Comprehensive Analysis of IoT Malware Evasion Techniques

Abdulsamad Al-Marghilani
Information Technology Department
College of Computer Science & Information Technology
Northern Border University
Rafha, Saudi Arabia
a.marghilani@nbu.edu.sa

Abstract-Malware detection in Internet of Things (IoT) devices is a great challenge, as these devices lack certain characteristics such as homogeneity and security. Malware is malicious software that affects a system as it can steal sensitive information, slow its speed, cause frequent hangs, and disrupt operations. The most common malware types are adware, computer viruses, spyware, trojans, worms, rootkits, key loggers, botnets, and ransomware. Malware detection is critical for a system's security. Many security researchers have studied the IoT malware detection domain. Many studies proposed the static or dynamic analysis on IoT malware detection. This paper presents a survey of IoT malware evasion techniques, reviewing and discussing various researches. Malware uses a few common evasion techniques such as user interaction, environmental awareness, stegosploit, domain and IP identification, code obfuscation, code encryption, timing, and code compression. A comparative analysis was conducted pointing various advantages and disadvantages. This study provides guidelines on IoT malware evasion techniques.

Keywords-IoT; malware; evasion techniques; challenges; security

I. INTRODUCTION

Internet of Things (IoT) is a system where various interconnected objects transfer data over a wireless network without requiring any human intervention [1, 2]. Various sensors, technologies, and software are embedded into these devices to connect and transfer data within the network [3]. IoT has evolved by utilizing various technologies such as embedded systems, machine learning, real-time analytics, and commodity sensors [4-6]. Many IoT applications are considered consumer applications, e.g. home security and wearable technologies [7]. Industrial applications of IoT usually monitor industrial systems such as smart logistics management and smart robotics [8]. In commercial applications, IoT devices work with each other to provide benefits such as smart offices and buildings, connected lighting, and so on [9]. Moreover, IoT is used in infrastructure to monitor and regulate areas, cities, or countries such as smart parking management and connected charging stations [10]. Moreover, IoT devices are connected to the internet and transfer large amounts of data [11]. As IoT continues to grow, a critical issue is emerging regarding the privacy and the security of data transferred over the network. One such issue that affects data security in IoT is malware [12].

IoT devices lack security features and are more vulnerable to malware attacks as they are always connected to the internet. Malware is software designed to gain unauthorized access to systems causing security threats [13]. The most common types of malware are worms ,viruses, spyware, adware, ransomware, and trojan horses [14]. Worms duplicate themselves and spread from one system to another without requiring any human intervention [15]. Viruses also duplicate themselves but differ from worms as they insert code in other programs [16]. Spyware steals sensitive information without the user's knowledge [17], while adware is a type of software that displays unnecessary advertisements [18]. Ransomware aims to lock a system and demand money to unlock it [19]. Trojan horses aim to give unauthorized access to a system without the user's knowledge [20]. Various attacks can affect IoT devices causing privacy and security issues. Some attacks that infect IoT devices are botnets, Mirai, and Prowli malware [21]. A botnet is a robot network controlled by a hacker who uses malware to hijack its devices [22]. Mirai is a malware that is capable of propagating itself and infects unsecured devices including IoT [23], while Prowli is used to redirect users to fake websites. Based on the type of strategy, approaches to detect malware can be categorized into two main domains: static and dynamic analysis [24]. Malware detection can be performed on three bases: Behavior-based, specification-based, and signature-based (Figure 1). In behavior-based malware detection, the object is evaluated based on its actions [26] before executing actions to analyze suspicious activities and get rid of threats. This technique is further classified as static, dynamic, and hybrid. In specification-based malware detection, a policy or specification mediates events from any program [27], and this is also classified as static, dynamic, and hybrid. Signature-based malware detection is working with known threats and detects them easily by establishing unique identifiers. It is also classified as static, dynamic, and hybrid [28]. This study aims to analyze the malware detection techniques in IoT applications, compare the existing studies on IoT malware evasion techniques highlighting their advantages and limitations, and identify the various malware evasion techniques.

Corresponding author: Abdulsamad Al-Marghilani

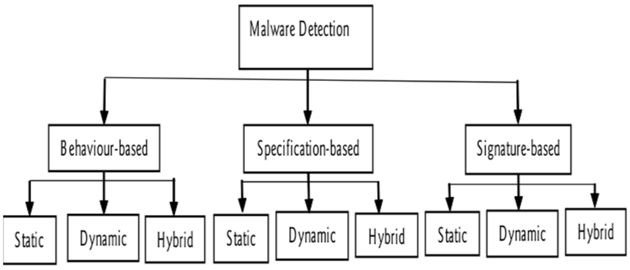

Fig. 1. Malware detection techniques [25].

II. SECURITY ISSUES IN IOT APPLICATIONS

Securing network communications more effectively and efficiently is considered a very critical issue. Mobile ad hoc networks are exposed to many packet-drop attacks because of their fundamental characteristics, such as vulnerabilities of the underlying typical routing protocols. The packet drop attacks include black-hole and grey-hole attacks. Various types of black-hole attacks and their defects were examined in [29]. Various schemes have been discovered for detecting black hole attacks, including learning, co-operative, and other schemes. Several techniques, including their core functionality and performance, were examined. The trust-based is a learning scheme, better than other schemes, as it had higher prevention nature against the attacks. On the other hand, most trust-based schemes failed to balance past and existing trust values. Moreover, as openness and flexibility made Android a popular mobile platform, it is targeted by massive mobile malware highlighting the need for better detection and prevention [30]. This study utilized a lightweight framework to identify malware in Android devices. Data analysis and malware detection were carried out on the server-side, reducing the use of mobile devices' resources and not affecting user's experience. In this method, machine learning was combined with network traffic analysis resulting in more accurate detection rates. Meanwhile, as this method is limited to existing malicious samples, more samples have to be collected and analyzed to improve it continuously.

IoT devices lack security and are highly heterogenous [31], so many challenges arise on the cross-architecture detection of IoT malware. Various studies utilize dynamic or static analysis. Static analysis is more suitable for detecting malware in IoT devices, as it is more effective on multi-architecture devices. In [31], non-graph and graph-based malware detection methods were used. Graph-based methods were found to detect more accurately unseen and complicated malicious codes. The advantages and limitations were summarized based on processing time, detection analysis, and mechanism, while efficiency is required to be further enhanced. A graph-based lightweight detection method to deal with various malicious executable files in IoT devices is yet to be designed and developed. A modern malware type that can evade system security is Advanced Persistent Threats (APTs), while its identification is a great challenge [32]. Antimalware and antivirus systems are conventional security systems that fail in APTs identification. This study used Advanced Evasive Techniques and examined the evasion and sophisticated attack techniques. As such malware can bypass a firewall with ease, a security system has to be effective to identify and avert such cyber-attacks in the future.

III. CHALLENGES AND ASSOCIATED TECHNIQUES TO ENHANCE THE SECURITY AGAINST MALWARE

IoT devices have various security issues as malware increases. Security researchers use machine learning techniques to deal with these security issues and enhance IoT devices' efficiency. A malware detection framework, called MalInsight, was proposed in [33]. In MalInsight, malware is described from three aspects: basic structure, high-, and low-level behavior. Malware was detected more effectively and accurately based on findings from file operations, structural features, network, and registry reflected from these three aspects. This framework can detect easily unseen malware. Various features are yet to be added, including work on privileged management schemes, authentication to restrict malware execution and reduce potential harm. Beaconing, another malware type difficult to detect, was studied in [34]. The collection and review of enough data to detect a Beaconing malware's behavior is a challenging task. Beaconing is one of the encryption-based attacks where hackers use encryption to hide their activities. Two unsupervised learning agents were used to detect malicious beaconing, a real-time and a periodic agent. The proposed algorithm can detect three different malicious beaconing behaviors: distortion, skipped exchanges, and combined distortion and skipped exchanges. Unsupervised machine learning algorithms can be used along with AI to check the accurate beaconing behaviors. Botnet activities detection is critical for the availability, security, and reliability of internet services. Existing systems find it difficult to detect novel botnets with high accuracy due to various reasons such as new botnets created to bypass current detection approaches, the similarity between normal and botnet traffic, and the high computational requirements of large amounts of data processing. A scalable and decentralized framework was utilized to address this problem in [35]. This framework discovered previously unseen botnet traffic, characterized the behavior of legitimate hosts, can detect novel botnets without any assumptions, and can be used in real-world scenarios. Despite the advantages of adaptive training and low numbers of false alarms, it has some drawbacks as network traffic increases and attackers change their methods constantly to avoid detection.

IV. VARIOUS MALWARE ATTACKS IN IOT

In [36], malware targeting mobile devices was explored as a considered serious threat. Fraudulent mobile apps and injected malicious apps are two types of mobile malware attacks. Three main phases were included in the analysis: pre-processing, extraction, and grouping. Grouping strategy was used to choose valuable APIs to identify android malware apps and it included the upcoming three strategies. An effective classification model was proposed that combined API calls and permission requests. Three different strategies were proposed to choose the valuable API calls. Empirical analysis showed that the proposed system was effective in detecting mobile malware and helped the process of mobile application analysis and malware forensic investigation. Cyber data breaches increase while investigating cyber-attacks manually is time-consuming and error-prone. A novel machine-learning-based framework was proposed in [37] that identified cyber threats and investigated cyber security issues with incomplete or partial information. Mitigations for the identified threat incidents are yet to be integrated and automated. Reviews about malware Android platform were examined in [38], including mobile malware attacks, detection techniques, vulnerabilities, and security solutions over a certain period. Ransomware hijacks in files and resources were studied in [39], presenting a ransomware taxonomy, various factors and counteraction types, and threat success factors and techniques. Existing and upcoming security threats in IoT-enabled smart grids were studied in [40], discussing various data privacy concerns, attack motives, and data transfer techniques. Threat vectors in smart grids were classified into attacks against privacy, integrity, availability, and authentication. This paper also discussed the cyber kill chain which is a seven-step attack procedure. Time Sensitive Networking (TSN) was adopted for IoT and smart grids to allow real-time communication, while six open directions were proposed for smart grid connectivity. The challenges to secure a smart manufacturing system were explored in [41]. Smart manufacturing is an important component for industry and connects physical and digital environments through IoT technologies. Data analytics, machine learning, and cloud with industrial systems integration lead to potential benefits and new challenges. Various factors were discussed which include existing vulnerabilities, weaknesses, security of existing manufacturing industrial systems, and preparing for future security challenges.

V. VARIOUS MALWARE EVASION TECHNIQUES IN IOT

In [42], four methods were proposed to detect malware using hamming distance. This approach helps discover similarities between various samples, and it included All Nearest Neighbours (ANN), Weighted All Nearest Neighbours (WANN), First Nearest Neighbours (FNN), and K-Medoid based Nearest Neighbours (KMNN). These machine learning methods were used to detect malicious software having high precision and recall rates. A software-defined visual analytic system was proposed in [43], which was preferred for large analysis. Various classifications were performed by extracting image features using machine learning algorithms. The utilized classifiers were decision tree, SVM, random forest, and logistic regression. Decision tree and random-based classifiers were found to be the most accurate. In [44], machine learning techniques to detect malware were studied by examining unsolved issues, challenges, limitations, recent trends, and new research directions.

The wide adoption of IoT by industrial systems led to an increase in malware. A malware analysis system was proposed in [45], where malware evasive behavior was detected by measuring the deviation from a program's normal behavior. The Analysis Evasion Malware Sandbox (AEMS) was very effective in malware detection. This system automatically detected the evasion in malware samples and provided reasonable accuracy. The Big Data Cybersecurity Analytics (BDCA) system, studied in [46], protects the organizational networks and data from cyber-attacks by analyzing data security. After conducting a systematic literature review, seventeen architectural tactics were identified to support twelve quality attributes such as scalability, performance, accuracy, security, and usability. Various factors are yet to be included such as analysis among tactics, trade-offs, and big data processing frameworks. As hacking attacks on industrial control systems increase and many security vulnerabilities are detected on industrial IoT, technical and regulatory perspectives were examined in [47] to solve the upcoming security threats. Resource exploration and energy consumption were significant challenges in the context of smart energy infrastructure. Two challenges arose from the legal perspective: balancing the obligations of Network and Information Security (NIS) with the desire for industrial IoT, and the need for guidance from authorities on IoT and Computer Emergency Response Teams (CERTS). Handling temporal dimensions of security, the shift of infrastructure from offline to online, the way to engage critical systems and their infrastructural complexity, the best way to address implementation gaps are areas yet to be focussed in detail. In [48], a malware analysis system was examined to characterize the malware behavior and improve the defense mechanism. This system considered the entire analysis environment which included the sandbox and a few other components. A fully automated system was developed as a solution to improve the dynamic malware analysis process. Integrating the malware analysis process with environment configuration made easy the deployment of a complex analysis environment. Malware Analysis Architecture based on SDN (MARS) provided useful analysis capabilities. Dynamic configuration is yet to be enhanced and an extensive analysis of the malware ecosystem is needed. Ensembles that comprise a set of classifiers were proposed as an effective approach to detect malware, but due to the high cost of data transfer, memory, and processing requirements, this approach failed to secure big data in the cloud. The Hybrid Consensus Pruning (HCP) method was proposed in [49] to address this problem, by combining several classifier classes into one scheme. HCP was found to be more effective than ensemble pruning through Directed Hill Climbing Ensemble Pruning (DHCEP), k-means pruning, and Ensemble Pruning via Individual Contribution (EPIC) ordering. This HCP method provided better ensemble classifiers to detect malware than the other methods, as shown in Table I.

A classification of malware dynamic analysis evasion strategies was presented in [50]. Conventionally, a sandbox was introduced to suffer unplanned impacts from unknown software [51]. Thus, the term sandbox represents a segregated or highly managed environment for testing unverified programs. Due to equivalence in nature, Virtual Machines (VMs) and emulated environments are frequently viewed as sandboxes. However, in this study, the term sandbox is used to denote the isolated and contained environments that automatically examine the specific program without any human intervention. The isolating link, in this study, is the system’s autonomous nature. Evasion comprises a sequence of methods applied by malware to maintain stealth, hinder efforts or avoid detection. For example, a major evasion strategy is fingerprinting [52]. The malware attempts to identify its environment by using fingerprinting and confirm if it is an analysis or production system. On the other hand, the counter evasion mechanisms try to hide the clues and cues which may reveal the analysis system. When a system exposes minimum clues to malware, then this system is highly transparent. Automated and manual analysis are the main terms that form the proposed classification. When an expert performs an analysis with the support of a debugger, then this is called manual analysis. On the other hand, if an expert utilizes the conventional sandboxing technology to execute a transparent debugger, it is considered as a Manual Dynamic Analysis (MDA). In contrast, automated analysis is performed by software or machine automatically. Detection is simply a perceptive process that checks whether a specific file is malicious. In addition, analysis is an understanding process that defines how malware functions. However, this segregating line is unclear at present as the functions of automated analysis implemented like sandboxes are expanding. Additionally, to report the behavior of malware, sandboxes are performing their functions as the primary automated detection techniques [53]. This study considers similar concepts, as the understanding of malware's behavior is regarded as manual and malware detection is regarded as automated. Although the MDA is efficient, it has serious drawbacks, e.g. it is time consuming. Examining a huge count of malware samples requests an effective agile method. Such requests led to an innovative pattern of analysis known as Automated Dynamic Analysis (ADA).

TABLE I. COMPARATIVE ANALYSIS OF IOT MALWARE DETECTION USING VARIOUS EVASION TECHNIQUES

Paper	Techniques used	Description	Outcome	Advantages / disadvantages
[29]	Learning, co-operative, and other schemes.	Fifteen techniques were involved and core functionalities were discussed. The performance of techniques to mitigate and detect a black hole attack was defined.	Trust-based scheme was better when compared with other schemes.	The trust-based scheme had high prevention nature. Nearly all trust-based methods failed to weigh balance accurately between past and existing trust values.
[30]	Lightweight network traffic analysis and machine learning.	Machine learning algorithm was combined with network traffic analysis. This helped the detection of android malware.	Android malware was detected.	The detection rate was found to have high accuracy but was limited to existing malicious samples.
[31]	Non-graph and graph-based malware detection methods.	Two groups of malware detection methods were used: non-graph and graph-based methods.	Graph-based methods detected more accurately unseen and complicated malicious codes.	This method can be used to improve efficiency in the future. A graph-based lightweight detection method is yet to be designed and developed.
[32]	Advanced evasive techniques.	This study explored evasion techniques and sophisticated attacks utilized by present-day malware.	Various malware analysis techniques were discussed.	Advanced evasive techniques can bypass a firewall easily. An efficient security system is required to identify and avert cyber-attacks in the future.
[33]	MalInsight.	Malware was summarized from three aspects: basic structure, low, and high-level behavior. Malware was detected more effectively based on findings from operations on files, structural features, network, and registry which are reflected from the three aspects.	The framework could easily detect unseen malware and help future researchers discover malware easily.	Work on privileged management schemes and authentication to restrict the malware execution and reduce the potential harm is yet to be done.
[34]	Unsupervised machine learning algorithms.	Two unsupervised learning agents, a real-time and a periodic one, were used to detect malicious beaconing.	Three different malicious beaconing behaviors were detected: distortion, skipped exchanges, and combined.	Unsupervised machine learning could be used along with AI to check beaconing behaviors.
[35]	Scalable and decentralized framework.	Scalable and decentralized frameworks were used.	Previously unseen botnet traffic was discovered and the behaviors of legitimate hosts were characterized.	Although the merits of adaptive training and the low number of false alarms, attackers changed their method constantly to avoid detection. The constant evolving of network traffic was also a drawback.
[37]	Novel machine learning based framework.	Investigating cyber-attacks through manual processes is time-consuming and error-prone. A novel machine learning based framework was proposed.	Based on observed attack patterns, the proposed method identifies cyber threats.	Proposed a method for investigating cybersecurity issues with partial information.
[42]	ANN, WANN, FNN, KMNN.	Four methods were proposed to detect malware using hamming distance, helping to discover similarities between various samples.	Machine learning methods were used to detect malicious software.	High precision and recall rates were obtained. Other similarity measures with different features between two programs are yet to be defined.
[49]	Hybrid Consensus Pruning (HCP).	An advanced ensemble pruning method combined several classifier classes into one scheme.	Several analyses were made by comparing HCP with several pruning methods. HCP was the most effective.	HCP provided better ensemble classifiers to detect malware. This work should be extended to internet traffic for security and mobile cloud computing.

VI. Conclusion

This paper reviewed IoT malware detection and evasion-based techniques. The advantages and disadvantages of existing evasion-based IoT malware detection techniques were discussed. Trust-based schemes, HCP, and graph-based methods are the most effective malware detection techniques. Malware evolves with high efficiency as attackers use advanced technologies to design malware that bypasses detection systems. As malware evolves, modern solutions are needed to detect and handle it. Malware evasion methods were analyzed, while classifications for automated and manual analysis were presented. The summarized advantages and limitations can be used by researchers to improve the efficiency of IoT malware detection systems [54-57]. The evasion attempts can be categorized as detection independent and detection dependent. Effective generic schemes, namely path exploration techniques, are still needed for detection independent strategy.

References

[1] S. Bhat, O. Bhat, and P. Gokhale, "Applications of IoT and IoT: Vision 2020," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, Jan. 2018.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, https://doi.org/10.1016/j.future.2013.01.010.

[3] F. Hüning, *Embedded Systems für IoT*. Springer Vieweg, 2019.

[4] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, https://doi.org/10.1109/COMST.2020.2986444.

[5] S. Verma, Y. Kawamoto, Z. Md. Fadlullah, H. Nishiyama, and N. Kato, "A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1457–1477, 2017, https://doi.org/10.1109/COMST.2017.2694469.

[6] S. J. Johnston, M. Scott, and S. J. Cox, "Recommendations for securing Internet of Things devices using commodity hardware," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Dec. 2016, pp. 307–310, https://doi.org/10.1109/WF-IoT.2016.7845410.

[7] M. Q. Aldossari and A. Sidorova, "Consumer Acceptance of Internet of Things (IoT): Smart Home Context," *Journal of Computer Information Systems*, vol. 60, no. 6, pp. 507–517, Nov. 2020, https://doi.org/10.1080/08874417.2018.1543000.

[8] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT," *IEEE Access*, vol. 3, pp. 622–637, 2015, https://doi.org/10.1109/ACCESS.2015.2435000.

[9] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Computer Networks*, vol. 148, pp. 241–261, Jan. 2019, https://doi.org/10.1016/j.comnet.2018.12.008.

[10] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," *IEEE Sensors Journal*, vol. 15, no. 9, pp. 5340–5348, Sep. 2015, https://doi.org/10.1109/JSEN.2015.2441113.

[11] R. F. Mansour and S. A. Parah, "Reversible Data Hiding for Electronic Patient Information Security for Telemedicine Applications," *Arabian Journal for Science and Engineering*, Jun. 2021, https://doi.org/10.1007/s13369-021-05716-2.

[12] N. O. Aljehane and R. F. Mansour, "Big data analytics with oppositional moth flame optimization based vehicular routing protocol for future smart cities," *Expert Systems*, 2021, Art. no. e12718, https://doi.org/10.1111/exsy.12718.

[13] N. Guizani and A. Ghafoor, "A Network Function Virtualization System for Detecting Malware in Large IoT Based Networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1218–1228, Jun. 2020, https://doi.org/10.1109/JSAC.2020.2986618.

[14] A. Malyshev, T. Biyachuev, and D. Ilin, "Systems and methods for malware classification," US8635694B2, Jan. 21, 2014.

[15] S. Edwards and I. Profetis, "Hajime: Analysis of a decentralized internet worm for IoT devices," Rapidity Networks, Oct. 2016.

[16] S. Sareen, S. K. Sood, and S. K. Gupta, "IoT-based cloud framework to control Ebola virus outbreak," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 3, pp. 459–476, Jun. 2018, https://doi.org/10.1007/s12652-016-0427-7.

[17] S. Elmalaki, B.-J. Ho, M. Alzantot, Y. Shoukry, and M. Srivastava, "SpyCon: Adaptation Based Spyware in Human-in-the-Loop IoT," in *2019 IEEE Security and Privacy Workshops (SPW)*, May 2019, pp. 163–168, https://doi.org/10.1109/SPW.2019.00039.

[18] X. de C. de Carnavalet and M. Mannan, "Privacy and Security Risks of 'Not-a-Virus' Bundled Adware: The Wajam Case," *arXiv:1905.05224 [cs]*, May 2019.

[19] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444–458, Dec. 2017, https://doi.org/10.1016/j.comnet.2017.09.003.

[20] C. Dong, G. He, X. Liu, Y. Yang, and W. Guo, "A Multi-Layer Hardware Trojan Protection Framework for IoT Chips," *IEEE Access*, vol. 7, pp. 23628–23639, 2019, https://doi.org/10.1109/ACCESS.2019.2896479.

[21] A. Lamba, S. Singh, and S. Balvinder, "Mitigating Zero-Day Attacks in IoT Using a Strategic Framework," *International Journal For Technological Research In Engineering*, vol. 4, no. 1, pp. 5711–5714, 2016, https://doi.org/10.2139/ssrn.3492684.

[22] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017, https://doi.org/10.1109/MC.2017.62.

[23] A. Marzano *et al.*, "The Evolution of Bashlite and Mirai IoT Botnets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2018, pp. 00813–00818, https://doi.org/10.1109/ISCC.2018.8538636.

[24] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, Jan. 2019, https://doi.org/10.1109/TSUSC.2018.2809665.

[25] R. Tahir, "A Study on Malware and Malware Detection Techniques," *International Journal of Education and Management Engineering*, vol. 8, no. 2, pp. 20–30, Mar. 2018, https://doi.org/10.5815/ijeme.2018.02.03.

[26] Q. Liu, X. Hong, S. Li, Z. Chen, G. Zhao, and B. Zou, "A spatial-aware joint optic disc and cup segmentation method," *Neurocomputing*, vol. 359, pp. 285–297, Sep. 2019, https://doi.org/10.1016/j.neucom.2019.05.039.

[27] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems," *IEEE Access*, vol. 7, pp. 118556–118580, 2019, https://doi.org/10.1109/ACCESS.2019.2917135.

[28] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Generation Computer Systems*, vol. 96, pp. 481–489, Jul. 2019, https://doi.org/10.1016/j.future.2019.02.064.

[29] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Computer Science Review*, vol. 32, pp. 24–44, May 2019, https://doi.org/10.1016/j.cosrev.2019.03.001.

[30] S. Wang, Z. Chen, Q. Yan, B. Yang, L. Peng, and Z. Jia, "A mobile malware detection method using behavior features in network traffic,"

Journal of Network and Computer Applications, vol. 133, pp. 15–25, May 2019, https://doi.org/10.1016/j.jnca.2018.12.014.

[31] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, and D.-H. Nguyen, "A survey of IoT malware and detection methods based on static features," *ICT Express*, vol. 6, no. 4, pp. 280–286, Dec. 2020, https://doi.org/10.1016/j.icte.2020.04.005.

[32] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Computer Science Review*, vol. 32, pp. 1–23, May 2019, https://doi.org/10.1016/j.cosrev.2019.01.002.

[33] W. Han, J. Xue, Y. Wang, Z. Liu, and Z. Kong, "MalInsight: A systematic profiling based malware detection framework," *Journal of Network and Computer Applications*, vol. 125, pp. 236–250, Jan. 2019, https://doi.org/10.1016/j.jnca.2018.10.022.

[34] Y. Borchani, "Advanced malicious beaconing detection through AI," *Network Security*, vol. 2020, no. 3, pp. 8–14, Mar. 2020, https://doi.org/10.1016/S1353-4858(20)30030-1.

[35] J. Álvarez Cid-Fuentes, C. Szabo, and K. Falkner, "An adaptive framework for the detection of novel botnets," *Computers & Security*, vol. 79, pp. 148–161, Nov. 2018, https://doi.org/10.1016/j.cose.2018.07.019.

[36] M. Alazab, M. Alazab, A. Shalaginov, A. Mesleh, and A. Awajan, "Intelligent mobile malware detection using permission requests and API calls," *Future Generation Computer Systems*, vol. 107, pp. 509–521, Jun. 2020, https://doi.org/10.1016/j.future.2020.02.002.

[37] U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories," *Future Generation Computer Systems*, vol. 95, pp. 467–487, Jun. 2019, https://doi.org/10.1016/j.future.2019.01.022.

[38] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Future Generation Computer Systems*, vol. 97, pp. 887–909, Aug. 2019, https://doi.org/10.1016/j.future.2019.03.007.

[39] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Computers & Security*, vol. 74, pp. 144–166, May 2018, https://doi.org/10.1016/j.cose.2018.01.001.

[40] A. Gupta, A. Anpalagan, G. H. S. Carvalho, A. S. Khwaja, L. Guan, and I. Woungang, "RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey," *Journal of Network and Computer Applications*, vol. 132, pp. 118–148, Apr. 2019, https://doi.org/10.1016/j.jnca.2019.01.012.

[41] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, pp. 93–106, Apr. 2018, https://doi.org/10.1016/j.jmsy.2018.04.007.

[42] R. Taheri, M. Ghahramani, R. Javidan, M. Shojafar, Z. Pooranian, and M. Conti, "Similarity-based Android malware detection using Hamming distance of static binary features," *Future Generation Computer Systems*, vol. 105, pp. 230–247, Apr. 2020, https://doi.org/10.1016/j.future.2019.11.034.

[43] P. Visu, L. Lakshmanan, V. Murugananthan, and Meenaloshini Vimal Cruz, "Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance," *Computer Communications*, vol. 147, pp. 14–20, Nov. 2019, https://doi.org/10.1016/j.comcom.2019.08.013.

[44] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications*, vol. 153, Mar. 2020, Art. no. 102526, https://doi.org/10.1016/j.jnca.2019.102526.

[45] M. Noor, H. Abbas, and W. B. Shahid, "Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis," *Journal of Network and Computer Applications*, vol. 103, pp. 249–261, Feb. 2018, https://doi.org/10.1016/j.jnca.2017.10.004.

[46] F. Ullah and M. Ali Babar, "Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review," *Journal of Systems and Software*, vol. 151, pp. 81–118, May 2019, https://doi.org/10.1016/j.jss.2019.01.051.

[47] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Computer Law & Security Review*, vol. 34, no. 3, pp. 450–466, Jun. 2018, https://doi.org/10.1016/j.clsr.2017.12.004.

[48] J. M. Ceron, C. B. Margi, and L. Z. Granville, "MARS: From traffic containment to network reconfiguration in malware-analysis systems," *Computer Networks*, vol. 129, pp. 261–272, Dec. 2017, https://doi.org/10.1016/j.comnet.2017.10.003.

[49] J. H. Abawajy, M. Chowdhury, and A. Kelarev, "Hybrid Consensus Pruning of Ensemble Classifiers for Big Data Malware Detection," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 398–407, Apr. 2020, https://doi.org/10.1109/TCC.2015.2481378.

[50] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware Dynamic Analysis Evasion Techniques: A Survey," *ACM Computing Surveys*, vol. 52, no. 6, pp. 126:1-126:28, Nov. 2019, https://doi.org/10.1145/3365001.

[51] Abhijit Mohanta, *Malware Analysis and Detection Engineering*, 1st ed. New York, NY, USA: Apress, 2020.

[52] C. S. Veerappan, P. L. K. Keong, Z. Tang, and F. Tan, "Taxonomy on malware evasion countermeasures techniques," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb. 2018, pp. 558–563, https://doi.org/10.1109/WF-IoT.2018.8355202.

[53] X. Carpent, N. Rattanavipanon, and G. Tsudik, "Probabilistic and Considerate Attestation of IoT Devices against Roving Malware," Cryptology ePrint Archive 2017/1216, 2017.

[54] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[55] S. Zafar, G. Miraj, R. Baloch, D. Murtaza, and K. Arshad, "An IoT Based Real-Time Environmental Monitoring System Using Arduino and Cloud Service," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3238–3242, Aug. 2018, https://doi.org/10.48084/etasr.2144.

[56] R. F. Mansour, S. Al-Otaibi, A. Al-Rasheed, H. Aljuaid, I. V. Pustokhina, and D. A. Pustokhin, "An Optimal Big Data Analytics with Concept Drift Detection on High-Dimensional Streaming Data," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 2843–2858, 2021, https://doi.org/10.32604/cmc.2021.016626.

[57] R. F. Mansour and M. R. Girgis, "Steganography-Based Transmission of Medical Images Over Unsecure Network for Telemedicine Applications," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 4069–4085, 2021, https://doi.org/10.32604/cmc.2021.017064.