Contents lists available at https://citedness.com/index.php/jdsi

Data Science Insights

Journal Page is available to https://citedness.com/index.php/jdsi

Research article

The need for an enhanced IoT-based malware detection model using Artificial Intelligence (AI) algorithm: A Review

Siti Sarah Maidin [1 ,*], *Norzariyah Yahya* [2]

[1] *INTI International University, Nilai, Malaysia*
[2] *International Islamic University Malaysia (IIUM), Malaysia*
email: [1,*] *sitisarah.maidin@newinti.edu.my*
** Correspondence*

ARTICLE INFO

Article history:
Received 03 02, 2023
Revised 05 01, 2023
Accepted 07 06, 2023
Available online 08 21, 2023

Keywords:
Malware detection
IoT
Security
Artificial Intelligence
Malicious

Please cite this article in IEEE style as:
S.S. Maidin, and N. Yahya, " The need for an enhanced IoT-based malware detection model using Artificial Intelligence (AI) algorithm: A Review, vol. 1, no. 1, pp. 50-54, 2023.

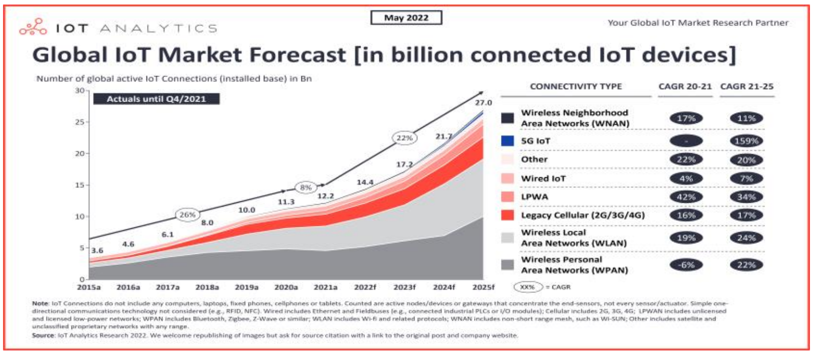
Correspondence:
Siti Sarah Maidin
INTI International University,
Nilai, Malaysia
sitisarah.maidin@newinti.edu.my

ABSTRACT

The interconnected world using technology has opened the door for cyberattacks. For example, the utilization of Internet of Things (IoT) devices has increased the exposure to malware attacks. The massive amount of data generated by the IoT devices leads to the possibility of infections in the network. Due to the diverse nature of the IoT devices and the ever-evolving nature of their environment, it can be challenging to devise very comprehensive security measures. Therefore, the application of Artificial Intelligence (AI) in detecting malware has gained attention as a suitable tool for detecting malware due to its strength in malware classification. This research aims to review malware detection in IoT devices using AI and its challenges.

1. Introduction

Internet of Things (IoT) technology has accelerated the development of computing devices. It is an emerging technology that enables smart devices connected via sensors to create and exchange data. IoT devices are constructed using a range of CPU architectures even on hardware with limited resources, like Unix-based operating systems [1]. Previously, malware attacks only personal computers. While the IoT continues to experience tremendous expansion across the globe, its security continues to lag far behind and the IoT devices were the target of more than 30% of all infections found in mobile network infrastructure [2]. Due to a lack of security design or implementation, IoT devices are growing in popularity as targets for attackers along with this transformation. IoT malware typically exhibits a number of traits, such as the ability to conduct DDoS attacks, search open ports for IoT services like FTP, SSH, or Telnet, and more [1]. As stated by [3], IoT devices have become an attractive target for cybercriminals since it is not closely monitored. Figure 1 depicts the Global IoT market forecast.



Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh, such as WI-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2022. We welcome republishing of images but ask for source citation with a link to the original post and company website.

Figure 1. Global IoT market forecast [4]

A hacker uses malware, which is malicious software, to monitor victims' keystrokes. In order to deceive users into downloading it, this spyware disguising itself as a regular program. Spyware, Adware, Trojan Horses, viruses, and Worm are examples of malware including:

a. Spyware: Used for the purpose of gathering information about a user and sending that information to another entity without first obtaining the user's consent. The term "spyware" refers to a variety of malicious software, including key loggers, tracking cookies, system monitors, and Trojan horses.
b. Adware: Displays obnoxious pop-up advertisements in order to earn money for its author. The malware may determine the user's preferences by monitoring the websites that are accessed. After that, it is able to send pop-up advertisements that are relevant to those sites.
c. Virus: One-way malware spreads is by embedding copies of itself into other programmes, or viruses. Following the execution of the programme, viruses infect computers by moving from one to another.
d. Worms: Like viruses, worms can spread from computer to computer by taking advantage of security holes in networks. Worms don't need a host programme to function. However, if the host has been attacked with the worm, it can quickly propagate throughout the connection.
e. Trojan Horses: A piece of malware known as a Trojan horse is a software package or a file that gives the appearance of being legitimate, but actually conceals harmful code within it that takes advantage of the privileges of the user who runs it.

The malware infected over 1.2 million IoT devices and targeted many popular online services such as Google, Amazon, etc [1]. Figure 2 illustrates the total malware detected from the year 2013 until 2022 while Figure 3 indicates the number of new malware from July 2020 until June 2022. It can be concluded that the number of malware keeps on increasing year by year due to technological advancement. Based on the rising trend of IoT devices and also the increasing numbers of malware, it is crucial to have an advanced algorithm which able to detect the malware in a speedy manner. Improving the security of IoT devices is becoming more vital for researchers.

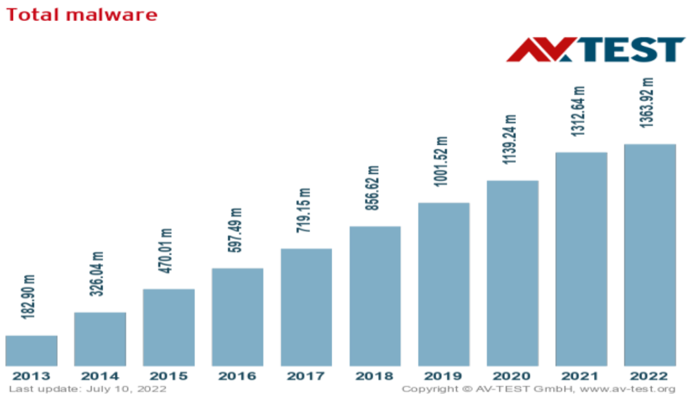


Figure 2. Total Malware from 2013 to 2022 [5]

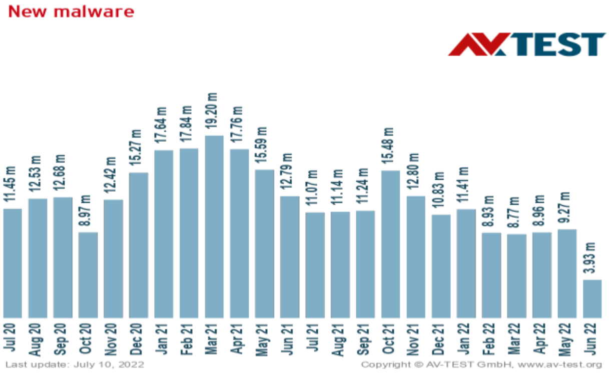


Figure 3. The number of new malware from July 2020 until June 2022 [5]

2. Literature Review

IoT is a vast and ever-growing array of connected devices. Many IoT malware families including Aidra, Bashlite, and Mirai are able to utilize scanners that are designed to identify vulnerable ports and credentials on the IoT devices [11]. In March 2019, IBM discovered a Mirai-like malware targeting at enterprises' IoT devices [11]. The popularity of DDoS-capable IoT malware is steadily increasing because malware authors will continue to mutate their malware for more critical infections on IoT devices [1]. The malware provides remote control to the attacker to use an infected system. Malicious software may compromise the privacy, security, and/or reliability of your data or system resources. For example, spyware and keylogger may attack the confidential authenticity and integrity of the data and system resources, Trojan Horse will impact the confidentiality and availability of the data and system resources while viruses can attack the integrity and availability of the data or system resources [6]. Figure 4 illustrates the types of attached in an IoT environment.

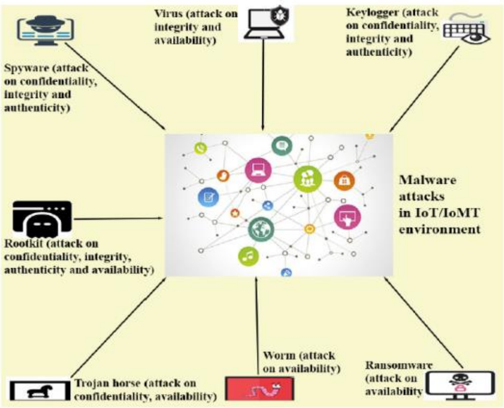

Virus (attack on integrity and availability)
Keylogger (attack on confidentiality, integrity and authenticity)
Spyware (attack on confidentiality, integrity and authenticity)
Malware attacks in IoT/IoMT environment
Rootkit (attack on confidentiality, integrity, authenticity and availability)
Worm (attack on availability)
Ransomware (attack on availability
Trojan horse (attack on confidentiality, availability)

Figure 4. Types of attacks in IoT environment [6]

Some of the active botnets which can launch various malware attacks in IoT environments include Mirai and Reaper [6]. Mirai is a kind of malware that provides the control of Linux operating system-based network devices to remote bots. Reaper is also called as IoTroop. It can compromise smart IoT devices very quickly as compared to the Mirai botnet. It is a variation of Mirai which uses twenty-six malicious scripts to spread itself. It was discovered by "Palo Alto Networks'' and designed to create a larger botnet. A mechanism for detecting malware on IoT devices was proposed by [7] which relies on blockchain technology and machine learning. Data about malware is automatically extracted by machine learning mechanisms, with the use of clustering and classification algorithms, and then stored on a distributed ledger. The proposed system uses the blockchain to reliably record the extracted features in a "distributed malware database," hence enhancing the effectiveness of run-time malware detection at high speeds and precision.

A recent survey conducted by [8] highlights security issues and risks of threats to IoT devices. Monitoring executing processes is resource-intensive, and in some cases, malware could infect real environments. The dynamic approach consists of analyzing and detecting malicious files without executing them. By contrast, static analysis can explore all possible execution paths without considering the diversity of processor architecture. In addition, [9] devised a method for detecting malware in internet-connected devices that they called EveDroid. It is a scalable and event-aware malware detection system for smart IoT devices. It detects malicious software by capturing the high-level semantics of Android applications running in an IoT context. The authors of this study included a technique that automatically converts calls made to an application programming interface into a feature vector based on the semantics of the data. This process was referred to by the authors as "function clustering." This resulted in the detection system becoming more resistant to the malware of this kind.

The application of machine learning to the detection of malicious software on these frequently unattended devices has produced encouraging results [2]. The majority of AI-based solutions for IoT security are either behaviour- or specification-based techniques, both of which are difficult to deploy in IoT systems [10]. Furthermore, the author has specified that the current technique in malware detection are: 1) signature-based technique which is not effective for a new or unknown malware because some malware is encrypted, and thus extracting the signature takes time and a large amount of processing energy 2) behavioural-based method is expensive to implement due to because each network software behaves differently 3) specification based-method precisely characterise a system's entire set of permissible behaviours but however it is very costly. Various research has been conducted to identify the challenges in detecting malware in IoT devices which include: the low computational power of IoT devices, the increasing number of malware, and the fast spread of malware to the IoT devices. The challenges need to be addressed using a robust, adaptive, and complex mechanism. Therefore, it can be concluded that there is a need to have enhanced IoT malware detection that offers foolproof protection against diverse forms of malware attacks. In addition, some of the existing techniques are attack-specific and do not protect against other sorts of attacks simultaneously. Therefore, we must create malware detection algorithms for IoT security that are resilient against numerous simultaneous malware attacks.

3. Conclusion

The effectiveness and efficiency of detecting harmful activity on IoT devices could be increased by enhancing the IoT-based malware detection model utilising an AI algorithm. Large-scale data analysis, pattern recognition, anomaly detection, and threat prediction are all possible with AI algorithms. This can aid in the speedy and accurate detection of malware on IoT devices and help to stop it from doing any damage. Additionally, an AI-based detection model has the capacity to learn and modify itself over time, increasing its efficiency in spotting new and developing malware types.

AI are increasingly being used in the detection of malware. These methods enable the development of more sophisticated and effective malware detection systems capable of adapting to new and evolving threats. One approach is to use AI to analyse software programme behaviour and identify patterns that indicate malware. A machine learning algorithm, for example, could be trained to recognise specific characteristics of a virus, such as how it spreads, the files it modifies, or the network connections it establishes. This method is known as behavioural detection. AI can also be used to enhance other malware detection techniques, such as signature-based detection and heuristic-based detection. By using AI to analyze large amounts of data and identify patterns, these systems can more accurately detect malware and reduce the number of false positives.

Another approach is to use AI to analyse the software code and identify any malicious instructions; this is known as static analysis. AI can be used to detect malware by analyzing patterns and behaviors in files and network traffic. Machine learning algorithms can be trained on known examples of malware to identify malicious software. One approach is to use deep learning to analyze the code of a file, looking for patterns and anomalies that indicate it may be malware. Another approach is to use behavioral analysis, where the AI system monitors the actions of a file or program to determine if it is behaving like malware. AI-based malware detection can be more effective than traditional signature-based detection methods, as it can detect new and unknown malware. However, AI-based malware detection can also be more prone to false positives and negatives and need to be updated frequently to adapt to new threats.

Therefore, the AI-based model would need to be properly trained on a wide range of IoT-related data, and it would need to be updated often in order to stay ahead of new and emerging risks. Malware has become a major security danger for the computing community, contributing to most Internet security issues. Malware remains a major concern on the Internet despite extensive research. Recently, Malware detection strategies and methodologies have been proposed. These strategies and approaches contain flaws that prevent problem elimination. As such, this paper proposes a new technique of using an AI algorithm to detect malware in an IoT environment.

References

[1] 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*, 6(4), 280–286, 2020, doi: 10.1016/j.icte.2020.04.005

[2] B. V. Dartel, “Malware detection in IoT devices using Machine Learning”, *35th Twente Student Conference on IT*, 2021, http://essay.utwente.nl/86854/

[3] Nokia, “Threat Intelligence Report 2020,” *Tech. Rep.*, 2020. [Online]. Available: https://onestore.nokia.com/asset/210088

[4] “Number of connected IoT devices growing 18% to 14.4 billion globally”. *IoT Analytics*, 2022 (May 18) https://iot-analytics.com/number-connected-iot-devices/

[5] AV-TEST, “Malware Statistics & Trends Report”, 2022. Retrieved September 17, 2022, from https://www.av-test.org/en/statistics/malware/

[6] M. Wazid, A.K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, “IoMT Malware Detection Approaches: Analysis and Research Challenges”. *IEEE Access*, 7, 182459–182476, 2019, Doi:

10.1109/access.2019.2960412

[7] R. Kumar, X. Zhang, W. Wang, R.U. Khan, J. Kumar, and A. Sharif, “A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features”, *IEEE Access*, 7, 64411–64430, 2019, Doi: 10.1109/access.2019.2916886

[8] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978.

[9] T. Lei, Z. Qin, Z. Wang, Q. Li and D. Ye, "EveDroid: Event-Aware Android Malware Detection Against Model Degrading for IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6668-6680, Aug. 2019, doi: 10.1109/JIOT.2019.2909745.

[10] H. Alrubayyi, G. Goteng, M. Jaber, and J. Kelly, “Challenges of Malware Detection in the IoT and a Review of Artificial Immune System Approaches”, *Journal of Sensor and Actuator Networks*, 10(4), 61, 2021, Doi: 10.3390/jsan10040061

[11] N. Kulkarni, “Internet of Things (IoT) Applications and Security” A Survey,” *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, 2020.