5G Core Security in Edge Networks: A Vulnerability Assessment Approach

Hisham A. Kholidy
Department of Networks and Computer Security, College of Engineering, SUNY Polytechnic Institute, Utica, USA.
kholidh@sunypoly.edu.

Andrew Karam
The Air Force Research Laboratory (AFRL), Rome, USA
andrew.karam@us.af.mil

James L. Sidoran
The Air Force Research Laboratory (AFRL), Rome, USA
james.sidoran@us.af.mil

Mohammad A. Rahman
Dept of Electrical and Computer Engineering, Florida International University
marahman@fiu.edu

***Abstract*—The 5G technology will play a crucial role in global economic growth through numerous industrial developments. However, it is essential to ensure the security of these developed systems, while 5G brings unique security challenges. This paper contributes explicitly to the need for an effective Vulnerability Assessment Approach (VAA) to identify and assess the vulnerabilities in 5G networks in an accurate, salable, and dynamic way. The proposed approach develops an optimized mechanism based on the Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS) to analyze the vulnerabilities in 5G Edge networks from the attacker perspective while considering the dynamic and scalable Edge properties. Furthermore, we introduce a cloud-based 5G Edge security testbed to test and evaluate the accuracy, scalability, and performance of the proposed VAA.**

***Keywords*—vulnerability analysis, 5G Edge security, 5G attack vector, 5G security testbed, 5G attack graphs.**

I. Introduction.

As the world prepares for the first debut of 5G cellular networks, many researchers started to focus on the security challenges that the new standard will face. A 5G network would dramatically improve military communication and situational awareness. Currently, The Department of Defense (DOD) is developing a secure 5G mobile telecommunication network strategy to address malicious activities against the 5G systems.[1] While the launch of 5G is poised to provide the DoD with a wide range of weaponry, detection, and data transfer opportunities, it also brings some security risks that will need to be addressed soon. Well known 5G equipment manufacturers, such as Ericsson [2], Cisco [3], and Huawei [4, 5] and other states of the art studies [6] stressed that it is essential to ensure that any security controls deployed at the 5G edge networks (e.g., vulnerability assessment, risk mitigation, access control policy at edge nodes) should minimally impact latency and bandwidth usage and be flexible, dynamic, and scalable.

The 5G Edge network refers to the 5G networks that are built on innovations in cloud virtualization, Network Functions Virtualization (NFV) [7], network slicing [7], and Software-Defined Networking (SDN) [7]. This architecture makes the 5G Edge network more dynamic and flexible while providing dynamic network slicing that is vital for 5G services. However, distributing the computation and data in different network nodes introduces new security challenges associated with scale and distribution. The 5G Edge network inherits the security issues related to these abovementioned technologies besides some specific vulnerabilities associated with the nature of the edge computing such as the edge applications' vulnerabilities, the network perimeter, IoT devices, and 5G UE at the network edge [7]. The US National Telecommunications and Information Administration (NTIA) developed the national strategy to secure 5G that expands on how the US Government will secure 5G infrastructure domestically and abroad [8]. This strategy establishes four lines of effort among them [8]: (1) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (2) promoting the responsible deployment of secure and reliable 5G infrastructure. In alignment with these two lines of effort, we develop:

(i) a Vulnerability Assessment Approach (VAA) to (1) analyze the vulnerabilities in the 5G core components (i.e., SDN, NFV, and cloud Edge servers) and User Equipment (UE) from the attacker perspective especially with regard to the dynamic, low latency, and scalable properties of the 5G networks, (2) generate attack graphs based on the 5G attack vector, and (3) quantify the security level of the network and attack cost by deriving each node's minimal effort. The VAA uses the TOPSIS [9, 10] to compute the shortest attack path by selecting the lowest attacker cost of actions that denotes the lowest attacker efforts to exploit a certain vulnerability. Such shortest paths can reduce the cardinality exponential growth of the system security state space that usually causes the state space explosion problem when applying a mitigation action in large-scale systems like 5G Edge networks. To the best of our knowledge, none of the current works introduces a real-time vulnerability assessment framework that specifically works for 5G Edge networks and considers these systems' real-time scalability and dynamic features due to the lack of publicly available 5G Edge testbeds, datasets, and attack graphs.

(ii) A cloud-based 5G security testbed to test and evaluate the accuracy, scalability, and performance of the proposed VAA. The testbed also allows us to build a 5G threat model and attack graphs that are required to evaluate the VAA. We make this testbed in the light of other states of the art such as 5G Playground [11], Cisco [3], and AWS [12].

The remainder of this paper is organized as follows. Section II presents the problem statement and related work. Section III describes the 5G Edge attack vectors and scenarios. Section IV introduces the new 5G Edge security testbed. Section V introduces the VAA. Section VI introduces a case study that evaluates the VAA. Section VII compares the accuracy and performance of the VAA with the Nessus [33]. Finally, Section VIII draws some concluding remarks and outlines future work.

II. Problem Statement and Related Work

Most of the current state of the art [34-39] focus on either the SDN or NFV security and do not consider the 5G Edge challenges such as (1) performance monitoring, (2) scalability, (3) orchestration and management, and (4) heterogeneous network support and integration of the SDN, NFV, and edge computing. Few works study the vulnerability analysis and risk assessment in 5G Networks. However, they are still at an early stage. Current traditional risk assessment and vulnerability analysis approaches that are based on ISO/IEC 2700 series [40] and NIST-SP800 [41] do not take into account the 5G Edge design principles. In [42], the authors introduced an intrusion prevention system that employed five layers of 5G systems to detect the flow table overloading attack. However, this work is more specific to a particular attack category and does not consider the rest of the 5G attack vectors. Furthermore, it lacks the vulnerability analysis of the 5G core components.

III. The 5G Edge Attack Vector

The attack surface of the 5G edge network is very big, see Fig.1. From our analysis, besides the traditional network, IoT, and cloud attack surfaces that are inherited to the 5G networks, there are additional attacks enabled by the integration of mobile Edge computing (MEC) and 5G networks, as depicted in Fig. 2, namely: 1- *(I): Insecure mobile backhaul network.* Data exchanged between MEC nodes often traverse insecure shared backhaul that is vulnerable to MITM attacks, including eavesdropping and spoofing. Such attacks can also come from edge nodes connected to the public internet through the edge Firewall Interfaces (e.g., SGi/N6). 2- *(S): Shared infrastructure with third-party applications.* MEC nodes can be opened to allow authorized participants to deploy applications/services to other users. However, poorly designed applications can create opportunities for attackers to invade the system and pose threats to the network applications running on the platform. *3- (P): Privacy leakage illegitimate access to the Multi-access MEC system.* In this case, an attacker can compromise the service infrastructure and the network hampering information privacy, and access the information stored at the edge system's upper layers that in turn poses a serious concern for privacy leakage. In this paper, we mainly target these attacks using the VAA.

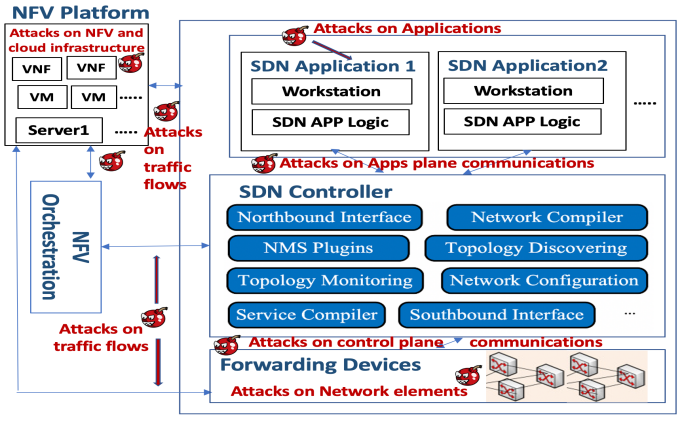

Fig. 1: Attack surfaces of the 5G Edge Network

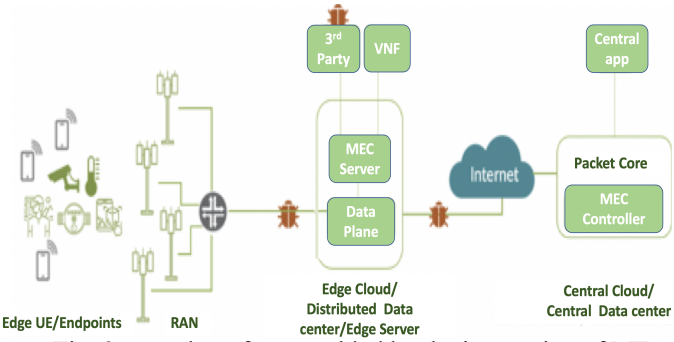

Fig. 2: Attack surfaces enabled by the integration of MEC

IV. The New 5G Edge Security Testbed and the Scalable Deployment of the Security Framework.

To consider the 5G characteristics, we introduce a hierarchical, scalable, robust, and flexible deployment architecture for our Autonomous Security Management Framework (ASMF) [13-29] see Fig. 3. In 5G Edge Networks, UE (e.g. mobile devices) at the edge of a coverage area, or the area where the signal strength of the base station and a Small Cell Access (SCA) point is very low, are connected to a relay which in turn is connected to a Base Station (BS) through SCA. Two or more devices at the relay also establish a direct connection link between each other. In the proposed testbed, the nodes, SCA, relay, and base stations are virtually deployed using the Open5GCore toolkit [4]. Each node/device/user equipment has a Mobile Agent IDS(MA-IDS) deployed to analyze system logs and forwards security alerts to the corresponding dedicated pre-processing server. Each of these servers has a dedicated Network IDS (NIDS) to analyze the network traffic. The pre-processing servers run the collection, normalization, integration, and correlation for the alerts forwarded through the relays, SCAs, and/or BS. After that, these servers forward the final correlated alerts to the risk assessment server. In this deployment, we have *m* slices correspond to m BSs. Each slice has n risk assessment servers and *n* SCA Security Servers (S3s) for risk mitigation.

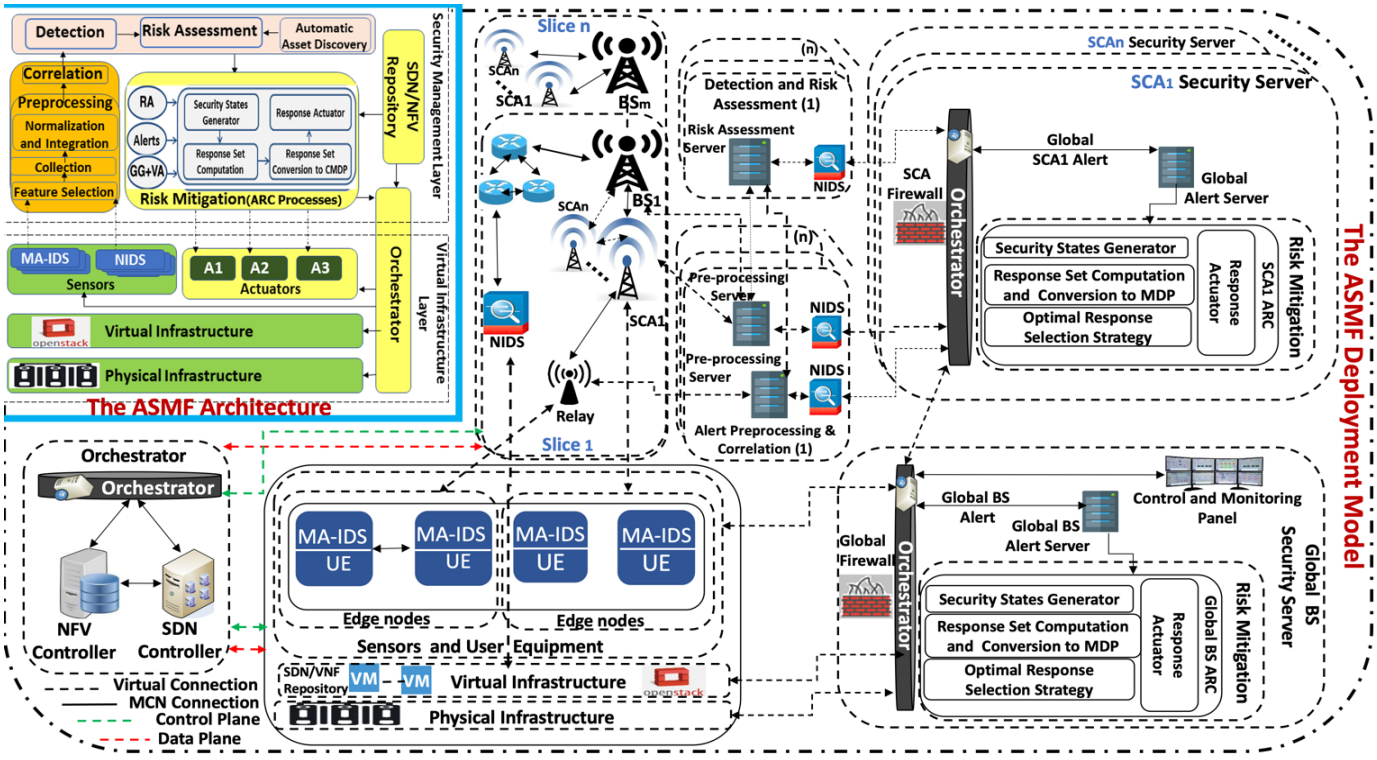

Fig. 3: The Proposed 5G Edge security testbed and the ASMF Architecture.

The risk assessment server assesses the risks based on all correlated alerts that are received from relays, SCAs, and/or BS. The correlated alerts and risk alert information produced by the VAA are forwarded to a Global BS Security Server (GBSS) which is located at each slice of the deployment. After that, each S3 applies a response against the ongoing attacks in its substation network. S3 forwards log information to the GBSS only if it can mitigate the attacks, otherwise, a response strategy is computed by the GBSS's ARC and applied to those substations where the S3 was not able to mitigate the attacks. The response strategy applied by the ARC of the GBSS is of two types, a manual action applied by the 5G administrator, or an automated action against multi-stage attacks requiring that each S3 correlates the alerts signaled from several substations in the 5G. This hierarchical deployment (1) enables ASMF to distribute the security analysis processes at several locations in the large 5G, (2) enables scalability, computationally efficient, and has low latency, (3) reduces the detection time and enables faster training, (4) helps to manage the information generated by every single S3 which in turn helps to identify the region from where an event started. This in turn is a very important contributing factor to provide a resilient and secure 5G system, and (5) helps in detecting multi-stage or compound attacks such as the DDoS attacks by correlating and integrating the alerts signaled from several locations in the 5G network. (b) The second challenge is that 5G architecture requests a clear separation between data and control planes and dynamic/customizable control of the mobile network operations. To tackle this issue, we will orchestrate the network slicing [7] in 5G networks to achieve the security requirements. We will use the SDN and NFV technologies for virtualizing the physical infrastructure and controlling network operations. For each slice, SDN provides a separation between the network control and data planes, as the red and green lines in Fig.3 indicate. We propose a Four-Functional Layered architecture to deploy the ASMF. The first layer is a virtual infrastructure layer that provides the abstraction of different hardware/software elements running in the 5G infrastructure and enables the monitoring of low-level metrics related to the network behavior/status using the IDS sensors. The second layer runs the alerts pre-processing operations (i.e., collection, normalization, integration, and correlation). The third layer runs the detection and risk assessment processes, and the fourth layer runs the mitigation process and includes the actuator components.

V. The New Vulnerability Analysis Approach (VAA).

The VAA develops (1) a scalable attack Graph Generator (GG) model. (2) A new dynamic Vulnerability Analysis (VA) model that hierarchically analyzes the generated attack graphs using the TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) [9, 10] to model the multiple criteria decision-making problem in the 5G Edge dynamic environment. TOPSIS is based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution. Ideal solutions in the current context refer to the lowest attacker cost of actions that denotes the lowest attacker efforts to exploit a certain vulnerability. E.g., in Fig. 4, if the computed TOPSIS cost of exploitation of CVE2004-0417 is lower than CVE2002-0392 and CVE2004-0415, this means if the attacker started exploiting CVE2004-0417 rather than the other vulnerabilities this will be considered a positive ideal solution. The following steps summarize the VA approach.

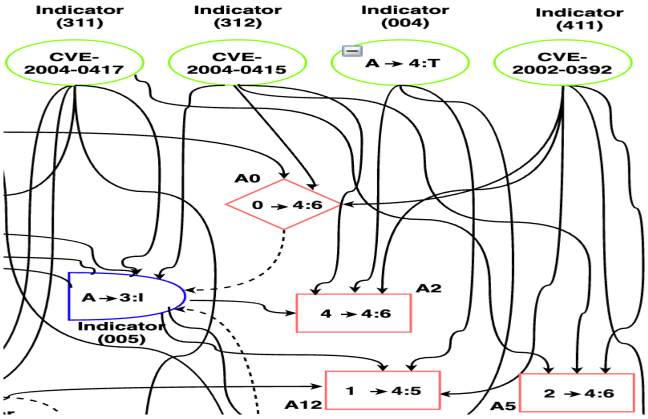

Fig. 4: Part of an example of the generated attack Graph

Step 1: Develop a scalable attack Graph Generator (GG) model. This model is based on the security attack vector that focuses on the attacks and threats that may harvest intelligence from the 5G network resources, states, and flows as a result of the integration of the NFV and SDN. The basic idea underlying this model is that the attacker action cost is under the constraint of certain vulnerability and network dynamic factors/indicators of the 5G network such as latency, accessibility, and other factors described in [30]. The vulnerability factors refer to the Common Vulnerability Scoring System (CVSS) factors/indicators namely Base, Temporal, and Environmental. Each of these factors composites of other several factors described in [31]. We model this problem as a multi-objective decision-making problem as follows.

(1) Create the GG three-layer hierarchical model based on the vulnerability and dynamic network factors, see Fig. 5. The attack graph is modeled based on these factors. An attack graph is defined as a tuple $G = (A, S, T)$, where A is a set of attack actions, S is a set of system states, T is a set of targets that the attacker tries to achieve. An attack graph GG consists of a set of nodes of four types, see Fig.4: (1) attack-step nodes (circular-shaped AND-nodes). Each node in this set represents a single attack step that can be carried out when all the predecessors (preconditions to the attack which are either configuration settings or network privileges) are satisfied. (2) Privilege nodes (diamond-shaped nodes). Each node in this set represents a single network privilege. The privilege can be achieved through any one of its predecessor AND node which represents an attack step leading to the privilege. Each node in this set represents a fact about the current network configuration that contributes to one or more attack possibilities (subaction). (3) Configuration nodes (circular-shaped). Each node in this set represents an initial vulnerability, configuration settings, or network privileges that are known to be true and have no variance in probability. (4) Final step nodes (rectangular-shaped). Each node in this set represents a final exploit action against a certain vulnerability.

(2) Construct a pair-wise evaluation matrix *M*, see Fig. 6, based on the attack graph. After that, we compute the combinatorial weights (W^i) which refer to the weight of the impact of each layer's dynamic factors, in the GG three-layer model, on the attacker decision as given in Eq.1.

$W^i = (W_j^{iL})_{j=1\to n} W^L$ ……………………..….(1)

Where i is the GG hierarchical layer index ∈ {1,2,3}, j refers to the dynamic factors, and W^L is the criteria layer combinational weight vector which is computed as given in Eq.2.

$W^L = M * W$……………………………….....(2)

Where, W is the relevant normalized characteristic vector/eigenvector = $\lambda_{max} * W$, *for all* $w = (w_1, w_2, w_3, \ldots w_n)$. λ_{max} *is the largest* eigenvalue of matrix *M*.

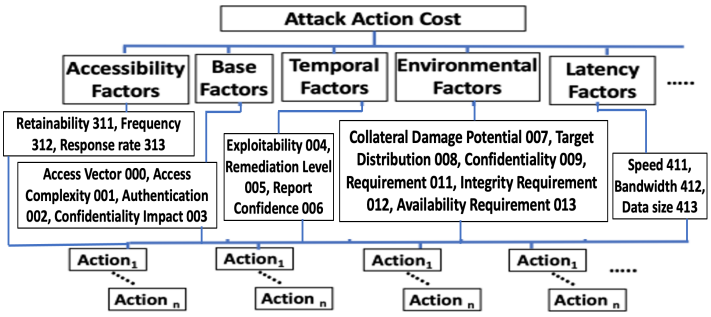

Fig. 5: The Hierarchical GG with corresponding factors' codes

$$(\boldsymbol{M})_{n\times n}=\begin{bmatrix} 1 & a_{12}\cdots & a_{1n} \\ a_{21} & 1 \ \cdots & a_{2n} \\ \cdots & \cdots \ \ \cdots & \cdots \\ a_{n1} & a_{n2} \ \ \cdots & 1 \end{bmatrix}$$

Fig. 6: The *M* pair-wise Matrix

Step2: Develop the new dynamic Vulnerability Analysis (VA) model. To compute the attack cost of actions, we will apply the TOPSIS approach as follows.

(1) Normalize the pair-wise decision matrix *M* to form the normalized decision matrix *N* as given in Eq.3.

$N_{ij} = (N_{ij})_{m\times n}$ ……..……..……..(3)

Where, $N_{ij} = \frac{M_{ij}}{\sqrt{\sum_{j=1}^{n} M_{ij}^2}}$, $i= 1,2,\ldots,m, j = 1,2,\ldots n$

(2) Calculate the weighted normalized decision matrix and the best and worth alternatives.

The weighted normalized decision matrix $D = N\times W$. *The best alternative* E^+ *and the worst alternative* E^- *are defines in* Eq. 4 and 5 respectively**.**

$E^+ = (E^+_1, E^+_2, E^+_3, \ldots\ldots, E^+_n)$ ……..……..……...(4)

$E^- = (E^-_1, E^-_2, E^-_3, \ldots\ldots, E^-_n)$ ……..……...……(5)

Let's define the benefit criteria as B and the cost criteria as C. The value of E+ and E- can be calculated using Eq. 6 and 7 respectively.

$e_i^+ = [\, MAX\,(d_{b,c}) \mid i \in B],\ [\, MIN(d_{b,c}) \mid i \in C\,]$ ……..(6)

$e_i^- = [\, MIN\,(d_{b,c}) \mid i \in B],\ [\, MAX(d_{b,c}) \mid i \in C\,]$ ……..(7)

(3) Calculate the cost of the attacker's actions. We use the L2-distance defined by the TOPSIS approach to calculate $L2_i^+$, the distance between the target alternative *i* and the best condition E^+ as given in Eq. 8, and $L2_i^-$, the distance between the target alternative *i* and the worst condition E^- as given in Eq. 9.

$L2_i^+ = \sqrt{\sum_{k=1}^{n}(e_{i,k} - e_k^+)^2}$ ……..…… (8)

$L2_i^- = \sqrt{\sum_{k=1}^{n}(e_{i,k} - e_k^-)^2}$ …….…… (9)

Based on the $L2_i^+$ and $L2_i^-$ distances, we compute the similarity to the worst condition as the cost of the attacker's actions (Atc_{Cost}) as shown in Eq.10.

$Atc_{Cost}(i) = \frac{L2_i^+}{L2_i^+ + L2_i^-}$ ……..(10)

Where $i \in \{1,2\ldots,m\}$ is the actions the attacker can choose from *m* possible actions. Using the attack graph in Fig. 4, we give a simple demonstration for the decision matrix of attacker actions compared to the network indicators (the network components where the attacker may start its exploitation), see Table. 1. The full case study of this example is detailed in Section 6. The computed attack graphs, actions, and the costs of these actions can be used by an intrusion response system to model the security reciprocal interaction between it and the attacker and can help in deploying the best countermeasures to mitigate the attacks in the 5G edge networks.

Table 1: Attacker Decision Matrix

Attacker Goal	Exploitation Starting Point		
	CVE-2004-0417	CVE-2004-0415	CVE-2002-0392
I: disruption for NFVI Services	A5	A5	A5
S: illegitimate access to Shared SDN	A12	A0-A12, A12,	A12
P: illegitimate access to the RAN	A2	A0-A2, A2	A2

VI. Performance and Accuracy Evaluation: Case Study

To evaluate VAA, we provide a 5G edge case based on the 3GPP architecture in Fig. 7 that is deployed in our testbed. This architecture is based on the concepts of control and user planes split, service base architecture, and network slicing. Their main network functionalities are the Network Slice Selection Function (NSSF), the Authentication Server Function (AUSF), the Unified Data Management (UDM), the Access and Mobility Management Function (AMF), the Session Management Function (SMF), the Policy Control Function (PCF), the Application Function (AF), the User Equipment (UE), the Radio Access Network (RAN), the User Plane Function (UPF), and the Data Network (DN). A two-level SDN controllers hierarchy bridges between the functions of the control and user planes, specifically, between the SMFs and the UPFs. The 5G core NFs are implemented as VNFs in an NFVI in which the SDN Controllers are virtualized and implemented. Fig. 8 shows the exploited assets in this case study.

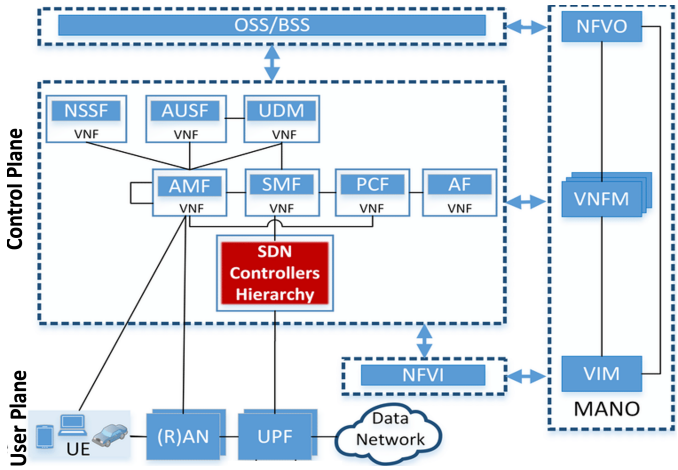

Fig.7: The 5G Edge-based 3GPP planes in our testbed.

Using the Metasploit framework [43], we run some exploits based on the 5G Edge attack vector described in Section 3. These exploits target 6 vulnerabilities in the testbed namely, the CVE-2019-15083 (allows for an XSS injection that leads to control what software is installed on the admin workstation), CVE-2013-0375(allows for remote injection of SQL code that leads to bypassing the AUSF), CVE-2019-16026 (leads to a denial of service (DoS) condition on the AMF), CVE-2004-0415 (allows for illegitimate access to portions of kernel memory that leads to illegitimate access to the SDN), CVE-2002-0392 (allows for remote execution of DoS attack that leads to disruption for the NFVI functionalities), CVE-2004-0417 (allows for an integer overflow in the CVS Apps that leads to illegitimate access to the RAN). Fig. 9 shows the attack graph that was created using the aforementioned approach described in Section 5. The main target of the attacker is to access and control the RAN module using the aforementioned vulnerabilities that belongs to the three attack categories described in section 3 (i.e., *I, S, P*).

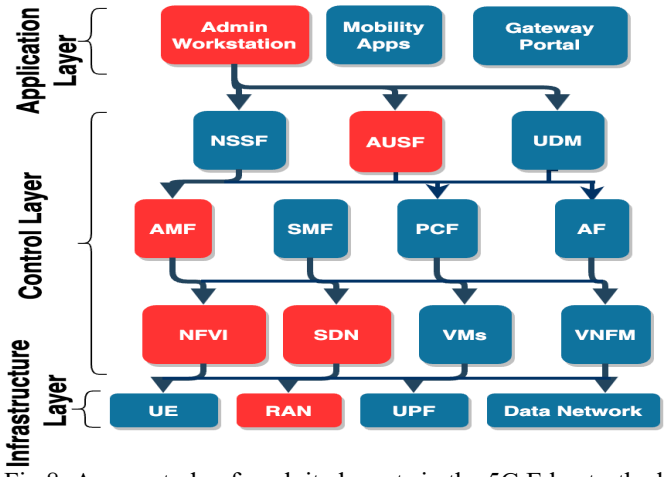

Fig.8: A case study of exploited assets in the 5G Edge testbed

Tables 2 shows an example of the pair-wise evaluation matrix *M* of the criteria layer (vulnerability factors) and the indicator layer (network dynamic factors).

Using Matrix *M*, we compute the Atc_{Cost} for each possible path of actions according to E.q 10. We then choose the lowest attacker efforts in three attacking schemes (i.e., I, S, P). As Table 3 debicts the lowest cost is achieved when the attacker exploits the CVE-2004-0417 first. Although the long attacking path increases the attacker's cost, it also enables the attacker to consider more vulnerability and network dynamic factors that in turn reduce the attacker's overall cost. Such long paths reduce the $L2_i^+$ and increase the $L2_i^-$, which in turn reduces the Atc_{Cost}, see Equations 8, 9, and 10. Fig. 10 shows the attack costs for all possible paths of the three attacking schemes (i.e., I, S, P).

Table 2: Pair-wise evaluation matrix of the criteria layer

	001	***002***	***003***	***004***	***005***	***006***	***007***	***008***	***009***	***011***	***012***	....
001	1	3	2	1/8	1/9	1/7	1/4	1/6	1/7	2	1/4	....
002	1/7	1	3	2	1	1/5	1/3	1/9	2	1/6	1/5	....
003	1/8	1/9	1	1/3	1/2	1/3	1/7	3	1/2	1/4	2	....
004	1/8	1/9	1/2	1	1/8	1/3	1/4	2	1/5	1/3	1/4	....
005	3	1/3	1/6	1/5	1	1/5	1/3	1/5	1/6	1/6	1/9	....
006	1/2	1/7	2	1/3	1/2	1	1/7	3	1/2	1/9	1/3	....
007	1/6	½	1/7	2	1/3	1/5	1	1/6	1/8	1/7	1/7	....
008	1/2	4	1/2	2	1/7	1/3	1/6	1	3	1/5	4	....
009	1/6	1/5	3	1/6	1/4	1/6	1/3	1/5	1	1/3	4	....
011	3	1	1/6	1/9	2	1/2	1/7	1/3	1/5	1	1/3	....
012	1/5	1/9	1/6	1/7	1	1/8	2	1/7	1/3	2	1	....
....	....	....	....	....	....	....	....	....	....	....	....	....

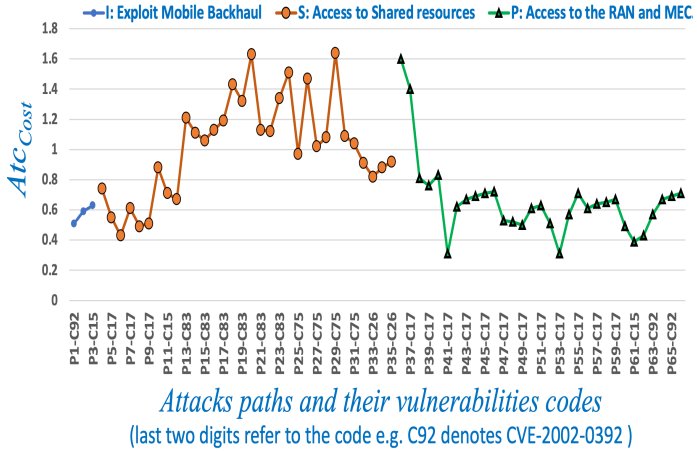

Fig.10: The I, S, and P attack costs and paths.

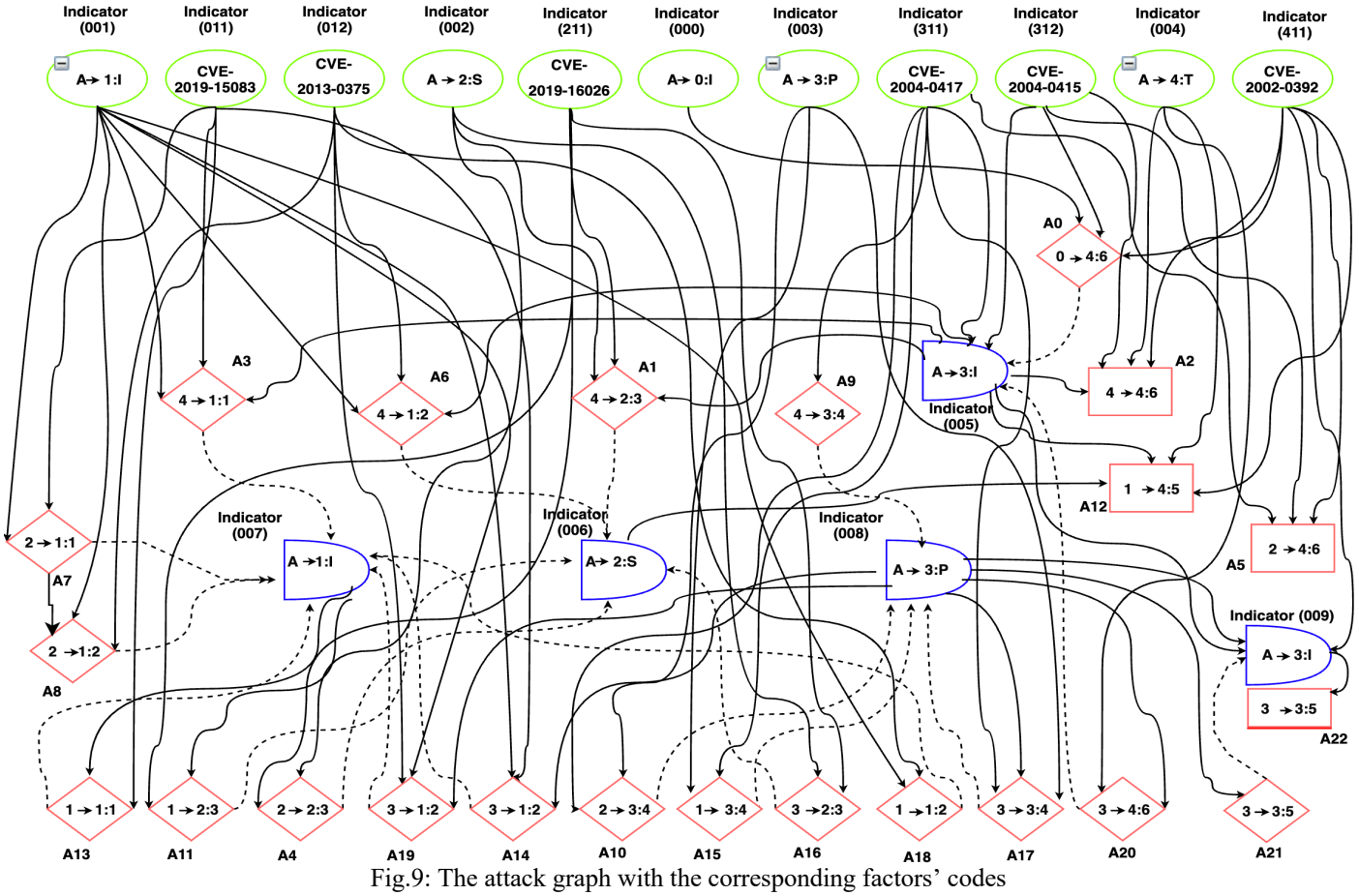

Fig.9: The attack graph with the corresponding factors' codes

Table 3: Attacker cost in three attacking schemes (I, S, P).

Attacker Goal	Exploitation Starting Point. Action paths with the lowest costs are underlined.						
		CVE-2004-0417	**CVE-2004-0415**	**CVE-2002-0392**	**CVE-2019-15083**	**CVE-2013-0375**	**CVE-2019-16026**
	I: Exploit mobile backhaul network.	**5**. Atc_{Cost}= 0.63	**5**. Atc_{Cost}= 0.51	**5**. Atc_{Cost}= 0.59	-	-	-
	***S:* Access to Shared resources**	12, 10-17-20-12, **9-17-20-12**, 9-20-12, 15-17-20-12, 15-20-12. Atc_{Cost}= 0.43	0-12, **12**. Atc_{Cost}= 0.71	**12**. Atc_{Cost}= 0.67	3-13-11-12, 3-11-12,**3-4-12**, 3-13-4-12, 7-8-4-12, 7-11-12, 7-4-12, 8-4-12, 8-11-12, 14-4-12, 14-11-12. Atc_{Cost}=1.06	8-12, **8-4-12**, 8-11-12, 19-11-12, 19-4-12, 6-12, 18-4-12, 18-11-12. Atc_{Cost}= 0.97	11-12, **4-12**, 1-12, 16-12 Atc_{Cost}= 0.82
	***P:* Access to the RAN and MEC.**	2, 22, 10-17-20-22, 10-17-21-22, 10-17-20-2, **10-17-22**, 9-17-20-2, 9-17-20-22, 9-17-21-22, 9-17-22, 9-22, 9-20-2, 9-20-12, 9-20-22, 9-21-22, 15-17-20-2, 15-17-20-22, **15-17-21-22**, 15-17-22, 15-22, 15-20-2, 15-20-12, 15-20-22, 15-21-22. Atc_{Cost}= 0.31	0-2, **2**, 0-22. Atc_{Cost}= 0.39	**2**, 22, 0-2, 0-22. Atc_{Cost}= 0.57	-	-	-

VII. Compare the accuracy and performance of the VAA with the Nessus.

The underlying idea behind the VEA-bility metric is that the security of a network is influenced by many factors, including the severity of existing vulnerabilities, distribution of services, connectivity of hosts, and possible attack paths. These factors are modeled into three network dimensions: Vulnerability, Exploitability, and Attackability. The overall VEA-bility score, a numeric value in the range [0,10], is a function of these three dimensions, where a lower value implies better security. The VEA-bility metric uses data from three sources: the 5G Edge testbed topology, attack graphs, and scores as assigned by the Common Vulnerability Scoring System (CVSS) [31]. To adjust the VEA-bility metric to validate the accuracy of the vulnerability assessment of the VAA and Nessus, we modify this metric by replacing the asset Attackability factor with the $Atc_{Cost}(i)$ value at Eq. 10 for each set of actions *i*. We let each vulnerability *v,* that corresponds to a set of actions *i*, have an impact score, exploitability score, and temporal score as defined by the CVSS. An impact and exploitability subscores are automatically generated for each common vulnerabilities identifier based on its CVE name defined by the CVSS, whereas the temporal score requires user input. We then define the severity, *S*, of a vulnerability to be the average of the impact and temporal scores, Eq. (11):

$$S(v) = (Impact\ Score(v) + Temporal\ Score(v)) / 2 \quad (11)$$

The Vulnerability score (*V*) of a 5G Edge testbed asset, e.g., UE, MEC server, SDN, NFV,…etc is an exponential average of the severity scores of the vulnerabilities on the 5G Edge asset, or 10, whichever is lower. The asset Exploitability score (*E*) is the exponential average of the exploitability score for all asset vulnerabilities multiplied by the ratio of network services on the asset. The asset Attackability score (*A*) refers to the toral CP values for all vulnerabilities at a certain asset. The Attackability score is multiplied by a factor of 10 to produce a number in the range [0,10], ensuring that all dimensions have the same range. For an asset, *a*, let *v* be an asset vulnerability. We then define the three asset dimensions as shown in Eq. 12, Eq. 13. and Eq.14:

$$V(a) = min(10, ln \sum e^{S(v)}) \quad (12)$$

$$E(a) = (min(10, ln \sum e^{Exploitability\ Score(v)})) (\#\ services\ on\ a)/(\#\ network\ services) \quad (13)$$

$$A(t) = (10) * \sum_{i=1}^{n} a_{CP(e_i)} \quad (14)$$

The overall VEA-bility equation for an asset *a is* then computed as in Eq. (15).

$$VEA\text{-}bility_a = 10 - ((V+E+A)_a / 3) \quad (15)$$

To test the performance of the proposed VEA-bility metric for both the VAA and Nessus, we developed an extensive set of scenarios described in sections 3 and 6 and used the vulnerabilities observed by the Nessus scan [33] and our VAA results after running the attacks scenarios. Fig. 11 shows the overall average VEA-bility scores observed in our experiments for the 5G Edge testbed assets. A higher score indicates a more secure configuration, which we call more "VEA-ble". Fig. 11 shows that the VAA, on average, is 9.53% more VEA-ble than Nessus.

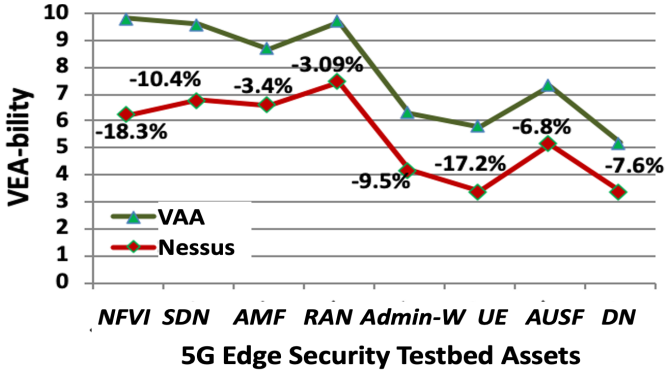

Fig. 11: The VEA-bility metric of the VAA and the Nessus.

To compare the performance of the VAA and Nessus, we run the experiment based on the above-mentioned 6 vulnerabilities. Fig. 12 shows the performance of the VAA and Nessus in milliseconds. The VAA, on average, outperforms Nessus by 37.29%, it takes 6151ms to compute the cost related to all possible paths of the 6 vulnerabilities while Nessus takes 8445ms to assess the same 6 vulnerabilities. This shows that our VAA introduces a more scalable and faster assessment.

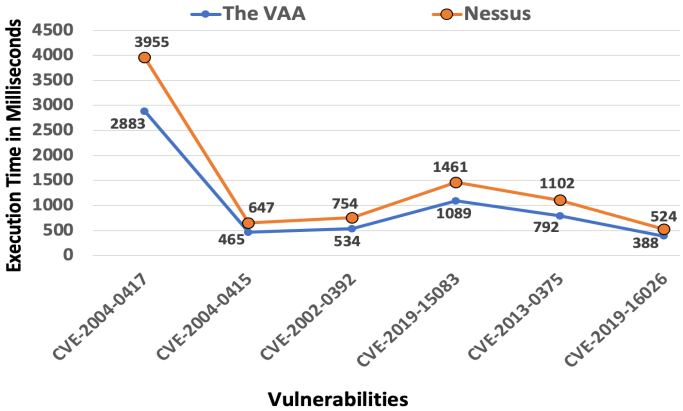

Fig.12: Execution time of the VAA and Nessus

VIII. CONCLUSION AND FUTURE WORK

The 5G system improves the bandwidth and capabilities of the current telecommunication infrastructure. However, it

introduces new threats and attacks. In this paper, we introduced a scalable and accurate vulnerability analysis approach that was tested and evaluated using our new developed 5G Edge testbed. The experiment results depict that VAA successfully analyzed the vulnerabilities with a low error rate. The VAA is more VEA-ble than Nessus by 9.53% and outperforms it by 37.29.%. In future work, we will integrate the VAA with an autonomous intrusion response system that considers the vulnerability assessment values of VAA to deploy countermeasures against cyber attacks. Furthermore, we will extend the VAA using a Hexagonal fuzzy method to improve the TOPSIS accuracy.

ACKNOWLEDGMENT

"This research was supported in part by the Air Force Research Laboratory through the Information Directorate's Information Institute® contract number FA8750-20-3-1003".

REFERENCES

[1] "DOD's Secure 5G Mobile Telecommunication Network Strategy", *https://www.defense.gov/explore/story/Article/1844423/dod-develops-secure-5g-mobile-telecommunication-network-strategy/*

[2] K. Norrman, P. Kumar Nakarmi, and E. Fogelstrm. "5g security enabling a trust-worthy 5g system", Ericsson, 2018.

[3] Michael Geller, Pramod Nair, "5G Security Innovation white paper", Cisco Public, 2018.

[4] "Huawei 5G Security White Paper", https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf

[5] "Huawei 5G MEC IP Network", https://carrier.huawei.com/~/media/CNBGV2/download/program/5G-MEC-IP-Network-White-Paper-en-v2.pdf

[6] Rodrigo Roman, Javier Lopez, Masahiro Mambo, Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges, Future Generation Computer Systems, Volume 78, 2018.

[7] Jaikumar Vijayan, "4 ways edge computing changes your threat model," May 2020, Available at https://www.csoonline.com/article/3543191/4-ways-edge-computing-changes-your-threat-model.html

[8] "Potential Threat Vectors to 5G Infrastructure", the US National Telecommunications and Information Administration (NTIA), https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf

[9] Behzadian, M., Khanmohammadi Otaghsara, S., Yazdani, M., & Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. Expert Systems with Applications, 39(17), 13051–13069. doi:10.1016/j.eswa.2012.05.056

[10] Abhishek K., Bikash Sah, Arvind R. Singh, Yan Deng, Xiangning He, Praveen Kumar, Ramesh Bansal, "Chapter 1 - Multicriteria decision-making methodologies and their applications in sustainable energy system/microgrids", Decision Making Applications in Modern Power Systems, 2020, Pages 1-40, ISBN 9780128164457.

[11] Elie Daniel Gheorghe-Pop FOKUS, "5G Ready Testbeds: Enabling Early Prototyping and Experimentation", IEEE 5G and Beyond Testbed Workshop, Toronto, Canada, 24th Sept. 2017

[12] "5G Network Evolution with AWS", July 2020. Amazon Web Services. https://d1.awsstatic.com/whitepapers/5g-network-evolution-with-aws.pdf

[13] Kholidy, H.A., Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cids/

[14] Kholidy, H. A. (2020), "Autonomous mitigation of cyber risks in the Cyber–Physical Systems", doi:10.1016/j.future.2020.09.002, Future Generation Computer Systems,Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002.

[15] Kholidy, H.A., Baiardi, F., Hariri, S., et al.: "A hierarchical cloud intrusion detection system: design and evaluation", Int. J. Cloud Comput., Serv. Archit. (IJCCSA), 2012, 2, pp. 1–24.

[16] Kholidy, H.A., "Autonomous mitigation of cyber risks in the Cyber–Physical Systems", Future Generation Computer Systems, Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002.

[17] Kholidy, H.A., Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607- 016-0495-8, June 2016.

[18] Kholidy, H.A., Abdelkarim Erradi, "A Cost-Aware Model for Risk Mitigation in Cloud Computing SystemsSuccessful accepted in 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[19] Kholidy, H.A., Ali Tekeoglu, Stefano Iannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, "Attacks Detection in SCADA Systems Using an Improved Non-Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), December 19-20, 2017.

[20] Qian Chen, Kholidy, H.A., Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017.

[21] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[22] Kholidy, H. A., & Erradi, A. (2019). VHDRA: A Vertical and Horizontal Intelligent Dataset Reduction Approach for Cyber-Physical Power Aware Intrusion Detection Systems. Security and Communication Networks, 2019, 1–15. doi:10.1155/2019/6816943

[23] Kholidy, H.A., "Detecting impersonation attacks in cloud computing environments using a centric user profiling approach", Future Generation Computer Systems, Volume 115, issue 17, December 13, 2020, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.

[24] Hisham A. Kholidy, "Detecting impersonation attacks in cloud computing environments using a centric user profiling approach", Future Generation Computer Systems, Volume 117, 2021, Pages 299-320, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.009.

[25] Kholidy, Hisham A.: 'Correlation-based sequence alignment models for detecting masquerades in cloud computing', IET Information Security, 2020, 14, (1), p.39-50, DOI: 10.1049/iet-ifs.2019.0409.

[26] H. A. Kholidy, "Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769494.

[27] Kholidy, H.A., Fabrizio Baiardi, Salim Hariri: 'DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks'. The IEEE Transaction on Dependable and Secure Computing, 10.1109/TDSC.2014.2327966, pp:164–178, June 2015.

[28] Kholidy, H.A., Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks ", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cidd/

[29] Nur Haque, Mohammad Rahman, Dong Chen, Hisham Kholidy, "BIoTA: Control-Aware Attack Analytics for Building Internet of Things," in the 18th IEEE International Conference on Sensing, Communication and Networking (SECON), July 2021.

[30] Bräuning, F., & Koopman, S. J. (2019). The dynamic factor network model with an application to international trade. Journal of Econometrics. doi:10.1016/j.jeconom.2019.10.007

[31] https://www.first.org/cvss/specification-document

[32] Tupper M, Zincir-Heywood A (2008) VEA-bility security metric: a network security analysis tool. In: Proc IEEE Third Int'l Conf. Availability, Reliability and Security.

[33] Nessus Vulnerability Scanner: http://www.nessus.org.

[34] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, W. Li, "Secsdn-cloud: Defeating vulnerable attacks through secure software-defined networks", IEEE Access (2018).

[35] D. Yin, L. Zhang, K. Yang, A ddos attack detection and mitigation with software-defined internet of things framework, IEEE Access (2018).

[36] Z. Fan, Y. Xiao, A. Nayak, C. Tan, An improved network security situation assessment approach in software defined networks, Peer-to-Peer Networking and Applications 12 (2) (2019).

[37] V. Varadharajan, K. Karmakar, U. Tupakula, M. Hitchens, A policy-based security architecture for software-defined networks, IEEE Transactions on Information Forensics and Security 14 (4) (2019).

[38] H. Li, F. Wei, H. Hu, Enabling dynamic network access control with anomaly-based ids and sdn, in: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, ACM, 2019, pp. 13–16.

[39] J. Yao, Z. Han, M. Sohail, L. Wang, A robust security architecture for sdn-based 5g networks, Future Internet 11 (4) (2019) 85. 941.

[40] ISO/IEC 27002: Code of Practice for Information Security Management. 2005. http://www.iso.org/iso/catalogue_detail?csnumber=54533

[41] National Institute of Standards and Technology. NIST-SP800 Series Special Publications on Computer Security.

[42] I. Abdulqadder, D. Zou, I. Aziz, B. Yuan, W. Dai, Deployment of robust security scheme in sdn based 5g network over nfv enabled cloud environment, 943 IEEE Transactions on Emerging Topics in Computing.

[43] The Metasploit framework, https://www.metasploit.com/