribution because it specializes in the probability of occurrence of abnormal or rare events, number of results occur in an interval, probability that more than one result occurs in a range is insignificant.

Equation (1) determines the average rate of requests in a time interval

$$\lambda = \frac{requests}{time} \tag{1}$$

Here:

λ = average request rate
requests = number of requests
time = time interval in seconds

Equation (2) is Poisson distribution that offers continuity in the requests, the probability of a request is the same in all intervals and the arrival of one request does not affect the others.

$$P(\mathrm{k}) = \frac{\lambda^{k} e^{-\lambda}}{k!} \quad (2)$$

Here:
$e = 2.7182818$
k = attacks per unit of time

Description of the method used:

The parameter λ is taken because the client platforms make a number of requests for services in a time interval to server; the requests are the demand to some platform that provides services. The parameters k are the false requests to server in a unit of time, these requests are also demands towards the offering platform. With this formula we obtain a rate of occurrence of legitimate and not legitimate requests addressed to server.

The simulation was given in a time interval of 60 seconds, Figure 5 shows the taking of four numbers of applications (600, 900, 1200, 2400) where the average rates are (λ = 10, λ = 15, λ = 20, λ = 40); for each λ there are 20 attack attempts (k = 1,2,4… 40). The intersection of attack attempts on the X-axis with the average rates generates the probability of arrival of the attack on the Y-axis.

In cases that λ=10 and number of requests is 600, when the number of attacks is 10 the attack arrival is 12.51%; when the number of attacks is 20 the attack arrival is 0.19%; when the number of attacks is 30 the attack arrival is 0.000017%.

In cases that λ=20 and number of requests is 1200, when the numbers of attacks is 10 the attack arrival is 0.581631%; when the number of attacks is 20 the attack arrival is 8.88%; when the number of attacks is 30 the attack arrival is 0.834354%; when the number of attacks is 40 the attack arrival is 0.002778%.

In cases that λ=40 and number of requests is 2400, when the number of attacks is 10 the attack arrival is 0.000001%; when the number of attacks is 20 the attack arrival is 0.0192%; when the number of attacks is 30 the attack arrival is 1.84%; when the number of attacks is 40 the attack arrival is 6.29%.

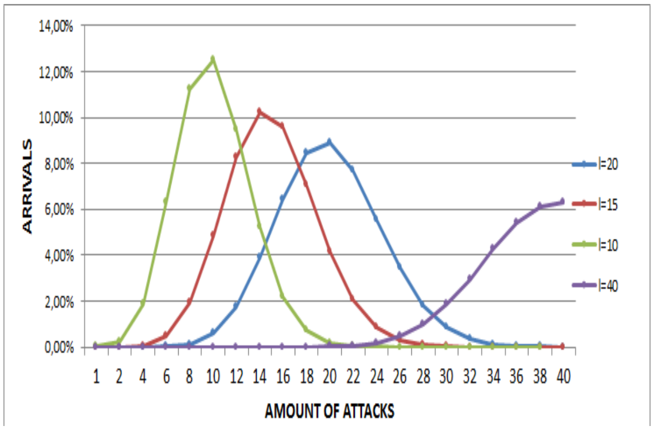

Figure 5: Probability of attack arrival.

It was observed that in a period of 60 seconds in the requests made to server; with low number of requests the percentage of attack arrival is low; when the number of requests grows there are also more hidden attacks that would be successful in their arrival; when the number of requests is higher the percentage of attack arrival drops because it would already be within the system; another behavior is to have high requests and high number of attacks, here the attack success is also high.

From the simulation, the highest attack arrival value was 12.51%, it was deduced that the proposal has an attack detection accuracy is 87.49%.

In the model when the average request rate rises, the number of requests to the server and the number of attacks decreases the probability of arrival of the attack to the server; the number of attacks is inversely proportional to the arrival of attacks; in other words by increasing attacks on the server, the model increases its efficiency.

4. Discussion

- This proposal is a model to minimize the cyberattack in public organizations of countries with similar cultures in Latin America; there is still a need to mature and increase security levels against denial of service attacks, at the moment it is 51%[6].
- The proposed research is related to the results with the following references: in [8] a management and monitoring architecture was defined through software to filter attacks; in [9] an algorithm of classification of the characteristics in the attacks was used; in [21] security levels were defined to prevent attacks; in [22] a set of policies for storage and data security was applied; in [27] a package registration procedure was used to minimize the denial of service in the network; in [29] the application of security policy and user control was used; in [30] an attack mitigation algorithm was used when entering ip addresses and invalid requests; in [32] the detection of attacks in the request and delivery messages was analyzed; in [33] and [34] they defined an architecture to detect attacks on the server and analysis of network traffic; in [37] analyzed a responsibility approach and rules to minimize individual and community risks; in [39] a security policy was applied to computer equipment.
- As exceptions there are issues that should be improved as Cyber Threat Socialization, Threat Tracking, Threat Intelligence and processes to manage attacks and incidents.

As theoretical consequences of this proposal are the denial of attacks, greater protection and security, which are set out below:

Attacks: With the proposed model through identification, defense, identification and recovery, it is intended to apply levels against attack regardless of the size of the organization; the hardware named in the network architecture minimizes the possible denial of services; The algorithm proposed in phases monitors the information or requests that are intended to damage the services.

Protection: The model proposed gives a higher level of defense against attacks that can be executed, faster and more effective reaction; network proposal is a hardware standard that many organizations can implement to protect the services delivered to citizens; The algorithm performs the analysis, filtering and passing of requests or legitimate information towards the services.

Security: The model provides confidence against attacks to apply in organizations with little or a lot of plant personnel, the activities of the model are independent of the infrastructure of an organization; the network proposal also gives confidence for the characteristics of the equipment to be used; The formula applied to calculate the effectiveness of the algorithm demonstrates a low arrival of attacks.

5. Future work and conclusions

As future work, a common policy model is foreseen to increase the security of digital services and prevent cyberattacks in public organizations.

- It was concluded that in order to maintain the continuity of services and activities of public organizations, secure platforms must be in place to monitor and minimize possible attacks; our proposal has an attack detection accuracy of 87.49%.
- ICTs allow the efficient delivery of public services, it is important to adopt a security strategy for normal performance of infrastructure and services of public organizations.
- Cyberattacks can have consequences on strategic, general and specific objectives; in order to meet social objectives, computer services are used, and it is necessary to be prepared for a possible attack.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors thanks to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt).

References

[1] Y. Guan and X. Ge, "Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks," *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 48–59, 2018.

[2] S. Gupta, S. Vashisht, and D. Singh, "A CANVASS on cyber security attacks and countermeasures," *2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016*, no. Iciccs, pp. 31–35, 2016.

[3] H. S. Castro, "The right to privacy and state intervention in the digital age," *Publ. Univ. Netw. Hum. Rights Democr. Lat. Am.*, pp. 73–93, 2015.

[4] G. A. Bustamante, J. R. Rivera, and S. S. Cañas, "Cyber defense as part of the South American integration agenda," *Línea Sur*, vol. 9, no. March 2016, pp. 100–116, 2015.

[5] Organization of American States, "Are We Ready in Latin America and the Caribbean," p. 193, 2016.

[6] Deloitte, "Cyber Risks and Information Security in Latin America & Caribbean Trends," *Risk Advis.*, 2019.

[7] Verizon, "2019 Data Breach Investigations Report," *Verizon Bus. J.*, vol. 2018, no. 1, pp. 1–60, 2018.

[8] F. Ahmadloo and F. R. Salmasi, "A cyber-attack on communication link in distributed systems and detection scheme based on H-infinity filtering," *Proc. IEEE Int. Conf. Ind. Technol.*, pp. 698–703, 2017.

[9] M. S. Abdullah, A. Zainal, M. A. Maarof, and M. Nizam Kassim, "Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News," *Proc. 2018 Cyber Resil. Conf. CRC 2018*, pp. 1–4, 2019.

[10] P. J. Shinde and M. Chatterjee, "A Novel Approach for Classification and Detection of DOS Attacks," *Biomed. Res.*, vol. 2016, pp. S22–S30, 2016.

[11] S. M. T. Toapanta, L. E. M. Gallegos, F. G. M. Quimi, and J. A. O. Trejo, "Analysis of efficient processes for optimization in a distributed database," *CITS 2018 - 2018 Int. Conf. Comput. Inf. Telecommun. Syst.*, pp. 1–4, 2018.

[12] S. M. T. Toapanta, M. A. M. Anchundia, L. E. G. Mafia, and J. A. T. Orizaga, "Biometric systems approach applied to a conceptual model to mitigate the integrity of the information," *CITS 2018 - 2018 Int. Conf. Comput. Inf. Telecommun. Syst.*, 2018.

[13] L. Mertz, "Cyberattacks on Devices Threaten Data and Patients: Cybersecurity Risks Come with the Territory. Three Experts Explain What You Need to Know," *IEEE Pulse*, vol. 9, no. 3, pp. 25–28, 2018.

[14] A. Kott, J. Ludwig, and M. Lange, "Assessing Mission Impact of Cyberattacks: Toward a Model-Driven Paradigm," *IEEE Secur. Priv.*, vol. 15, no. 5, pp. 65–74, 2017.

[15] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[16] C. G. Akcora, J. Z. Bakdash, Y. R. Gel, M. Kantarcioglu, L. R. Marusich, and B. Thuraisingham, "Attacklets: Modeling high dimensionality in real world cyberattacks," *2018 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2018*, pp. 55–57, 2018.

[17] I. Perera, J. Hwang, K. Bayas, B. Dorr, and Y. Wilks, "Cyberattack Prediction Through Public Text Analysis and Mini-Theories," *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018*, pp. 3001–3010, 2019.

[18] Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, "Deep learning approach for cyberattack detection," *INFOCOM 2018 - IEEE Conf. Comput. Commun. Work.*, pp. 262–267, 2018.

[19] K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: A deep learning approach," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2018-April, pp. 1–6, 2018.

[20] O. Oksiiuk, L. Tereikovska, and I. Tereikovskiy, "Adaptation of the neural network model to the identification of the cyberattacks type 'denial of service,'" *14th Int. Conf. Adv. Trends Radioelectron. Telecommun. Comput. Eng. TCSET 2018 - Proc.*, vol. 2018-April, pp. 502–505, 2018.

[21] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," *2016 IEEE Int. Conf. Cybercrime Comput. Forensic, ICCCF 2016*, pp. 1–9, 2016.

[22] D. Polverini, F. Ardente, I. Sanchez, F. Mathieux, P. Tecchio, and L. Beslay, "Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process," *Comput. Secur.*, vol. 76, pp. 295–310, 2018.

[23] P. Black, I. Gondal, and R. Layton, "A survey of similarities in banking malware behaviours," *Comput. Secur.*, vol. 77, pp. 756–772, 2018.

[24] K. Pipyros, C. Thraskias, L. Mitrou, D. Gritzalis, and T. Apostolopoulos, "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual," *Comput. Secur.*, vol. 74, pp. 371–383, 2018.

[25] H. S. Lallie, K. Debattista, and J. Bal, "Evaluating practitioner cyber-security attack graph configuration preferences," *Comput. Secur.*, vol. 79, pp. 117–131, 2018.

[26] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, 2018.

[27] A. Y. Nur and M. E. Tozal, "Record route IP traceback: Combating DoS attacks and the variants," *Comput. Secur.*, vol. 72, pp. 13–25, 2018.

[28] K. A. Molinaro and M. L. Bolton, "Evaluating the applicability of the double system lens model to the analysis of phishing email judgments," *Comput. Secur.*, vol. 77, pp. 128–137, 2018.

[29] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user," *Comput. Secur.*, vol. 75, pp. 1–9, 2018.

[30] D. S. N. Mary and A. T. Begum, "An Algorithm for Moderating DoS Attack in Web based Application," pp. 26–31, 2017.

[31] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, and P. Maciel, "Impact of a DDoS attack on computer systems: An approach based on an attack tree model," *12th Annu. IEEE Int. Syst. Conf. SysCon 2018 - Proc.*, pp. 1–8, 2018.

[32] N. Tripathi, N. Hubballi, and Y. Singh, "How Secure are Web Servers? An empirical study of Slow HTTP DoS attacks and detection," *Proc. - 2016 11th*

Int. Conf. Availability, Reliab. Secur. ARES 2016, pp. 454–463, 2016.

[33] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna, and R. Mahajan, "Detection of DoS/DDoS attack against HTTP servers using naive Bayesian," *Proc. - 1st Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2015*, pp. 280–285, 2015.

[34] Sornalakshmi.K, "Detection of DoS attack and Zero Day Threat with SIEM," pp. 1–7, 2017.

[35] N. E. Herald and M. W. David, "A Framework for Making Effective Responses to Cyberattacks," *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018*, pp. 4798–4805, 2019.

[36] E. N. Yılmaz and S. Gönen, "Attack detection/prevention system against cyber attack in industrial control systems," *Comput. Secur.*, vol. 77, pp. 94–105, 2018.

[37] K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron, "Is the responsibilization of the cyber security risk reasonable and judicious?," *Comput. Secur.*, vol. 78, pp. 198–211, 2018.

[38] R. AlShboul, F. Thabtah, N. Abdelhamid, and M. Al-diabat, "A visualization cybersecurity method based on features' dissimilarity," *Comput. Secur.*, vol. 77, pp. 289–303, 2018.

[39] K. Adi, L. Hamza, and L. Pene, "Automatic security policy enforcement in computer systems," *Comput. Secur.*, vol. 73, pp. 156–171, 2018.

[40] D. Mitropoulos, P. Louridas, M. Polychronakis, and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," *IEEE Trans. Dependable Secur. Comput.*, vol. 16, no. 2, pp. 188–203, 2019.

[41] M. E. Ahmed, S. Ullah, and H. Kim, "Statistical Application Fingerprinting for DDoS Attack Mitigation," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1471–1484, 2019.

[42] A. Bhadane and S. B. Mane, "Detecting lateral spear phishing attacks in organisations," *IET Inf. Secur.*, vol. 13, no. 2, pp. 133–140, 2019.

[43] S. Dong, K. Abbas, and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," *IEEE Access*, vol. 7, pp. 80813–80828, 2019.

[44] G. Aranda *et al.*, "BWManager: Mitigating Denial of Service Attacks in Software-Defined Networks Through Bandwidth Prediction," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 4, pp. 1235–1248, 2018.

[45] FBI, "FBI 2018 Internet Crime Report," pp. 1–28, 2018.

[46] S. Pournouri, S. Zargari, and B. Akhgar, "An Investigation of Using Classification Techniques in Prediction of Type of Targets in Cyber Attacks," *Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3 2019*, pp. 202–212, 2019.