**Machine learning based solutions for security of Internet of Things (IoT): A survey**

*by Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos*

**A summary of the research paper**

*by Shashank Agarwal*

**Introduction**

IoT devices are objects embedded with specialized hardware, and connect to the internet with a wireless network to collect and share data. They contain sensitive data of the users which must be protected from potential threats. They usually transmit data to and fro servers wirelessly, which make them more vulnerable to attacks.

Machine learning is the study of computer algorithms that can improve automatically through experience and by the use of data. Thus machine learning is effective against zero-day vulnerabilities.

**Security of Internet of Things**

Surveys have predicted an exponential increase in the use of IoT devices, reaching 75 billion devices by 2025. Due to its limited computing functionality and use of open network, sometimes without authentications, its security is a matter of serious concern.

An IoT architecture consists of three layers:

1. *Application layer*: The layer with which the users interact, through mobile or web applications.

2. *Network layer:* The layer through which users connect with the devices using Wi-Fi, Bluetooth, etc.

3. *Perception layer:* It has sensors for sensing and gathering information about the environment.

**Attacks in IoT**

**Active Attacks:**

1. *Denial of service (DoS):* Sending excessive amount of requests which disrupt services if they are not filtered. Distributed Dos is a type of attack in which DoS is performed through multiple IPs.

2. *Spoofing and Sybil attack*: attackers attempt to obtain personal information by pretending to be the legitimate user or users.

3. *Jamming Attack:* a subset of DoS attacks in which malicious nodes block legitimate communication by causing intentional interference in networks.

4. *Man-in-the-middle attack*: Connecting to the IoT device by pretending to be part of the network.

5. Selective forwarding attacks: Attacker Intentionally drops data packets before it gets to the user.

6. *Malicious input attacks*: inject malicious script into the IoT device to cause damage.

7. *Data tampering*: modifying data, usually in-transit, to disrupt someone’s privacy.

**Passive Attacks:**

*Eavesdropping* and *traffic analysis* are the main two ways to perform a passive attack through an IoT network. Network analysis is monitoring the networks to collect user’s information.

**Surface Attacks:**

There are four attack surfaces-

1. *Perception surface*: This includes physical devices. They carry confidential information of users.

2. *Network surface*: User’s information is transmitted openly, which motivates attackers to find vulnerabilities in the network.  
3. *Cloud surface*: remote storage of user’s data which may be prone to being read, modified or deleted by an attacker.

4. *Web and application surface*: Some IoT devices use mobile or web application interface to interact with their users. This opens up another surface for the attackers to launch different malicious attacks to access IoT devices with/without a user’s permission.

**Other Attacks:**

Social surface attacks refer to social engineering where the user is manipulated into giving out sensitive information. The interconnectedness of IoT devices also opens doors for new attack methods.

**Effects of attacks**

The listed IoT attacks pose a threat to the following features:  
1. *Identification* prevents the attacker from masquerading as the user.

2. *Authorization* limits the accessibility the attacker has to the user’s information.

3. *Accessibility* guarantees only the authorized user has the access to their information.

4. *Privacy* ensures confidentiality of user’s data from attackers.

5. *Integrity* prevents modification of user’s information by an unauthorized user.

**Machine learning (ML) in IoT security**

Machine learning techniques are different algorithms that can be used for IoT’s security. They are:

1. **Supervised learning**- This technique uses well labelled datasets (or inputs) to predict outcomes.

**Classification Learning**: Dividing output into predetermined groups or classes. It includes:

*Support Vector Machine (SVM):* This method uses hyperplane to classify data points. Data points falling on either side of the hyperplane can be attributed to different classes. It is one of the most robust prediction methods, making it suitable for detecting intrusion, malware, smart grid attack, etc.

*Bayesian Theorem:* Prediction of class of unknown data sets based on Baye’s theorem. This way of classification technique is called Naive Bayes (NB).

*K-nearest neighbor (KNN):* KNN relies on finding the Euclidian distances between a query and all the examples in the data, then using this distance to classify data points into classes. It has a major drawback of becoming significantly slows as the size of that data in use grows.

*Random Forest (RF):* This method uses several Decision trees, collectively called random forest, whose output is the class selected by most trees. It is used to detect DDoS attacks.

*Associated Rule (AR):* This technique is used to find unknown relations among large sets of data. It has been used for intrusion detection, but due to the large amount of time taken by its algorithm, it is not suitable for use in IoT.

**Regression Learning:** This technique is used to predict continuous values. It aims to plot a best-fit curve between the data. It includes:

*Decision Tree (DT):* It is a classification and predication method in which each internal node denotes a test on an attribute, each branch represents an outcome of the test, and each leaf node (terminal node) holds a class label. It is used for DDoS and intrusion detection.

*Neural Network (NN):* It mimics the way how neurons work, but are difficult to use in IoT.

*Ensemble Learning (EL):* Combines multiple algorithms to improve predictive power and is used for anomaly, malware and intrusion detection.

**2. Unsupervised learning-** There are no predetermined classes. The algorithm tries to identify patterns within the data set and groups them in clusters. There is no output data.

*Principal Component Analysis (PCA):* Decreases time complexity by converting large data set into smaller ones. It can be used for detecting real time intrusion attacks.

*K-mean clustering:* In this method, clusters of the given data samples is formed. It is useful in IoT system when labelled data is not required. However, it is less effective compared to supervised learning. This method is usually used in anomaly and Sybil attack detection.

**3. Reinforcement learning (RL) –** In reinforced learning, atrial and error method is employed to the model to make a sequence of decisions. A reward might be associated with each correct decision.

**ML based solution for IoT security**

Machine learning solutions are categorized based on the architectural layers of IoT:

**1. Perception layer:**

Radio fingerprinting is a process that identifies radio transmitter by the "fingerprint" that characterizes its signal transmission. This method is not sufficient for securing due to false negatives. A reinforcement learning method, Q-learning, was observed to substantially reduce auth errors.

Supervised ML techniques such as Distributed Frank Wolf and Incremental Aggregated Gradient were applied to determine the model’s parameters in order to reduce the communication overhead and increase the efficiency of spoofing detection. Besides these, unsupervised learning like Incremental Gaussian Mixture Model (IGMM) is used to ensure the authentication of IoT devices.

**2. Network layer:**

A support vector machine based model was capable of detecting 99.4% of attacks. ML classifier algorithms have also been used for device identification, thus preventing attacks by non-IoT devices. The authors comment that *identification in the variation of accuracy and training data set* can be a potential research topic.

Another research used time intervals between packets and calculated endpoints to detect DDoS attacks in local IoT devices. They had compared KNN, KDTree, LSVM, DT and RF using Gini impurity scores, and NN; all of which had an accuracy higher than 0.99.

**3. Web/application layer:**

One of the research concluded that RF methods with data set of MalGenome give better detection rate than K-NN. In another research, Q-learning performed better in detecting latency and accuracy than Dyna-Q-based detection learning method.

**Research Challenges**

**Data Security –** Providing high-quality training data set is an important challenge in ML techniques for effective security of the IoT network. We can use data augmentation based on the existing data to sufficiently train the model. Identifying different kinds of attacks and the probability of their occurrence in the network is a critical future research field in IoT.

**Computational Restriction and Exploitation of Algorithms –** Machine learning algorithms consume large memory and computation power, and IoT devices provide limited resources. So ML methods must be improved to be incorporated with IoT.

**Privacy Leakage –** IoT devices carry confidential and sensitive information/data of the users, there is a possibility for it to be misused if it’s leaked. So they must be properly encrypted and follow basic protocols.

To provide defence against zero-day vulnerabilities, IoT security needs to adopt an intelligent and real-time updated machine learning algorithm to detect unknown attacks.

RF, SVM and DT have been the most popular ML algorithms in IoT security in recent years.