WILLIAM & MARY
CHARTERED 1693

WM-2102: Privacy-preserving online botnet classification system utilizing power footprint of IoT connected devices

Inventors: Gang Zhou, Sabbir Ahmed Khan. Chunsheng Xin, Yizhou Feng, Woosub Jung, Danella Zhao

Technology Field: Computer science, Internet of Things, Cybersecurity

Technology Summary: The patented system is a privacy-preserving botnet detection and mitigation technology designed for Internet of Things (IoT) devices. It uses a smart auditor to monitor and analyze power consumption patterns of IoT devices, leveraging machine learning to detect anomalies indicative of botnet activity. The system can autonomously shut down compromised devices to prevent further damage while ensuring data privacy through advanced encryption protocols. This technology addresses a critical gap in IoT security by offering a novel, privacy-preserving solution that is both effective and scalable. It holds significant potential for commercialization in industries increasingly reliant on connected devices.

Key Innovations

- Power Footprint Analysis: Utilizes IoT device power consumption data as a unique identifier to detect botnet activity, reducing reliance on traditional network traffic monitoring.
- Machine Learning Integration: Employs algorithms trained on historical power usage data to distinguish between normal and malicious behaviors.
- Autonomous Mitigation: Automatically generates commands to disconnect compromised devices upon detecting anomalies.
- Privacy-Centric Design: Implements encryption protocols to protect sensitive data, ensuring secure communication and safeguarding the integrity of the detection models.

Potential Applications

- IoT Security: Enhances protection for smart home devices, industrial IoT systems, and connected healthcare equipment.
- Enterprise Networks: Safeguards corporate IoT ecosystems, such as smart offices and supply chain sensors.
- Critical Infrastructure: Secures IoT deployments in energy grids, transportation systems, and public safety networks from botnet attacks.

Competitive Edge

- Innovative Detection Approach: Unlike traditional methods that rely on network traffic analysis, this system uniquely focuses on power consumption patterns, making it harder for attackers to evade detection.
- Proactive Defense: The ability to autonomously mitigate threats in real-time minimizes downtime and reduces the risk of widespread botnet infections.
- Scalability: Designed to handle diverse IoT environments with varying device types and usage patterns.
- Data Privacy Assurance: Prioritizes user privacy with robust encryption measures, addressing growing concerns about data security in IoT ecosystems.

Licensing Status: Available for license

Intellectual Property: Issued United States patent 12,015,622

Contact Information: Jason McDevitt (757-221-1751); jason.mcdevitt@wm.edu