| Attack Type | Description | Research References | Dataset |
| --- | --- | --- | --- |
| 1.Cloud-Specific Attacks | Attacks targeting cloud infrastructures, exploiting vulnerabilities such as misconfigurations, insecure APIs, and data breaches. | 1. Towards Deep Federated Defenses Against Malware in Cloud Ecosystems https://ieeexplore.ieee.org/abstract/document/9014377 2. CELEST: Federated Learning for Globally Coordinated Threat Detection |  |
| IoT-Based Attacks | Exploits targeting IoT devices due to their limited security, including botnets, DDoS attacks, and spoofing. | 1. FedMADE: Robust Federated Learning for Intrusion Detection in IoT https://arxiv.org/html/2408.07152v1 2. Federated Learning for Decentralized DDoS Attack Detection in IoT Networks https://ieeexplore.ieee.org/abstract/document/10474358/ 3. Federated Learning for Malware Detection in IoT Devices https://arxiv.org/pdf/2104.09994 4. Federated Learning for IoT Intrusion Detection https://www.mdpi.com/2673-2688/4/3/28 | 1. CICIoT2023 Dataset https://arxiv.org/html/2408.07152v1 2. N-BaIoT Dataset https://arxiv.org/pdf/2104.09994 |
| Watering Hole Attacks | Attacks where adversaries compromise frequently visited websites to deliver malware to specific target groups. | 1. 'Watering Hole Attacks, Explained' https://www.splunk.com/en\_us/blog/learn/watering-hole-attacks.html |  |
| Command and Control (C2) Attacks | Techniques where attackers establish communication channels with compromised systems for remote control, often using botnets or malware. | 1. 'Detecting Cyberattacks Using Anomaly Detection in Industrial Control Systems: A Federated Learning Approach' https://www.researchgate.net/publication/353321363\_Detecting\_cyberattacks\_using\_anomaly\_detection\_in\_industrial\_control\_systems\_A\_Federated\_Learning\_approach | 1. CICIDS 2017 Dataset https://www.unb.ca/cic/datasets/malmem-2021-dataset.html |
| DNS Tunneling | A method of encoding data in DNS queries and responses to bypass security measures, often used for data exfiltration. |  |  |
| Logic Bombs | Malicious code that triggers harmful actions when specific conditions are met, often used in insider attacks or sabotage. |  |  |
| Advanced Persistent Threats (APTs) | Sophisticated, continuous attacks where intruders establish a long-term presence on a network to steal sensitive information, often targeting critical infrastructure or intellectual property. | 1. 'Robust Federated Learning for Mitigating Advanced Persistent Threats in Cyber-Physical Systems' https://www.mdpi.com/2076-3417/14/19/8840 2. 'A Federated Learning Approach for Multi-stage Threat Analysis in Advanced Persistent Threat Campaigns' https://arxiv.org/abs/2406.13186 | 1. CICIDS 2017 Dataset https://www.unb.ca/cic/datasets/malmem-2021.htm |