ADOPTING A CONCEPTUAL ARCHITECTURE TO MITIGATE AN IOT ZERO-DAY THREAT THAT MIGHT RESULT IN A ZERO-DAY ATTACK WITH REGARD TO OPERATIONAL COSTS AND COMMUNICATION OVERHEADS

Dr. Vinod Varma Vegesna
Sr. IT Security Risk Analyst, The Auto Club Group, United States of America.
Email: vinodvarmava@gmail.com

ABSTRACT—Internet of Things (IoT) aims at providing connectivity between every computing entity. However, this facilitation is also leading to more cyber threats which may exploit the presence of a vulnerability of a period of time. One such vulnerability is the zero-day threat that may lead to zero-day attacks which are detrimental to an enterprise as well as the network security. In this, a study is presented on the zero-day threats for IoT networks and a context graph based framework is presented to provide a strategy for mitigating these attacks. The proposed approach uses a distributed diagnosis system for classifying the context at the central service provider as well as at the local user site. Once a potential zero-day attack is identified, a critical data sharing protocol is used to transmit alert messages and reestablish the trust between the network entities and the IoT devices. The results show that the distributed approach is capable of mitigating the zero-day threats efficiently with 33% and 21% improvements in terms of cost of operation and communication overheads, respectively, in comparison with the centralized diagnosis system.

Key words—IoT, Zero-day attacks, 5G, context-graphs, cloud computing; deployment model; service level agreement; utility computing; privacy; platform as a service; software as a service; infrastructure as a service; Denial of service attack; Cyber Security; Cloud Security; Network ; Cyber; Cyber Threats; Threat Analysis; Information Security; Data security.

1. Introduction

The communication networks are observing a tremendous increase in the number of devices which are predicted to go beyond 40% (of that were active in 2012) by 2020. All these devices have been arranged under a common term of “Internet of Things” (IoT). IoT allows integration of the vast variety of communication devices irrespective of their operational technology, which is also a challenging issue as a common firmware is required for all the devices [1-7]. A common firmware makes it easier to control and manage various IoT devices without many overheads. Common software platforms allow easy configurations as well as easy diagnosis of faulty operations. However, a common firmware also subjects the IoT components to various types of threats which can infiltrate the operational defense of these devices. Some of the key features required by IoT networks are remote diagnosis and management, data analytic, software upgrades, information passing and processing, and user mobility identification. All these form a type of application which allows access to the entire network once a particular feature is exploited [8-19].

Since there is no formal definition of IoT, same attacks which are applicable to any computing entity hold true in their case. Also, reduction in the human interventions and use of more automated systems in the IoT networks make it extremely important to secure the entire network as it may reveal critical information. Apart from these, IoT networks are also considered as an integral part of civilian and military expeditions focusing surveillance, navigation, localization, equipment control, and

currency transfers, etc. Recent trends have focused on using RFID tags as embedded sources for IoT devices that do not connect to the network directly. Although, such strategy holds safe for the majority of application scenarios, but manipulation with RFID tags can easily make these vulnerable similar to a normal computing entity [20-31]. Thus, security of IoT devices irrespective of the mode and type of connectivity is of utmost importance and has been an area of concern for a majority of the security researchers across the globe.

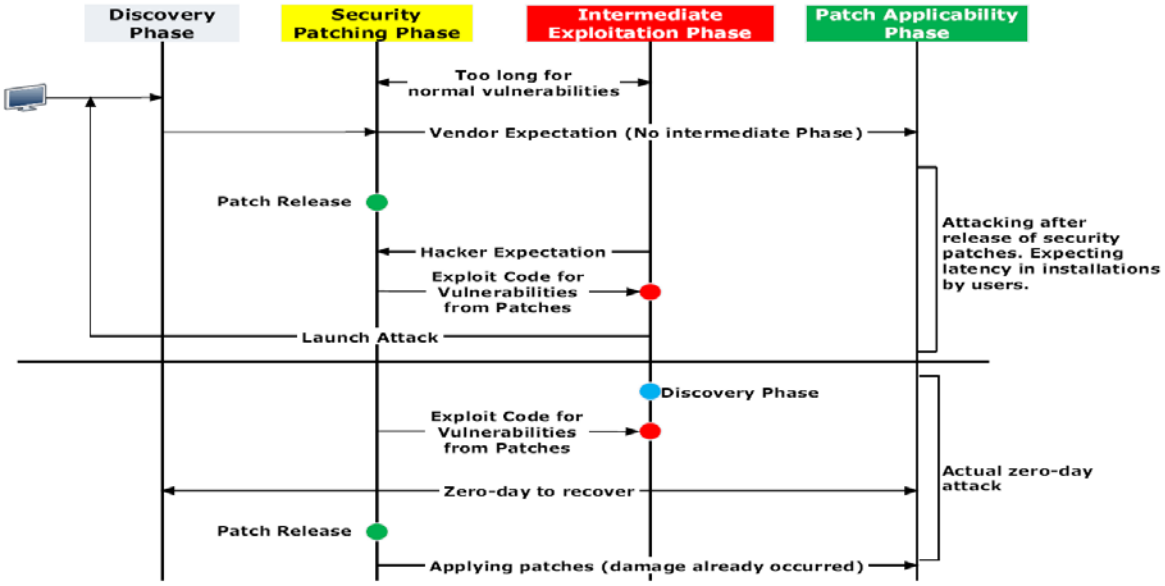

Fig. 1: An illustration of the window of vulnerability for zero-day attacks

Considering a common platform for IoT devices, most of the business enterprises and vendors focus on making version-based IoT firmware that can be easily upgraded and controlled. Such scenarios are possible by using a software-assisted networking. However, a software-assisted networking suffers from a major issue of zero-day vulnerabilities. Considering the level of deployment and configuration of networks, zero-day vulnerabilities are extremely dangerous for IoT networks. Exploitation of a zero-day vulnerability can lead to a zero-day attack. Control over a single unit of IoT software may expose the entire architecture [32-43].

2. Background: Zero-day Attacks

The name “Zero-day” is coined considering the negligible time available in mitigating these threats. The number of days for which an anomaly has been known directly affects the countermeasures and also the probability of remaining affected. It also has to do a lot with those software users who do not update security patches regularly. Once a vulnerability is publicized, it is mandatory for the particular application users to immediately switch to the stable releases. However, failure in doing so leads to various consequences in the form of cyber-attacks.

The effect of a zero-day vulnerability also depends on the mode of detection. If a vulnerability is identified by white hat hackers, it allows keeping it low profile until the security patches are not available; whereas identification of such vulnerabilities by a notorious group (black hat hackers) may subject the entire enterprise to failure. The vulnerability cycle for a zero-day attack may vary from scenario to scenario. In some cases, after identification of a bug, the hackers operate covertly leading to the full zero-day attack, while in some cases, the hackers may come forward (overt) and make threat public. Thus, it can be analyzed that a zero-day attack is not only because of the covert behavior of a hacker but also because of the delays in updating security patches once these are available in the public domain. This is often explained in the terms of window of vulnerability. The window of vulnerability is the time gap in which the number of vulnerable systems remaining is negligible. It is evaluated as a software timeline considering the discovery phase, security patching, intermediate exploitation phase and patch applicability phase, as shown in Fig. 1.

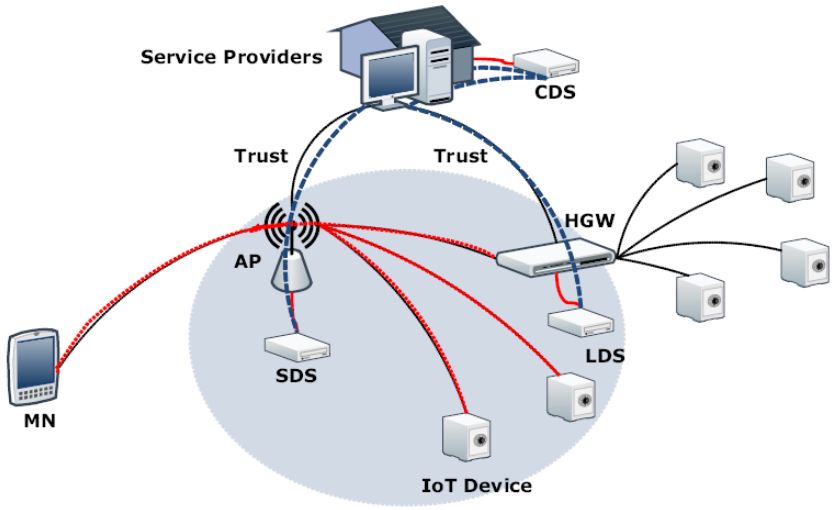

Fig. 2: An illustration of DDS-assisted IoT network

3. Proposed Approach

The network comprises various IoT devices and gadgets that operate either individually or collectively via a common gateway. The communication can be directly between the Mobile Node (MN) and the IoT device or indirectly between the MN and the IoT device via a gateway. The service providers are responsible for maintaining trust between the IoT and the MN. Currently, the proposed model emphasizes on a particular scenario in which an IoT device receives security updates that may lead to zero-day attacks; or when an attack is already launched and security updates confirm the attacks. The proposed approach uses strategic context graphs to ensure the safety of IoT devices against the zero-day attacks. The context graphs are implemented using Distributed Diagnosis System (DDS). The DDS are divided into three parts (shown in Fig. 2), namely.

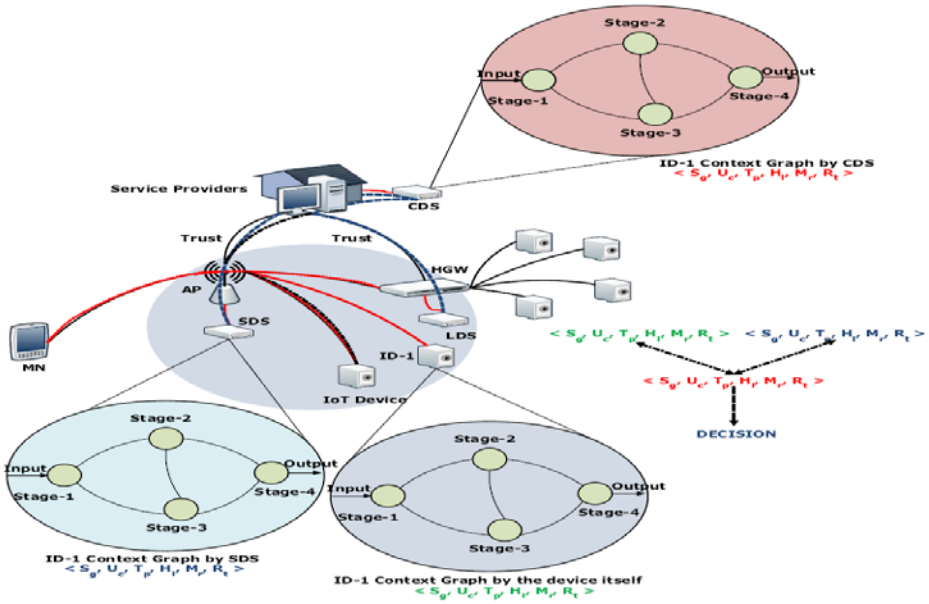

Fig. 3: An illustration of strategic context graph formation for an IoT device between the SDS and CDS. The decision on matching context is performed at CDS. The counter updates and firmware version decisions are also evaluated at the SDS and the CDS.

(1) Central Diagnosis System (CDS): CDS is installed by the service providers on the central node of the network which is responsible for generating trust as well as the updates for the entire network. CDS is responsible for managing the Access Points (APs) control, and the operations of gateways for maintaining security in the case of high possibilities of threats.

(2) Local Diagnosis System (LDS): LDS is operated as a dedicated device over the gateways. Usually, these are installed with the Home Gateways (HGW). LDS interacts with the CDS and shares its context graphs with it to ensure that all the security procedures are followed by the corresponding IoT device.

(3) Semi Diagnosis System (SDS): SDS is responsible for directly managing the APs trust with the CDS. It shares the context of IoT devices which directly interacts with an MN without relying on the local gateway.

Strategic Context

The types of devices operable in a network are considered to have valid pre-registered signatures along with a counter value. The counter value manages the count for the number of times the firmware of an IoT device is validated or encountered [44-48]. The context for each IoT device is managed by its diagnosis system and periodically stored in logs and shared with the CDS. The context outline used in the proposed model is as follows:

Device signatures (Sg): This is the unique identity for each device. The signature is the embedded information about the IoT device which is stored at the CDS once it gets activated in the network.

Update Counter (Uc): This is the firmware update counter which is randomly selected at the beginning of network registrations. These are updated using random integer values which are finalized by the CDS and change periodically without affecting the performance.

Traffic Type (Tp): This defines the context for the type of traffic to be generated for and by an IoT device. This helps the diagnosis system to analyze the content over a particular channel for its correctness.

Header Length (Hl): It defines the bit length of the header field used by the diagnosis system. It contains all the necessary context metadata which is to be shared between the LDS, SDS, and CDS.

Memory Range (Mr): It denotes the maximum and minimum size of the packets generated by the IoT device. This helps to simply analyze if the size of the initial code is affected or not. Usually, these are not mishandled by the attackers, but still, in some cases, this is very useful to identify if the binaries of the firmware are altered or not.

Route (Rt): This field is used to check whether an IoT device is operable in LDS, SDS, or CDS region. This also allows tracking the actual route for managing the context between the network entities.

A. Context Graphs and Strategic Attack Detection

The context graphs are used to generate the strategies which help in taking a decision regarding the presence of a threat amongst the IoT devices. The number of vertices in the context graphs is equal to the number of processing procedures an IoT device follows before generating an output and demanding an input. The context explained above forms the edges of the graph. After the time instance decided in the configuration of the network, the LDS and SDS evaluate these graphs for every corresponding IoT device ad share it with the CDS which also forms its own context graph for every IoT device. Along with the context graphs, the CDS also forms the context graphs for the subordinate network which includes the layers of APs, and gateways.

In order to take a strategic decision on the management of IoT devices against the zero-day attacks, the CDS follows a principle of modeling the counter and the random integer value used to manage the counter by the LDS, SDS and the device itself. Then, it performs mutual exclusion rule to trace the presence of a zero-day threat in the IoT network. The failure in the matching of the context stored and the

context received from all the subordinates as well as the IoT device indicates the presence of a zero-day attack. The operational view of the proposed approach is illustrated in the Fig. 3.

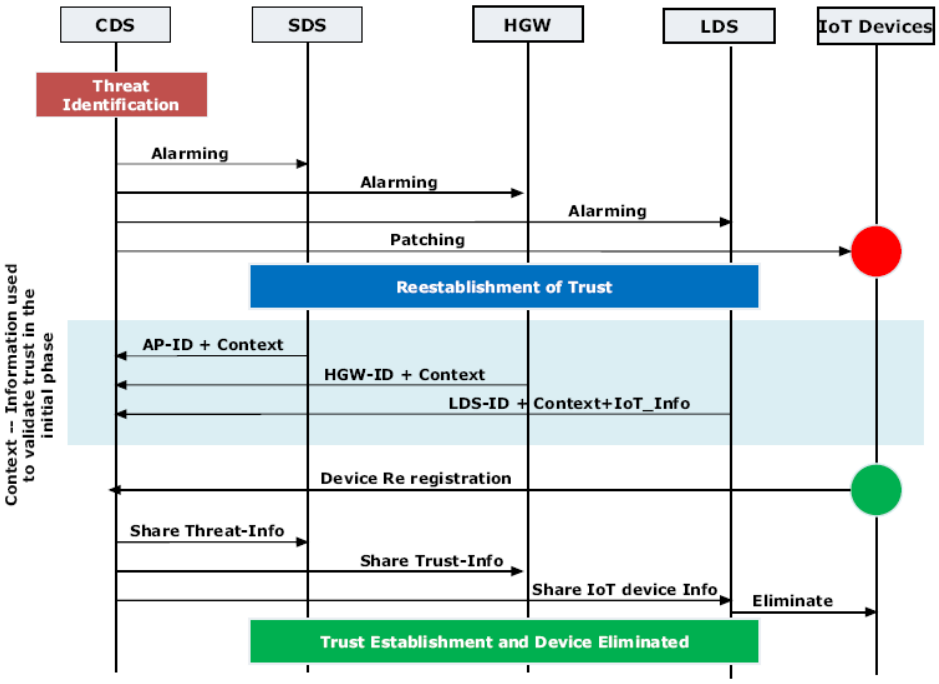

Fig. 4: An illustration of critical context/data sharing protocol used after the identification of potential zero-day threat or attack in the IoT network.

It is to be noted that the strategic context graphs are applicable in the network only in the deployment phase, but not in the development phase. Thus, the proposed strategy can come handy only when a vulnerability is identified by the development team at lateral stages as well as during the release of security updates as it helps in tracking the contextual behavior of every IoT device. Once a possibility of attack is found, the proposed approach utilizes the critical data sharing protocol that helps in eliminating a particular IoT device before it exploits the entire network.

B. Critical Data Sharing Protocol

The proposed approach uses a critical context/data sharing protocol in the scenarios with a potential zero-day threat. The protocol, shown in Fig. 4, illustrates the procedures opted by the CDS once a threat is identified amongst the IoT devices leading to a zero-day exploitation. Once a threat policy is violated, the CDS sends alarming messages to its connected components that are its subordinates in the network. The alarming messages are followed by the patch for fixing the affected IoT device. This is followed by the reestablishment of the trust between all the connected components with the CDS. Once an alarming request is received, each subordinate's diagnosis system shares context information to revalidate the trust. By the time, these steps are performed, the affected device updates its security mechanisms, and registers itself again with the CDS leading to the elimination of the threat without eliminating the device. On the contrary, CDS shares threat information with the SDS, trust information with the HGW, device information with the LDS, and finally, leads it to eliminate the incorrect device. This allows mitigating zero-day threats in IoT networks.

4. Performance Evaluation

The proposed approach is evaluated by deploying 500 sensors in two modes, namely, with CDS only and with CDS, LDS, and SDS. The proposed approach is evaluated to analyze the effect of DDS on the performance of the proposed framework.

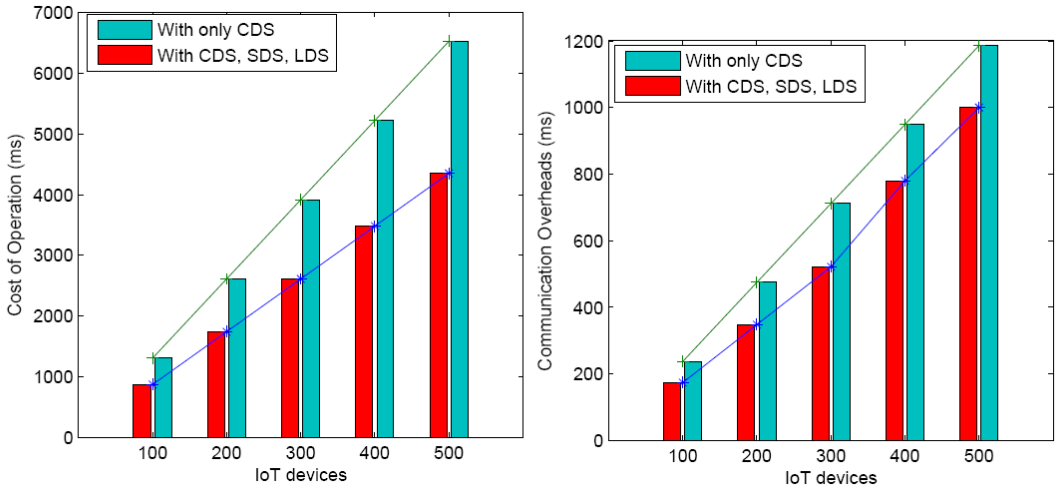

Fig. 5: Simulation Results

The model defined with similar attacker scenario (20% nodes as the attacker) is used to evaluate the formation in the proposed approach for cost of operation and communication overheads. The cost of operation is calculated as the time required by the diagnosis system to arrive at the decision of zero-day possibility. It includes the communication time including the context sharing procedures as well as the formation of the context graphs at the interacting entities.

5. Conclusion

In this, a study was presented on zero-day threats for IoT networks. A context graph based framework was presented to provide a strategy for deciding on the zero-day attacks. The proposed approach used a distributed diagnosis system for classifying the context at the central service provider as well as at the local user site. Also, once a zero-day attack was potentially identified, a critical data sharing protocol was used to transmit alert messages and reestablish the trust between the network entities and the IoT devices. This is a progressive paper and the details on the full-fledged implementation along with critical evaluations will be presented in future reports.

References

[1] Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutorials 18(2), 1153–1176 (2015)

[2] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., Ming, H.: Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0305–0310, IEEE (2019)

[3] Vinod Varma Vegesna (2022). “Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems,” Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[4] Dua, S., Du, X.: Data mining and machine learning in cybersecurity. CRC press (2016)

[5] Apruzzese, G. Colajanni, M., Ferretti, L., Guido, A., Marchetti, M.: On the effectiveness of machine and deep learning for cyber security. In: 2018 10th International Conference on Cyber Conflict (CyCon), pp. 371–390, IEEE (2018)

[6] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[7] Mukherjee, B., Heberlein, L.T., Levitt, K.N.: Network intrusion detection. IEEE Netw. 8(3), 26–41 (1994)

[8] Kumar, V., Sangwan, O.P.: Signature based intrusion detection system using snort. Int. J. Comput. Appl. Inf. Technol. 1(3), 35–41 (2012)

[9] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[10] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. comput. Security 28(1–2), pp. 18–28 (2009)

[11] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[12] Bilge, L., Dumitraş, T.: Before we knew it: an empirical study of zero-day attacks in the real world. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 833–844 (2012)

[13] Vinod Varma Vegesna (2021). "Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage," Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[14] Hamid Ali Abed Al-Asadi, "Mobile Clustering Algorithm for Effective Clustering in Dense Wireless Sensor Networks," European Journal of Advances in Engineering & Technology (EJAET), Vol. 4, Issue 1, PP. 1-6, 2017.

[15] Stellios, I., Kotzanikolaou, P., Psarakis, M.: Advanced persistent threats and zero-day exploits in industrial internet of things. In: Security and Privacy Trends in the Industrial Internet of Things, pp. 47–68, Springer (2019)

[16] Mell, P., Grance, T.: Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme, tech. rep., National Inst of Standards and Technology Gaithersburg MD Computer Security Div (2002)

[17] Vinod Varma Vegesna (2020). "Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications," Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[18] Ganame, K., Allaire, M. A., Zagdene, G., Boudar, O.: Network behavioral analysis for zero-day malware detection–a case study. In: International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, pp. 169–181, Springer (2017)

[19] Hamid Ali Abed Al-Asadi and et., "Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement", Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[20] Sinclair, C., Pierce, L., Matzner, S.: An application of machine learning to network intrusion detection. In: Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99), pp. 371–377, IEEE (1999)

[21] S. Sahu and B. M. Mehtre, Network intrusion detection system using j48 decision tree. In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE (2015)

[22] Vinod Varma Vegesna (2019). "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[23] Xian, Y., Schiele, B., Akata, Z.: Zero-shot learning-the good, the bad and the ugly. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4582–4591 (2017)

[24] Wang, W., Zheng, V.W., Yu, H., Miao, C.: A survey of zero-shot learning: settings, methods, and applications. ACM Trans. Intell. Syst. Technol. (TIST) 10(2), 1–37 (2019)

[25] Hamid Ali Abed Al-Asadi and et., "Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15.

[26] Zhang, Z., Liu, Q., Qiu, S., Zhou, S., Zhang, C.: Unknown attack detection based on zero-shot learning. IEEE Access 8, 193981–193991 (2020)

[27] Sommer, R., Paxson, V.: Outside the closed world: on using machine learning for network intrusion detection. In: 2010 IEEE Symposium on Security and Privacy, pp. 305–316, IEEE (2010)

[28] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[29] Casas, P., Mazel, J., Owezarski, P.: Unsupervised network intrusion detection systems: detecting the unknown without knowledge. Comput. Commun. 35(7), 772–783 (2012)

[30] Holm, H.: Signature based intrusion detection for zero-day attacks:(not) a closed chapter?. In: 2014 47th Hawaii International Conference on System Sciences, pp. 4895–4904, IEEE (2014)

[31] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[32] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.-N., Bayne, E., Bellekens, X.: Utilising deep learning techniques for effective zero-day attack detection. Electronics 9(10), 1684 (2020)

[33] Li, Z., Qin, Z., Shen, P., Jiang, L.: Zero-shot learning for intrusion detection via attribute representation. In: International Conference on Neural Information Processing, pp. 352–364, Springer (2019)

[34] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100.

[35] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[36] Kumar, V., Sinha, D.: A robust intelligent zero-day cyber-attack detection technique. Complex Intell. Syst. 7(5), 2211–2234 (2021)

[37] Siddique, K., Akhtar, Z., Aslam Khan, F., Kim, Y.: Kdd cup 99 data sets: A perspective on the role of data sets in network intrusion detection research. Computer 52(2), 41–51 (2019)

[38] Felix, R., Harwood, B., Sasdelli, M., Carneiro, G.: Generalised zero-shot learning with domain classification in a joint semantic and visual space. In: 2019 Digital Image Computing: Techniques and Applications (DICTA), pp. 1–8, IEEE (2019)

[39] Breiman, L.: Random forests. Mach. Learn. 45(1), 5–32 (2001)

[40] Hinton, G. E.: Connectionist learning procedures. Mach. learn., pp. 555–610, Elsevier (1990)

[41] Breiman, L.: Some properties of splitting criteria. Mach. Learn. 24(1), 41–47 (1996)

[42] Agarap, A. F.: Deep learning using rectified linear units (relu). arXiv preprint arXiv:1803.08375 (2018)

[43] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107.

[44] Moustafa, N., Slay, J.: Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1–6, IEEE (2015)

[45] Sarhan, M., Layeghy, S., Moustafa, N., Portmann, M.: Towards a Standard Feature Set of NIDS Datasets. arXiv preprint arXiv:2101.11315 (2021)

[46] Corchado, E., Herrero, Á.: Neural visualization of network traffic data for intrusion detection. Appl. Soft Comput. 11(2), 2042–2056 (2011)

[47] Layeghy, S., Gallagher, M., Portmann, M.: Benchmarking the Benchmark - Analysis of Synthetic NIDS Datasets. arXiv preprint arXiv:2104.09029 (2021)

[48] Ramdas, A., Trillos, N.G., Cuturi, M.: On wasserstein two-sample testing and related families of nonparametric tests. Entropy 19(2), 47 (2017).