Defense Mechanism based on Game Theory for Securing Cloud Infrastructure against Co-Resident DoS Attacks

Lee Chen, Zheng Xiang , Bing Pan, Don Chen
Faculty of Computer Science and Information System, Universiti Teknologi MARA (UiTM), Malaysia

ABSTRACT

Evolution in cloud services and infrastructure has been constantly reshaping the way we conduct business and provide services in our day to day lives. Tools and technologies created to improve such cloud services can also be used to impair them. By using generic tools like nmap, hping and wget, one can estimate the placement of virtual machines in a cloud infrastructure with a high likelihood. Moreover, such knowledge and tools can also be used by adversaries to further launch various kinds of attacks. In this paper we focus on one such specific kind of attack, namely a denial of service (DoS), where an attacker congests a bottleneck network channel shared among virtual machines (VMs) co-resident on the same physical node in the cloud infrastructure. We evaluate the behavior of this shared network channel using Click modular router on DETER testbed. We illustrate that game theoretic concepts can be used to model this attack as a two-player game and recommend strategies for defending against such attacks.

KEYWORDS: Cloud computing infrastructure, denial of service (DoS), game theory, cyber security

1.0 INTRODUCTION

As the cloud service providers (CSPs) begin to offer cheaper technology and computing resources to the cyber community, the decision of large and small enterprises to move into the cloud becomes easier. As more of these entities move to the cloud, the utility of conducting such online attacks also increase [1-7]. Recent research shows that by using generic network testing tools, an attacker can successfully identify a target VM on the cloud with a high probability and instantiate VMs co-resident to the target VM to conduct a variety of attacks. In this work, we focus on the possibility of the attacker conducting a denial of service by congesting a network queue shared by all the VMs. We emulate and evaluate the shared queue on DETER testbed and using game theory model this attack scenario as a two player game. The weakness of traditional network security solutions is that they lack a quantitative decision framework. As game theory deals with problems in which multiple players with contradictory objectives compete with each other, it can provide a mathematical framework for modeling and analyzing network security problems [8-15]. As an example, a system administrator (defender) and an attacker can be viewed as two competing players participating in a game. In addition, game theory has the capability of examining large possible scenarios before taking the best action; hence, it can considerably enhance the decision making process of the system administrator. Cloud computing service providers like Amazon‟s EC2 (Elastic Compute Cloud), Microsoft‟s Azure and Rackspace‟s Mosso provide users with the ability to rent computational resources for hosting and offering their services efficiently and cost-effectively to their customers. Users can rent these computational resources in the form of virtual machines (VMs) which run on servers controlled by these providers. We illustrate a game theoretic security model which can be used for defending the virtual machines deployed by such service providers against various kinds of denial of service attacks. As a case study, our model is illustrated using Amazon‟s EC2. Users interested in using Amazon‟s EC2 begin by creating an account and setting up their billing preferences [15-21]. Users can then instantiate their required number of virtual machines for hosting their services and applications. Each of these VMs is called an instance and when instantiated, is deployed on a physical machine. These machines or servers have the ability to run various VMs simultaneously. EC2 uses Xen Hypervisor for virtual machine monitoring, which is the dominant virtual machine (Domain 0) per each physical node and is responsible for system resource allocation to other virtual machines running on that node. The physical machines deployed by EC2 for providing such cloud computing services are distributed geographically at various locations known as regions. Each of these regions further has availability zones which are intended to be isolated from each other in case of failure. When requesting for cloud resources, users can specify the region and availability zone they would like their VMs to be instantiated in [22-29]. They can also specify the instance type of the VMs they are interested in. EC2 currently offers several kinds of instances (e.g. small, large, extra-large, etc.) with varying pricing schemes ranging from approximately $0.10 per hour to $2.60 per hour. These are varied based on the amount of resources (memory, CPU, etc.) they offer in a particular type of instance [30-41].

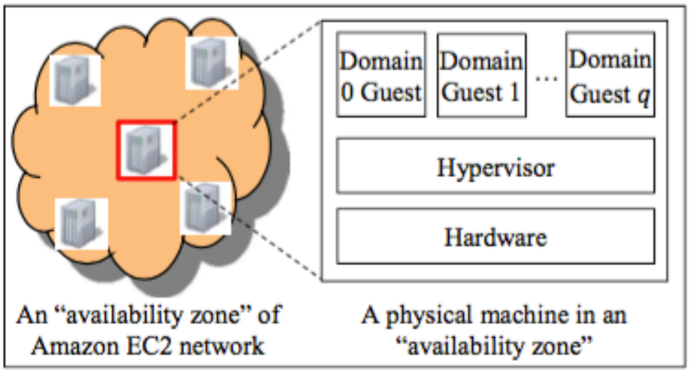
Domain 0 Guest
Domain Guest 1
...
Domain Guest q
Hypervisor
Hardware
An "availability zone" of Amazon EC2 network
A physical machine in an "availability zone"

Figure 1: Illustration of a region and a physical machine in Amazon EC2 network

In Figure 1, the cloud on left depicts an availability zone in Amazon EC2 network. The nodes in the cloud represent physical machines which are used to instantiate new VMs as requested by the users. The layered block diagram on right depicts one such physical machine which can be used to run VMs. The bottom layer represents the hardware resources of the physical machine which are shared among all the VMs. These resources include system hardware like main memory, secondary storage, CPU, network interface cards (NIC), etc [42-48]. The layer above the Hardware layer represents the Hypervisor. The Hypervisor is a virtual machine monitor which provides the instantiated VMs with access to the physical system hardware and also provides isolation among co-resident VMs. Amazon‟s EC2 uses Xen hypervisors. The blocks above the Hypervisor layer represent the various VMs running in the physical machine. The first block "Domain 0" represents a privileged guest VM which is used to manage other guests VMs (domain 1... domain). The domain 0 VM manages the physical resource partitioning of the other guest VMs. In EC2, traffic for all VMs in a physical machine is routed through the Domain 0 VM. In this work we focus on a particular kind of denial of service attack which can take place when malicious VMs co-resident with a victim VM use the shared network channel unfairly such that the victim VM is depleted of network resources. In this work we focus on Xen hypervisor which is used by Amazon‟s EC2 and the shared network channel here is the queue in the NIC installed in the physical machine [49-54].

2.0 LITERATURE REVIEW

Recent work demonstrates how the internal cloud infrastructure of such service providers (they use Amazon‟s EC2) can be mapped and the location of a particular VM can be identified. They further show that new VMs can be instantiated until one is placed co-resident with the victim VM. They explore how such placement can be used to mount cross-VM side-channel attacks or cause denial of service attacks on the victim VM. In this work we focus on the impact of such placement when it is performed by the attacker to launch denial of service attacks on a victim VM and propose a game model to defend against the same. Figure 2 illustrates the network virtualization architecture as implemented by Xen hypervisor [1-17]. We use Amazon‟s EC2 along with this network virtualization architecture of Xen hypervisor to explain the potential denial of service attack and our proposed game model. The Domain 0 VM uses the NIC Driver to interface directly with the network interface card (NIC) of the physical machine to transmit and receive data packets and driver control. The solid arrows in Figure 2 depict transfer of packet data and driver control between the Domain 0 and the NIC. Moreover, all traffic from other guests VMs (Domain Guest 1, Domain Guest 2, and Domain Guest 3) is also routed through Domain 0 (depicted by dashed arrows in Figure 2). All guest VMs commonly share the "transmit and receive queue" (T/R Queue) in the NIC during their data transmissions [18-26].

This T/R Queue is susceptible to potential network congestion which can be exploited by denial of service attacks.

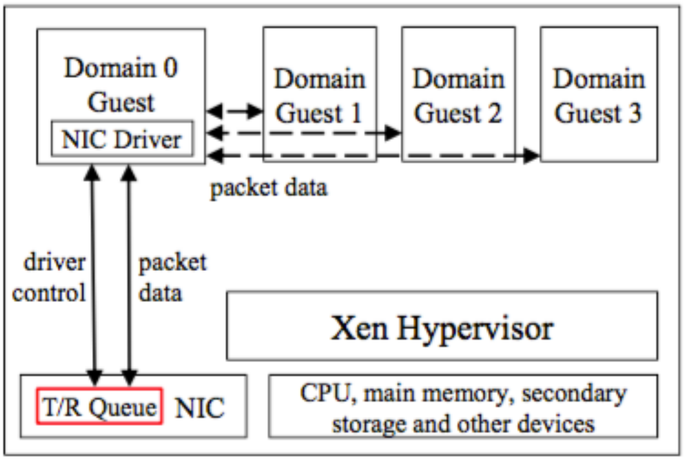

Figure 2: Network virtualization architecture of a physical machine running a Xen hypervisor

An attacker can perform DoS attacks on a victim VM by placing several VM instances as co-resident to the victim VM and then proceed to deplete the available shared network resources. The malicious VMs can send bogus traffic across such shared communication channels such that the victim VM does not get its fair share shared channel space [27-36]. In our case, the shared network channel is the T/R Queue which is present in the NIC of the physical machine which is running on Xen hypervisor. To obtain such VM placements which are co-resident to the victim VM, the attacker begins by enumerating a potential set of target victims. Then by using EC2"s DNS service which provides means to map public IP addresses to private IP addresses, the attacker is able to infer which of these targets belong to a particular availability zone and instance type. Once the availability zone and instance type of a target VM is identified. The attacker rents several VM instances from the cloud service provider (CSP) which can then be instantiated as required. A VM instance depending on the instance type can cost the attacker anywhere from approximately $0.10 per hour (small instance: e.g. EC2"s m1.small) to $0.40 (larger instance: e.g. EC2"s m1.large). The attacker then repeatedly runs probe instances in the target zone and target type until he is successful in placing his VM as co-resident with the target VM. Co-placement can be verified by performing network based co-residence checks (e.g. matching Domain 0 IP address, small packet round-trip times) or by performing cross-VM covert channel communication [37-44]. The more VMs the attacker can rent the more probes he can perform simultaneously and thus the faster he can place one of his VM"s as co-resident with the target VM. Moreover by employing more malicious VMs, the attacker needs to send less bogus traffic per VM over the shared network channel to cause a DoS attack. This also makes it harder for the CSP to identify the attack. However, renting more VM"s has a higher cost to the attacker. Thus there exists a tradeoff for the attacker such that employing more VMs makes his attack easier to implement and execute, however it also becomes more expensive. Thus the attacker"s action set includes, a) identifying the number of VMs to rent from the CSP to conduct the DoS attack and b) deciding the bitrate of bogus traffic to send from each rented VM. The Domain 0 Guest (Dom0), on the other hand aims to handle such by throttling the traffic bitrate of VMs which use more than their fair share of the shared network channel. That is, if a VM tries to use more than their fair share of bandwidth, their traffic would be dropped. In this case, Dom0 uses a firewall that functions based on a threshold value which is used to guide its traffic dropping policies. If the bandwidth used by a VM crosses this threshold value, its traffic is dropped. The use of firewall also incurs a tradeoff. That is, if Dom0 uses a low threshold value then even legitimate VMs will have their traffic dropped. If Dom0 uses a high value, then several malicious VMs may not have their traffic dropped. This would eventually lead to degraded performance for the legitimate VMs. Hence, the action set of the defender includes deciding the optimum threshold for the firewall, so that it can drop maximum bogus traffic from malicious VMs and at the same time not punish legitimate traffic [45-54].

3.0 RESEARCH METHODOLOGY

Our proposed model is based on the following assumptions. The T/R Queue is shared among all guest VMs and is susceptible to congestion. We assume that the amount of time required for packet processing by the NIC is a constant average for each incoming packet. Hence, as per Little‟s law, the queue usage (queue dynamic length) is directly proportional to the incoming traffic rate. A single attacker controls all of the attacking VMs. We assume that the victim VM is a legitimate VM. Traffic from all VMs (legitimate and attacker) use UDP as their transport protocol [1-13]. All traffic per VM is represented as one flow. It should be noted that even if this assumption is not true, i.e. traffic consists of both UDP and TCP flows, our proposed solution will still defend against DoS attacks caused by UDP traffic. There is infinite bandwidth available on the channel between 1) the NIC Driver in Domain 0 and the T/R Queue in NIC and 2) the transmission channels between the Domain 0 and other guest VMs. Moreover, Domain 0 is able to process all of the incoming packets. Dom0 monitors the shared network channel usage among the various VMs co-residing on a single physical machine. Our model would also work if this monitoring functionality was carried out externally by the CSP instead of Dom0. In this case, the game model would be executed by CSP instead of the Dom0 VM. Dom0 has no knowledge of whether the traffic is coming from the attacker or a legitimate VM [14-21]. Its belief on the legitimacy of the traffic decreases with the increase of its bitrate. A packet from traffic from a VM is dropped in either of the two situations: 1) the traffic does not pass the firewall rule, 2) there is congestion in the queue and it overflows. We do not consider the case where an attacker might spoof the source address uniquely for each packet in a single flow. Moreover, spoofing can be avoided by using anti-spoofing methods such as ingress filtering or link-layer security protocols. In the next section we determine the behavior of the shared T/R queue under congestion and verify the same using on DETER. In this work, we assume that the bottleneck T/R queue which is shared among all the VMs co-residing on the same physical machine is generic in nature and employs the widely used drop- tail queue management algorithm. A queue implementing drop- tail mechanism accepts incoming packets as long as it has available space. Once the queue is full, it begins to drop packets at its tail until it has enough space to accept new incoming packets. Queues implementing drop-tail do not identify individual flows and react similarly to each flow during congestion. That is, during congestion packets from each flow are dropped at similar rates. We verify the above behavior of a queue which uses drop-tail algorithm for its management using the publicly available testbed DETER and open source router software Click [22-31].

Figure 2 illustrates the process where co-residing VMs share a common T/R queue among them. To replicate their behaviour on DETER, we setup the following network topology as illustrated in Figure 3. Nodes Source 1, Source 2 and Source 3 emulate the co- resident VMs (Domain Guest 1, Domain Guest 2 and Domain Guest 3) which aim to share a common T/R queue to send and receive data. Switch SW emulates the Domain 0 Guest which forwards the traffic from Domain 1, 2, and 3 to the NIC which houses the T/R queue as shown in Figure 2. On DETER node Gateway emulates the network router which houses the T/R queue which is shared by all VMs and is prone to congestion [32-41]. Node Sink emulates an external machine to which the co-resident VMs send and receive data. These nodes on DETER are connected to each other as shown in Figure 3. Each link has a capacity of 100 Mbits/sec. Node Gateway is machine with dual 3Ghz Intel Xeon processor and 2 GB of RAM. To emulate the behavior of the drop-tail T/R queue which is prone to congestion in node Gateway, we implemented a custom router configuration using Click in kernel level [42-54].

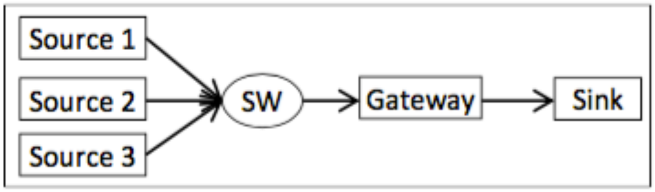

Figure 3: Network topology on DETER

4.0 RESULT

This model extends our prior work in this domain where we defend target system against various kinds of denial of service attacks in different network systems. We model the present attack scenario as a two player zero-sum static game between the attacker which hosts malicious VMs and the defender which maintains the firewall settings for the T/R queue. We begin by profiling the behaviour of a legitimate and malicious VMs followed We define legitimate VMs as the ones which share the common network channel (T/R Queue) fairly with other co-resident VMs. Fairness implies that each legitimate VM controls their traffic bandwidth such they do not exceed their share of the queue usage. We assume that the target VM is a legitimate VM and will not exceed its fair share of the T/R queue. We define malicious VMs as the ones which co-reside with other legitimate VMs on a physical machine and do not share the T/R queue with other VMs fairly. That is, they use more than their fair share of queue in order to induce congestion in the T/R queue and make it drop traffic from the legitimate VMs. In this model, we consider that a single attacker controls all the attacking VM, whose count is denoted by . We define the attack as a distributed denial of service (DDoS) attack when the attacker employs more than one attacking VM and a denial of service (DoS) attack when the attacker employs only one attacking VM. Based on the behavior of the legitimate and malicious VMs defined in the previous section, we design the game model between the attacker and defender with the following actions sets. The attacker"s action set includes a) deciding the number of malicious VMs to use to conduct the attack and b) deciding the bitrate of traffic through each of them to congest the T/R queue. The defender"s action set includes a deciding the firewall threshold value to prevent the T/R queue from congestion from the malicious VMs. The defender, which is the Dom0 VM in our attack scenario, uses a firewall to drop traffic from malicious VMs and at the same time allow traffic from the legitimate VMs. When no defense mechanism is in place, that is, no firewall is installed by Dom0; all traffic is allowed to pass through the T/R queue unrestricted. In this case if , only a percentage of traffic from each VM is allowed by the T/R queue. We denote this percentage by and it is the same for each VM. Thus, if a VM sends bitrate of traffic, only bitrate will pass the queue during congestion. We assume that the queue is shared in a fair and equitable manner and thus . That is, equal percentage of traffic is dropped from each VM. In real world scenarios, it is well observed that definition of traffic from a node (or a flow in particular) as being alive or dead is largely based on the application and transport protocols used. It is common to consider a flow (or traffic from a node) as dead if it is below a certain threshold. In this work we define the minimum threshold for traffic from a legitimate VM to be considered as alive by . If a CSP does not require such a minimum threshold, this model can be used by setting to 0.

5.0 DISCUSSION

Significant research has been carried out in the domain of network congestion and denial of service attacks. Project experimented with various queuing algorithms to determine which queuing method in the target router could provide better management of the bandwidth during a DDoS attack. Andersen proposed a proactive protection against DDoS attacks, by imposing overhead on all transactions to actively prevent attacks from reaching the server. Their architecture generalizes the Secure Overlay Services (SOS) to choose a particular overlay routing. The set of overlay nodes are used to distinguish legitimate traffic from the attack traffic. Researchers proposed a flow based mitigation filter for DDoS flooding attacks called Stateless Internet Flow Filter (SIFF). This approach uses a per-flow state, where the flows are classified into two categories privileged flows, and unprivileged flows with the goal of protecting privileged packets from unprivileged packet flows. NetFence uses a congestion feedback mechanism to enable robust congestion policing inside the network. The DoS victims can use the secure congestion policing feedback as capability tokens to suppress unwanted traffic and recover from attacks. Cloud computing infrastructure being the new paradigm shift is corporate and personal computing has significant room for improvement. Wang in their recent work present a measurement study to characterize the impact of virtualization on the networking performance of the Amazon Elastic Cloud Computing (EC2) data center. Their results show that virtualization can cause significant throughput instability and abnormal delay variations even when the data center is only lightly used. Hao propose a new data center architecture where users are allowing to share physical hardware resources, but network resources are isolated and shared in a controlled manner similar to that of enterprise networks. Projects explain in depth the potential of a target VM running in a cloud data center to be identified geographically by an attacker and its vulnerability to various kinds of attacks.

Recently, researchers have started exploring the applicability of game theory to model network security problems as multiplayer games. proposed a game- theoretic model to defend a web service under DoS attack. They use several metrics to measure the performance of their system. Wu perform similar research where they primarily focus on DoS/DDoS attacks launched using UDP based traffic. Researcher focuse on mitigating DoS and DDoS attacks for TCP-friendly flows using a game theoretic approach.

6.0 CONCLUSION

In this paper, we demonstrated the potential of denial of service attacks caused due to congestion of a shared router queue in the physical machines of a cloud service provider. These attacks are made possible by instantiating malicious VMs and making them co-resident with the victim VM on the physical machine. We emulate and evaluate the behavior of this shared router queue the Click modular router on DETER testbed. We model this attack scenario as a two player game and design a model to determine the best strategies for the defender to defend against such attacks. We are currently verifying the effectiveness of our proposed game model by performing extensive mathematical simulation and emulation. We perform simulation using MATLAB where consider a sub-set of the attacker"s and defender"s possible action set. For example, we consider the following scenario. The target physical machine on Amazon"s EC2 (prone to attack) can run upto 10 VMs at any given time. The bitrate capacity of the transmit and receive (T/R) queue this physical machine is 1 Gb/s. The attacker has the resources to rent up to 10 VMs from Amazon"s EC2. The attacker can vary the traffic bitrate of each of its rented VM between 1Mb/s to 100Mb/s. The defender can vary the firewall threshold between 1 Mb/s to 1000 Mb/s. Based on the set of payoffs obtained for each player, we then identity the Nash equilibrium whose co-ordinates denote the best strategy for the defender (optimum firewall threshold bitrate) to maximize the dropping of bogus traffic from malicious VMs. Hence by performing the above kind of simulation, we aim to illustrate that by using the Nash equilibrium strategy obtained by our game model, the defender is able to obtain a better payoff when compared to the defender choosing any other defense strategy. We are also working on verifying the applicability of our proposed defense solution by performing emulations using DETER testbeds and Click modular router. We create a topology where each of the various nodes behave as VM instances placed under one physical machine. These nodes share a T/R queue which is emulated by another node which acts as a gateway to the Internet. We run Click modular router on this gateway node in kernel level to monitor the bitrates of traffic coming from the other nodes. Our implementation of Click also includes the capability to drop traffic based on the firewall threshold variable defined in our model. We aim to study the potential of the applicability of our proposed game defense solution on other cloud service infrastructure like Microsoft"s Azure and Rackspace"s Mozzo, as we only consider the effect of generic user traffic on such machines to provide immunity against congestion based DoS attacks.

REFERENCES

[1] Melnyk, Steven A., et al. "New challenges in supply chain management: cybersecurity across the supply chain." International Journal of Production Research 60.1 (2022): 162-183.

[2] Spott, Jessica L., Kara Page, Narges Hadi, Terra Tindle Williams, and Kamau O. Siwatu. "Exploring the formal and informal stages in the socialization process in graduate students' professional development." Empowering student researchers (2021): 237-252.

[3] Cheung, Kam-Fung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. "Cybersecurity in logistics and supply chain management: An overview and future research directions." Transportation Research Part E: Logistics and Transportation Review 146 (2021): 102217.

[4] Golmohammadi, Amir-Mohammad, Negar Jahanbakhsh Javid, Lily Poursoltan, and Hamid Esmaeeli. "Modeling and analyzing one vendor-multiple retailers VMI SC using Stackelberg game theory." Industrial Engineering and Management Systems 15, no. 4 (2016): 385-395.

[5] Boyes, Hugh. "Cybersecurity and cyber-resilient supply chains." Technology Innovation Management Review 5.4 (2015): 28.

[6] Hadiana, Hengameh, Amir Mohammad Golmohammadib, Hasan Hosseini Nasabc, and Negar Jahanbakhsh Javidd. "Time Parameter Estimation Using Statistical Distribution of Weibull to Improve Reliability." (2017).

[7] Owen, Guillermo. Game theory. Emerald Group Publishing, 2013.

[8] Osborne, Martin J. An introduction to game theory. Vol. 3. No. 3. New York: Oxford university press, 2004.

[9] Do, Cuong T., et al. "Game theory for cyber security and privacy." ACM Computing Surveys (CSUR) 50.2 (2017): 1-37.

[10] Chukwudi, Amadi Emmanuuel, Eze Udoka, and Ikerionwu Charles. "Game theory basics and its application in cyber security." Advances in Wireless Communications and Networks 3.4 (2017): 45-49.

[11] Melnyk, Steven A., et al. "New challenges in supply chain management: cybersecurity across the supply chain." International Journal of Production Research 60.1 (2022): 162-183.

[12] Simon, Jay, and Ayman Omar. "Cybersecurity investments in the supply chain: Coordination and a strategic attacker." European Journal of Operational Research 282.1 (2020): 161-171.

[13] Hadi, Narges. "Examining the effect of distance learning environment on graduate students’ research self-efficacy: An investigation of the mediating effects of achievement goal orientations." PhD diss., 2021.

[14] Kumar, Subodha, and Rakesh R. Mallipeddi. "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions." Production and Operations Management 31.12 (2022): 4488-4500.

[15] Zavareh, Bozorgasl, Hossein Foroozan, Meysam Gheisarnejad, and Mohammad-Hassan Khooban. "New trends on digital twin-based blockchain technology in zero-emission ship applications." Naval Engineers Journal 133, no. 3 (2021): 115-135.

[16] Wong, Lai-Wan, et al. "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities." International Journal of Information Management 66 (2022): 102520.

[17] Bozorgasl, Zavareh, and Mohammad J. Dehghani. "2-D DOA estimation in wireless location system via sparse representation." In 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), pp. 86-89. IEEE, 2014.

[18] Gupta, Nikhil, et al. "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks." IEEE Access 8 (2020): 47322-47333.

[19] Hadi, Narges, Jessica L. Spott, and Raegan Higgins. "Underrepresented Students' Experiences in STEM at Community Colleges: A Qualitative Exploration of Self-Identified Challenges and Supports." Journal of The First-Year Experience & Students in Transition 34.2 (2022): 65-82.

[20] Sawik, Tadeusz. "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains." International Journal of Production Research 60.4 (2022): 1368-1385.

[21] Nazari Enjedani, Somayeh, and Mahyar Amini. "The role of traffic impact effect on transportation planning and sustainable traffic management in metropolitan regions ." International Journal of Smart City Planning Research 12.9 (2023): 688-700

[22] Sobb, Theresa, Benjamin Turnbull, and Nour Moustafa. "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions." Electronics 9.11 (2020): 1864.

[23] Jahanbakhsh Javidi, Negar, and Mahyar Amini. "Evaluating the effect of supply chain management practice on implementation of halal agroindustry and competitive advantage for small and medium enterprises ." International Journal of Computer Science and Information Technology 15.6 (2023): 8997-9008

[24] Boiko, Andrii, Vira Shendryk, and Olha Boiko. "Information systems for supply chain management: uncertainties, risks and cyber security." Procedia computer science 149 (2019): 65-70.

[25] Amini, Mahyar, and Negar Jahanbakhsh Javidi. "A Multi-Perspective Framework Established on Diffusion of Innovation (DOI) Theory and Technology, Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises ." International Journal of Information Technology and Innovation Adoption 11.8 (2023): 1217-1234

[26] Pandey, Shipra, et al. "Cyber security risks in globalized supply chains: conceptual framework." Journal of Global Operations and Strategic Sourcing (2020).

[27] Amini, Mahyar and Ali Rahmani. "Agricultural databases evaluation with machine learning procedure." Australian Journal of Engineering and Applied Science 8.6 (2023): 39-50

[28] Luo, Suyuan, and Tsan-Ming Choi. "E-commerce supply chains with considerations of cyber-security: Should governments play a role?." Production and Operations Management 31.5 (2022): 2107-2126.

[29] Amini, Mahyar, and Ali Rahmani. "Machine learning process evaluating damage classification of composites." International Journal of Science and Advanced Technology 9.12 (2023): 240-250

[30] Li, Yanhui, and Lu Xu. "Cybersecurity investments in a two-echelon supply chain with third-party risk propagation." International Journal of Production Research 59.4 (2021): 1216-1238.

[31] Amini, Mahyar, Koosha Sharifani, and Ali Rahmani. "Machine Learning Model Towards Evaluating Data gathering methods in Manufacturing and Mechanical Engineering." International Journal of Applied Science and Engineering Research 15.4 (2023): 349-362.

[32] Nagurney, Anna, Patrizia Daniele, and Shivani Shukla. "A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints." Annals of operations research 248 (2017): 405-427.

[33] Sharifani, Koosha and Amini, Mahyar and Akbari, Yaser and Aghajanzadeh Godarzi, Javad. "Operating Machine Learning across Natural Language Processing Techniques for Improvement of Fabricated News Model." International Journal of Science and Information System Research 12.9 (2022): 20-44.

[34] Amini, Mahyar, et al. "MAHAMGOSTAR.COM AS A CASE STUDY FOR ADOPTION OF LARAVEL FRAMEWORK AS THE BEST PROGRAMMING TOOLS FOR PHP BASED WEB DEVELOPMENT

FOR SMALL AND MEDIUM ENTERPRISES." Journal of Innovation & Knowledge, ISSN (2021): 100-110.

[35] Amini, Mahyar, and Aryati Bakri. "Cloud computing adoption by SMEs in the Malaysia: A multi-perspective framework based on DOI theory and TOE framework." Journal of Information Technology & Information Systems Research (JITISR) 9.2 (2015): 121-135.

[36] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Heuristic Solution For IaaS Cloud Placement Problem Without Migration." International Journal of Computer Science and Information Technologies 6.11 (2014): 25-30.

[37] Amini, Mahyar. "The factors that influence on adoption of cloud computing for small and medium enterprises." (2014).

[38] Amini, Mahyar, et al. "Development of an instrument for assessing the impact of environmental context on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.10 (2014): 129-135.

[39] Amini, Mahyar, et al. "The role of top manager behaviours on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.1 (2014): 490-498.

[40] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Solution For IaaS Cloud Placement Problem Using Simulated Annealing." International Journal of Computer Science and Information Technologies 6.11 (2014): 52-57.

[41] Sadat Safavi, Nazli, Nor Hidayati Zakaria, and Mahyar Amini. "The risk analysis of system selection and business process re-engineering towards the success of enterprise resource planning project for small and medium enterprise." World Applied Sciences Journal (WASJ) 31.9 (2014): 1669-1676.

[42] Sadat Safavi, Nazli, Mahyar Amini, and Seyyed AmirAli Javadinia. "The determinant of adoption of enterprise resource planning for small and medium enterprises in Iran." International Journal of Advanced Research in IT and Engineering (IJARIE) 3.1 (2014): 1-8.

[43] Sadat Safavi, Nazli, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 70-75.

[44] Safavi, Nazli Sadat, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 61-66.

[45] Amini, Mahyar, and Nazli Sadat Safavi. "Critical success factors for ERP implementation." International Journal of Information Technology & Information Systems 5.15 (2013): 1-23.

[46] Amini, Mahyar, et al. "Agricultural development in IRAN base on cloud computing theory." International Journal of Engineering Research & Technology (IJERT) 2.6 (2013): 796-801.

[47] Amini, Mahyar, et al. "Types of cloud computing (public and private) that transform the organization more effectively." International Journal of Engineering Research & Technology (IJERT) 2.5 (2013): 1263-1269.

[48] Amini, Mahyar, and Nazli Sadat Safavi. "Cloud Computing Transform the Way of IT Delivers Services to the Organizations." International Journal of Innovation & Management Science Research 1.61 (2013): 1-5.

[49] Abdollahzadegan, A., Che Hussin, A. R., Moshfegh Gohary, M., & Amini, M. (2013). The organizational critical success factors for adopting cloud computing in SMEs. Journal of Information Systems Research and Innovation (JISRI), 4(1), 67-74.

[50] Khoshraftar, Alireza, et al. "Improving The CRM System In Healthcare Organization." International Journal of Computer Engineering & Sciences (IJCES) 1.2 (2011): 28-35.

[51] Amini, Mahyar, and Zavareh Bozorgasl. "A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology ." International Journal of Computer Science and Engineering Research 11.4 (2023): 549-560.

[52] Zhang, Lixuan, et al. "Predicting Nodes' Performance in peer-to-peer network based on game theory." International Journal of Information Systems and Management 17.18 (2023): 2418-2426.

[53] Pan, Bing, et al. "Supply Chain Management System's Cybersecurity based on Blockchain Technology." International Journal of Science and Advanced Technology 11.9 (2023): 76-83.

[54] Vasiu, Ioana, and Lucian Vasiu. "Cybersecurity as an essential sustainable economic development factor." European Journal of Sustainable Development 7.4 (2018): 171-178.