Chapter 1: Theoretical Framework

1.1 INTRODUCTION

The Internet of Things (IoT) [1] is a large group of devices containing sensors or actuators connected together over wired or wireless networks. IoT has been rapidly growing over the past decade. During the growth, security has been identified as one of the weakest areas in IoT. To approach the challenges in securing IoT devices, we propose using machine learning within an IoT gateway to help secure the system.

Types of IoT Attacks:

- **Physical cyber-attacks:** These attacks result from breaches to the IoT device's sensors. Click to read more about vulnerabilities of IoT embedded devices [2]. It's estimated that approximately 70% of all cyber-attacks are initiated from the inside, whether purposeful or the result of human error. With an IoT physical cyber-attack, the hacker most often accesses the system through close proximity, like inserting a USB drive. Tampering can enable the intruder to take over the controls, extract data, and/or infuse the system with malicious code (similar to malware) that opens a door to the system without being noticed. Hackers can also strike with a distributed denial of service (DDoS) that basically shuts down the system. Another physical cyber-attack hits the batteries in the devices and the system. While you think you have them set to sleep mode, the power is actually draining from the batteries.
- **Network cyber-attacks:** These don't require physical access to create a major disruption—like DDoS—in your network. These attackers gain access to your network devices to see what's flowing. They can insert themselves between user and user devices also as known as Man in the Middle [2], creating fake identities, stealing information, and redirecting packets to their desired location, away from user network. It is also referred to as a sinkhole attack.
- **Software attacks**: The third area that poses an IoT security risk is your software. Software attacks occur when malware is installed into your network's program. This malicious software [2] sends a virus, corrupts or steals data, and can both interrupt and spy on the activities. A software attack can launch a DDoS, too.
- **Encryption attacks**: Finally, Encryption attacks strike at the heart of our algorithmic system. Hacker analyze and deduce our encryption keys, to figure out how we create that algorithms. Once the encryption keys [2] are unlocked, cyber-attackers can install their own algorithm and take control of the system.

As reported by CERT/CC in the year 2008 in comparison to 1998 the number of discovered vulnerabilities has increased by a factor of 25 resulting in an average of 20 new vulnerabilities per day. Although not all of these flaws may spawn severe network attacks, the growth indicates a basic problem with developing secure network software and is one root of insecurity in today's Internet.

Case Study:

The Mirai Botnet (The day of DDOS):

In 2016, the first wave of IoT security attacks brought down the Internet. The Mirai Botnet [8] hacked into some Internet of Things devices. In this case mainly routers and Internet Protocol (IP) cameras — and transformed the devices into botnets. The centrally-controlled IoT botnets flooded Dyn's, a Domain Name Services (DNS) provider, traffic causing a disruptive bottleneck that blocked Internet access for millions of users worldwide. The Mirai malware code is easily accessible and adaptable, which makes it harder to prevent its effects. Hackers modify the code to create unique strains of the malware with its own novel Internet interruption tactics while dodging security solutions used in previous iterations of the malware.

Dahua:

March 5, 2017, major IoT device manufacturer Dahua [9] learned about a software flaw when a researcher discovered he could bypass authentication on some devices, possibly allowing for display of usernames and hashed passwords. While a hashed password is great, simple encryption makes for simple cracking. Dahua issued immediate patches, but we should know about this attack because of Dahua's size (it's the second largest IoT hardware manufacturer) and again, because of the implications, if they can't harden devices before release, who can.

Miele: Washer/Sanitizer Gets Dirty

In November 2016, a German researcher discovered a vulnerability in the Miele Professional PG 8528 appliance, a washing and sanitizing device for medical instruments, such as those used in surgery and laboratory work. When the researcher, Jens Regel, informed the company, he didn't receive a response for three months. The Web Server Directory Traversal vulnerability allows remote attackers to access directories other than the directories needed by web server, giving them the ability to thieve data and insert and initiate malicious code. With no patch released, the bug persisted, leaving hospital systems vulnerable. Not only is health-related data highly sensitive and subject to strict compliance mandates, but an attack executed via malware injected into a device such as this could render a hospital unable to operate, potentially affecting revenue, reputation and literal life.

IDS (Intrusion Detection System)

An intrusion detection system (IDS) [3] is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses. Several types of IDS technologies exist due to the variance of network configurations. Each type has advantages and disadvantage in detection, configuration, and cost.

1.2 Types of Intrusion Detection System:

1. Network-Based Intrusion Detection System
2. The Host Intrusion Detection System
3. Network Behavior Anomaly Detection
4. Wireless Intrusion Detection System

Network-Based Intrusion Detection System: A Network Intrusion Detection System (NIDS) [4] is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity. Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once. A term becoming more widely used by vendors is "Wireless Intrusion Prevention System" (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks. The NIDS are also called passive IDS since this kind of systems inform the administrator system that an attack has or had taken place, and it takes the adequate measures to assure the security of the system. The aim is to inform about an intrusion in order to look for the IDS capable to react in the post. Report of the damages is not sufficient. It is necessary that the IDS react and to be able to block the detected doubtful traffics. These reaction techniques imply the active IDS.

The Host Intrusion Detection System: Host Intrusion Detection System (HIDS) [4] can be classified in two types The HIDS Based Application. The IDS of this type receive the data in application, for example, the logs files generated by the management software of the database, the server web or the firewalls. The vulnerability of this technique lies in the layer application. The HIDS Based Host. The

IDS of this type receive the information of the activity of the supervised system. This information is sometimes in the form of audit traces of the operating system. It can also include the logs system of other logs generated by the processes of the operating system and the contents of the object system not reflected in the standard audit of the operating system and the mechanisms of logging. These types of IDS can also use the results returned by another IDS of the Based Application type. Host-based intrusion detection systems (HIDS) analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. A HIDS must be installed on each machine and requires configuration specific to that operating system and software. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Network Behavior Anomaly Detection: Network behavior anomaly detection (NBAD) [4] views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and baselining to determine the nominal amount of a segment's traffic. The NIDS-HIDS combination or the so called hybrid gathers the features of several different IDS. It allows, in only one single tool, to supervise the network and the terminals. The probes are placed in strategic points, and act like NIDS and/or HIDS according to their sites. All these probes carry up the alerts then to a machine which centralize them all, and aggregate the information of multiple origins.

Wireless Intrusion Detection System: A wireless local area network (WLAN) [4] IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Many previous NIDS tools will include enhancements to support wireless traffic analysis. Some forms of IDPS are more mature than others because they have been in use much longer. Network based IDPS and some forms of host-based IDPS have been commercially available for over ten years. Network behavior analysis software is a somewhat newer form of IDPS that evolved in part from products

created primarily to detect DDoS attacks, and in part from products developed to monitor traffic flows on internal networks. Wireless technologies are a relatively new type of IDPS, developed in response to the popularity of wireless local area networks (WLAN) and the growing threats against WLANs and WLAN clients.

1.2 Detection Types

Signature-Based Detection: Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available.

Anomaly-Based Detection: Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious. Most of the existing IDSs suffer from the time-consuming during detection process that degrades the performance of IDSs. Efficient feature selection algorithm makes the classification process used in detection more reliable.

Stateful Protocol Inspection: Stateful protocol inspection is similar to anomaly based detection, but it can also analyze traffic at the network and transport layer and vender-specific traffic at the application layer, which anomaly-based detection cannot do.

It is currently not feasible for an IDS to be perfect, primarily because network traffic is so complicated. The erroneous results in an IDS are divided into two types: false positives and false negatives. False positives occur when the IDS erroneously detects a problem with benign traffic. False negatives occur when unwanted traffic is undetected by the IDS. Both create problems for security administrators and may require that the system be calibrated. A greater number of false positives are generally more acceptable but can burden a security administrator with cumbersome amounts of data to sift through. However, because it is undetected, false negatives do not afford a security administrator an opportunity to review the data. IDPSs cannot provide completely accurate detection; they all generate false positives (incorrectly identifying benign activity as malicious) and false negatives (failing to identify malicious activity.

Machine Learning

Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves.

The process of learning begins with observations or data, such as examples, direct experience, or instruction, in order to look for patterns in data and make better decisions in the future based on the examples that we provide. The primary aim is to allow the computers learn automatically without human intervention or assistance and adjust actions accordingly. Machine learning algorithms are often categorized as supervised or unsupervised. Machine learning enables analysis of massive quantities of data. While it generally delivers faster, more accurate results in order to identify profitable opportunities or dangerous risks, it may also require additional time and resources to train it properly. Combining machine learning with AI and cognitive technologies can make it even more effective in processing large volumes of information.

Formally, dependencies can be represented as a learning model θ that is inferred from data using a learning function g. The model θ parameterizes a prediction function f θ that allows extrapolating dependencies to unseen data. To see how intrusion detection fits into this framework of learning. Below categorize learning methods using the paradigm of supervised and unsupervised learning.

Supervised learning: Supervised learning as the name indicates a presence of supervisor as teacher. Basically supervised learning is a learning in which we teach or train the machine using data which is well labeled that means some data is already tagged with correct answer. After that, machine is provided with new set of examples (data) so that supervised learning algorithm analyses the training data (set of training examples) and produces a correct outcome from labeled data. For instance, suppose we are given a basket filled with different kinds of fruits. Now the first step is to train the machine with all different fruits one by one like this:

- If shape of object is rounded and depression at top having color Red then it will be labelled as –Apple.
- If shape of object is long curving cylinder having color Green-Yellow then it will be labelled as –Banana.

In the supervised setting, data from the domain X provided for learning is labeled from a set Y. These labels can take the form of classes, numbers or even structures the instances of X are assigned to. The task is to learn a model θ, such that labels can be predicted on unseen data. Thus, g and f (θ) are defined as follows:

$$g : (\mathcal{X} \times \mathcal{Y})^n \rightarrow \theta \quad \text{and} \quad f_\theta : \mathcal{X} \rightarrow \mathcal{Y},$$

Where n denotes the size of the learning set. Examples for supervised learning are classification and regression. In the realm of intrusion detection this concept corresponds to misuse detection, where labeled data is used for learning a discrimination between normal and attack instances.

Supervised learning classified into two categories of algorithms:

- Classification: A classification problem is when the output variable is a category, such as “Blue” or “Green” or “disease” and “no disease”.
- Regression: A regression problem is when the output variable is a real value, such as “Height” or “Calories”.

Unsupervised learning: Unsupervised learning is the training of machine using information that is neither classified nor labeled and allowing the algorithm to act on that information without guidance. Here the task of machine is to group unsorted information according to similarities, patterns and differences without any prior training of data.

Unlike supervised learning, no teacher is provided that means no training will be given to the machine. Therefore machine is restricted to find the hidden structure in unlabeled data by our-self. For instance, suppose it is given an image having both dogs and cats which have not seen ever.

Thus machine has no any idea about the features of dogs and cat so we can’t categorize it in dogs and cats. But it can categorize them according to their similarities, patterns and differences i.e., we can easily categorize the above picture into two parts. First may contain all pics having dogs in it and second part may contain all pics having cats in it. Here user didn’t learn anything before, means no training data or examples.

Unsupervised learning classified into two categories of algorithms:

- Clustering: A clustering problem is where user want to discover the inherent groupings in the data, such as grouping customers by purchasing behavior.
- Association: An association rule learning problem is where user want to discover rules that describe large portions of your data, such as people that buy X also tend to buy Y.

Semi-supervised learning: is a kind of learning process which combines both labeled and unlabeled examples to generate an appropriate function or classifier.

Reinforcement learning: is the algorithm that learns a policy of how to act given an observation of the world. Every action has some impact in the environment, and the environment provides feedback that guides the learning algorithm.

The most widely used Supervised Learning algorithms are:

- Analytical learning
- Artificial neural network
- Backpropagation
- Boosting
- Bayesian statistics
- Case-based reasoning
- Decision tree learning
- Inductive logic programming
- Gaussian process regression
- Genetic Programming
- Group method of data handling
- Kernel estimators
- Learning Automata
- Learning Classifier Systems
- Minimum message length (decision trees, decision graphs, etc.)
- Multilinear subspace learning
- Naive Bayes classifier
- Maximum entropy classifier
- Conditional random field
- Nearest Neighbor Algorithm
- Probably approximately correct learning (PAC) learning
- Ripple down rules, a knowledge acquisition methodology
- Symbolic machine learning algorithms
- Subsymbolic machine learning algorithms
- Support vector machines
- Minimum Complexity Machines (MCM)
- Random Forests
- Ensembles of Classifiers
- Data Pre-processing

- Handling imbalanced datasets
- Statistical relational learning
- Proaftn, a multicriteria classification algorithm

To understand which algorithm is more appropriate for processing and decision-making on smart data generated from the things in IoT, it is essential to consider the following three concepts. First, the IoT application. Second, the IoT data characteristics and third, the data-driven vision of machine learning algorithms.

PROBLEM DEFINITION:

OBJECTIVES:

1. To study Supervised Machine Learning technique that are applicable to IoT environment.

2. To design an Intrusion Detection algorithm using Supervised Machine Learning technique for IoT Environment.

MATERIAL AND METHODS:

METHODOLOGY: Machine Learning, IoT, Signature IDS.

MATERIALS: Linux OS and Python.

Task Name	Start	Finish	Duration	Feb 19	March 19	April 19	May 19
Planning	1/2/19	10/2/19	10 days				
Literature Review	11/2/19	12/3/19	30 days				
Data Collection	13/3/19	22/3/19	10days				
Design	23/3/19	6/4/19	15days				
Coding	7/4/19	6/5/19	30days				
Testing	7/5/18	14/5/19	9days				
Deployment	14/5/19	21/5/19	8days				
Documentation	5/8/18	5/11/18	114days				

Figure 1: Gantt chart

Chapter 2: Literature Survey

2.1 Related Work

B.Santos Kumar, and his team in their research paper titled “Intrusion Detection System- Types and Prevention” [4] discussed different types of the techniques and types of the intrusion detection and prevention systems. It also provides in-depth description of the evaluation, comparison and classification features of the IDS and the IPS. Both the intrusion detection systems and the intrusion prevention systems still need to be improved to ensure an unfailing security for a network. This paper provided a new way of looking at network intrusion detection research including intrusion detection types that are necessary, complete, and mutually exclusive to aid in the fair comparison of intrusion detection methods and to aid in focusing research in this area.

Saroj Kr. Biswas in his research paper titled “Intrusion Detection Using Machine Learning: A Comparison Study” [6], proposes an IDS using machine leaning for network with a good union of feature selection technique and classifier by studying the combinations of most of the popular feature selection techniques and classifiers. In this paper a set of significant features is selected from the original set of features using feature selection techniques and then the set of significant features is used to train different types of classifiers to make the IDS.

Nutan Farah Haq and his team in their research paper titled “Application of Machine Learning Approaches in Intrusion Detection System: A Survey” provides overview where a number of techniques for intrusion detection have been described. It also provides a statistical overview of articles over the years on the algorithms that were frequently used, the datasets for each experiment and the consideration of feature selection step.

Mohammad Saeid and his team in their paper titled “Machine learning for internet of things data analysis: a survey” assesses the various machine learning methods that deal with the challenges presented by IoT data by considering smart cities as the main use case. The key contribution of this paper is the presentation of a taxonomy of machine learning algorithms explaining how different techniques are applied to the data in order to extract higher level information. The potential and challenges of machine learning for IoT data analytics is discussed. A use case of applying a Support Vector Machine (SVM) to Aarhus smart city traffic data is presented for a more detailed exploration.

In this paper "Expert Systems with Applications" written by has reviewed which technique has been used and what are the experiments that has been conducted in the past 2000 - 2007 and what should

be considered as a future work for the prevention and detection of the anomaly going on the network. Further they have described about the machine learning techniques such as

- Pattern classification
- Single Classifier
- K-nearest neighbor
- Support vector machines
- Decisions Trees

And further they have discussed about the type of the classifiers namely single hybrid and ensemble and the type of datasets used for the experiment. And lastly they have concluded from the research of 2000-2007 they have come to the conclusion that machine learning in IDS still needs to be improved for that the research process for future is encouraged in this paper.

In this paper "IDS Using Machine Learning - Current State of Art and Future Directions " published on 21st march 2016 focus on the behavior of an attacker is trying to be predicted by placing oneself on the place of an attacker and in contrast of that behavior the counter as in IDS algorithm are designed. Further the paper discuss about the techniques employed in IDS similarly like in paper the type of datasets are been discussed performance parameters used to check the effectiveness of the works surveyed. Various problems pertaining to current IDS and their possible solutions as well as the future research directions have been discussed.

In the paper "Machine Learning Algorithm of Detection of DOS Attacks on an Automotive Telematics Unit" by Eric Perraud has focused on the attacks that can be caused on the vehicle which are connected to the internet he says that the more the year passes the more the vehicle are connected to the public internet. Hackers can attack the wireless connectivity unit of the vehicle with Distribution Denial of Services (DDOS) attacks, so that the wireless connectivity unit of the vehicle is not available and the service is lost Therefore, it is critical to developing a mechanism to detect such an attack and eliminate it, to maintain the availability of the wireless connectivity unit This paper proposes an algorithm which proceeds in 2 steps: it uses an unsupervised machine learning algorithm to detect DDOS attacks in the incoming Internet data. When it detects an attack, it uses the results of the machine learning algorithm to split the legitimate flow and the rogue flows. The rogue flow is filtered so that the availability of the wireless connectivity unit of the vehicle is restored. This proposed algorithm needs very few CPU computing power and is compatible with low-cost CPUs which are used in an automotive wireless connectivity unit.

In this paper "Intrusion Detection System for Internet of Things" written by Tariqahmad Sherasiya, Hardik Upadhyay has discussed about the Lightweight Intrusion Detection System to detect Hello flood attack and Sybil attack in IoT network. Though the encryption and authentication of packets are not feasible in the world of IoT it says that among many other issues, security issue of IoT cannot be ignored. IoT devices are accessed from anywhere via untrusted network like the internet so IoT networks are unprotected against a wide range of malicious attacks. If security issues are not addressed then the confidential information may be leaked at any time. Thus, the security problem must be addressed the types of cyber-attacks discussed in paper are Sinkhole Attack , Wormhole Attack , Selective Forwarding Attack, Sybil Attack, Hello Flood Attack, Denial of Service (DOS) Attack The architecture of IDS: All sensor nodes are connected to internet using IPv6 border router (6BR). The placement for IDS system uses hybrid approach, in which Centralized module on 6BR (GIDS) and Distributed module (NIDS) on the sensor nodes which cooperates with each other to detect attacks. Centralized module detects the hello flood attack and distributed module detects the Sybil attack and attacker.

References

1. Brown Eric (13 September 2016) Who Needs the Internet of Things? Linux.com.
2. Perera, C.; Liu, C. H.; Jayawardena, S. (December 2015). "The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey". IEEE Transactions on Emerging Topics in Computing. 3 (4): 585–59
3. S. N. Pawar Associate Professor (E &TC), Jawaharlal Nehru Engineering College, Aurangabad, MS, India. Intrusion Detection in Computer Network Using Genetic Algorithm Approach: A Survey International Journal of Advances in Engineering & Technology, May 2013. ©IJAET
4. B.Santos Kumar, T.Chandra Sekhara Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar, "Intrusion Detection System- Types and Prevention", B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 77 - 82.
5. A data processing algorithm in epc internet of things Cyber-enabled Distributed Computing and Knowledge Discovery (CyberC), 2014 International Conference on, IEEE (2014), pp. 128-131
6. Saroj Kr. Biswas, "Intrusion Detection Using Machine Learning: A Comparison Study", International Journal of Pure and Applied Mathematics Volume 118 No. 19 2018, 101-114
7. Nutan Farah Haq, Md. Avishek Khan Hridoy, Abdur Rahman Onik, Dewan Md. Farid, "Application of Machine Learning Approaches in Intrusion Detection System: A Survey", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, Vol. 4, No.3, 2015
8. Mohammad Saeid,Mahdavinejad Mohammadreza Rezvan, Mohammadamin Barekatain Peyman, Adibi PayamBarnaghi and Amit P.Sheth, "Machine learning for internet of things data analysis: a survey", Computer Network, 54 (15) (2010), pp. 2787-2805