**Periodicals of Engineering and Natural Sciences**
Vol. 9, No. 3, August 2021, pp.603-614

ISSN 2303-4521
*Methodology/Method*

# An implementation of an Artifact for security in 5G networks using Deep Learning methods.

**Carlos Estrada-Vásquez, Walter Fuertes, and Henry Cruz**
Department of Computer Sciences, Universidad de las Fuerzas Armadas ESPE, 171 5 231 – B, Sangolquí, Ecuador

## ABSTRACT

The Fifth-Generation networks are vital in telecommunications, which reaches a substantial increase in transmission speed. However, due to this dynamism, cyber attackers try to take advantage of certain configuration flaws. Under this problem, this study aims to design and implement an artifact capable of protecting and improving security in this cellular network type. The artifact uses a neural network structure based on Depp Learning, Gödel's theorem, Dijkstra's graph theory, a sigmoid function for faster activation in the designed neural network, and a mathematical model able to perform a recursive and logical process for the analysis of attacks. Considering the Gödel method, this artifact can evade Worms, Ransomware, Phishing, Doxing attacks and can be used in the OPC, Profibus, EtherCat, Profinet DNP3, and Modbus protocols. Its implementation allows us to create evasive actions in case of an attack and improve the configuring flaws in the security protocols, changing its parameters and making it secure. We developed the artifact through Extreme Programing with the combination of Python and Matlab. The results prove the functionality of the algorithms and demonstrate the success in evading an attack or making the best decision to protect the 5G network.

**Keywords**: Deep Learning, 5G networks, Information security, Neural Network

***Corresponding Authors:***

Carlos Andrés Estrada Vásquez, Walter Fuertes, and Henry Cruz
Department of Computer Science,
Universidad de las Fuerzas Armadas - ESPE,
Sangolquí, Ecuador
E-mail: caestrada4, wmfuertes, hocruz{@espe.edu.ec}

## 1. Introduction

The arrival of the Fifth-Generation networks (5G) to the world of technology has significantly increased data transmission speed and the ease of connectivity between devices. This kind of technology created a new concept, where there are great benefits. 5G networks will provide opportunities for developing new services, new business models, and new players to enter the mobile market [1]. However, also vulnerabilities increased the network's security, one of the essential risks being larger-scale DDoS attacks.

Nowadays, the industry and the scientific community argue relevant security risks and threats, and various vulnerabilities, to which 5G cellular networks are exposed [2]. Furthermore, as 5G services grow, they become attractive targets for cyberattacks due to increasing volumes and poor and weak information security levels [3]. In fact, in recent years, 5G has posed serious cybersecurity challenges, motivated by the number of cyberattacks that have grown dramatically, as well as its complexity [4].

This study aims to improve the security of 5G cellular networks due to failures in security and network protocols due to their recent adaptation [5]. For this, a vulnerability detection artifact was developed using Deep Learning techniques with convolutional networks, which will act as a learning process to detect the sectors with vulnerabilities. An artifact is a tangible product resulting from the software development process. Then, we implement a real-time detection algorithm, which stores the data to convert it into an input for the designed neural network layer assignment based on a mathematical model.

We used the sigmoid function as an activation, which speeds up the process in a binary 1 or 0 state. In addition, we applied Extreme Programming (XP) to develop the artifact [6]. For the statistical validation of the model, we employed Gödel’s theorem for algorithms of complexity four [7]. Concerning the neural network, we use the Tensor Flow and Numpy libraries of Python for its development for discrete variables.

For the proofs of concept, we used a virtual machine with an Ubuntu server. In addition, we configured a virtual network environment to simulate the 5G network [8]. Likewise, the Matlab functions were used, which allows applying the tests of Gödel’s theorem [9]. Finally, the inflection points in the performance curves were measured in the execution of the mathematical model. The results show the algorithm's efficiency to detect any attack and the effectiveness of knowing the best evasion to counteract an external hack. Our development is expected to drive a change in computer science security and increase security levels in 5G cellular networks.

The main contribution of this study is to create an artifact that improves the configuration of security protocols in 5G networks [10], which can analyze, which is the best evasion technique against a computer attack. All of this is achieved through neural network training, capable of identifying the vulnerabilities against the attack. This analysis identifies similar patterns from other existing attacks and assesses the correct way to prevent them from affecting the stability of the network.

The article is structured as follows: Section 2 describes some previous related works. Section 3 explains in depth the methods and techniques that were used to develop the model. In section 4, the results are evaluated. Finally, section 5 concludes with the main findings and lines of future work.

## 2. Related Work

The Fifth-Generation of telecommunications represents a technological revolution that a few years ago was not foreseen that could be possible. However, it has already begun to be developed and implemented in several countries since 2019 [11]. Within this context, in the industry, several solutions have been proposed. A summary is described below:

As mentioned in [12], the expectations in 5G networks enhance the wireless network services, which have much more advanced cryptographic security algorithms. Thus, in 2017 a Physical layer security (PLS) solution provides advantages over the features in the wireless channels that receive the signal against attacks from malicious users. Moreover, PLS techniques match the features of 5G networks. Therefore, the application of PLS to 5G networks is a promising solution to address security threats. This article presents a comprehensive review of the state-of-the-art PLS techniques and discusses their applications in 5G networks [13].

In the study proposed of [14], a PLS is used in 5G networks, which continuously examines security as the transmission inherent and vulnerable for the deficiencies in the security of this type of network. This work proposes a solution based on safeguarding data randomly in the middle of communications.

The three most promising ones are discussed among various technologies: heterogeneous networks, massive multiple-input multiple-output, and millimeter-wave. Based on the fundamental principles of each technology, we identify the rich opportunities and the significant challenges that security designers must tackle [15]. Such identification is expected to advance the understanding of future physical layer security decisively.

Another study that has been observed based on 5G technologies refers to [16]. Their technique based on quantum computing protocols involves a range of possibilities due to their perceptual states, so they mention mechanisms in QoS, which work for data sharing and security. The statistical data sample presents an excellent efficiency in the equation raised concerning the bit-by-bit vector operation. Besides, the protocols are based on Quantum Hash function schemes [17]. A function is generated, which evaluates the diffusion and distribution of the data curves through different analysis tests. Our work allows the help of using the data as bi-neutral techniques in deep learning algorithms [18].

In perspectives of using techniques based on Deep Learning [19], the article proposed by [20] mentions the principles of cybersecurity and defense in systems that work with this type of technology. The techniques used for the existing traffic in the network are analyzed. The authors' proposal allows adapting and automating the configuration in the architecture of a defense system against computer attacks, the experiments that were conducted in virtualized environments. Also in [21], a wide range of Machine Learning techniques can accomplish the above requirements, e.g., it has no strict time restrictions in the NAD module if the ASDs have adequate classification performance.

In another study based on Deep Learning techniques presented by [22], a solution based on a framework is mentioned. The authors propose a Blockchain-based secure FL framework to create intelligent contracts and prevent malicious or unreliable participants from being involved in FL. In doing so, the central aggregator recognizes malicious and unreliable participants by automatically executing intelligent contracts to defend against poisoning attacks [23].

Within this context, in preliminary studies, authors used neural cryptography, which uses a modified artificial neural network called the Tree Parity Machine or TPM to establish a private key through an insecure channel [24]. Furthermore, in [25], the authors increased the security of the RSA encrypted message by investing a minimum amount of extra time in encryption and decryption (i.e., multi-encryption) in networks and mobile devices. Finally, in [26], researchers evaluated the malware life cycle. They developed a custom and unpublished keylogger using Python and added the necessary methods to avoid the leading security tools used in Windows environments successfully.

## 3. Materials and methods

The proposed artifact uses an Artificial Intelligence technique called Deep Learning. According to [27], Deep Learning is a form of Machine Learning that enables computers to learn from experience and understand the world in terms of a hierarchy of concepts. Because the computer gathers knowledge from experience, there is no need for a human-computer operator formally to specify all the knowledge needed by the computer.

On the other hand, the 5G is a technology with a good present and future. It aims to make a significant leap in connectivity, automation, and among these, one of the most important, information security.

Information security plays an essential role in everyday life since the evolution of technology increases vulnerability risk factors. Within this viewpoint, electronic devices have an essential role in the 5th Generation of telecommunications by sending and receiving vital information from users. As stated by [28] the security of information transfer, messages, and user data depends on the guarantees provided by authentication protocols and encryption techniques.

With 5G technology being a high-speed network, information packets travel the path shorter than its predecessor technology. However, this also poses more significant risks regarding privacy, confidentiality, and integrity of the information, which malicious people can receive for profit or harm third parties. Therefore, one alternative is the use of encryption techniques to reduce the chances of unauthorized access. Also, in the opinion of Gonzalez [28], thanks to the high speed of the 5G network, physical layer security (PLS) type encryption techniques can be implemented to prevent the interception of data traffic..

Thus, we propose to use some techniques to create a new artifact that can interpret the vulnerable data and insecure network sectors, also prevent informatics attacks in a 5G network [16]. On the other hand, considering the 5G network can be targeted by cybersecurity attacks, it is necessary to detect and learn the offense used so that the algorithm can solve the different situations and risks that may occur [29]. For example, suppose there is an attacker or a problem of insecurity in the network. In that case, the artifact will apply specific protocols to avoid exposing any vulnerability to the user.

We configured a virtual network environment with Linux service with Virtual Box as the central platform to create the 5G simulation. Within the context of this research, we defined a virtual network as a set of virtual network devices connected collectively in a given topology, which emulates an equivalent system in which the environment is perceived as if it were real [30]. Figure 1 shows the topology, from connection to a network, access to the web, connection to the virtual machine, subsequent algorithm execution, performing maintenance to the web, and network configuration.

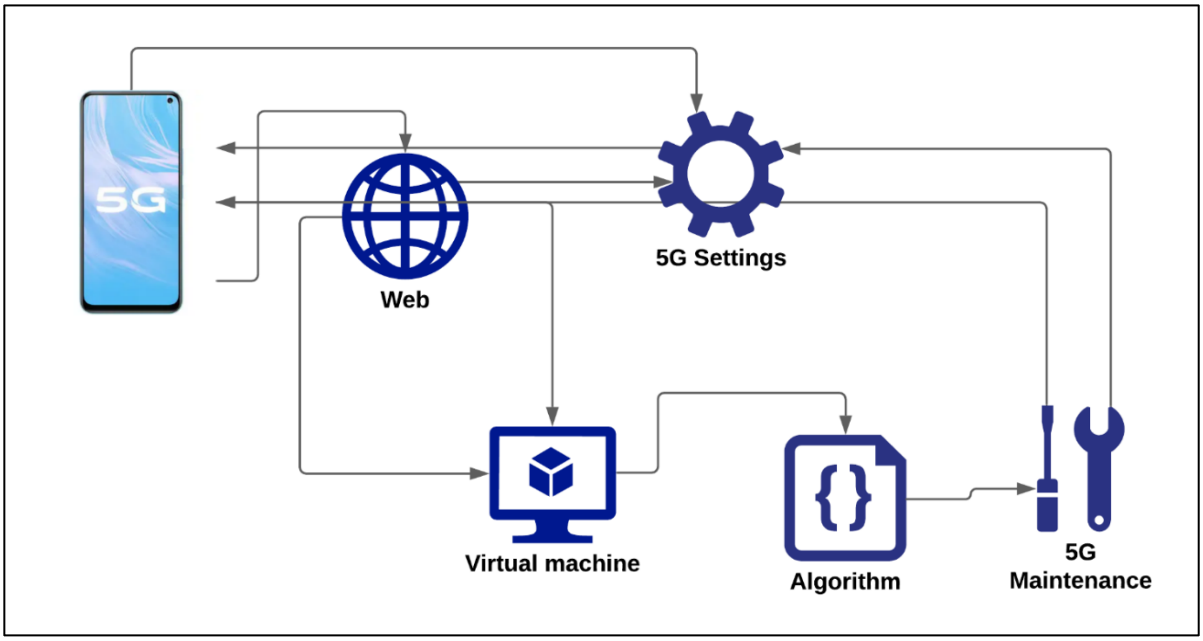


Figure 1. Design of the experimentation topology

An experimental research proposal has conducted, applying Extreme Programming as a software engineering development methodology over a controlled virtualized environment, allowing emulating any event generated during network use with this type of technology. As it is known, the use of a Bayesian network that has several learning layers helps to diversify the computational mathematics for the continuous analysis of data that will enter this input function to give a resultant functional output.

For the development of this study, we considered using a sigmoid function. According to [31] sigmoid is a bounded and differentiable function defined for all real input values. It has a non-negative derivative at each point and precisely one inflection point. Figure 2 reveals the configuration of sigmoid neural network activation.

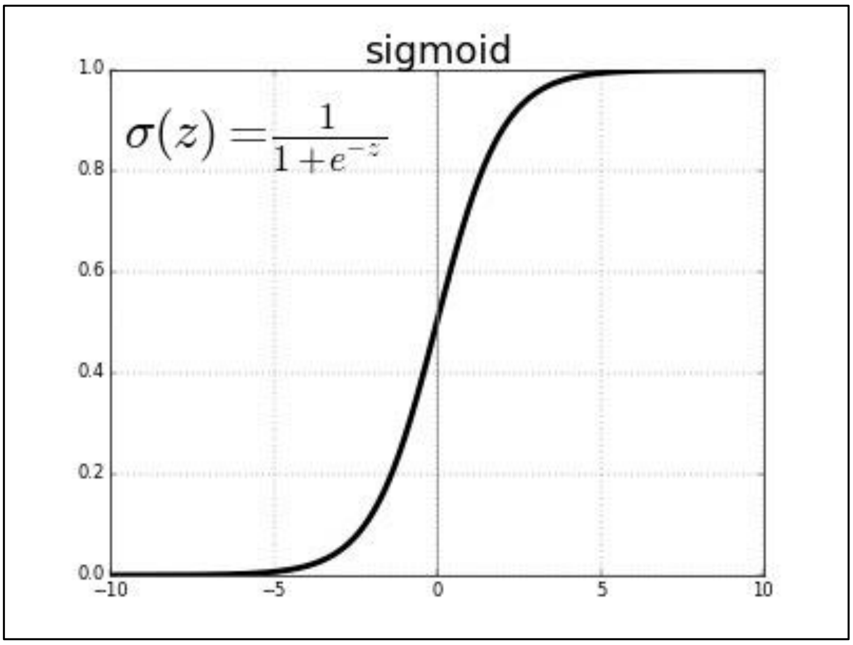


Figure 2. Sigmoid function as network activation.

We have developed our own customized and previously reviewed algorithm that has not been published yet. We have added different techniques concerning the needs of 5G networks. The algorithm uses a different neural network structure, based on a Sigmoid, which was developed in Python, Matlab, and R programming languages, tested on Windows-based operating systems, using a server-based on Linux-Ubuntu. The following equation shows the mathematics behind the network created (see equation 1).

$$L1 = Sigmoid(W_1 X + a_1 + b_1) \qquad \text{(Equation 1)}$$

The neural network was concise, assembled in the following factorial form, where it's learning definition works with the respective derivatives in each recursive equation.

$$W_1 = W_1! - lr \times \frac{\partial L}{\partial W_1} \qquad \text{(Equation 2)}$$

The equations comply with the respective loss rule. Five layers will be used to allow the algorithm to be efficient in analyzing 5G networks. Therefore, the output function generates the following result according to linear computer algebra.

$$Y_1 = w_{11} \times x_{11} \times a_{11} + w_{21} \times x_{12} \times a_{12} + w_{31} \times x_{13} \times a_{13} + w_{41} \times x_{14} \times a_{14} + w_{51} \times x_{15} \times a_{15}$$

Once the connection was conducted, the process of algorithmic complexity and evaluation of the neural network had to be used. Then the respective tests were carried out in XP, which according to the graph provided by Matlab, inferred that the performance of the network with sigmoid activation is based on a speed of one Gbps.

As can we observe in Figure 3, two synapses of the neural network are shown. The red function expresses the input of the network connection, while the blue function expresses the output function. It can be interpreted that both are in connection at the same activation speed and efficiency. In this way, being interconnected between them, the deep network is configured based on the input and output protocols.

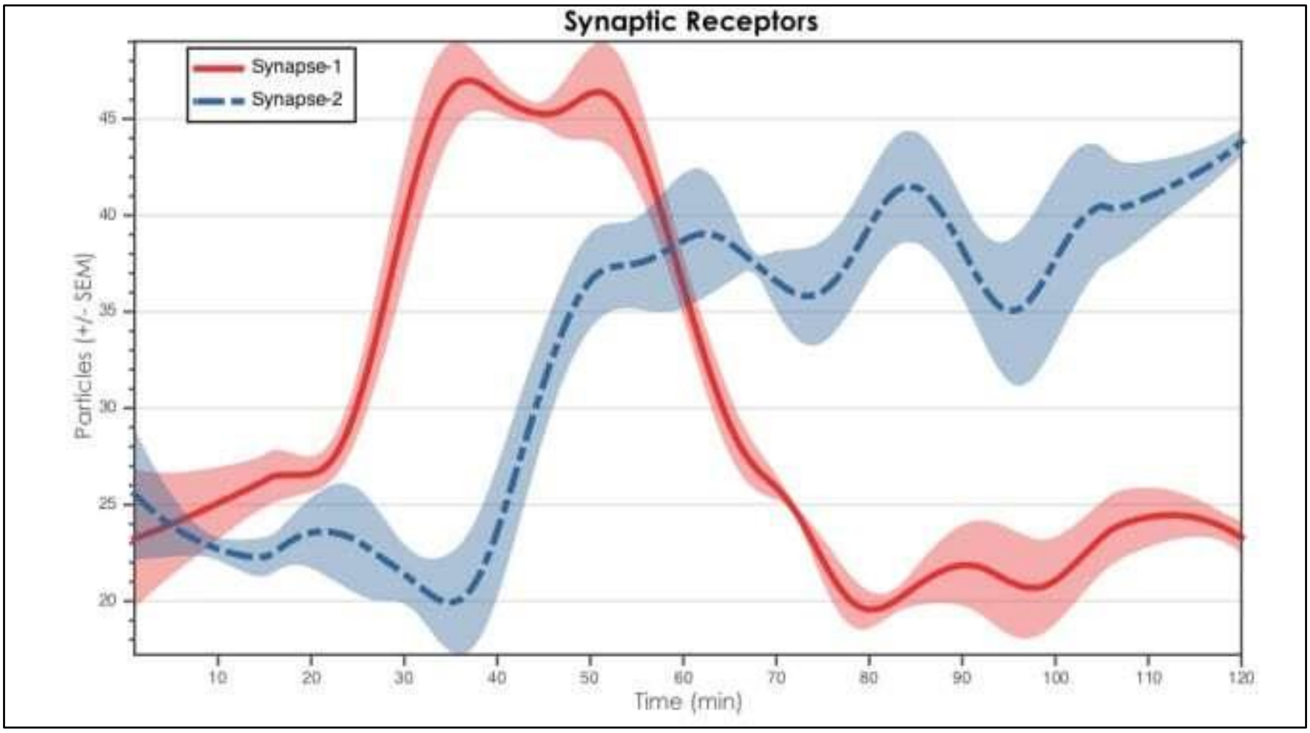


Figure 3. Graph representing the synapse between input and output of the neural network.

Figure 4 shows that a neural network with five layers designed for the project explains the interconnection between networks. The factorial mathematical model is responsible for an initial layer with four inputs that interact: network speed, security protocols, the different possibilities of IP networks, and finally, the network parameters. The other three layers oversee activating methods to prevent the network from being compromised through the training of existing security methods to combine different ethical hacking techniques. Finally, we have a layer with a single output that will apply the technique to counter the attack on the 5G network. The circular shape was established for its short path according to Dijkstra's graph theory, and the network can analyze evasions much faster.

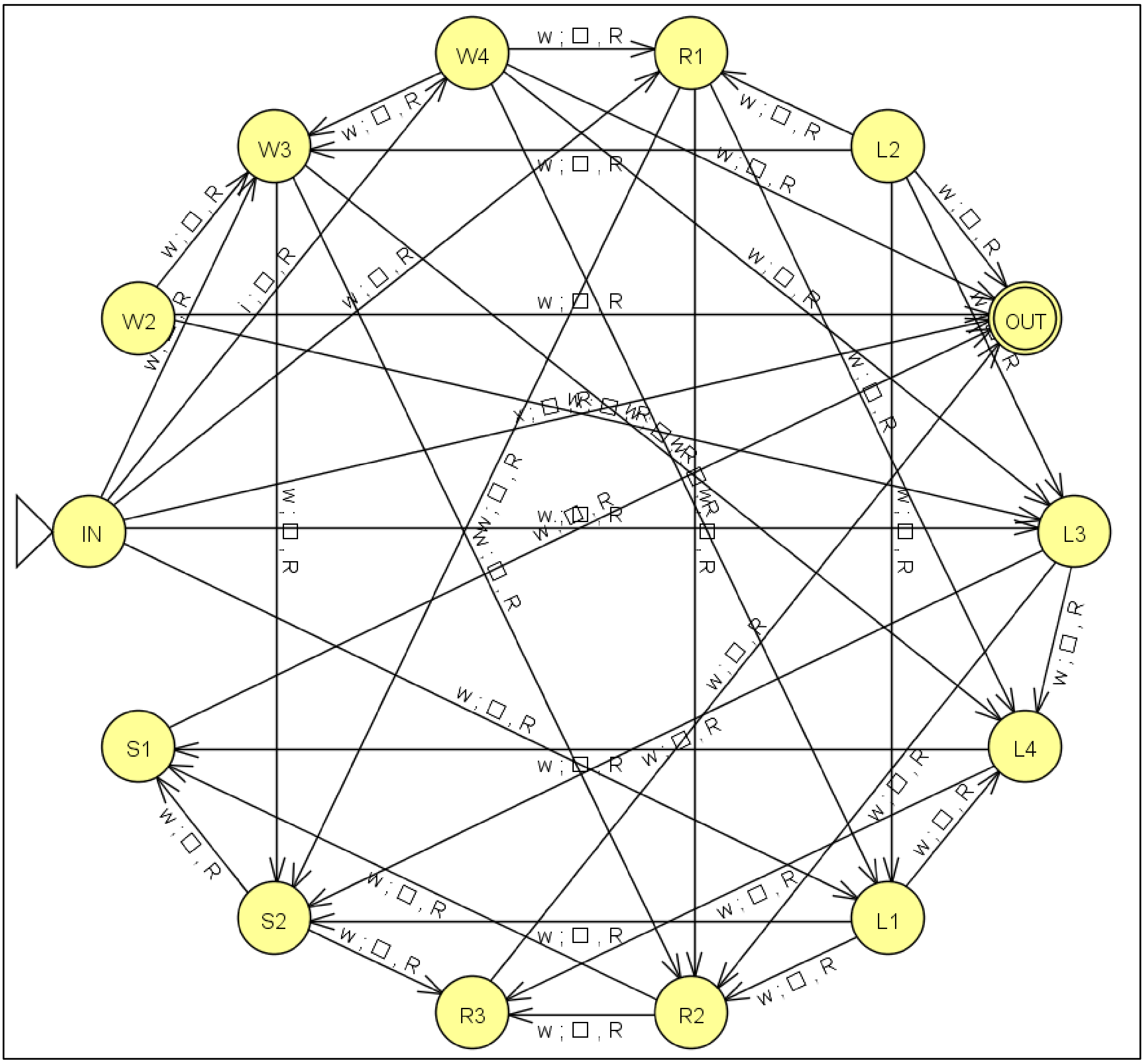
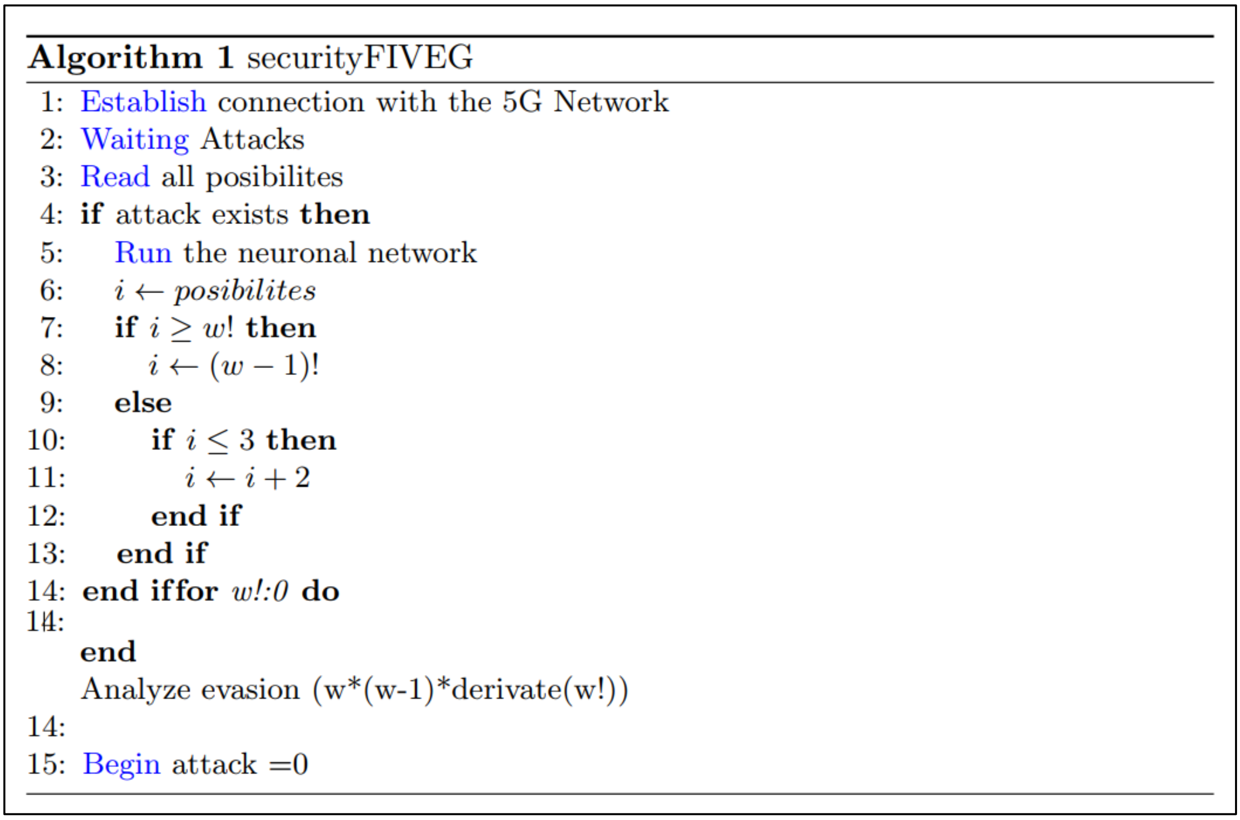


Figure 4. Diagram of the neural network.

Algorithm 1 is a set of consecutive instructions, theories, and techniques for measuring algorithmic completeness. The algorithm uses a neural network structure based on Deep Learning, including Gödel's theory, Dijkstra's graph theory, a mathematical model, and a sigmoid activation function. The algorithm allows us to create evasive actions in an attack and solves the limitations in the configurations in the security protocols (SSH, TCP / IP, and DNS). Therefore, changing the network parameters such as IP, DNS, subnet, netmask makes the 5G network more secure. We develop the algorithm through Extreme Programing with the combination of Python and Matlab (See algorithm 1).

Algorithm 1 oversees counteracting and mitigating the attack, i.e., with the neural network run, it performs a recursive process, which chooses the best attack method, based on the direct inputs and network connection; thus, it is named a smart network.



```
Algorithm 1 securityFIVEG
Establish connection with the 5G Network
Waiting Attacks
Read all posibilites
if attack exists then
    Run the neuronal network
    $i \leftarrow posibilites$
    if $i \geq w!$ then
        $i \leftarrow (w-1)!$
    else
        if $i \leq 3$ then
            $i \leftarrow i+2$
        end if
    end if
end iffor $w!$:$0$ do

end
Analyze evasion (w*(w-1)*derivate(w!))

Begin attack =0
```

Algorithm 1. securityFIVEG

### 3.1. Proof of concept

The artifact developed has undergone various tests, including statistical and performance tests, and as a result, has demonstrated its effectiveness. Having been tested in an environment of two virtual machines with 64-bit operating systems and Ubuntu 20.04, the algorithm had a previous estimate of 1.2 to 1.3 seconds in receiving the data, so it is much faster than other existing algorithms.

On the other hand, the virtualized server, which oversaw evaluating the 5G network when transmitting the data to the virtual machines, verified that it did not collapse, despite the large amount of data to which it was subjected convoluted neural network.

As shown in Figure 4, a neural network with five layers was designed for the project and explained the interconnection between networks. The factorial mathematical model is responsible for an initial layer with four inputs, where the network speed, security protocols, IP networks, and the network parameters enter. The other three layers oversee activating methods to prevent the network from being compromised by training existing security methods. Hence, it can combine different ethical hacking techniques. Finally, we have a layer with a single output that will apply the technique to counter the attack on the 5G network. According to Dijkstra's graph theory, the circular shape was established for its short path; the network can analyze evasions much faster.

At this point in the research, cybersecurity is the most relevant issue, as it became a crucial element in estimating the risks of massive networking of devices with connectivity through virtualized 5G networks [32], which means more utility and potential for IoT, but less security in the transmission and reception of data. Decentralized security in this network is the leading risk to achieve the speed that highlights 5G. There are more traffic routing points and not being monitored all these points. When an attack occurs, it takes longer to detect and address the problem, so more monitoring is needed since the loss of information can be catastrophic for an organization or user, even if the attack has a duration of 5 to 10 seconds.

## 4. Evaluation Results and discussion

We test the artifact using Gödel's incompleteness theorems [33] to measure the complexity of the algorithms. We exported its results in different graphs. Figure 5 shows the results of this test, i.e., the first illustration shows the relationship between the processing and its data loss. The second graph shows the propagation of the analysis when performing the tests in Matlab. The third figure shows how the processing goes when choosing the best evasion method. Finally, the last graph shows the cook distance, which is to say that the algorithm has chosen the best way to avoid an attack. In this way, it performs the efficiency operation concerning the 5G network[34].

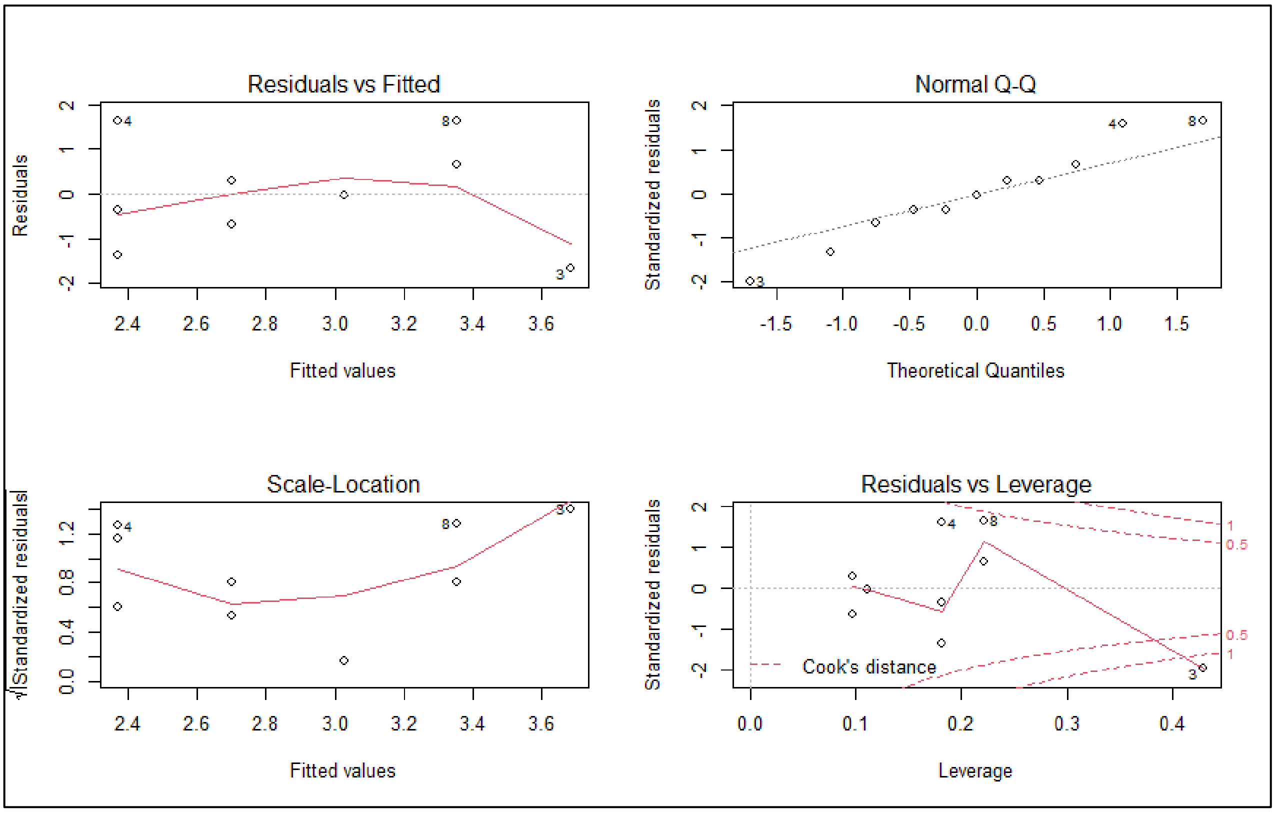


Figure 5. Results of the test applied Gödel's incompleteness theorems

Table 1 presents the results obtained by subjecting the algorithm to the validation process according to the Gödel completeness test [35] at 1Gbps of network speed. As can be seen, it examines the security status of the communication protocols involved during transmission; the evasion techniques applied, the speed of algorithm execution, and data storage capacity. Before executing the neural network, the first level of complexity of security level is calculated.

Table 1. Results of configurations before the algorithm execution according to the Gödel theorem

| Before applying the algorithm | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Speed network** | 1Gbps | | | | | | | | | | |
| **Protocols** | TCP/IP | DNS | SSH | FTP | OPC | Profibus | CIP | EtherCAT | Profinet | DNP3 | Modbus |
| | x | X | x | X | | | | | | | |
| **Evasion Attacks** | Trojan | Spyware | Adware | Worm | Ransomware | Phishing | Malware | Doxing | | | |
| | x | X | x | | | | x | | | | |
| **Speed algorithm** | - | | | | | | | | | | |

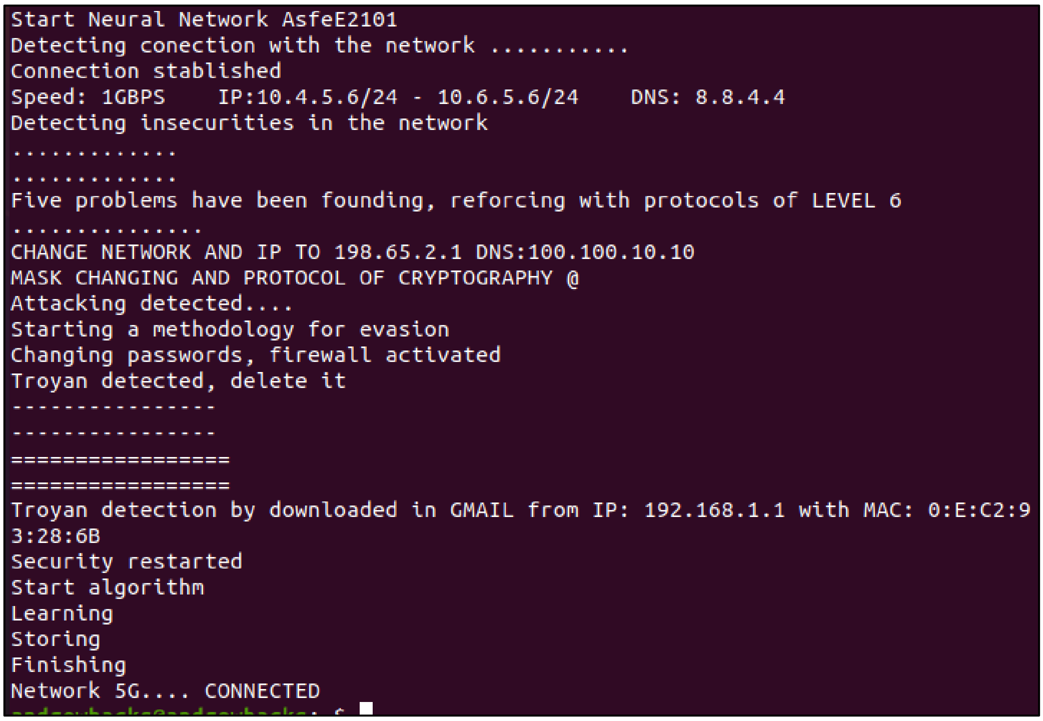
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Capacity** | 1EB | | | | | | | | | | |
| **Complex** | 1 | | | | | | | | | | |

Table 2 presents the results after the neural network execution. Here, the algorithm has an execution speed of up to one Ebps. In addition, security is activated in a more significant number of communication protocols and evasion techniques against attacks compared with Table 1, consequently increasing the complexity level of security to four. These results demonstrate the functionality and efficiency of our proposal.

Table 2. Results of configurations after the algorithm execution according to the Gödel theorem.

| **After applying the algorithm** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Speed network** | 1Gbps | | | | | | | | | | |
| **Protocols** | TCP/IP | DNS | SSH | FTP | OPC | Profibus | CIP | EtherCAT | Profinet | DNP3 | Modbus |
| | x | x | x | X | x | x | x | x | x | X | x |
| **Evasion Attacks** | Trojan | Spyware | Adware | Worm | Ransomware | Phishing | Malware | Doxing | | | |
| | x | x | x | X | x | x | x | x | | | |
| **Speed algorithm** | 1EB/S | | | | | | | | | | |
| **Capacity** | 1EB | | | | | | | | | | |
| **Complex** | 4 | | | | | | | | | | |

Given the respective analysis of the completeness of this algorithm, the expected results of an attack may vary due to the type of attack external to 5G networks. However, as can be appreciated in the neural network, the event creates a single output that generates a counterattack or improves the security protocols of the 5G network. For this reason, Figure 6 presents the results in real-time after running the algorithm and receiving a simulated external attack by sending a virus and downloading it via email. That is, once this indirect attack has been carried out, the algorithm can defend the network.



```
Start Neural Network AsfeE2101
Detecting conection with the network ..........
Connection stablished
Speed: 1GBPS    IP:10.4.5.6/24 - 10.6.5.6/24    DNS: 8.8.4.4
Detecting insecurities in the network
.............
.............
Five problems have been founding, reforcing with protocols of LEVEL 6
...............
CHANGE NETWORK AND IP TO 198.65.2.1 DNS:100.100.10.10
MASK CHANGING AND PROTOCOL OF CRYPTOGRAPHY @
Attacking detected....
Starting a methodology for evasion
Changing passwords, firewall activated
Troyan detected, delete it
----------------
----------------
=================
=================
Troyan detection by downloaded in GMAIL from IP: 192.168.1.1 with MAC: 0:E:C2:9
3:28:6B
Security restarted
Start algorithm
Learning
Storing
Finishing
Network 5G.... CONNECTED
```

Figure 6. Algorithm execution and attack evasion.

Once the algorithm is executed, a comparison of the network security is conducted while new protocols are activated. As a result, the neural network can infer the best evasions techniques and improve security. Figure 7 shows an illustration where the network becomes more secure with the implemented protocols. The graph on the right side shows how it improved after executing the neural network and the algorithm with the deep learning technique.

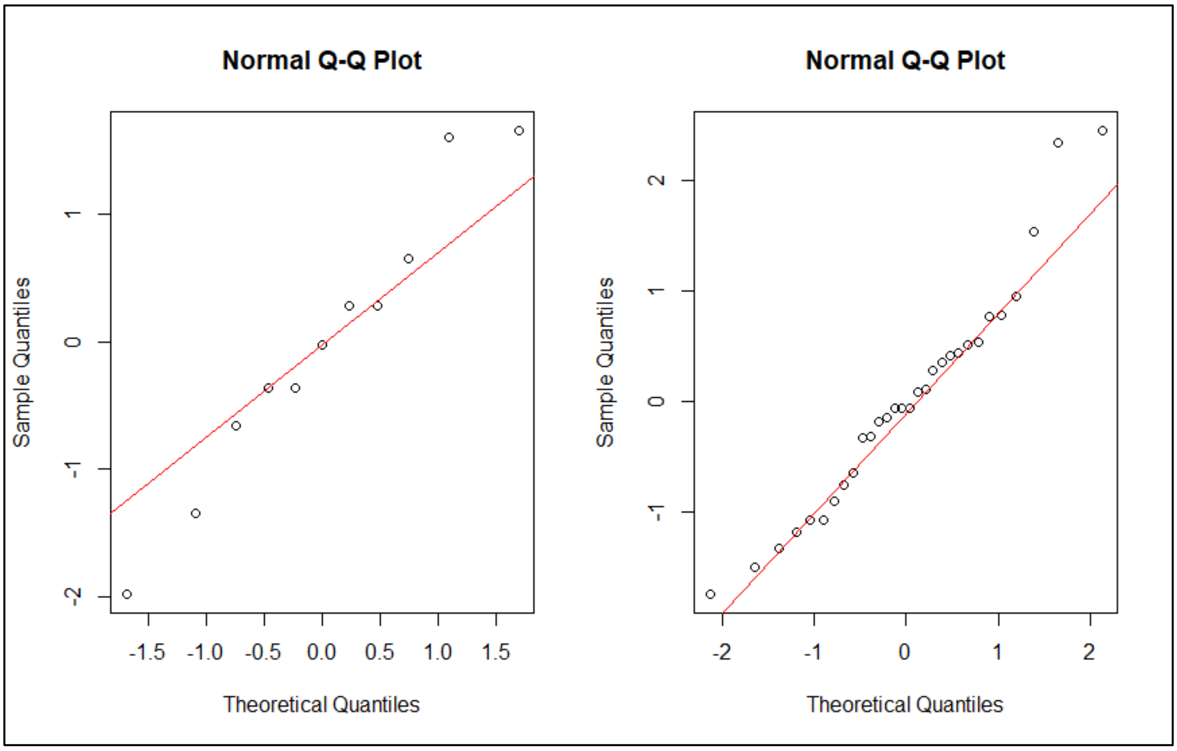


Figure 7. 5G Network before and after the execution of the algorithm.

The results are as expected according to Gödel's completeness test [36]. Moreover, since the neural network was tested, the efficiency and data propagation are adequate. In addition, as shown in the illustrations, it can be seen how the network can detect the best way to counter an attack. On the other hand, due to the algorithm model and the mathematical model statistics, it is considered that the algorithm can benefit the security in 5G networks.

## 5. Conclusions and future work

This study focused on the design and implementation of an unprecedented artifact to improve the security of 5G networks. We implemented the artifact with XP methodology and Python, designing a mathematical model that included a sigmoid activation function. Gödel's method applied to the mathematical model was able to evade Worms, Ransomware, Phishing, Doxing attacks and could be used in OPC, Profibus, EtherCat, Profinet, DNP3, and Modbus protocols. Among the results, we highlight the Gödel test results that show the efficiency of the mathematical model and its correct interpretation at the time of the simulation. In addition, the artifact functionality offers network security when entering data types before and after its execution and its stability and protection against any thread. Finally, the algorithm achieved the training of a neural network to analyze any pattern of insecurity and opt for evasion in the face of an external computer attack. With this, we can state that the algorithm can learn based on the experience of each attack obtained and improve the protection of a 5G network.

As future work, we planned to apply a mathematical model and Deep Learning to implement early warnings and vulnerability assessment in attacks to 5G cellular networks.

**Acknowledgments**
The authors would like to thank the Universidad de las Fuerzas Armadas-ESPE of Sangolquí, Ecuador, for the resources granted to develop the research project entitled: "Design and Implementation of the IT infrastructure and service management system for the ESPE Academic CERT", coded as PIC-2020-ESPE-CERT.

## References

[1] G. Arfaoui *et al.*, “A security architecture for 5G networks,” *IEEE Access*, vol. 6, pp. 22466–22479, 2018.

[2] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera, “A stakeholder-oriented security analysis in virtualized 5G cellular networks,” *Comput. Networks*, vol. 184, p. 107604, 2021.

[3] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, “Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks,” *Electronics*, vol. 10, no. 13, p. 1549, 2021.

[4] E. Rodríguez, B. Otero, N. Gutiérrez, and R. Canal, “A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks,” *IEEE Commun. Surv. Tutorials*, 2021.

[5] J. Cao *et al.*, “A survey on security aspects for 3GPP 5G networks,” *IEEE Commun. Surv. tutorials*, vol. 22, no. 1, pp. 170–195, 2019.

[6] L. Yao and Z. Ge, “Distributed parallel deep learning of hierarchical extreme learning machine for multimode quality prediction with big process data,” *Eng. Appl. Artif. Intell.*, vol. 81, pp. 450–465, 2019.

[7] B. J. Copeland, C. J. Posy, and O. Shagrir, *Computability: Turing, gödel, church, and beyond*. Mit Press, 2013.

[8] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5G and beyond,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[9] O. Shagrir, “Gödel on Turing on computability,” in *Church’s Thesis after 70 Years*, De Gruyter, 2013, pp. 393–419.

[10] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, 2019.

[11] S. Buffa, M. Cozzini, M. D’Antoni, M. Baratieri, and R. Fedrizzi, “5th generation district heating and cooling systems: A review of existing cases in Europe,” *Renew. Sustain. Energy Rev.*, vol. 104, pp. 504–522, 2019.

[12] L. Sun and Q. Du, “Physical layer security with its applications in 5G networks: A review,” *China Commun.*, vol. 14, no. 12, pp. 1–14, 2017, doi: 10.1109/CC.2017.8246328.

[13] R. Dong, C. She, W. Hardjawana, Y. Li, and B. Vucetic, “Deep learning for radio resource allocation with diverse quality-of-service requirements in 5g,” *IEEE Trans. Wirel. Commun.*, 2020.

[14] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015, doi: 10.1109/MCOM.2015.7081071.

[15] U. Challita, W. Saad, and C. Bettstetter, “Cellular-connected UAVs over 5G: Deep reinforcement learning for interference management,” *arXiv Prepr. arXiv1801.05500*, 2018.

[16] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, “Efficient quantum-based security protocols for information sharing and data protection in 5G networks,” *Futur. Gener. Comput. Syst.*, vol. 100, pp. 893–906, 2019, doi: https://doi.org/10.1016/j.future.2019.05.053.

[17] M. S. Hossain and G. Muhammad, “A deep-tree-model-based radio resource distribution for 5G networks,” *IEEE Wirel. Commun.*, vol. 27, no. 1, pp. 62–67, 2020.

[18] J. Lansky *et al.*, “A Survey and Classification of the Misuse-Based Intrusion Detection Systems with Deep Learning Techniques,” *IEEE Access*, 2021.

[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A survey of deep learning methods for cyber security,” *Information*, vol. 10, no. 4, p. 122, 2019.

[20] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, “A self-adaptive deep learning-based system for anomaly detection in 5G networks,” *IEEE Access*, vol. 6, pp. 7700–7712,

2018.

[21] X. Xu, D. Li, Z. Dai, S. Li, and X. Chen, “A heuristic offloading method for deep learning edge services in 5G networks,” *IEEE Access*, vol. 7, pp. 67734–67744, 2019.

[22] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, “A Secure Federated Learning Framework for 5G Networks,” *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 24–31, 2020, doi: 10.1109/MWC.01.1900525.

[23] E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, “Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review,” *Dev. Adv. Def. Secur.*, pp. 51–64, 2020.

[24] É. Salguero Dorokhin, W. Fuertes, and E. Lascano, “On the development of an optimal structure of tree parity machine for the establishment of a cryptographic key,” *Secur. Commun. Networks*, vol. 2019, 2019.

[25] W. Fuertes, F. Meneses, L. Hidalgo, and J. Torres, “RSA OVER-ENCRYPTION IMPLEMENTATION FOR NETWORKING: A PROOF OF CONCEPT USING MOBILE DEVICES.”

[26] Á. A. Royo, M. S. Rubio, W. Fuertes, M. C. Cuervo, C. A. Estrada, and T. Toulkeridis, “Malware Security Evasion Techniques: An Original Keylogger Implementation BT - Trends and Applications in Information Systems and Technologies,” 2021, pp. 375–384.

[27] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, *Deep learning*, vol. 1, no. 2. MIT press Cambridge, 2016.

[28] C. González, “Desaf{\'\i}os de Seguridad en Redes 5G,” *Technol. Insid. by CPIC*, vol. 3, pp. 36–45, 2019.

[29] M. H. Abidi *et al.*, “Optimal 5G network slicing using machine learning and deep learning concepts,” *Comput. Stand. \& Interfaces*, vol. 76, p. 103518, 2021.

[30] W. Fuertes, “An emulation of VoD services using virtual network environments,” *Electron. Commun. EASST*, vol. 17, 2009.

[31] K. Hara, D. Saito, and H. Shouno, “Analysis of function of rectified linear unit used in deep learning,” in *2015 international joint conference on neural networks (IJCNN)*, 2015, pp. 1–8.

[32] P. Zambrano *et al.*, “Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach,” *IEEE Access*, vol. 7, pp. 142129–142146, 2019.

[33] P. Codara, G. Maurina, and D. Valota, “Computing Duals of Finite Gödel Algebras,” in *2020 15th Conference on Computer Science and Information Systems (FedCSIS)*, 2020, pp. 31–34.

[34] P. Singh, P. Pawar, and A. Trivedi, “Physical layer security approaches in 5G wireless communication networks,” in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 477–482.

[35] A. Di Nola, R. Grigolia, and G. Vitale, “On the variety of Gödel MV-algebras,” *Soft Comput.*, vol. 23, no. 24, pp. 12929–12935, 2019.

[36] L. A. Nguyen and D. X. Tran, “Computing fuzzy bisimulations for fuzzy structures under the Gödel semantics,” *IEEE Trans. Fuzzy Syst.*, 2020.