Efficient Security Solutions for IoT Devices

Faleh Alfaleh[1] Salim Elkhediri[2]
Department of Information Technology
College of Computer, Qassim University, Buraydah, Saudi Arabia

***Abstract*—The Internet of Things (IoT) is a technological innovation that has revolutionized society. The IoT will forever change the way we use simple things that do very little things to smart, fully capable things. IoT devices can process and automate everyday household and workplace tasks through simple sensors. Yet despite the benefits of these devices, they are vulnerable to violations such as privacy issues and security breaches. This paper aims to provide a clearer understanding of the IoT and current threats to it by explaining why IoT devices are susceptible to attack. Moreover, the technologies used in the IoT are examined, as well as the different communication layers of the IoT and their functioning. The findings reveal that IoT devices are prone to many software and hardware vulnerabilities, not to mention the challenges that come with IoT. Solutions to these challenges are proposed, notably through the use of anomaly-based intrusion detection systems, which are critical components of network security. Using machine learning (ML) to detect potential attacks is recommended. Many proposed anomaly-based detection systems use different ML algorithms and techniques. However, there is no standard benchmark to compare these in terms of power consumption. A benchmark that measures both accuracy and power consumption to calculate and evaluate each algorithm's implementation is proposed.**

Keywords*—*Efficient; IoT; Systems on a Chip (SoC); ML; Network

I. Introduction

The world is undergoing a rapid and exciting transformation because of the wide availability of systems on a chip (SoCs), as shown in Fig. 1. SoCs enable the creation of very intricate and small computer models that are able to connect to the network.

When an SoC connects to the Internet, it become the Internet of Things, forming an essential foundation for many utilities. Our everyday lives rely on their functionality and the quality of their operations. For example, industrial applications. Traditional security approaches are typically more expensive for IoT in terms of energy usage as well as overhead costs. Most security frameworks, in the event of a threat, tend to be centralized. They are therefore not appropriate for devices with a distributed network, given the difficulty of size, the existence of increased traffic and the single point of failure [2]. Acquiring data through multiple aspects of the industrial life cycle may significantly improve performance, thereby allowing a company to collect more data and monitor their industrial operations.

Moreover, many new devices can be linked to the network. Such systems tend to use most of their resources and computing power for the application's key features; thus, ensuring protection and privacy at a lower cost will be extremely difficult. For example, the primary differentiator between elliptic curve cryptography (ECC) and Rivest Shamir Adleman (RSA) is the key size compared with cryptographic strength. ECC can deliver much smaller key sizes with the same cryptographic strength as an RSA system. A 256-bit ECC key, for example, is equal to a 3072-bit RSA key [3]. This growing threat has prompted the development of new strategies to detect and block IoT botnet attack traffic. Recent research has highlighted the promise of machine learning (ML) in identifying malicious Internet traffic [4]. Nevertheless, ML models mainly targeting IoT application networks or IoT attack flux have met with limited success. Thankfully, IoT traffic often varies from other Internet-connected products (e.g., notebooks and smartphones) [5].

The rest of this paper is organized accordingly. First, IoT layers will be presented with the wireless network technology options and the characteristics of each technology. Then the most common attacks on IoT devices and the core design challenges of IoT devices will be covered. After that, a review of recent related literature will be discussed. Then we will give an overview on the UNSW-NB15 dataset. Then, anomaly-based intrusion detection method will be introduced with six classifiers. The purposed solution will be presented with the methodology on how to evaluate Intrusion Detection System (IDS) performance. The analyzed results will be provided with and without the purposed solution. Finally, we will summarize our work and mention the future work.

Fig. 1. Raspberry Pi SoC [1].

II. Internet of Things

Although the term "Internet of Things" is being used more frequently in everyday life, there is no universal definition of what IoT truly means. The term was first used in 1999 by Kevin Ashtonof, one of the members who created a global standard system for the Radio Frequency Identification (RFID) at the Massachusetts Institute of Technology [6][7].

A. *Internet of Things Technologies*

Deploying a large number of devices with limited memory and storage capabilities increases the threat to IoT applications. This is because attackers can take advantage of this weak IoT device capability to penetrate connected IoT applications. To understand the security issues related to the IoT, first we need to understand the way in which the IoT works. Some of the network technologies used in IoT:

1) Short-Range Device (SRD): Short range devices or SRDs are radio frequency transmitters used to transmit information. Their ability to cause harmful interference to other radio equipment is very low. SRDs are low power transmitters; depending on the frequency range, their effective radiated power (ERP) is usually limited to 25 to 100 megawatts or less, which limits their effective range to a few hundred meters and does not require user permission. Most of the SRD protocols are considered personal area networking (PAN). Most used SDR in IoT environment:

a) Radio Frequency Identification (RFID): An SRD that is frequently used in the IoT environment is RFID. This technology allows circuit boards with radio frequency design for wireless connections to transmit data. Tags perform the automatic identification of objects.

b) Bluetooth: Bluetooth is used for data transmission via radio waves, allowing two or more devices to connect. It is considered a short-range wireless technology. Further, Bluetooth Low Energy (BLE) protocols are well suited to the IoT because these are designed and enhanced for short-range use, low bandwidth, and low latency application. [8].

c) ZigBee: Zigbee has low energy consumption; therefore, it has many uses in smart homes, for example, for smart lighting. However, because its range is short, it is typically used in mesh networks where data are passed from one device to another until they reach their destination. This makes Zigbee ideal for the IoT. [9].

2) Wireless Fidelity (Wi-Fi) IEEE 802: Wireless Fidelity or Wi-Fi is a well-known wireless communication protocol. It offers very high data rates with a longer range than Bluetooth or RFID. IEEE 802.11ax is the most recent version [10]. with speeds reaching 600 to 9 608 megabits per second [11]. Wi-Fi can connect to various frequencies, such as 2.4, 5, 6, and 60 gigahertz. Depending on the frequencies, the range, speed, and power will vary.

3) Cellular networks: Cellular networks depend on the region or cell covered by the communication station. Each cell will provide the IoT application to move between sites. Example of a cellular network is the 5G communication protocol, which is an open standard under the supervision of GPP3. These networks currently support the requirements for 5G mobile communications. As of 2020, 5G networks have two types of bands which are 1- “Mid-band” uses frequencies of 2.5 to 3.7 gigahertz, currently allowing speeds of 100 to 900 megabits per second, with several miles of radius. And the “High-band” uses frequencies of 25 to 39 gigahertz to achieve download speeds of 1 to 3 gigabits per second. It only has a range of about one mile of radius.

4) Low-Power Wide-Area Network (LPWAN): Low Power Wide Area Network or LPWAN is a wide-area network with low power consumption, resulting in very low speeds. This type of network was intended for use in large areas, with simple commands, such as a smart light sign. LPWAN data rates are very low, ranging between 0.3 and 50 kilobits per second with long-range communications of up to 40 kilometers. Example of LPWAN is Long Range Wide Area Network (LoraWAN) which is a low-cost, long-range, low-power wireless platform that can be used in many IoT applications. It uses the frequencies of 433, 868, and 915 megahertz with a bit rate of 3 to 5 kilobits per second. LoRa-enabled devices can survive with a battery for years in sleep mode. In Fig. 2 we can see A comparison of Cellular networks in terms of data rate and range.

B. *Internet of Things Layers*

Every IoT device has at least three layers, namely, the network layer, the data processing layer, and the application layer, as shown in Fig. 3. Further, some applications have a fourth, sensing layer, not unlike a camera.

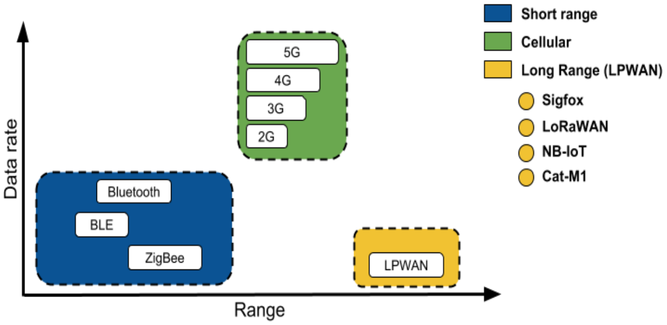


Fig. 2. A Comparison of Cellular Networks Data Rate and Range[12].

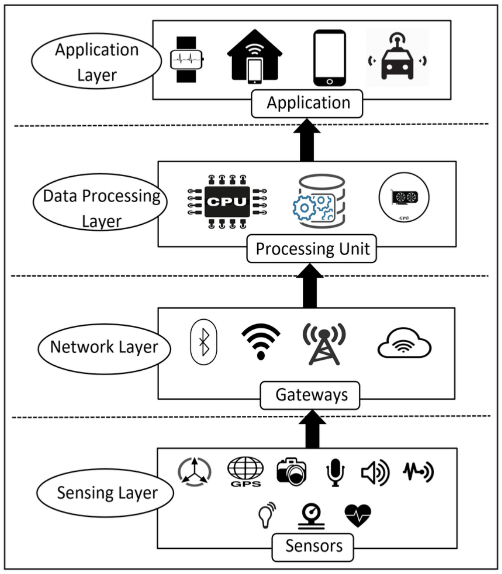


Fig. 3. IoT Architecture Layers [13].

Each layer has its unique components and role to play. These roles are not interchangeable, and each has its own technologies. The first layer contains specific applications for the IoT, for example, cloud computing platforms and middleware technology. The second layer includes data processing units such as a Central Processing Unit or Graphics Processing Unit. These are mainly used for collecting and processing data and controlling other objects. The third layer contains networks including access control, firewalls, and gates. This layer also contains technology such as 5G networks, ad hoc networks, and Wi-Fi. Different network transmissions have different technologies. Last, the sensing layer includes the technology needed to collect information, such as images, location, sound, and many other collected data from the environment. The data are then sent to the processing unit via the network layer.

C. Attacks on the Internet of Things

As the IoT evolves, the full definition of protection must be re-examined. Individuals and organizations are increasingly using IoT devices to improve productivity. The greater the number of users, the higher the chance of an attack or a vulnerability. For example, a large number of malicious nodes that used CCTV may have been part of a disseminated denial-of-service (DoS) attack from an individual home [14]. Some of the main attacks:

1) Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: As the IoT evolves, the full definition of protection must be re-examined. Individuals and organizations are increasingly using IoT devices to improve productivity. The greater the number of users, the higher the chance of an attack or a vulnerability. For example, a large number of malicious nodes that used CCTV may have been part of a disseminated denial-of-service (DoS) attack from an individual home [15].

2) Spoofing attack: Spoofing nodes impersonate the legitimate IDs of IoT devices such as media access control or RFID tags to gain illegal access to IoT systems. These attacks may launch other attacks, such as DoS and man-in-the-middle (MITM) attacks [16].

3) Jamming attack: In jamming attacks, the attacker sends corrupt transmitted packets to interrupt the continuous wireless transmission of the IoT device, exhausting bandwidth, power, CPU, and memory resources of the and this prevents the device from sending a signal leading to a series of system crashes. These may have serious consequences, especially in IoT applications that involve human health or internal security [17]. One example is opening a door while jamming the security sensor, as shown in Fig. 4, which results in a security breach.

4) Man-In-The-Middle (MITM) attack: In an MITM attack, the attacker can read and change contact between two parties believed to be communicating directly with each other. An example of an MITM attack is active eavesdropping, in which the attacker establishes independent communication with the victims and transmits messages between the victims, leading them to believe that they are talking directly to each other via a dedicated connection. At the same time, the entire conversation are with the attacker. The attacker is thus able to intercept all relevant messages that have been passed between the two victims, and is also able to send new messages.

5) Malware attacks: Malware attacks consist of viruses, worms, Trojans, or rootkits. These attacks behave similarly to attacks on traditional networks. Usually, the attacker uses malware to gain sensitive data or access sensitive or critical industrial infrastructure [18].

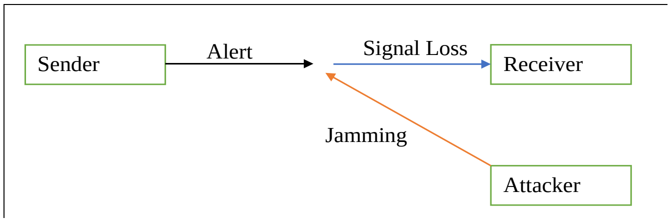


Fig. 4. Jamming Attack.

D. Challenges of The Internet of Things

The IoT is faced with many challenges from a wide variety of standards and applications, with different capabilities in terms of processing power and memory. With many traditional threats and new threats every single connection could make the networks vulnerable. Most IoT devices marketed with many features without carefully planning for security in the long term. Some of the main challenges of the IoT are described in the following sections.

1) Lack of standard: There are no standard IoT each device with its unique spaces and technology; most IoT devices that are released onto the market have at least one different wireless module or type of controller.

2) Privacy concerns: Recent developments in the IoT have introduced IoT devices into our homes, our doors, our cars—even into stores, such as Amazon’s self-service grocery stores [19]. Therefore, it is becoming increasingly difficult to protect personal privacy and prevent the unsolicited collection of personal information. Moreover, different attacks can violate personal identity and location [20].

3) Distributed nature: The ability to distribute devices according to need and required distance means it is difficult to manage a large number of distributed devices.

4) Insecure physical interface: Several physical factors compound the threats to the proper functioning of IoT devices. This is especially so when sensors and equipment are installed in a public area, making them vulnerable to physical attack.

5) Scalability: The IoT is a scalable technology, which creates many challenges, for example, the need for scalable technology and algorithms.

6) Specification: Each IoT device has different capabilities in terms of processing power, storage, RAM, and battery. For that, considering what type of security solution used is critical.

7) Real-Time: IoT devices are required to be used in real time. Because sensors are included in IoT systems, fast and stable sensor is a must to ensure continuous real-time performance. Therefore, even for embedded devices with limited functionality, the IoT system must support the device or user in real time.

III. Literatrue Review

A literature review of recent works on the security in resource-constrained devices like IoT devices. These devices remain one of the most cost-effective solutions for many day to day applications. The quantity of devices connected to the Internet continues to grow at a steady pace. A recent forecast from the International Data Corporation estimates that there will be 41.6 billion connected IoT devices, generating 79.4 zettabytes of data in 2025 [21].

A. Related Work

Sicari et al.[22] The authors discuss the confidentiality, authentication, data security issues, network security, and intrusion detection systems and the continuing lack of communication standards. Proper implementations must be developed and implemented regardless of the system used to guarantee security, access control, and the privacy of users and objects as well as the performance of the devices Compliance of specific policies on security and data protection. Despite many attempts in this field, many challenges and research problems remain. In particular, the author maintains that there is still a lack of systems and a unified vision to ensure the security of the Internet of Things. Then the author provides an analysis of international projects in this field, indicating that these efforts usually aim to design and implement specific applications of the Internet of Things. The study is also concerned with the need to address the use of IoT technologies, also communications into protected middleware, capable of meeting specific security constraints.

Hongchun et al.[23] proposed a knowledge-based intrusion detection strategy to detect multiple types of attacks under different types of network structures. The purpose was to create an independent detection model that depends on the structure of the WSN network. The suggested mechanism was based on the fact that different types of attacks may have different forms of density. The authors collected network traffic and used it as a feature of random network behavior in the feature space. The density form can be considered an indication of normal and abnormal network behavior. Simulation results from attacks, such as a sinkholes, flooding, or DoS, indicate that the method had the appropriate detection accuracy and high compatibility with the network structure.

Stergiou et al.[24] Present the IoT with a cloud computing survey that reflects on and how to secure the security problems on both technologies they specifically combine the two technologies as mentioned earlier (i.e., cloud and computing and IoT) to examine the usual attributes and to find out about the advantages of their integration. They demonstrate how the security problems of IoT integration can be strengthened by cloud computing. The theoretical application design and the integration of IoT and Cloud Computing with security benefits are further analyzed by the two encryption algorithms which are used (AES and RSA).

Doshi et al.[25] Presented that high precision DDoS attacks in IoT traffic may be identified with several machine learning algorithms, including neural networks, through the use of IoT network behavior to notify feature attacks. The results suggest that main gateways or other central network boxes will classify locally based IoT DDoS attack sources automatically using inexpensive machine learning algorithms and an independent flow-based traffic-based data protocol. DoS identification can reliably differentiate between usual and DoS attack traffic by using the packet level machine learning for IoT consumer devices. They used a small set of features to reduce computational overhead, which is essential for the real-time identification and deployment of the middlebox. Their selection of features was based on the assumption that network traffic habits for IoT applications clients differentiate from those of well-known non-IoT networked devices. The test array accuracy of all five algorithms reached 0.99. The way they test this is shown in Fig. 5. These initial findings inspire further studies on anomaly machine learning to protect IoT devices.

Damopoulos et al. [26] discusses the importance of IDS for mobile devices and the importance of personal files designed for each user in order to create an effective IDS to prevent an attack. They measured several algorithms in the Phone activity data set they built and recorded the results. The authors found that they could detect anomaly with high accuracy. They also collected some useful indicators for each algorithm used in mobile phone identifiers. Their main focus was on creating IDSs that can be used with the data set and specifically for an anomaly.

Moreover, a related work comparison for all previous studies was provided in Table I.

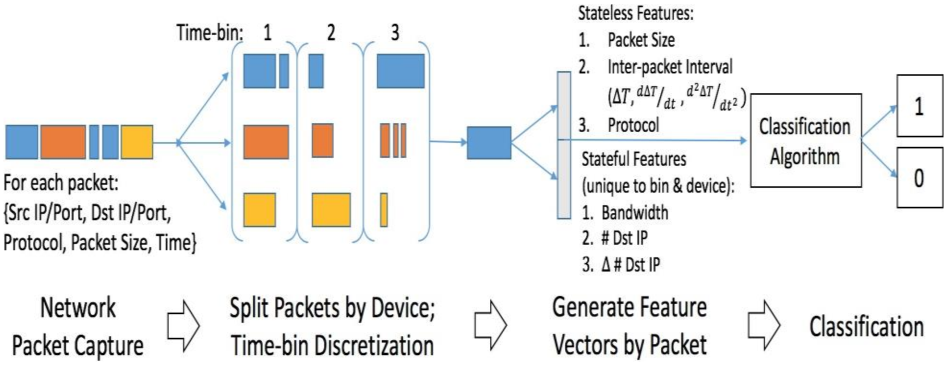


Fig. 5. IoT DDoS Detection Pipeline [25].

TABLE I. RELATED WORK COMPARISON

Paper Title	About	Advantage	Disadvantage
Security, privacy and trust in the Internet of things: The road ahead [22]	Internet of Things Survey	Present challenges and the existing solutions that may help in the field of IoT security.	The authors do not indicate in deep the physical challenges faced IoT in terms of resources.
An Adaptive Intrusion Detection Method for Wireless Sensor Networks [23]	IDS	The authors proposed a knowledge-based intrusion detection strategy (KBIDS) to detect multiple forms of attacks.	The authors proposed IDS for the WSN generally, but they do not consider the limited resources.
Secure integration of IoT and Cloud Computing [24]	Cloud Crypto-graphy	The authors suggested cloud computing as a solution for IoT integration to processing and dealing with data.	The authors did not discuss their solution practically.
Machine learning DDoS detection for the consumer internet of things devices [25]	IDS	The authors purposed an IDS that detect DDoS attack by using lightweight machine learning algorithms.	The authors only discuss the DDoS attack.
Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers [26]	IDS	The author reviewed and present the important of using IDS on mobile devices and how it impacts on discovering anomaly.	The author only suggests a standard that can be used for future research.

IV. UNSW-NB15 DATASET

The UNSW-NB15 dataset was designed at the Cyber Range Lab of the Australian Centre for Cyber Security at the University of New South Wales [27].

A. Why UNSW-NB15

UNSW-NB15 was chosen because it is one of the most recent datasets, compared to using older datasets such as the KDD Cup 99 dataset and the NSLKDD dataset, which lack new low-fingerprint attack methods and do not include the most recent normal traffic scenarios. As a result, it can accurately represent both traditional network traffic and multiple botnets cyberattacks. IXIA PerfectStorm was used to create the dataset. This tool mixes legitimate user network traffic with malicious network traffic [27].

B. UNSW-NB15 Attacks

In this dataset, there are nine types of attacks, namely, Fuzzers, Analysis, Backdoor, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, as shown in Table II.

The detailed number of instances in each category can be found in Table III.

TABLE II. ATTACK TYPES [27]

Attack	Description
Exploit	This attack exploit a glitch, bug, or vulnerability of a host or network.
Fuzzers	This is an attack that tries to discover security loopholes in a system and by flood it with random data until it crashes.
DoS	This attack disrupts the computer resources via flood the system with requests, making it too busy to be accessing a device.
Analysis	This is a type of intrusion that attacks web applications via ports, emails, or web scripts.
Backdoor	This is a technique of stealthily bypassing authentication, and provide unauthorized remote access.
Reconn-aissance	This can be defined as a probe; probing attacks involve a method to gain information about a network, for example, port scanning.
Generic	This is a technique used against block cipher using a hash function to collision without looking how the configuration of the block cipher.
Shellcode	This is an attack in which the attacker exploit vulnerability in a program to open remote shell to control the compromised machine.
Worm	This is an attack that can replicates itself to spread to other computers via the network.

TABLE III. NUMBER OF INSTANCES OF EACH ATTACK TYPE OF UNSW-NB15 DATASET [27]

Category	Total number
Normal	93 000
Analysis	877
Backdoor	2 329
DoS	16 353
Exploits	44 525
Fuzzers	24 346
Generic	58 871
Reconnaissance	13 987
Shellcode	1 511
Worms	174
Total number of attacks	164 673
Total	257 673

V. ANOMALY USING MACHINE LEARNING

With the growing popularity of the Internet and the widespread use of computers and IoT devices, the opportunities for attacks have increased in smart and industrial IoT applications. It is difficult to counter this problematic environmental advantage using traditional techniques to detect traffic anomalies. This emerging threat has prompted the development of new techniques to identify and block attacks. In this paper, supervised learning techniques were used, namely, the Decision Table, K-nearest neighbor (K-NN), Decision Tree, LogitBoost, Naive Bayes and Random Forest.

A. *Machine Learning and Classification Algorithms*

The ML technique known as classification is used to distinguish attacks or intrusions from ordinary events that occur in the network. It analyzes a given dataset and assigns the instance to a particular class to minimize classification error and extract models that accurately define important data classes within the given dataset. Most ML algorithms can be classified according to the expected structure of the model. In this paper, the focus is on classification. This refers to ML algorithms that are provided with a labeled training dataset. In this paper, the UNSW-NB15 training dataset was used to build the classification model. Fig. 6 shows two types of ML. The first uses supervised ML and the second uses unsupervised ML.

For classification, six classifiers were chosen because of their accuracy while maintaining a reasonable time for testing. These are discussed below.

1) Decision tree: A decision tree resembles a flowchart; it uses a supervised classification technique and consequently, it requires a labeled training dataset such as the UNSW-NB15 dataset to construct a decision tree. This is done by repeating the input data through a learning tree [29].

2) Random forest: A random forest is a mixture of tree predictors. Each tree depends on random vector values that are sampled independently, with the same distribution for all trees in the forest [30].

3) Decision table: A decision table is a descriptive visual representation of actions to be performed based on conditions. An algorithm's output represents a set of operations that build in the decision-making table. A decision table can be used to describe and analyze a situation. The decision is taken based on the number and interrelationships of conditions [31].

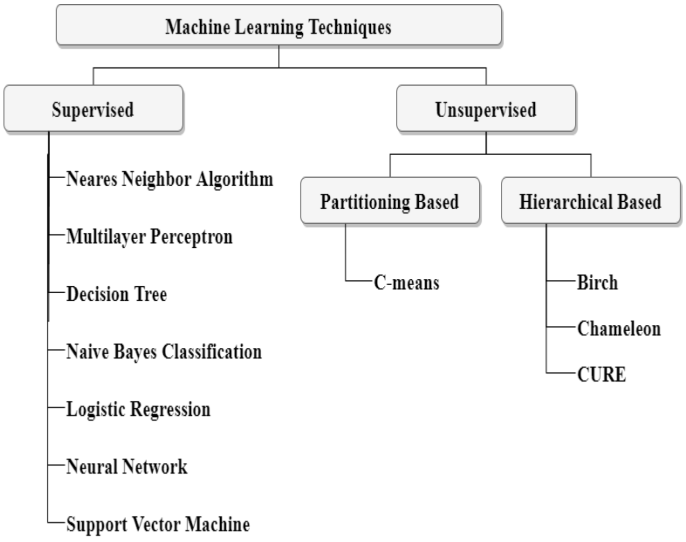


Fig. 6. Machine Learning Techniques[28].

4) K-nearest neighbour (K-NN): The K-NN classifier uses a supervised learning algorithm. This algorithm does not build a model; instead, it uses a distance measure to locate K. "Close" instances in the training data for each test instance and uses those selected instances to make a prediction. This function is calculated concerning K the nearest point, so the K-nearest neighbors do not need high computing power to run. This factor, in addition to the relative readings of adjacent nodes, makes neighboring neighbors a distributed learning algorithm suitable for WSNs [32].

5) Naive bayes: Naive Bayes is a simple probability classifier used to represent binary and multi-class classification problems. It is assumed that the value of a variable affects a specific class independently of the values of other variables. This assumption reduces the number of parameters. In practical terms, this is not a serious problem because even if this assumption does not apply to the data being analyzed, a naive Bayesian model performs well while significantly reducing computation time without sacrificing performance [33].

6) LogitBoost: This is an algorithm from the "boosting" category. It works by training a series of weak models (e.g., regression, boosting algorithms focus on increasing the ability of prediction). This algorithm was written by Jerome Friedman, Trevor Hastie, and Robert Tibshirani in 1998 [34]. It was designed to address the ability of AdaBoost to deal with noise and outliers. LogitBoost's algorithm uses a probability binomial logarithmic equation, which changes the loss function linearly. In comparison, AdaBoost uses the exponential loss function, which changes greatly with classification error. Therefore, LogitBoost is more effective to outliers and noise in general.

VI. Evaluation Methodology

The methodology on how to evaluate IDS ML that operates in the IoT environment, comparing the accuracy results while also taking into account efficiency. To use ML, compare different algorithms and evaluate the performance of each algorithm in the IDS, the evaluation methods discussed below were used.

A. *Performance Measurement*

IDS creates alarms (intrusion) detecting general conditions of attack and normal behaviour. This behaviour is identified as

- True-positive (TP): The number of actual attacks detected.
- *True-negative (TN):* The number of regular activities detected as normal.
- *False-positive (FP):* (intrusion Missed) The number of attacks detected as regular traffic.
- *False-negative (FN):* The number of regular activities detected as an attack.

Table IV shows a simple metrics to identify each of the classifier output.

The percentage number of true alarms and false alarms for each classifier is then provided and the correct number of "Intrusions Detected" or "Intrusions Missed" measured. Then the overall accuracy of the classifier is indicated.

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{\text{total number of instances}} \quad (1)$$

$$\text{Missed Intrusions} = \frac{\text{missed intrusions}}{\text{total number of intrusions} * 100} \quad (2)$$

B. Feature Selection

Selecting the features from a dataset is a way of improving the efficiency of ML algorithms. Some of the data in the dataset are irrelevant, redundant, or noisy features. Feature selection reduces the number of features by removing irrelevant, redundant, or noisy features. Feature selection speeds up the ML algorithm; it can improve learning accuracy, and lead to better model comprehensibility [35]. As shown in Fig. 7 the info gain attribute evaluation method was used, which is a Filter feature selection method that uses statistical techniques to evaluate the relationship between each input variable and the target variable with low computation power. It employs a ranked system that assigns a value from 0 to 1 for each attribute. Those attributes with higher value have a higher information value and can be selected in the optimal feature, while those with lower information value are removed.

C. Evaluation of Power Consumption

Metrics regarding power consumption were collected, as in the time, the classifier needs first to build the model then testing it. After that, the time needed to finish the task will be used to calculate the power consumption.

TABLE IV. CONFUSION METRICS

	Is the IDS correct?	
	Yes	**No**
Attack	True positive (TP) = Actual Attacks	False-positive (FP) = Intrusion Missed
Normal	True negative (TN) = Actual Normal	False-negative (FN) = False Alarm

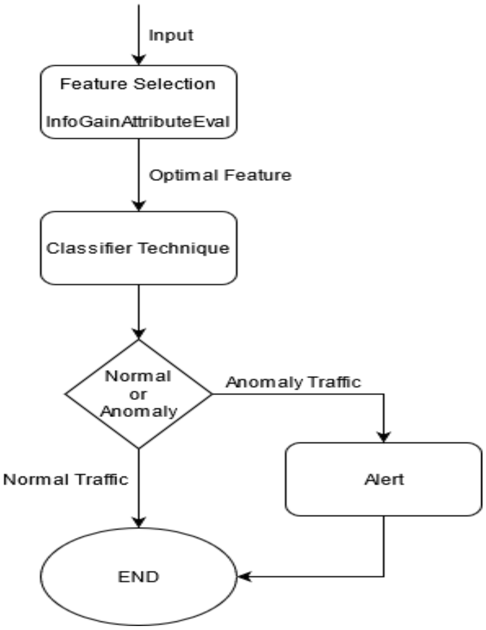


Fig. 7. Feature Selection Techniques Model for Classification.

Building Time: Time taken in the learning phase when the model is constructed from the network traffic dataset.

Testing Time: Time taken in the detection phase, showing the efficiency of the IDS.

VII. IDS PERFORMANCE RESULT

As discussed previously, the evaluation method on the UNSW-NB15 dataset was applied on the Decision Table, K-NN, Decision Tree, LogitBoost, Naive Bayes, and Random Forest.

A. Evaluation Metrics

For comparison, metrics were evaluated, as discussed. Below tables show the result parameters taken from the testing phase for the Decision Table, K-NN, Decision Tree, LogitBoost, Naive Bayes and Random Forest approaches respectively. Table V to Table VIII shows the evaluation metrics result of the original dataset and after applying Feature Selection.

TABLE V. EVALUATION METRICS PERCENTAGE OF THE ORIGINAL DATASET

Classifier	**TP Rate**	**FP Rate**	**TN Rate**	**FN Rate**
Decision Table	98.50%	5.20%	94.80%	1.50%
K-NN	96.10%	5.40%	94.60%	3.90%
Decision Tree	98.70%	1.60%	98.40%	1.30%
LogitBoost	94.00%	12.60%	87.40%	6.00%
Naive Bayes	67.20%	9.80%	90.20%	32.80%
Random Forest	98.80%	2.40%	97.60%	1.20%

TABLE VI. EVALUATION METRICS PERCENTAGE AFTER APPLYING FEATURE SELECTION

Classifier	**TP Rate**	**FP Rate**	**TN Rate**	**FN Rate**
Decision Table FS	97.80%	5.10%	94.90%	2.20%
K-NN FS	97.80%	2.40%	97.60%	2.20%
Decision Tree FS	98.50%	1.50%	98.50%	1.50%
LogitBoost FS	97.50%	24.20%	75.80%	2.50%
Naive Bayes FS	87.10%	26.50%	73.50%	12.90%
Random Forest FS	98.50%	2.00%	98.00%	1.50%

TABLE VII. EVALUATION METRICS OF THE ORIGINAL DATASET

Classifier	**Actual Attacks**	**Intrusion Missed**	**False Alarm**	**Actual Normal**
Decision Table	40723	623	1194	21878
K-NN	39715	1631	1244	21828
Decision Tree	40806	540	379	22693
LogitBoost	38871	2475	2900	20172
Naive Bayes	27783	13563	2270	20802
Random Forest	40854	492	554	22518

TABLE VIII. EVALUATION METRICS AFTER APPLYING FEATURE SELECTION

Classifier	Actual Attacks	Intrusion Missed	False Alarm	Actual Normal
Decision Table FS	40450	896	1174	21898
K-NN FS	40438	908	551	22521
Decision Tree FS	40714	632	342	22730
LogitBoost FS	40311	1035	5591	17481
Naïve-Bayes FS	35995	5351	6119	15953
Random Forest FS	40731	615	465	22607

B. *Missed Intrusions*

From the data collected from the test, the missed intrusions were calculated. The difference in the percentage of missed intrusions was between the original dataset and after applying feature selection.

As shown in Fig. 8, all six classifier algorithms were tested. In terms of missed intrusions, the detailed analytical results show the number of missed intrusions and the percentage of missed intrusions compared with the total number of intrusions. The feature selection was conducted with the Info Gain Attribute Eval algorithm. The result for the Naive Bayes and LogitBoost classifiers comes with a massive improvement in terms of intrusion detection. Testing Naive Bayes on the original dataset caused 13 563 (32.80%) intrusions to be missed while LogitBoost caused 2 475 (5.99%) intrusions to be missed. The result after applying the feature selection on the dataset improved the Naive Bayes' ability to detect intrusions to 5 351 (12.94%) and LogitBoost to 1 053 (2.50%). For the other four classifiers, the difference between the original dataset and feature selection the change in missed detection is minimum.

C. *Accuracy*

In terms of accuracy, the best detection was achieved by obtaining accuracy as close to 100% as possible. The feature selection was applied to the dataset using Info Gain Attribute Eval via the ranked selection method. The 13 most useful features were chosen.

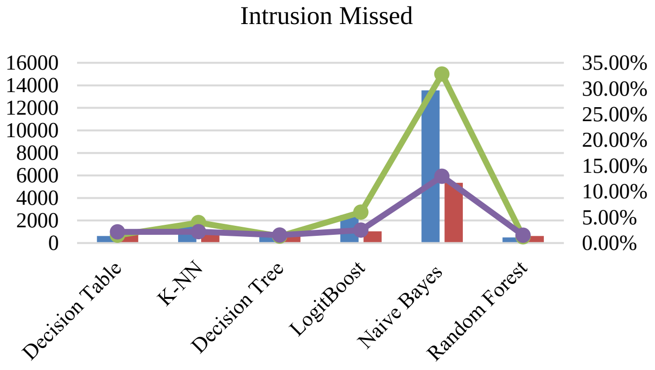


Fig. 8. Intrusion Missed.

As shown in Fig. 9, there were six classifiers algorithms. The detailed analytical results were for the accuracy of each classifier with the two parameters of performance, namely, accuracy and accuracy FS (Feature Selection). FS means that the feature selection was applied on the dataset. As a result of the six parameters with the Info Gain Attribute Eval algorithm, the FS method shows that the Decision Tree had the highest accuracy of all six classifiers at 98.57%. This accuracy decreased, but after applying the FS, it still had the highest accuracy at 98.49%. Thereafter, Random Forest was used at an accuracy of 98.37% and 98.32% after FS was applied, resulting in only a 0.05% loss of accuracy. The same results were recorded for the Decision Table with an accuracy of 97.17% and 96.78%. For K-NN, the result had increased accuracy after applying the FS, rising from 95.53% to 97.73%, which is a 2.20% improvement. Then LogitBoost was tested, with decreased accuracy recorded after FS was applied at a reduction of 1.94%, which dropped from 91.65% to 89.71%. Finally, Naive Bayes was tested, which showed the greatest improvement after FS was applied at 6.77%. This carried the result from 75.42% to 82.19%.

D. *Power Consumption*

In this test, the build time is calculated, which is the time it takes for the ML algorithm to build a model in the building phase, and also, the test time, which is the time it takes in the detection phase, as shown in Table IX.

Fig. 10 shows the time taken to build a model.

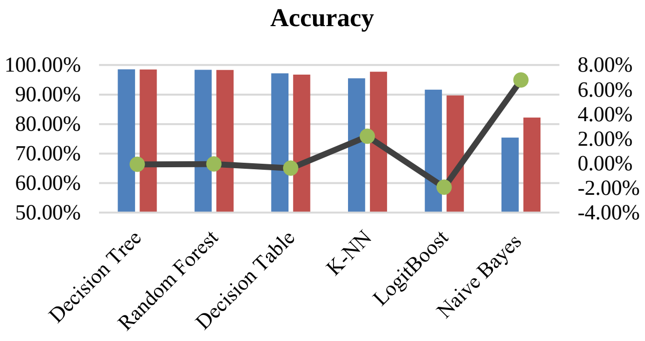


Fig. 9. Classifier Accuracy.

TABLE IX. CLASSIFIER BUILD \ TEST TIME

Classifier	Build Time	Build Time (FS)	Test Time	Test Time (FS)	Total Time	Total Time (FS)
Decision Table	391.7	162.56	0.24	0.45	392.15	163
K-NN	0.17	0.04	1529	1701	1701.8	1701
Decision Tree	73.66	23.83	0.27	0.06	73.72	23.89
Logit-Boost	37.15	11.82	0.37	0.31	37.46	12.13
Naive Bayes	2.95	0.83	1.81	0.47	3.42	1.3
Random Forest	315.	201.72	3.85	2.94	318.6	204.6

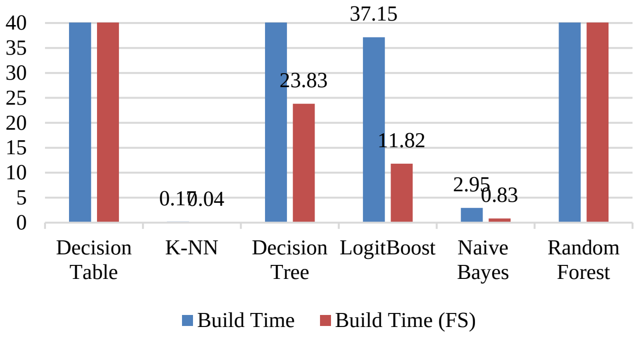


Fig. 10. Build Time (Seconds).

After building the model, the classifier used the model to test the accuracy of detecting attacks. The result shown in Fig. 11 shows the time to complete a test. The test phase considered more important because it shows the time needed from the device to finish the test and correspond directly to power consumption. As shown the decision tree has the fastest test time after applying FS at 0.06s from 0.27s, same result goes on to logitboost as it achieved 0.31s after applying FS from 0.37s. The Naïve Bayes has a mass boost in speed after applying FS as it was 1.81s to 0.47s, the result continues with random forest as it gain preforms boost after applying FS from 3.85s to 2.94s. Some classifiers loss some performs after applying FS, K-NN decreased preforms as it was 1529.38s and after applying the FS the time increased to 1701.7, same result goes to Decision Table as it was 0.24s to 0.45s after applying FS.

E. Result Conclusion

Fig. 12 shows the fastest three tests of six. The results indicate the impact of using FS in terms of time and accuracy changes.

As can be seen in Fig. 12, using FS in terms of time has improved considerably. As discussed previously, the use of FS helps to remove any unhelpful data to improve the power consumption. The time needed to test the model in the Decision Tree classifier decreased from 0.27 to just 0.06 seconds, which was the fastest classifier with the highest accuracy of all the six classifiers that were tested. There was minimal reduction in terms of accuracy because of the FS technique.

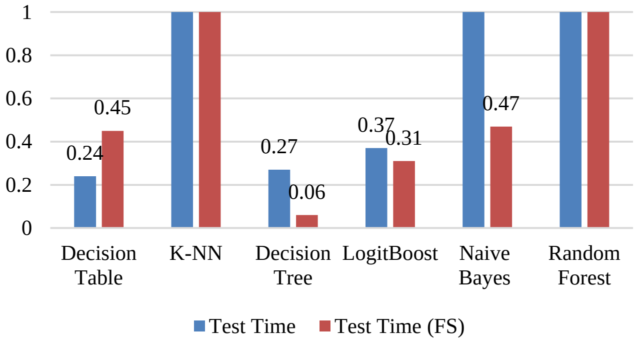
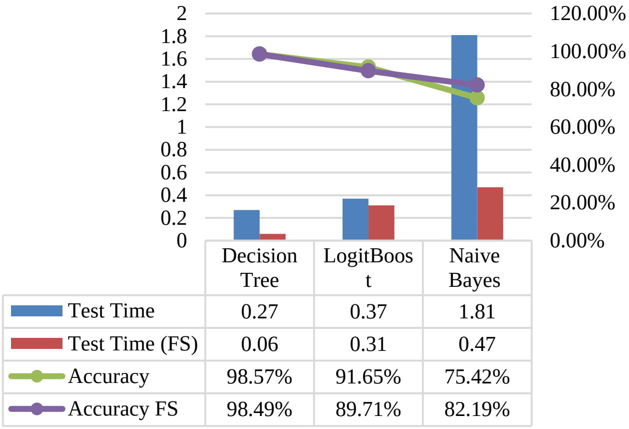


Fig. 11. Test Time (Seconds).



	Decision Tree	LogitBoost	Naive Bayes
Test Time	0.27	0.37	1.81
Test Time (FS)	0.06	0.31	0.47
Accuracy	98.57%	91.65%	75.42%
Accuracy FS	98.49%	89.71%	82.19%

Fig. 12. Test Time (Second) with the Accuracy for the Selected Classifiers.

Moreover, in IoT applications, real-time networking, and power consumption is key. This means the important result is in the test time, which is the time it takes the IDS to test incoming traffic. The Decision Tree had the lowest time in terms of testing the incoming traffic, at only 0.6 seconds, after applying the FS. This resulted in much lower total CPU usage and battery consumption while maintaining the highest accuracy.

VIII. Conclusion

The aim of this paper was to provide an overview of several algorithms, implemented in a constrained environment, while maintaining protection for the IoT environment. The paper demonstrated how supervised ML could be applied to analyze network traffic data to detect intrusion accurately. It demonstrated the efficiency of the method in terms of selecting the important features to speed up training and testing time. Specific use cases focus on metrics. In contrast, the aim was to identify the most efficient classifier. This test provides definitive numbers that can be used to compare these algorithms. The results demonstrated the advantages and disadvantages of each algorithm used for anomaly-based IDS.

IX. Future Work

With the development of the Internet of Things with many distinctive features, it has put the IoT in a situation where standards and specifications for these devices are very different from any traditional solutions. For that, the available traditional solutions are not suitable for the IoT environment. Furthermore, the architecture of IoT environment usually made with arm environment that are way different than traditional x86. Moreover, the rapid growth of IoT with unique specifications has placed us in a situation where more research on efficient security solutions that suit most IoT is a must.

References

[1] "System on a chip - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/System_on_a_chip. [Accessed: 12-Mar-2020].

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.

[3] F. Alfaleh, H. Alfehaid, M. Alanzy, and S. Elkhediri, “Wireless Sensor Networks Security: Case study,” 2019, pp. 1–4, doi: 10.1109/cais.2019.8769510.

[4] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Computing Surveys, vol. 41, no. 3. 01-Jul-2009, doi: 10.1145/1541880.1541882.

[5] N. Apthorpe, D. Reisman, and N. Feamster, “A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,” May 2017.

[6] F. Wortmann and K. Flü, “Internet of Things Technology and Value Added,” Bus. Inf. Syst. Eng., doi: 10.1007/s12599-015-0383-3.

[7] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[8] F. Samie, L. Bauer, and J. Henkel, “IoT Technologies for Embedded Computing: A Survey,” doi: 10.1145/2968456.2974004.

[9] S. C. Ergen, “ZigBee/IEEE 802.15.4 Summary,” 2004.

[10] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, “A tutorial on IEEE 802.11ax high efficiency WLANs,” IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 197–216, Jan. 2019, doi: 10.1109/COMST.2018.2871099.

[11] “Wi-Fi - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Wi-Fi. [Accessed: 14-Mar-2020].

[12] “Connectivity Now and Beyond; exploring Cat-M1, NB-IoT, and LPWAN Connections.” [Online]. Available: https://ubidots.com/blog/exploring-cat-m1-nb-iot-lpwan-connections/. [Accessed: 24-May-2020].

[13] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications,” Feb. 2018.

[14] “Threat Advisory: Mirai Botnet | Akamai.” [Online]. Available: https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/akamai-mirai-botnet-threat-advisory.jsp. [Accessed: 11-Nov-2019].

[15] J. Fruhlinger, “The Mirai botnet explained: How IoT devices almost brought down the internet,” CSO Online, Mar. 2018.

[16] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks,” IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 10037–10047, Dec. 2016, doi: 10.1109/TVT.2016.2524258.

[17] R. Halloush, “Transmission Early-stopping Scheme for Anti-jamming over Delay-sensitive IoT Applications (IEEE Internet of Things Journal) Transmission Early-stopping Scheme for Anti-jamming over Delay-sensitive IoT Applications,” 2019, doi: 10.1109/JIOT.2019.2911683.

[18] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, “Malware Threats and Detection for Industrial Mobile-IoT Networks,” IEEE Access, vol. 6, pp. 15941–15957, Mar. 2018, doi: 10.1109/ACCESS.2018.2815660.

[19] “Amazon opens a supermarket with no checkouts - BBC News.” [Online]. Available: https://www.bbc.com/news/business-42769096. [Accessed: 14-Mar-2020].

[20] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.

[21] “The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.” [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219. [Accessed: 29-Mar-2020].

[22] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of things: The road ahead,” Computer Networks, vol. 76. Elsevier B.V., pp. 146–164, 15-Jan-2015, doi: 10.1016/j.comnet.2014.11.008.

[23] H. Qu, Z. Qiu, X. Tang, M. Xiang, and P. Wang, “An Adaptive Intrusion Detection Method for Wireless Sensor Networks,” 2017.

[24] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” Futur. Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.

[25] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer internet of things devices,” in Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.

[26] D. Damopoulos, S. A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke, and S. Gritzalis, “Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers,” Secur. Commun. Networks, vol. 5, no. 1, pp. 3–14, Jan. 2012, doi: 10.1002/sec.341.

[27] J. Slay and N. Moustafa, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” Artic. Inf. Secur. J. A Glob. Perspect., 2016, doi: 10.1080/19393555.2015.1125974?tab=permissions.

[28] N. A. Mahadi, M. A. Mohamed, A. I. Mohamad, M. Makhtar, M. F. A. Kadir, and M. Mamat, “A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication,” in Recent Advances in Cryptography and Network Security, InTech, 2018.

[29] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, “A novel framework for intrusion detection in cloud,” in Proceedings of the 5th International Conference on Security of Information and Networks, SIN’12, 2012, pp. 67–74, doi: 10.1145/2388576.2388585.

[30] B. Kumar Baradwaj, R. Scholor, S. Pal, and S. Lecturer, “Mining Educational Data to Analyze Students" Performance,” 2011.

[31] M. Kryszkiewicz, “Rough set approach to incomplete information systems,” 1998.

[32] P. P. Jayaraman, A. Zaslavsky, and J. Delsing, “Intelligent processing of K-nearest neighbors queries using mobile data collectors in a location aware 3D wireless sensor network,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2010, vol. 6098 LNAI, no. PART 3, pp. 260–270, doi: 10.1007/978-3-642-13033-5_27.

[33] A. L. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” IEEE Commun. Surv. Tutorials, vol. 18, no. 2, pp. 1153–1176, Apr. 2016, doi: 10.1109/COMST.2015.2494502.

[34] J. Friedman, J. Friedman, T. Hastie, and R. Tibshirani, “Additive Logistic Regression: a Statistical View of Boosting,” Ann. Stat., vol. 28, p. 2000, 1998.

[35] H. Liu, H. Motoda, R. Setiono, and Z. Zhao, “The Fourth Workshop on Feature Selection in Data Mining.”.