**LITERATURE SURVEY**

**TITLE:** "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection"

**ABSTRACT:** Currently, expert systems and applied machine learning algorithms are widely used to automate network intrusion detection. In critical infrastructure applications of communication technologies, the interaction among various industrial control systems and the Internet environment intrinsic to the IoT technology makes them susceptible to cyber-attacks. Given the existence of the enormous network traffic in critical Cyber-Physical Systems (CPSs), traditional methods of machine learning implemented in network anomaly detection are inefficient. Therefore, recently developed machine learning techniques, with the emphasis on deep learning, are finding their successful implementations in the detection and classification of anomalies at both the network and host levels. This paper presents an ensemble method that leverages deep models such as the Deep Neural Network (DNN) and Long Short-Term Memory (LSTM) and a meta-classifier (i.e., logistic regression) following the principle of stacked generalization. To enhance the capabilities of the proposed approach, the method utilizes a two-step process for the apprehension of network anomalies. In the first stage, data pre-processing, a Deep Sparse AutoEncoder (DSAE) is employed for the feature engineering problem. In the second phase, a stacking ensemble learning approach is utilized for classification. The efficiency of the method disclosed in this work is tested on heterogeneous datasets, including data gathered in the IoT environment, namely IoT-23, LITNET-2020, and NetML-2020. The results of the evaluation of the proposed approach are discussed. Statistical significance is tested and compared to the state-of-the-art approaches in network anomaly detection.

**TITLE:** "A survey of IoT malware and detection methods based on static features"

**ABSTRACT:** Due to a lack of security design as well as the specific characteristics of [IoT](https://www.sciencedirect.com/topics/engineering/internet-of-things" \o "Learn more about IoT from ScienceDirect's AI-generated Topic Pages) devices such as the heterogeneity of processor architecture, IoT [malware](https://www.sciencedirect.com/topics/engineering/malware) detection has to deal with very unique challenges, especially on detecting cross-architecture IoT malware. Therefore, the IoT malware detection domain is the focus of research by the security community in recent years. There are many studies taking advantage of well-known dynamic or [static analysis](https://www.sciencedirect.com/topics/computer-science/static-program-analysis) for detecting IoT malware; however, static-based methods are more effective when addressing the multi-architecture issue. In this paper, we give a thorough survey of static IoT malware detection. We first introduce the definition, evolution and security threats of IoT malware. Then, we summarize, compare and analyze existing IoT malware detection methods proposed in recent years. Finally, we carry out exactly the methods of existing studies based on the same IoT malware dataset and an experimental configuration to evaluate objectively and increasing the reliability of these studies in detecting IoT malware.

**TITLE:** "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey"

**ABSTRACT:** Through three development routes of authentication, communication, and computing, the Internet of Things (IoT) has become a variety of innovative integrated solutions for specific applications. However, due to the openness, extensiveness and resource constraints of IoT, each layer of the three-tier IoT architecture suffers from a variety of security threats. In this work, we systematically review the particularity and complexity of IoT security protection, and then find that Artificial Intelligence (AI) methods such as Machine Learning (ML) and Deep Learning (DL) can provide new powerful capabilities to meet the security requirements of IoT. We analyze the technical feasibility of AI in solving IoT security problems and summarize a general process of AI solutions for IoT security. For four serious IoT security threats: device authentication, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks defense, intrusion detection and malware detection, we summarize representative AI solutions and compare the different algorithms and technologies used by various solutions. It should be noted that although AI provides many new capabilities for the security protection of IoT, it also brings new potential challenges and possible negative effects to IoT in terms of data, algorithm and architecture. In the future, how to solve these challenges can serve as potential research directions.

**TITLE:** "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey",

**ABSTRACT:** The Internet of Things (IoT) has emerged as a technology capable of connecting heterogeneous nodes/objects, such as people, devices, infrastructure, and makes our daily lives simpler, safer, and fruitful. Being part of a large network of heterogeneous devices, these nodes are typically resource-constrained and became the weakest link to the cyber attacker. Classical encryption techniques have been employed to ensure the data security of the IoT network. However, high-level encryption techniques cannot be employed in IoT devices due to the limitation of resources. In addition, node security is still a challenge for network engineers. Thus, we need to explore a complete solution for IoT networks that can ensure nodes and data security. The rule-based approaches and shallow and deep machine learning algorithms- branches of Artificial Intelligence (AI)- can be employed as countermeasures along with the existing network security protocols. This paper presented a comprehensive layer-wise survey on IoT security threats, and the AI-based security models to impede security threats. Finally, open challenges and future research directions are addressed for the safeguard of the IoT network.

**TITLE:** "The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives",

**ABSTRACT:** The past decade has seen a rapidly growing interest in IoT-connected devices. But as is usually the case with computer systems and networks, malicious individuals soon realized that these objects could be exploited for criminal purposes. The problem is particularly salient since the firmware used in many Internet connected devices was developed without taking into consideration the expertise and best security practices gained over the past several years by programmers in other areas. Consequently, multiple attacks on IoT devices took place over the last decade, culminating in the largest ever recorded DDoS attack, the Mirai botnet, which took advantage of weaknesses in the security of the IoT. In this survey, we seek to shed light on the evolution of the IoT malware. We compare the characteristic features of 28 of the most widespread IoT malware programs of the last decade and propose a novel methodology for classifying malware based on its behavioral features. Our study also highlights the common practice of feature reuse across multiple malware programs.