TechXplore

A 5G-enabled AI-based malware classification system for the next generation of cybersecurity

November 8 2022

Credit: Pixabay/CC0 Public Domain

The Industrial Internet of Things, or IIoT, has recently gained popularity due to its ability to create communication networks between different components of an industry and bring about the new revolution—Industry 4.0. Powered by wireless 5G connectivity and artificial intelligence (AI), IIoT holds the ability to analyze critical problems and provide solutions that can improve the operational performance of industries ranging from manufacturing to health care.

IoT is highly user-centric—it connects TVs, voice assistants, refrigerators, etc.—whereas IIoT deals with enhancing the health, safety, or efficiency of larger systems, bridging hardware with software, and carrying out data analysis to provide real-time insights.

However, while IIoT does have many advantages, it also comes with its share of vulnerabilities such as security threats in the form of attacks trying to disturb the network or siphoning resources. As IIoT is getting more popular in industries, it is becoming crucial to develop an efficient system to handle such security concerns. So, a team of multinational researchers led by Prof. Gwanggil Jeon from Incheon National University stepped up to the challenge

They took a deep dive into the world of 5G-enabled IIoT to explore its threats and come up with a novel solution to the problem. In a recent review published online on September 9, 2022 in *IEEE Transactions on Industrial Informatics*, the team presented an AI- and deep learning-based malware detection system for 5G-assisted IIoT systems.

Prof. Jeon explains the rationale behind the study: "Security threats can often lead to operation or deployment failure in IIoT systems, which can create high-risk situations. So, we decided to investigate and compare available research, find out the gaps, and propose a new design for a security system that can not only detect malware attacks in IIoT systems, but also classify them."

The system developed by the team uses a method called grayscale image visualization with a deep learning network for analyzing the malware, and further applies a multi-level convolutional neural network (CNN) architecture to categorize the malware attack into different types. The team also integrated this security system with 5G, which allows for low latency and high throughput sharing of real-time data and diagnostics.

Compared to conventional system architectures, the new design showed an improved accuracy that reached 97% on the benchmark dataset. They also discovered that the reason behind such high accuracy is the system's ability to extract complementary discriminative features by combining multiple layers of information.

This new malware classification system can be used to secure real-time connectivity applications such as smart cities and autonomous vehicles. It also provides solid groundwork for the development of advanced security systems that can curb a wide range of cybercrime activities.

"AI-based technology has dramatically changed our lives. Our system harnesses the power of AI to enable industries to recognize miscreants and prevent the entry of unreliable devices and systems in their IIoT networks," concludes Prof Jeon.

More information: Imran Ahmed et al, A Multi-layer Deep Learning Approach for Malware Classification in 5G-Enabled IIoT, *IEEE Transactions on Industrial Informatics* (2022). DOI: 10.1109/TII.2022.3205366

Provided by Incheon National University

Citation: A 5G-enabled AI-based malware classification system for the next generation of cybersecurity (2022, November 8) retrieved 27 April 2024 from https://techxplore.com/news/2022-11-5g-enabled-ai-based-malware-classification-cybersecurity.html