[Microcontrollers in IoT devices can be susceptible to several types of attacks](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf" \t "_blank)[1](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf)[2](https://ieeexplore.ieee.org/document/9065145/)[3](https://www.st.com/resource/en/application_note/dm00493651-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf)[4](https://www.particle.io/iot-guides-and-resources/mcu-vs-soc-vs-microprocessor-for-iot/)[5](https://towardsdatascience.com/training-a-deep-learning-model-to-detect-dos-attacks-on-microcontrollers-with-the-help-of-chatgpt-e548a56ff062):

1. [**Control Flow Manipulation Attacks**: These attacks manipulate the control flow of the microcontroller’s program, potentially leading to unintended behavior1](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf).
2. [**Side-Channel Attacks**: These attacks involve analyzing information gained from the physical implementation of a system, such as timing information, power consumption, or even sound to extract sensitive information1](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf).
3. [**Read-out Protection Bypass Attacks**: These attacks aim to bypass the read-out protection mechanisms of the microcontroller to gain access to protected information1](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf).
4. [**Denial of Service (DoS) Attacks**: These attacks aim to make a machine or network resource unavailable by disrupting the services of the host connected to the Internet5](https://towardsdatascience.com/training-a-deep-learning-model-to-detect-dos-attacks-on-microcontrollers-with-the-help-of-chatgpt-e548a56ff062).
5. [**Firmware Attacks**: These attacks exploit flaws in the firmware upgrade models of microcontroller-based IoT systems2](https://ieeexplore.ieee.org/document/9065145/).
6. [**Hardware Attacks**: These attacks involve manipulation of the hardware components of the microcontroller1](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf).

[It’s important to note that each open port and available IoT protocol is also a potential vulnerability4](https://www.particle.io/iot-guides-and-resources/mcu-vs-soc-vs-microprocessor-for-iot/). [Therefore, security should be an essential part of the development of IoT systems](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf)[5](https://towardsdatascience.com/training-a-deep-learning-model-to-detect-dos-attacks-on-microcontrollers-with-the-help-of-chatgpt-e548a56ff062). [Even if no system is completely secure, it is possible to make the attack more expensive](https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Study-on-Hardware-Attacks-against-Microcontrollers.pdf)[3](https://www.st.com/resource/en/application_note/dm00493651-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf).

[Training a Deep Learning Model to Detect DoS Attacks on Microcontrollers | by Déborah Mesquita | Towards Data Science](https://towardsdatascience.com/training-a-deep-learning-model-to-detect-dos-attacks-on-microcontrollers-with-the-help-of-chatgpt-e548a56ff062)