REPUBLIC OF TURKEY

ALTINBASUNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

DESIGNING A SMART SYSTEM TO DETECT THE INTRUSION IN IOT

Zainab ABDALJABAR

Master of Science

Supervisor

Prof.Osman Nuri UCAN

Istanbul, 2022

DESIGNING A SMART SYSTEM TO DETECT THE INTRUSION IN IOT

Zainab ABDALJABAR

Electrical and Computer Engineering

Master of Science

ALTINBAŞ UNIVERSITY

2022

The thesis titled " DESIGNING A SMART SYSTEM TO DETECT THE INTRUSION IN IOT **"** prepared by ZAINAB ABDALJABAR and submitted on 14/2/2022 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering

Prof. Dr. Osman Nuri UÇAN

Supervisor

Thesis Defense Jury Members:

Prof. Dr. Osman Nuri UÇAN	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof.Dr.Sefer KURNAZ	Faculty of Engineering and Architecture, Altinbas University	_____
Prof.Dr. Mesut RAZBONYALI	School of Engineering and, Natural Sciences Maltepe University	_____

I hereby declare that this thesis meets all format and submission requirements of a master thesis

Submission date of the thesis to the Graduate Education Institute: ___/___/___

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Zainab ABDALJABAR

Signature

DEDICATION

I am dedicating this thesis to the soul of my beloved father Engineer Hussam ABDALJABAR. The person who has meant and continues to mean a lot to me and to my life. Although he is no longer in this world, his memories continue to inspire my life. May you find peace and happiness in Paradise Though your life was short, I will make sure your memory lives on as long as I may live. My love to you and missing you is much more beyond these words. May Allah (SWT) grant you Al- Jannah Ameen.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank ALLAH, my merciful God who enlightened my way and my life to be strong and continuing achieving success in this life. My greatest expressions of appreciation to my beloved mother Narmeen, her being in my life was like the candle that lit up the darkness and opened the way ahead to continue towards the final achievements. I would like to show a great word of thank to my brother Saif, his wife Sarah and my beloved nephews Raghad and Omar for their exceptional love, efforts, non-ending encouragement, motivation and support regardless of the taught situation of CO-19 and the difficult circumstances which were a great inspiration to me. From the deep of my heart I would like to address my highest words of thank to my supervisors Prof. Dr. Osman and Assist. Prof. Dr. Khattab their guidance and scientific background made my steps easier to the final step. Their keen support and seamless help since the startup to the eventual stage promoted me for a deeper understanding of the project that I worked on. I would also like to thank to all my colleagues and friends who prayed for me, encouraged me and for being so positive to strengthen me along my masters journey.

ABSTRACT

DESIGNING A SMART SYSTEM TO DETECT THE INTRUSION IN IOT

Abdaljabar, Zainab

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor:Prof. Dr. Osman nuri UCAN

Date:01/2022

Pages: 72

The Internet of Things (IoT) has been quickly growing during the previous few years, with the intention of having a wider impact on every aspect of life, from daily activities to vast industrial systems. Unluckily, A group of cybercriminals took notice of this, those responsible for turning the IoT into a vector for cybercrime, potentially exposing end nodes to attack. Since there are so many different kinds of IoT devices, There are difficulties to defend infrastructure for the IoT using a normal intrusion detection system (IDS). IoT devices need to be protected. We looked at data flow in the IoT. in this work taking two datasets (UNSW-NB15 and DoH20) and using three Machine Learning (ML) classifiers: Random Forest (RF), K-Nearest Neighbors (KNN) and Decision Tree (DT). For each method, we determined the Error Rate (ER), Accuracy(Acc), Precision, Recall, and F1 score. We received outstanding results (100%) when we combined these two classifiers. Detection rates are extremely high. A succinct summary of the results is presented.

Keywords: Internet of Things, Intrusion Detection System, Machine Learning, Random Forest, K-Nearest Neighbors.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

IoT	:	Internet of Things
IDS	:	Intrusion Detection System
ML	:	Machine Learning
RF	:	Random Forest
KKN	:	K-Nearest Neighbors
DT	:	Decision Tree
RFID	:	Radio Frequency Identification
DDoS	:	Distributed Denial-Of-Service
ER	:	Error Rate
ACC	:	Accuracy
DR	:	Detection Rate
ROC	:	Receiver Operating Characteristic
TP	:	True Positive
TN	:	True Negative
FP	:	False Posative
FN	:	False Negative
TPR	:	True Positive Rate
TNR	:	True Negative Rate
FPR	:	False Posative Rate
FNR	:	False Negative Rate

1. INTRODUCTION

IoT: There are numerous things that might be linked with each other and have the ability to exchange information automatically between them through standard internet protocols namelyIoT, it uses various technologies such as Radio Frequency Identification (RFID) tag, Sensors, Actuators and Smartphone and cloud computing support etc. [1], IoT technologies are classified into two classes as shown in figure (1.1).

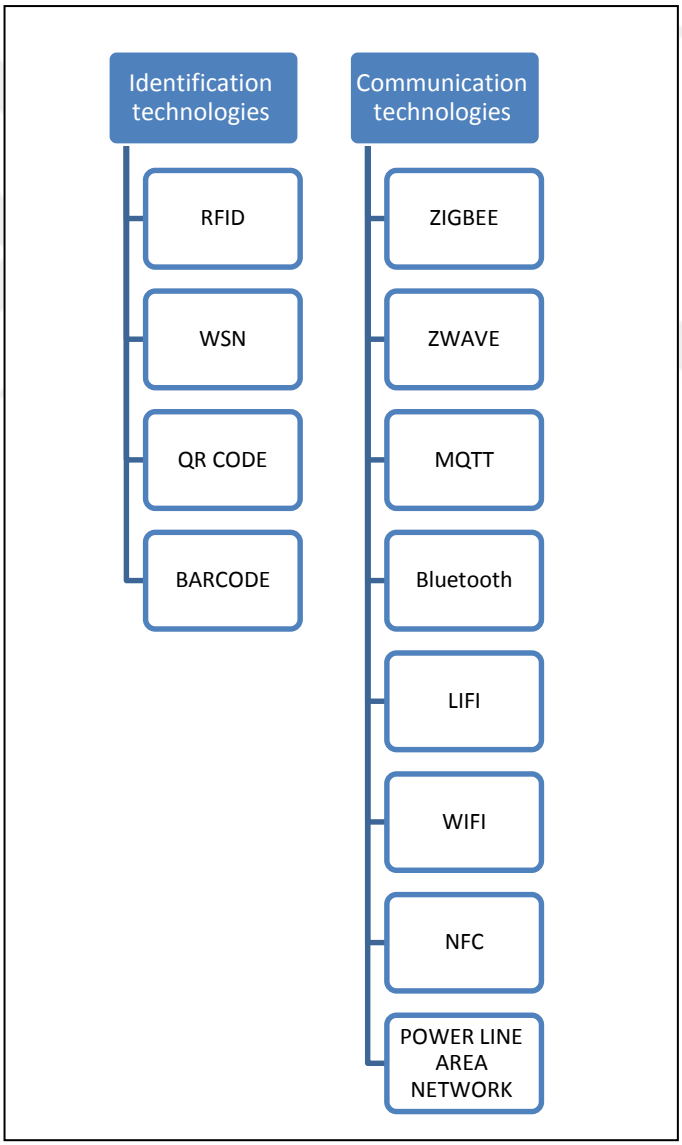

Figure 1.1: Technologies of IoT [2]

The undeniably high performance of IoT is combined with severe safety problems, mostly because of restricted devices, not protection and lack of legislation is a priority for manufacturers. Poorly conceived IoT devices cause assaults to perform negative action; attacks on implantable medical devices [3], smart cars [4], smart toys, illegal access to voicemail, attacks on intelligent meters [5], and so on. In addition to being a possible danger for IoT, the vulnerability of these linked computers threatens the entire internet [6]. These restricted computers can quickly be converted by attackers and their harmful activities are carried out. For example, Mirai was among the first renowned IoT botnet to target many insecure IoT devices. In internet history, some of the most destructive a Distributed Denial-Of-Service (DDoS) attacks have been completed, in October 2016 Twitter, Github, Netflix, CNN, etc., have been dropped in the United States and Europe [7]. Figure (1.1) shows the applications of IoT.

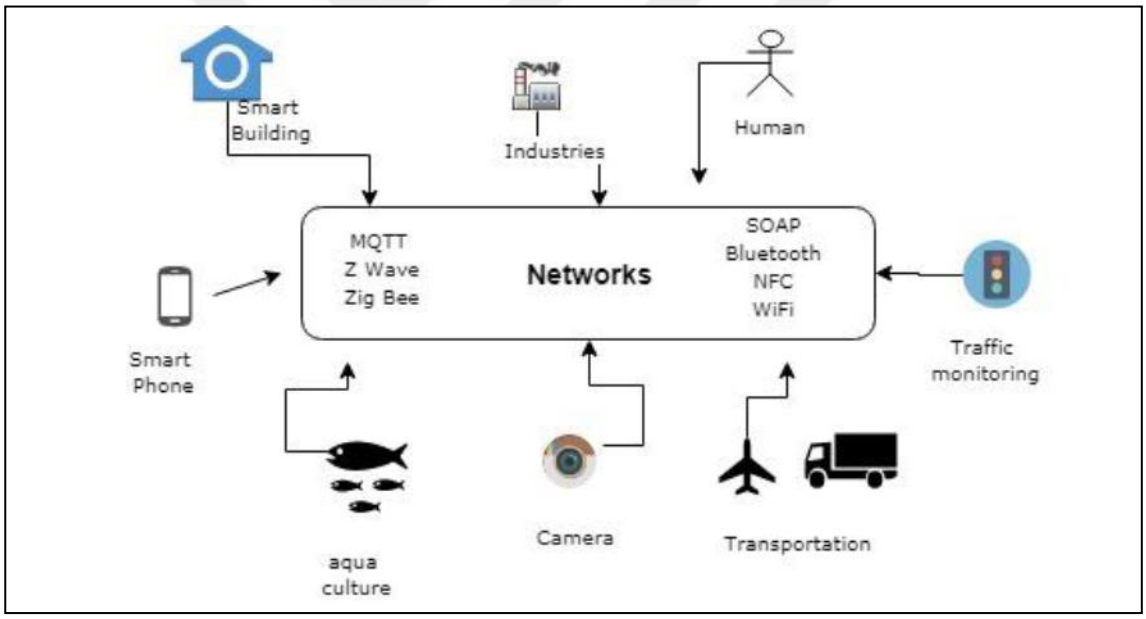

Figure 1.2: IoT Representation

1.1 IDS

Intrusion is a superfluous or malignant action and is risky for nodes in the sensor. The system of intrusion detection is used to monitor malignant network traffic. IDS can serve as a second security line it safeguards the network from unauthorized access. Software or hardware may be involved [8]. IDS can check and explore machines and user activities, detect well-known attack signatures and classify activities of the malignant network. IDS aims to check networks and

nodes reveal different network intrusions and alert users about intrusions. The IDS functions as an alarm or network controller, preventing system damage by making an alert before attacking the attackers. IDS can discover attacks both internally and externally. Internal attacks are caused by malignant or restricted nodes in the network, while external attacks by third parties started by external networks are launched. IDS reveal the network packages and locate if intruders or legal users are involved. Including three ID components: monitoring, analysis and detection, alarm. The monitoring observes traffic, type and resources in the network.

Analysis and detection is a central IDS module that reveals intrusions by identified algorithms. Alert area elevates an alert when intruders are discovered[7]. Figure (1.2) illustrates the IDS classification for IoT.

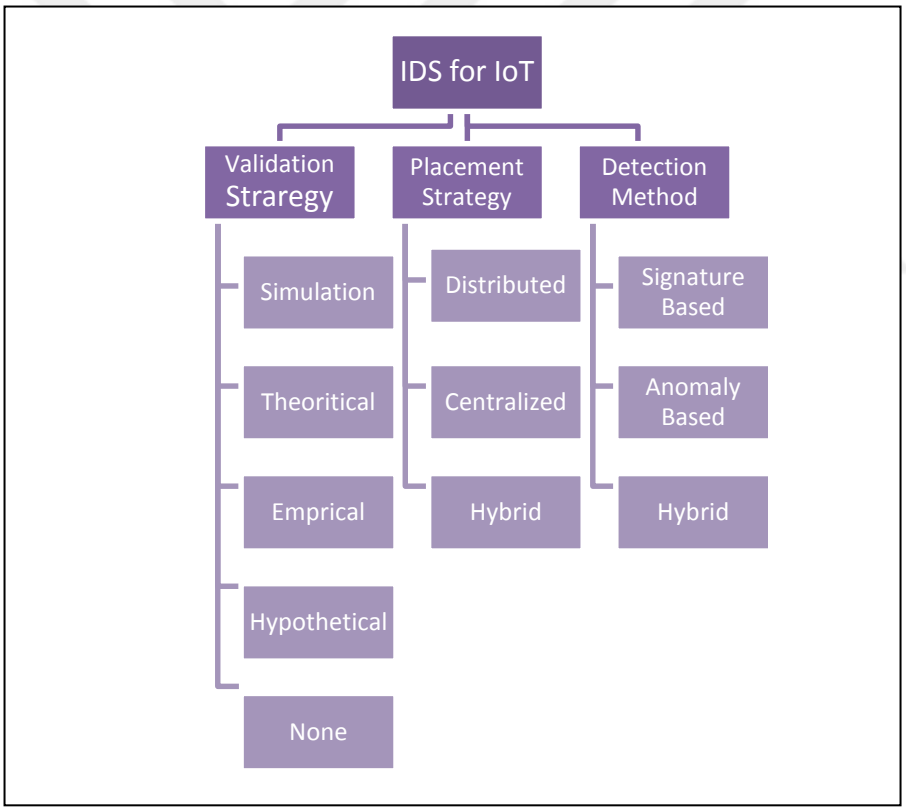

Figure 1.3: Classification of IDS for IoT

1.2 RELATED WORKS

Many scientists have been debating the IoT for the past ten yearsto improve highly sophisticated methods and IDS to increase and raise the safety of various applications[9]. The below part present many types of last researches which relative to this work:

Larriva-Novo et al. (2021) Used two datasets, namely Unified Glare Rating (UGR16) and an inclusive dataset (UNSW NB15) for network IDS, for its estimated, as well as most often used KDD99. Preparation methods have been assessed according to the functions of scaling and normalization. It was possible to implement each of these models by a variety of traits based on a classification system consisting of four distinct types: Features of a network's basic connection as well as its data content and statistics, as well as a grouping made up of features related to network traffic and features related to network traffic direction. Aims of this investigation include estimating the classification's accuracy with different techniques of preprocessing data to achieve the most accurate model, this proposition has shown that the accuracy can be increased by up to 45% by applying network traffic categories and several pre-processing methods, When features are preprocessed, the machine learning system can better distribute these parameters in relation to potential assaults [10].

Alkadi et al.(2020) Submitted a Deep Blockchain Framework (DBF), aiming at providing distributed intrusion detection based on security and privacy with intelligent IoT network contracts. The intrusion detection method is used with the sequential network data utilizing a deep-level Bidirectional Langle Short-Term Memory (BiLSTM), which is evaluated through the use of the UNSW-NB15 and BoT-IoT datasets. The ethereum library has developed a privacy-based block chain and intelligent contract methods to ensure that the distributed IDS engines are confidential. The DBF framework is evaluated in comparison to IDS approaches that safeguard

personal privacy as well as experimental evidence showing that DBF outperforms its counterparts. The platform should be used to facilitate decision-making and can help users and cloud services migrate data safely and promptly[11].

Taghavinejad et al. (2020) : Presented detect interference, the mixture of three decision trees has been provided with the Support Vector Machine (SVM), KNN and DT procedures being correlated with the output in relation to the suggested procedure. Experiments on the NSL-KDD data sets have been carried out and the results suggest the proposed approach to IDS (IoT-based SG) works well than other approaches [12].

Yahyaoui et al.(2021) : Submitted a dependable framework for detecting IoT Events and anomalies (READ-IoT for short). The designed architecture combines monitoring of events and disturbances into a single, common mechanism, which centrally manages all concepts. The framework depends on the reputational supply of detection capacity to improve its reliability, taking the insecurity of the hosts deployed into account [13].

Maniriho et al.(2020) : 2020 Submitted New IoT networks' anomaly-based solution, includes a hybrid engine for filtering that extracts in order to focus on the most critical features; and the RF algorithm that categorizes all traffic as either natural or abnormal. IoTID20 an example of new datasets obtained in IoT invironment, has been used for performance evaluation. The experiential results indicate that the approach suggested is fairly accurate when Denial-of-Service DoS (99.95%) is detected, Man-In-The-Middle attack MITM (99.97%), Scanning (99.96%) [14].

Susilo et al.(2020) : 2020 Discussed various ML and Deep Learning (DL) techniques and common datasets for upgrading the process of security in IoT networks. He also created a DoS algorithm for attacks using a DL algorithm. And using the programming language of Python

with packages like scikit-learn, And Seaborne, tensor flow. He founded find that a deep learning model could enhance accuracy to make attack prevention on an IoT network as successful as possible [15].

Ullah et al. (2020) : Submitted a technique used to produce abnormal behaviour identification in IoT networks from an existing Botnet dataset. There are a larger network and a flow-dependent functionality in the current IoT Botnet dataset. An IDS with flow-based functionality possible to evaluated and checked as well as the precision of suggested data collection can be tested using various ML methods. The ACC of the suggested dataset was also checked through numerous attribute correlations and the recursive exclusion technique. The botnet dataset suggested supplies a basis for the analysis and estimate of the IoT abnormal paradigm for behavior detection. He publicly exchanged Botnet's newly created dataset and the connection [16].

Roopak et al. (2020) : Suggested IDS based on the merger of the NSGA-II adapted multi-target optimization system for reducing data dimensions, and the (CNN) which incorporates Long Short Term Memory (LSTM). The experiment is performed with a High-Performance Computer (HPC) on the most recent DDoS attacks datasets of CISIDS2017, with 99.03 per cent accuracy and a 5 times decrease in training time. Through comparing it to other algorithms in ML, the suggested method was assessed, confirming that the proposed method exceeds other methods [17].

Eskandari et al. (2020) : Proposed Pass ban, an IDS capable of protecting directly attached IoT computers. Pass ban was the IDS, The feature of the suggested approach that it may be immediately utilized on very inexpensive IoT gateways, for example, single-board PCs cost only some dozen U.S. dollars, so that cyber-attacks can be detected as closely as possible to the

appropriate data source using the cutting edge computing method. And he had shown that the Pass ban is in a position to detect different forms of malicious traffic, including port scanning, Secure Shell Protocol (SSH) and Hypertext Transfer Protocol (HTTP) Brute Force, as well as SYN Flood attacks with very low False-Positive Rates (FPR) and good ACC [18].

Nie et al. (2020) : Designed an IDS powered by data by analyzing the Road Side Unit (RSU) connection load behaviors facing numerous attacks that led to irregular traffic fluctuations in IoV. The CNN deep-learning architecture is produced to remove connection load features and to identify intrusion to RSUs. Because of the merging of the back propagation algorithm, the proposed architecture include a standard CNN and a fundamental error expression. The probabilistic description of the intended CNN-based deep architecture gives a computational overview of the convergence [19].

Ullah et al. (2020) : Introduced an abnormal paradigm for IDS in IoT networks in two levels. In the Level 1 model, the flow of network is classified as natural flows or irregular flows, whilst Level 2 categorize the detected harmful operation according to its type or sub-category. If the network flow is identified by the level-1 model as an anomaly, then the level-2 model transfers the flow to the level-2 model for further analysis recognize the aberration category or subcategory. His proposed model was built on the IoT networks flow-based. Flow-based detection methodology inspects packet headers for Network Traffic Classification only. A flow-based functionality was examined and evaluated using multiple cross-fold validation examine to choose the best algorithm from the IoT Botnet data collection and separate master learning algorithms. The decision tree classification has provided the most accurate predictions for level 1 and level 2 for RF classification. ACC, recall and F1 score of the recommended model for level 1 is as follows: 99.99 and 99.90 percent. A two-stage irregular IoT network activity detection

system he is proposing would offer a strong basis for improving malicious IoT network activity detection systems [20].

Verma et al. (2020) : Studied botnet traffic using three machine learning arrangements in IoT setting: logistic reversal, SVM and random forest. Every assault on nine computers was listed in each botnet. He has computed for each algorithm, precision, recall, F1 value, True Positive, False Negative, and Precision. These three classifiers provided excellent results (above 99%) [21].

Pundir (2019) : Presented the risk model information related to the safety of communications dependent on Wireless Sensor Network (WSN) and IoT. Often discussing security standards and potential attacks in communications settings focused on WSN and IoT. WSNs are also being updated on new initiatives built into IoT. The architecture of various WSN and IoT-based communications environments is then given in-depth. Next, the discussion will address the latest WSN and IoT problems and challenges. He is also providing, along with comparative analyzes, important literature surveys of recent IoT and WSN intrusion detection protocols. The Taxonomy of WSN and IoT protection and privacy protocols are also highlighted [22].

Anthi et al. (2019) : Provided a three-layer IDS that appoint a monitored strategy to the detection of various common IoT network-based cyber-attacks. The system is divided into three distinct roles: 1) classification the standard behavior of every IoT linked network system by category and profile, 2) identifying malicious network packets in the event of an attack and 3) Identifying the type of assault that was carried out with the use of eight ordinary commercially available equipment in a smart home testbed, the system is tested in 12 attacks from four principal category network-based attacks, as the efficacy of the proposed IDS architecture is estimated as: Denial of service (DoS), MITM/Spoofing, Recognition and Replay. Furthermore, four situations

of multi-stage attacks of dynamic case chains are tested for the method. The three core functions of the device are done by an F-measurement of: (1) 96,2%, (2) 90,0% and (3) 98,0%. And shows that the suggested architecture able to differentiate among networks IoT equipment, whether the network operation is malicious or benevolent and identify which intrusion on which system was linked successfully to the network [23].

Yang et al. (2019) : Proposed the architecture of the neuronal LM-BP network. This architecture applies to a detection scheme and the LM-BP algorithm gives intrusion detection flaws. This feature uses the LM algorithm to improve the weight limit of standard neural network BP with fast optimization and powerful robotic properties. LM algorithm The KDD CUP 99 intrusion detection set is imported into an LM-BP neural network classifier and the best results are done by continuous training by setting up a neural network classifier. The experiential simulation findings show that the BP neural network models and DOS, R2L, U2L, and investigation neural network model have a higher DR and a lower false warning than the standard BP neural network model and PSO-BP. The model has a proven advantage [24].

Liu et al. (2019) : Proposed an IDS taxonomy that classifies and summarizes machine-based and deep-learning IDS literature using data objects as the principal dimension. He thinks this kind of framework for taxonomy is suitable for researchers in cyber security. in the beginning, the survey clarifies IDSs definition and taxonomy. Then, the algorithms used in IDSs, metrics and data sets are also used for machine learning. Next, we use the suggested taxonomic scheme as a base in conjunction with the representative literature and demonstrate why IDS problems with ML and DL techniques can be solved [25].

Jan et al. (2019) : Created a technique of lightweight attack detection using a supervised SVM machine to detect the opponent trying to insert unwanted data into the IoT network. The results of simulations show that the proposed SVM-based classification will perform well when it comes to categorization ACC and detection time, by the use of a combination of two or three incomplete features [26].

Thamilarasu et al. (2019) : Improved An IoT-customized intelligent IDS. In particular, it used an IoT network dedication detection algorithm to detect malicious traffic. The approach offers encryption for the service and makes it easier for the different network exchange protocols used in IoT to interoperate. The suggested detection system was tested utilizing both the real-network traces for proof of concept and the simulation for proof of scalability. The empirical findings demonstrate the successful detection of real-world intrusions by the suggested intrusion-detection method [27].

1.3 PROBLEM STATEMENT

Mainly, this study is focused on improving the following::

i. Low DR deficiencies, high false warning rate and poor intrusion detection device Internet scalability of objects [24].

ii. IoT safety concern cannot be overlooked. IoT computers are accessible through a network like the Internet from all over, meaning that IoT networks are not shielded from a wide range of malicious attacks. If security concerns are not resolved, classified information will at any time be leaked [7].

iii. IoT systems are often unattended (e.g. remote sensors) and this allows the intruder to obtain physical access to them. Secondly, wireless networking is a major part, making eavesdrop simpler [28].

iv. Most IoT devices have a low capacity of storage and minimal memory; the IoT devices were unable to install external security features[28].

Another challenge with modern IDSs is that they lack the potential to track unknown threats. Since network environments evolve rapidly, attack variations and new threats appear continuously. Thus, It is necessary to construct IDSs that can reveal unknown attacks[25].

1.4 THESIS OBJECTIVES

i. Achieve the highest possible accuracy and the lowest possible Error Rate.

ii. Prove the benefits of ML and its efficacy in detecting intrusions via the IoT.

iii. Illustration of the benefits of the normalization process to enhance the performance

1.5 THE STRUCTURE OF THESIS

This thesis includes five chapters:

Chapter one: [introduction] is an introduction to the entire thesis. Adding to this chapter, the insides of individual chapters of this thesis are briefly reviewed. Chapter Two: [Background Information] presents the background of IDS for IoT Based on Smart Techniques.

Chapter Three: [The Proposed System] explains the steps of the suggested system and techniques used. A whole description of the suggested system is given.

Chapter Four: [Results and Discussion] contain the results of tests that have been implemented to estimate the system performance. The results of experimental examinations are discussed.

Chapter Five: [Conclusions and Future Works] conclude the thesis and explore directions for future work.

2. THEORITICAL BACKGROUND

TheIoT is typically a networked environment Intelligent objects, where any "thing" physical has an integrated digital feature. IoT is defined as a vibrant universal self-contained infrastructure for the network standard and interoperable configuration ability communication protocols which distinguishes between actual and virtual entities by giving them names, physical characteristics, computer characters and intelligent interfaces into the network of knowledge. There is also a similar description in. Billion-plus computers and networking gadgets can be connected via the Internet of Things. Objects of daily use may could be converted transformed into intelligent things capable of communicating relating to one another thanks to entities that exist in the digital world like sensors, RFID, Internet, and location-based services [29]. The Sensors incorporated into intelligent devices track and collect data pertaining to the environment, human society, and the use of equipment, among other factors. A key issue with the IoT is that it is vulnerable to attack.People, devices, sensors, and services are all connected in a continuous and global manner. It doesn't matter how well-thought-out a product maybe, intelligently programmed, efficiently carried out and carefully managed a security system may be Because they are created by humans and are not impervious to security risks. Consequently, a human element is required in the creation of cyber security solutions[30]. While technological advancements have further enhanced and in many cases completely safeguarded security solutions, security solutions are still needed to evolve and improve, to address new security challenges[31]. In contrast to traditional internet technology (IT) infrastructure, IoT devices are restricted by the processor, memory and power, typically used in aggressive, complex, and heterogeneous environments. The IoT may include a wide range of devices and networks, compared to traditional IT infrastructures.IoT's main objective is to deliver applications, sensors, and interoperable protocols for communication, network infrastructure and physical objects integration. People's day-to-day activities are made possible by the integrated gadgets' array of digital services. It's now possible to keep track of and communicate data in real time over great distances using equipment that can be monitored and run. However, The quick and wide-scale application of IoT products raises a lot of safety concerns. The main safety challenges in IoT are, for example, authentication, authorization, system settings, verification, access control, and information storage and management verification. Vital data may still be leaked or manipulated. The safety,

knowledge and privacy of IoT devices are not guaranteed. IoT deployment will be more successful if consumers feel secure about their personal information, and strong protection is needed to do so.

2.1 APPLICATION OF IOT

Applications have many protection, privacy and trust threats that differ between applications and environment. IoT applications to ensure safe communication and to allow IoT to help people without jeopardizing their privacy, Dependingto types of application and functionality, suitable IoT security solutions should be deployed. Security, confidence and privacy concerns in a variety of contemporary application fields are addressed in this section.

i. Smart Home: Smart and automatic devices such as smart illumination, refrigerator, washing machines, air conditioning and electronic devices are part of a modern house. Meter, CCTV and warning system. For protection and security Safety, smart cameras drive these homes, Sensors, intelligent locks and alarms. These are intelligent Equipment can be run from the internet Long distances. When these intelligent technologies are implemented, they provide comfort and convenience in smart homes while also improving safety, confidence and privacy in general while reducing overall cost[32]. The usage of criteria like as secrecy, auto-immunity, and durability can help to assure protection and keep intelligent dwellings safe from theft or intrusions. Must be fulfilled. Enabled in clever homes IoT devices Password should be safe and the login of the user should be Privacy policy.

ii. IoT-Based Industry: The cyber-physical system serves as the foundation for industrial IoT, as it continuously monitors, diagnoses, and regulates physical processes. And remotely output. Smart industry ready for IoT and plants optimize production processes, enable Production of intelligent goods and provision of information intelligent programs by use of capita Support the IoT system's collected data. the clever Digital identity products typically have RFID driven That also allows data to be collected and saved[33]. But, the IoT and its industrial goods connected to it,Trust, secrecy, and privacy are all issues that digital businesses face.Additionally, they raise issues such as standardization of manufacturing processes, as well as social and legal concerns. The various

manufacturing sectors IoT devices need a highly flexible system of addressing, Data protection and security solutions. Because of the resources Restrictions, low-cost industrial IoT architecture, Low xstrength, but fully integrated infrastructure robust solutions for defense.

iii. Smart City**:** The idea of an intelligent city is based on the convergence of different IoT technologies in different industries. In a clever city, incorporation in a distributed and dependable environment benefits its stakeholders Way. Providing confidentiality and confidence Smart City applications among the stakeholders an essential matter remains. Security problems exist hacking, terrorist activity and physical harm Might break smart city applications infrastructure in fields like energy, healthcare, business of the manufacturers, factories, traffic structures of the Federal Republic of Argentina [34].

iv. IoT-Based Healthcare: it is anIoT technology fields that is one of the most influential and fascinating [35]. Intelligent hospital or online health facilities in recent years, it has gained popularity. Medicine IoT Remote health control, elderly treatment, facilities, some of the chronic wellness and exercise plans is Applications that can increase [36]. A patient, however, is Private and confidential data could be at risk Robbed or treated. Personal details of the patient are and it is, therefore, necessary to protect them confidentially any unauthorized access from exposure. If a patient's medical report is leaked and changed, a patient may be mistreated and treated by the doctor. Patients' deadly and life-threatening. Medical IoT solutions should be particularly important because of the need of patient data privacy and authentication.

v. Intelligent Traffic Control Mechanism: The employment of RFIDs and other sensors in urban driving and traffic control improves the quality of life in the city. IoT's intelligent traffic control machanism offer people the 'future life' feel. IoT makes the traffic system able to offers information about travel and vehicles in way which to go; details of parkinglike the number of cars in the lot and the location of available parking spaces; public transportation like the number of people on board and the number of seats available. Automakers are already using ultrasonic sensors to make their vehicles safer to drive in metropolitan areas[37]. However, system automation can lead to problems with

passengers' security and confidence. Since the internet is linked to intelligent vehicles, buses, and trains, among others, passenger data run the risk of being hacked.

vi. Smart Grid**:** an intelligent electrical infrastructure, which is used primarily as an electricity transmission network, transmitters and substations, is known as the Smart Grid Spread electricity through homes and enterprises the most powerful way of the power plant. Intelligent meters, some power functions include renewable energy supplies, intelligent machines and productive energy properties. Intelligent grid. IoT use in electrical applications Grid distributes and manages electricity far more effective contact in two directions It also decreases climate impact [38]. Increased security vulnerabilities and risks by technological changes to intelligent power grid networks. The main areas of concern that need to be addressed when working with the intelligent grid include authentication, confidentiality, trust, honesty and availability.

vii. Smart agriculture**:**The fusion of many sensors and RFID technology can make traditional farming, animal husbandry and fisheries more intelligent. In smart farming, various sensors can track temperature, humidity, soil humidity and pollutants caused by microbes [39]. Animal body or fish farm-sensor and RFID sensor systems can monitor health conditions, monitor the activity and communicate remotely to stakeholders. Intelligent agriculture, however, is prone to many problems with security. Fish and animals may be carted or injured in agricultural products unless the safety of such applications is guaranteed.

2.2 BENEFITS AND FACILITIES OF IOT

Many benefits are provided by IoT such as Efficiency, improvement, asset optimization, physical premises, equipment security [40], Although the applications of IoT are not limited, they may be divided into the following areas based on their usability:

i. Smart Wearable’s

ii. Smart Homes

iii. Smart City

iv. Smart Enterprise

v. Smart Environment

IoT goods display a variety of features depending on their sector of use [41].

2.3 DIFFICULTIES IN SECURITY

In order to implement security in IoT, Consideration must be given to the application, network, and physical layers of security.

a. Difficulties of the application layer can be summarized as follows: IoT gadgets can't always run the heavyweight software because of its size. IoT security modules must be installed before they can be used, there are various caveats to be aware of [42].

I. In-Chip Programming: Low-memory IoT devices often include either a General-Purpose Operating System (GPOS) or a Real-Time Operating System (RTOS). Because of the size is small of these IoT operating systems' network protocol stacks and the lack of accompanying security modules, it is possible that they will be vulnerable. Consequently, such a minimal software and protocol stack needs lightweight, robust, and fault-tolerant security mechanisms [43].

II. Security Patch: The IoT can be used in remote locations. Security or software updates cannot be granted to sensor devices without affecting safety functionally. A costly update may be required patch security[44]. Mitigation of potential safety problems such as IoT OS and protocol would be impossible. Maybe the stack can not be accepted and added to a new stack. Patch security.

III. Data and Storage Volume: Security and privacy are compromised by massive amounts of information generated by a wide range of uses.

b. Difficultiesat the Network Layer: Communication and data routing through the internet are only some of the functionalities of the IoT Layer network and Low Power Wireless Personal

Area Networks (6LoWPAN) networks between different equipments. The layer of the network is prone to various routing attacks Subsequent restrictions [42].

I. Topological Changes and Mobility: Mobility is a key characteristic of IoT, and its gadgets are frequently mobile. At any time, IoT devices can depart or join a network. The common security algorithm cannot be adapted to such a dynamic change in topology.

II. Scalability: Every day there are more and more new, dynamic IoT devices, Moreover, more and more gadgets are connected to the worldwide network. Existent scalability and appropriateness of security measures for the proliferation of IoT devices are impossible to achieve.

III. Diverse Communication Medium: Smart devices link to private, public, global, and local networks using a variety of wired and wireless media. Various cable and wireless connectivity elements complicate the creation of a comprehensive safety system.

IV. Protocol Switching and Routing: Both communication IP or non-IP or a merger two protocols are possible with IoT devices. A standard security algorithm that takes multiple communication protocols into consideration is difficult to create for IoT devices.

c. Difficultiesat the Physical Layer: Because heterogeneous IoT devices connected through IP are typically resource constrained, they are more susceptible to security risks and assaults [4]. For IoT devices, however, traditional heavy-duty safety solutions are not suitable because of the following properties..

I. Processor, Memory, and Power: Due to limited power processor/CPUs have a comparatively low clocked cycle time,IoT devices powered by rechargeable batteries are inefficient. Therefore those devices not computer-strong. It cannot be used in such devices to perform heavy cryptographic algorithms. The IoT device is embedded with limited RAM and cash memory. Thus, Memory-efficient security systems should be carried over. After the operating system is booted, the device can run out of memory if IoT is used for heavy security schemes designed for the normal network [45].

II. Packaging: Certain IoT applications may require remote locations to be placed which may remain unattended. An opponent can trap and manipulate devices of IoT. In order to alter

the programs or replace rogue nodes, cryptographic data might be retrieved. Thus, the manipulative To resolve this issue, IoT device packaging is required [43].

2.4 ARCHITECTURE OF IOT SYSTEM

These architectures are generally classified in the following three categories (a glossary is presented for every abbreviation and acronym as specified in Table (2.1) :

Table 2.1: Abbreviation Glossary

1.	Abbreviation	2.	Defination
3.	**API**	4.	Application Programming Interface
5.	**GPS**	6.	Global Positioning System
7.	**NFC**	8.	Near-Field Communication
9.	**DoS**	10.	Denial-of-Service
11.	**RFID**	12.	Radio-frequency identification
13.	**GPRS**	14.	General Packet Radio Services
15.	**SSL**	16.	Secure Sockets Layer
17.	**WSN**	18.	Wireless Sensor Network
19.	**SCM**	20.	Supply Chain Management
21.	**SOA**	22.	Service Oriented Application
23.	**EPC**	24.	Electronic Product Code
25.	**UID**	26.	Unified Information Devices
27.	**SCMaaS**	28.	Supply Chain Management as a Service
29.	**CPS**	30.	Cyber Physical System
31.	**REST**	32.	Representational State Transfer
33.	**SOAP**	34.	Simple Object Access Protocol
35.	**XSS**	36.	Cross-Site Scripting
37.	**DFA**	38.	Deterministic finite automaton
39.	**CoAP**	40.	Constrained Application Protocol
41.	**DTLS**	42.	Datagram Transport Layer Security
43.	**NDP**	44.	Neighbor Discovery Protocol
45.	**RPL**	46.	Routing Protocol for Low-Power and Lossy Networks
47.	**SSO**	48.	Single Sign On
49.	**IETF**	50.	Internet Engineering Task Force
51.	**DNSSEC**	52.	Domain Name System Security
53.	**DoT**	54.	DNS over TSL

a. Architecture with three levels: this is the most often used class in most publications and researchers. The layers of the application are ordered by a top-down method called a) There run b) Network/ Transmission Application and Utility functions Layer c) Layer of perception/edge that applies to items or endpoints Architectural equipment.

b. The architecture of four levels: the configuration of the three-layer architecture of this category is quite similar, whereas the program and service are specified on a different architecture layer.

c. An architecture with five layers: add-ons are included in this design: a) a company layer over the application layer for a large variety of functions across the various IoT domains; or b) a layer that sits on top of application layer; For really sensitive IoT applications the apparatuses grade, an edge layer is required.

Application layer: While the IoT application layer does not provide a comprehensive specification, a variety of services may be provided for various applications by the application layer. In smart cities, IoT applications, smart grids, autonomous vehicular applications [46]are also included. Additionally, the application layer may perform some functions like a service support middleware software[47], a networking protocol, and cloud computing; the environmental and industrial concerns of the application are distinct. As can be seen in Figure (2.1) the architecture of the application layer defines various components and depends on the application of each component operation the climate the environment. For example, medical records can be found in healthcare

A specific application programming interface (API) or special application interface is needed. User and server sides of binary software [48]. Protection in most applications the coAP protocol is secured using DTLS, which the architecture focuses on. Instead, the other defense framework architectures suggested their model focused on HTTP payload encoding [49].

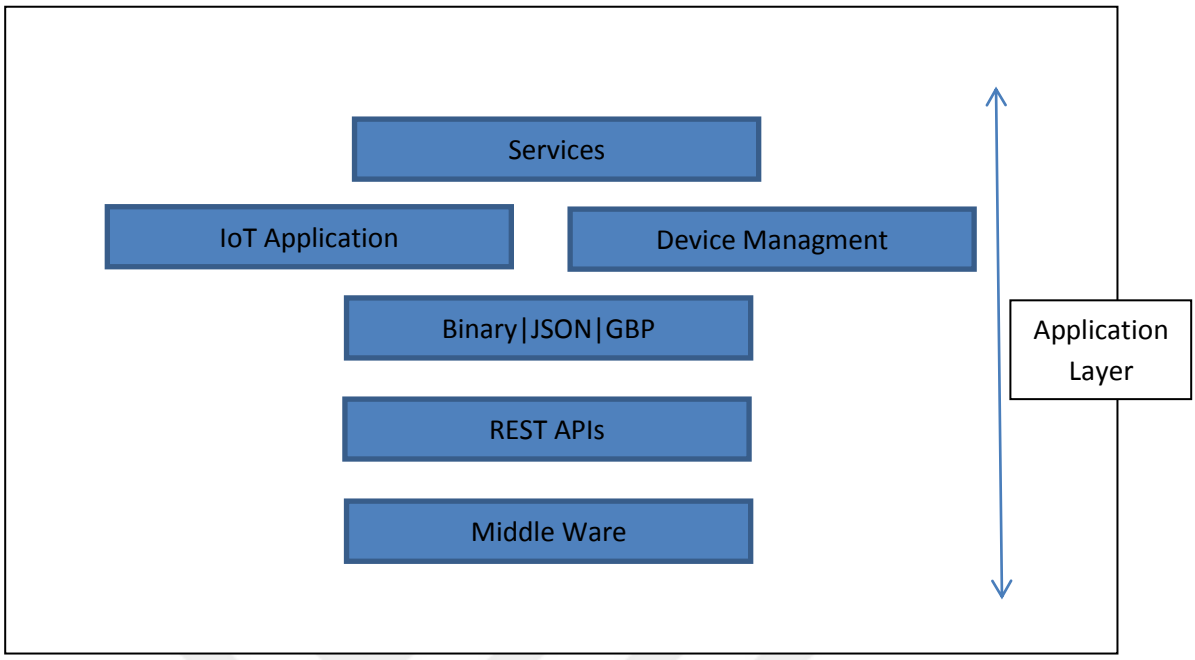

Figure 2.1: Ingredient of Application layer in IoT Architecture

Network Layer: transfer of data between other layers is handled in the network layer. Additionally, this layer offers connectivity to sensor layer by various standards and protocols including IEEE 802.x (GPS) Communication on the Near-Field (NFC). Figure (2.2) also shows that the cloud back-end architecture, mobile devices and Internet protocol are supported in this layer [50]. The network layer is able to process in light of the applied context in various aspects. However, the most common security feature in IoT architecture network layers involves block chains, ISDS and key management and encryption systems [51]

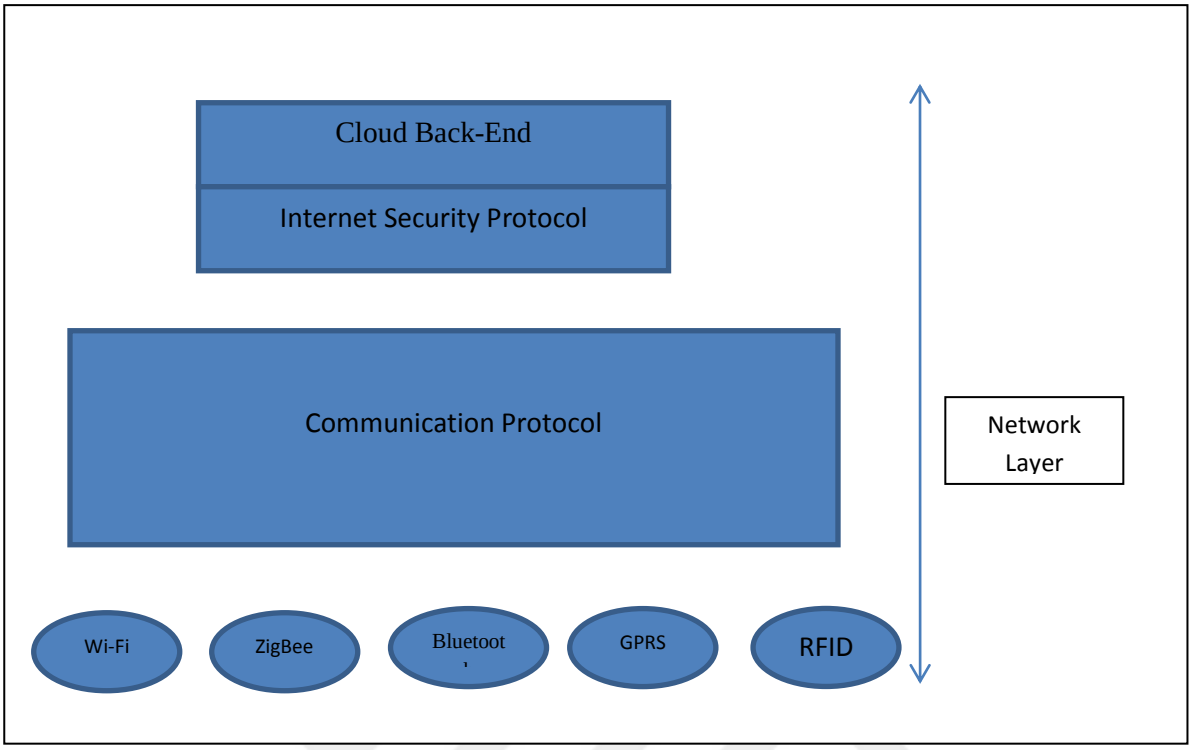

Figure 2.2: Network layer architectural elements of IoT

Edge Layer in this level, cloud users can interface with client/client domain(s) like gateways that have a coordinator position in the job domain, e.g. sensors, smart meters or IoT edge layer servers. Because the physical exposure of the IoT layer, this layer facing many threats. The most famous safety elements multi-factor authentication method, endpoint, implemented in this layer. Anti-malware approach, stable channeling and learning solutions for machines Cloud-based anomaly identification [52][53]. Disorders in IoT devices with increased computer power have contributed to a variety of deficiencies in IoT settings in various applications. These vulnerabilities can lead to fatal knowledge and failures lost in various fields. The safety of IoT habitats has therefore been drawing science group deemed in recent years, one of the most talked-about subjects. Table (2.2) displays the latest work on safety as evidence of this pattern In the IoT architecture vulnerabilities. Concerning defense, any tier in an IoT architecture can be a target for hackers, however complex or simple IoT system's design may be. To deter, identify and compensate for the attack, each threat requires an adequate security response. Therefore, protection from the top-down method application risks typically includes robbery of information, malware online applications dissemination and assault botnet

Table 2.2: Recent research on IoT architecture security flaws

Layer	Vulnerabilities	Environment
Edge-Layer	Inadequate Physical Protection, Inadequate Capture of Electrical Power	Processing of Large Amounts of Data, m- Health, Military, Physical Security
Network Layer	a lack of verification, Encryption Errors, Unnecessary ports left open	Financial, Smart-City, Industrial, Physical protection, Cloud Computer
Application Layer	Inadequate Patch Management, Inadequate Programming Skills (e.g. root user, lack of SSL, plain text pass word, backdoor, etc.), Inadequate Mechanism for Auditing	Military, Fog Computering, Smart- City, Physical Security

The network is very advantageous to leverage vulnerabilities that occur in IoT environment attackers the norm and protocols. Service denial (DoS), hijacking and corruption the protocols and norms are the most often threatened [54]. Users face various security risks and flaws, such as misconfiguration and lack of proper identity management in cloud storage components of IoT, Improper access management, protection of networks and infringements of privacy [55]. The orientation of the attached edge layer is predictable. IoT environment computers with limited computing power layer faces various risks, such as node sabotage, node Failure, server disconnection, offline data collection, fake message node Abuse, exhaustion, Sybil, jamming, mischief and trafficking [56], Figure (2.3) also shows the elements of Edge (Device) layer in IoT Architecture.

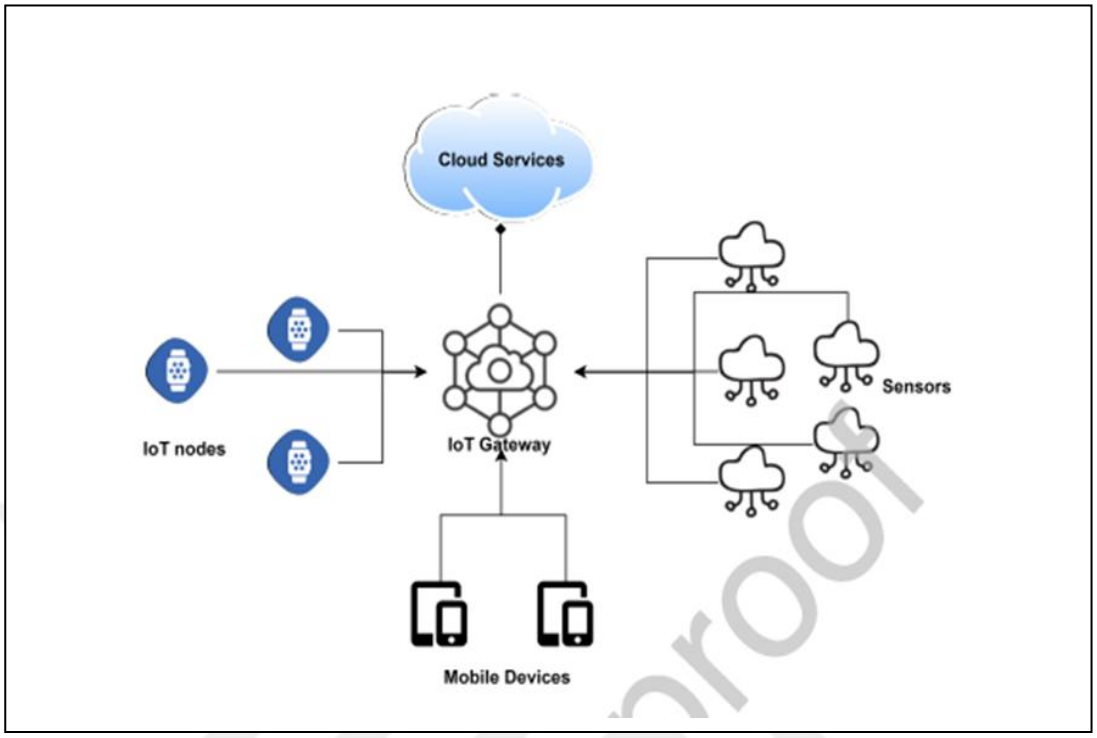

Figure 2.3: The elements of edge layer in IoT.

2.5 AIDIOTS SYSTEM

In our opinion, ADIoTS consists of a project-oriented individual or IoT device (i.e. nodes), of which all ADIoTS nodes are required to execute mission and IDS activities to attain mission objectives. We do not distinguish the member from the IoT device in this work, rather we treat him synonymously. IDS operations are conducted by the ADIoTS where the participant of intrusion detection is responsible for each node regularly at any interval (that is, T IDS). IoT computers may be corrupted by grab attacks and become insiders executing multiple malicious attacks (by physical or virtual space). A founder is a valid member and therefore gaining access to community protection core for the purpose of group communication and will stay unrecognized until the malicious activity is shown and IDS detected. The internal attacker will target packets by falling packets unexpectedly, by attacking packet modifications for integrity and by denying access attack by suffocating network/service request traffic. When it comes to a server phase, A node authorized to observe a neighboring target node can use its host IDS capabilities to identify lightweight abnormality to determine if the adjacent objective node is

behaving or misbehaving (see Fig 2.4), We presume that in the well-protected region at the device level, the commander in the mission shall deploy a mobile sink node to the destination (for instance, a drone) at any interval for IDS (namely, T IDS) to get votes from the IoT node designated to control an objective node. Notice that the mission commander's mobile sink node is not just a failure point, as its only role gather votes from nodes in the network performing intrusion detection at the host level on the target node. If there is no return of votes to the mission commander by the mobile sink node, the mission commander will automatically send another. When asked to share his view of the behavior of the neighborhood target node, the node must either vote 'yes' or 'no' against the target node. A malicious node will attack by voting "yes" to another malicious node to maintain a malicious target node in the system malicious node attacks, including ballpoint stuffing, by voting 'yes' to other malicious nodes to hold a malicious target node in the system and balloting attacks by voting 'no' to a decent node to exclude a good target node from the system can also be used to prevent the malicious target node from occurring. The goal node is expelled until the balance of the votes is 'no.' In the event of a plurality vote for a fraudulent node, the mechanism leads to a false negative (FN). In the case of a vote by a majority on a successful node "no," the mechanism leads to a false positive. Malicious nodes applied "Best" attack tactics to shorten the lifespan of the system. On the other side, good nodes (i.e., defenders) choose the "right" defensive tactics to last the lifespan of the scheme. Therefore, the attack/defense behavior, which measures its efficacy by false-negative (FN) probability and false-positive (FP) probability affecting all systems' lifespan, is defined within the framework of IDS votes. We remember that an IDS host is not optimal for a good node because a bad node may not be detected. That is, a good node could not find a bad node with a FN probability H pfn a host-level, and a good node could be misidentified as a bad node with a FP probability H pfn host-level. This values are always minimal (e.g. less than 5%) and are believed to be understood before software engineering tests release each node into operation [57].

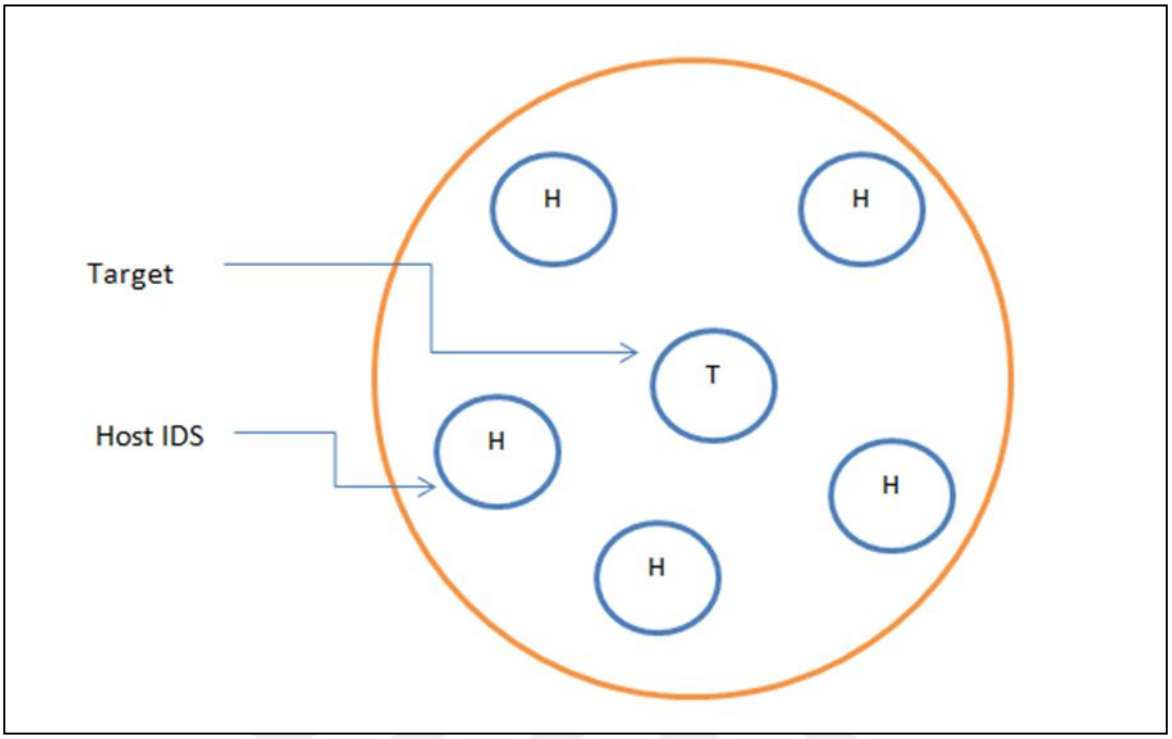

Figure 2.4:distributed voting-based IDS

2.6 IDS IN IOT CONTEXT

Network IDS (NIDS) is distinct from host IDS (HIDS) while some analysis was carried out based on both hybrid IDS methods. However, emphasized whichever kind of data is obtained, two methods can be used for detection: Mistreatment Detection or detection of abnormalities. The first detection form depends on a system of experts focusing on Signature of identified risks, with compiled rules Data or state machine changes while monitoring seconds the conduct of the device to find defects and Potential intruders, thus. The advantages of these approaches are the effective identification of abuses and identified risks. They perform well [58], but unlike anomaly, cannot detect further attacks Detection and detection. However, the identification of anomalies involves characterization and defines the system's usual conduct that can be hard to accomplish. Intrusion prevention devices have long been researched [59]. For 3 connected devices, the traditional IDS failed to defend Key explanations for this: computers with minimal

storage, mostly Smart devices are normally inadequate to operate a conventional agent working under a mesh network to transfer packets are an endpoint and there is a lot Technology and network protocol heterogeneity The IoT is used. However, a whole architecture was created to implement a software-defined network (SDN) host-based intrusion detection system, but the researcher continues to rely on network knowledge to find intrusion [60]. SDNs mostly aren't used in households, making this approach uncomfortable for the time being. Intrusion detection, in particular device abnormalities, has been used for a long time in tracking typically Systems that are embedded [61]. Tracking from intrusions may be observed Incoherent events (for example, /bin/bash execution) Systems not supposed to be) or sequences of unusual occurrences.

2.7 TYPES OF IDS

IDS can be categorised into three kinds according to their behaviour: shown in Figure (2.5), We'll go into how IDS works based on their research approach. The following are some examples:

a. Signature-based detection: Another name for this approach is rule-based detection. It contrasts the network's current form to previously-stored attack patterns [7].

b. Anomaly-based detection: Another name for this approach is event-based detection. It determines network's normal behavior, and if any activity is discovered that deviates from this, it is labeled as an intrusion [7].

c. Specification-based: It's similar to a methodology for detecting anomalies. In this case, the network's daily identified physically operations are disrupted by the user, and if malicious behavior is detected, an alarm is raised. It is time-consuming compared to the anomaly technique [7].

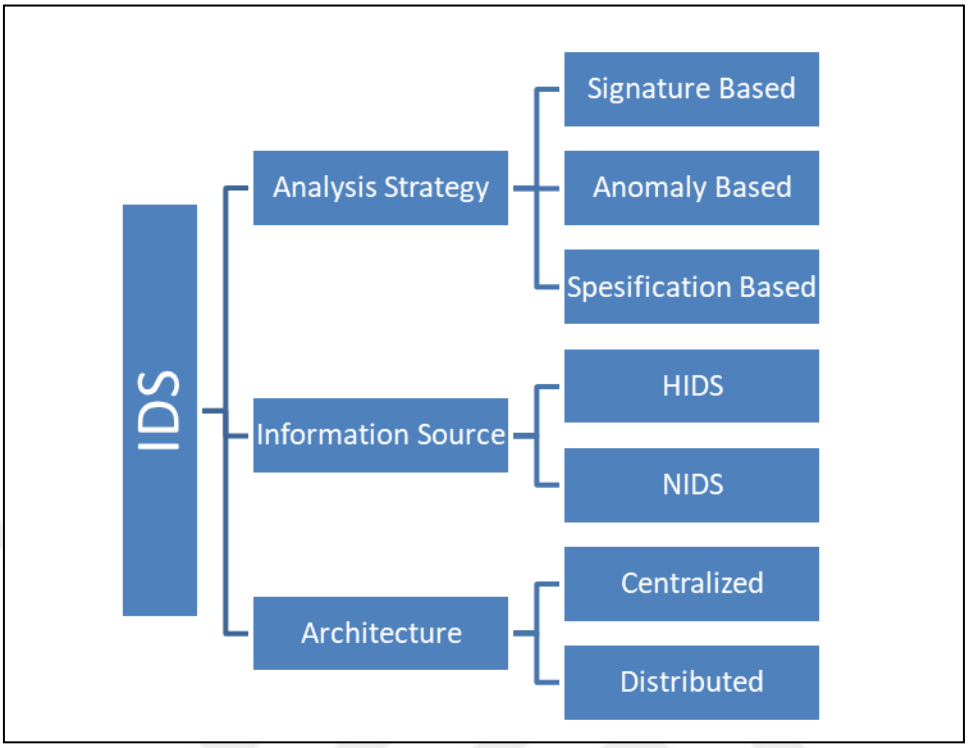

Figure 2.5: Classification of intrusion detection system based on their behavior

2.8 SECURITY GOALS

Figure (2.6) depicts the IoT security objectives, which include lightweight security solutions and privacy. As well as the CIA triad to achieve safe IoT contact, the following security principles must be taken into account.

a. SOLUTIONS THAT ARE LIGHTWEIGHT

Due to the fact of computationally intensive of IoT devices, lightweight security solutions is possible to implement as a distinguishing factor. Less efficient and with minimal memory embedded. The use of a lightweight solution should be viewed as a security measure. Design, development, and implementation requirements For IoT, there are encryption and authentication protocols [61]. RFID tags in e-passports, for example, may be affected. Un-traceability attacks; as a result, protection that is both lightweight and robust is required. These ultra-light protocols necessitate solutions that are developed specifically for them. As intended by the security algorithms or protocols IoT devices must be compliant to run on them. Restricted capabilities of the unit.

b. AUTHENTICITY

The verification and confirmation of users involved in communication are important to overcome the constraints of the IoT. ProvIt supplies a complete look of authentication mechanisms. lightweight authentication mechanism has recently been suggested for resource-constrained applications [62], RFID tags and NFC are just two examples of sophisticated technology that IoT devices may be advantageous from as a method of verification. To ascertaining resources and processors are not used at end nodes, an NFC-based authentication mechanism has been suggested [63]. Other considerations include confidence building, data, system, and user identification.

i. Validation in Context: Observed data and control information, functional effects and system statements should be pre-authenticated.

ii. Trust Management: plays a major role in reducing elements that raise the possibility of disaster and enabling client approval. Adaptive routing in the smart grid is a fully trust-based scheme for IoT elements, as stated in. Confidence building not just helps to protect IoT devices, it enhances network efficiency overall too [64]. There are various algorithms for aggregating data or machine learning methods for obtaining reliable IoT data.

iii. Identity Verification Using a User and a Device: IoT devices and the centralized control unit can authenticate a users' identity automatically, which requires a specific activity. The method can be used as a technique that utilizes a single sign-on, Users able to communicate with many once verified devices.

c. CONFIDENTIALITY

It is a major factor for IoT security. During any transmission, any information must be secured against unauthorized nodes. This can be done through a common key, which both senders and recipients use to encrypt and decrypt data.

i. Data storage: Autonomous decisions to preserve the confidentiality of vital data during local and cloud storage should be taken.

ii. Security keys: Upgrading the security key to confidentiality is difficult because of the restricted existence of IoT. An extensive research effort is required to address the difficulties of supporting the autonomous revisions of these main mechanisms for managing them. IoT with an appropriate overhead can be supported by symmetric key programs [65].

d. INTEGRITY

The integrity of data guarantees that during transmission the data is unaffected. A cryptographic symmetric the algorithm is usually used to aid the transmission of data By making them with signatures. A second way, that is, Message Integrity Check (MIC) in usage for fidelity verification information from receipt. An independent protection solution can IoT data integrity standard appropriates irrespective of insufficient resources [65]. The elements of autonomous decision-making are as follows.

a. Logs integrity: In this instance of changes, the autonomous system must have the ability to expose the direction through operation log generation. You should save the logs for a short or long time, either locally or centrally Time [65].

b. Software Integrity: the framework should ensure Software honesty that computers are running. It captured any system should be able to track pseudo-data is a network-specific pseudo-data [65].

e. AVAILABILITY

Availability ensures the availability at all times of the whole device and its elements, functional properties and services. The availability and components of these services Defence assaults [66], could be hindered. That's how it is. Invasion of IoT nodes and networks can be physically harmed. The Related stuff should always be accessible and usable they’re needed the following availability protection objectives Constant data and device availability must be taken into account.

i. Fault Tolerance: In the event of failure or an attack, the device must have ability to use the self-protection method in addition to auto-healing.

ii. Scalability: Nodes in the IoT may be arranged in a hierarchical structure in order to increase scalability. The package to get this function can be centralized [67].

f. PRIVACY

Data protection refers to the circumstance or status under which a person is to access the data or service. To ensure that nodes are scalable and different IoT applications are taken into account The Data Protection Policy must be developed. IoT devices are available it has RFID tags that have ability to easily tracked. Privacy should be safeguarded. for such devices. Multiple investigations of IoT privacy work [68] have been completed. The privacy objectives are mentioned in the following categories [65].

i. Non-Link-Ability: relates to private data which cannot be connected to another person. Unauthorized users cannot construct a profile from other users' data. Group-based signature mechanisms for solving non-linkability privacy problems are proposed in [69].

ii. Location Privacy: This ensures that no IoT device location is exposed at the current or previous location. In [68] an effective method for privacy prevention is outlined. For wireless networks, the authors suggested anonymous authentication. During authentication, the proposed architecture achieves low calculation costs.

iii. Data Privacy: portable devices link the human body to the Internet and should also maintain the protection of personal information (e.g. health).

iv. Device Privacy: RFID tags are used to render sensor nodes Traceable and recognizable. The identity of resources constrained devices is needed for anonymous communication the protocols of contact. The authors. A decentralized identifier centred in [70] was proposed Method for IoT user protection. The authors. Alleged that in small IoT the model could be implemented Devices.

g. SERVICE LEVEL AGREEMENTS

Standardized policies and processes to implement policies need to be developed to safeguard and communicate data efficiently. The implementation of standards and policies for any entity in the

network is also necessary. A contract for the level of service (S Level) that may be a means of keeping a set of rules and regulations should be clearly identified by all providers. Given the type of IoT, classical SLAs does not apply; therefore, autonomous policies to comply with SLAs by various services are to be decided. These policies must be implemented to build trust in the IoT paradigm.

Figure 2.6: Security goals of IoT

2.9 SECURITY ATTACK MECHANISMS

The properties and solutions of various types of attacks in IoT assets has been given in this paragraph. The opponent it might possibly be an insider or a network outsider and a danger to those properties a protocol stack, equipment and communication channels personal data. Computer, network, location or location the adversary carries out malicious operations on other assets unauthorized access or physical interruption to IoT services Harm the apparatus. The below are the following parts IoT-based taxonomy of security attack styles and Literature properties of them [43].

i. DEVICE PROPERTY

Heterogeneity of IoT devices. An invader can therefore target IoT devices based on device characteristics. The following are such two processes.

a. Low-End Device Attack: Low-memory devices, Power and computing capacity are taken into account like computers of low-end. This unit is used by the attacker, A cyber-attack on another IoT device are being initiated. As an example, Access to a smart TV without permission is given to an opponent clever fridge and multiple attacks with the aid of Wearable IoT devices like smart watch Threaten anonymity, completeness, or condemnation [71].

b. High-End Device Attack: An efficient and completely functioning computer is called a high-end device. An opponent can initiate attacks with advanced gadgetry (i.e., PC, laptop) to acquire access to IoT gadgets and harming them and any where's networks.

ii. LOCATION POSSESSION

IoT devices are worldwide linked and vulnerable to on-line or 6LoWPAN attacks. These attacks have the following methods [72].

a. Internal Attack: attack of an opponent by an indigenous person either your own computer or an affected network. Legitimate instrument. Such routing attacks can include Flooding, Black hole and Sinkhole Assaults Aggression.

b. External Attack: Starting an IoT attack or the assailant could install networks outdoors and away from the network of the native people. For instance, certain attacks Anti-malware software, SSL, and Secure sockets layer attacks on the DNS (Domain Name System).

iii. ATTACK GRADE

IoT devices and networks may be attacked by an opponent, like a passive or an active participant, to alter regular features or simply to get important facts. The following strategies are outlined.

a. Active Attacks: Direct attacks are categorized as active attacks to disrupt the normal operability of IoT networks or computers. Two examples of these attacks are DoS and black hole.

b. Passive Attacks: This type of attack is initiated to collect essential pieces of information from IoT networks and computers. They will also disrupt IoT privacy, including eavesdropping and data transmission tracking

iv. ATTACK PROCEDURE

There are a variety of groups that an assailant might be a part of. You may use various tactics to assault IoT and network computer.

a. Physical Attacks: the first round of this assault is launched for harm IoT devices or alter the configuration of devices. Injection of nefarious software and manipulation are some of physical attacks.

b. Logical attacks: this assault starts dysfunctional IoT devices or networks unaccompanied damaging them physically. An example of a logical attack is the traffic analysis of the communications channel.

v. HARM LEVEL

IoT computers, systems, networks, and software are susceptible to multiple attacks that can cause a variety of damage levels. It may include data breaches, service delays, and physical damage to the IoT system. The following are two such processes.

a. Service Unavailability Attack: Power failure and service shutdown, resource fatigue, and various forms of resources depletion may arise spontaneously, as a result of which service is rendered impossible. These attacks will interrupt the service (for example, a DoS attack). In addition, recovery methods should be provided in the event of this interruption [73]. These intrusions are possible to find appropriate system usage of intrusion detection (IDS).

b. Interruption Attacks: An intruder is situated between two (IoT) devices in this form of attack, the contact is intercepted, and they are tricked into connecting. this

means that: the attacker hears private messages sent discretely over private communications. Examples of such attacks include Eavesdropping, Shift, Manufacturing and Man-in-the-Middle (MitM). These assaults may confuse IoT users or lead to confusion. The intruder can modify or manufacture additional information. These attacks may be perpetrated either outside or internally. Such attacks can result in RFID devices becoming vulnerable.

vi. ATTACKS ON THE HOSTDOMAIN

IoT system is included into software that may hold confidential information, encryption keys and many other data of a sensitive nature. The data could be attackers' goals.

Any of these methods of attack are the following:

a. User Authentication Code: The opponent may deceive a user into search their personal login details like usernames and passcodes. Passcodes for logged-in users should be kept private and never shared.

b. Software Compromise: not very efficient IoT devices and integrated software. There are therefore security risks that may make the operating system and other applications vulnerable. An opponent can Make advantage of this to put embedded software in danger.

c. Compromised Hardware: The enemy can harm IoT equipments with removing credentials in the form of hardware (keys, data, or computer code) that are integrated into electronic gadgets. Hardware compromise. To initiate such attacks, physical access is typically necessary. To stay free from these attacks, IoT devices should be hard to meddle with.

vii. PROTOCOL ATTACKS

Malicious aggressors compromised IoT system and network standard protocols to interfere with device communication. The following are only a few instances of such assaults:

Protocol perversion: The opponent is breaching and diverging from normal communications or device protocols.

Protocol Disruption: The attacker may interrupt standard protocols from inside of a network or outside of it, like synchronization, collecting data, or critical management procedures.

2.10 INVESTIGATION AND DEFENSE AT LAYERS

IoT construction is is composed of a variety of technologies. that render a full device independently. We looked at the three-layered design of the IoT in the last segment. IoT-based attacks in this section define the application's three-layered architecture, Physical layers and network. Attacks on security can lead to Millions in damages for big companies and the intellectual Theft of land. The following subparagraphs include a summary of the proposed taxonomy of attack the figures in Figure (2.7). Application-based IoT attacks provide a network and physical layers classification. Many assaults are classified as multi-layer/ Dimensional assaults, which may be used for a variety of malicious purposes. IoT architecture layer; e.g. DoS or cryptanalysis Application, network and physical attacks can occur IoT's layers. An analytical comparison is given in Table 3 the system of various attacks on various IoT layers Start and the effects of the IoT attacks.

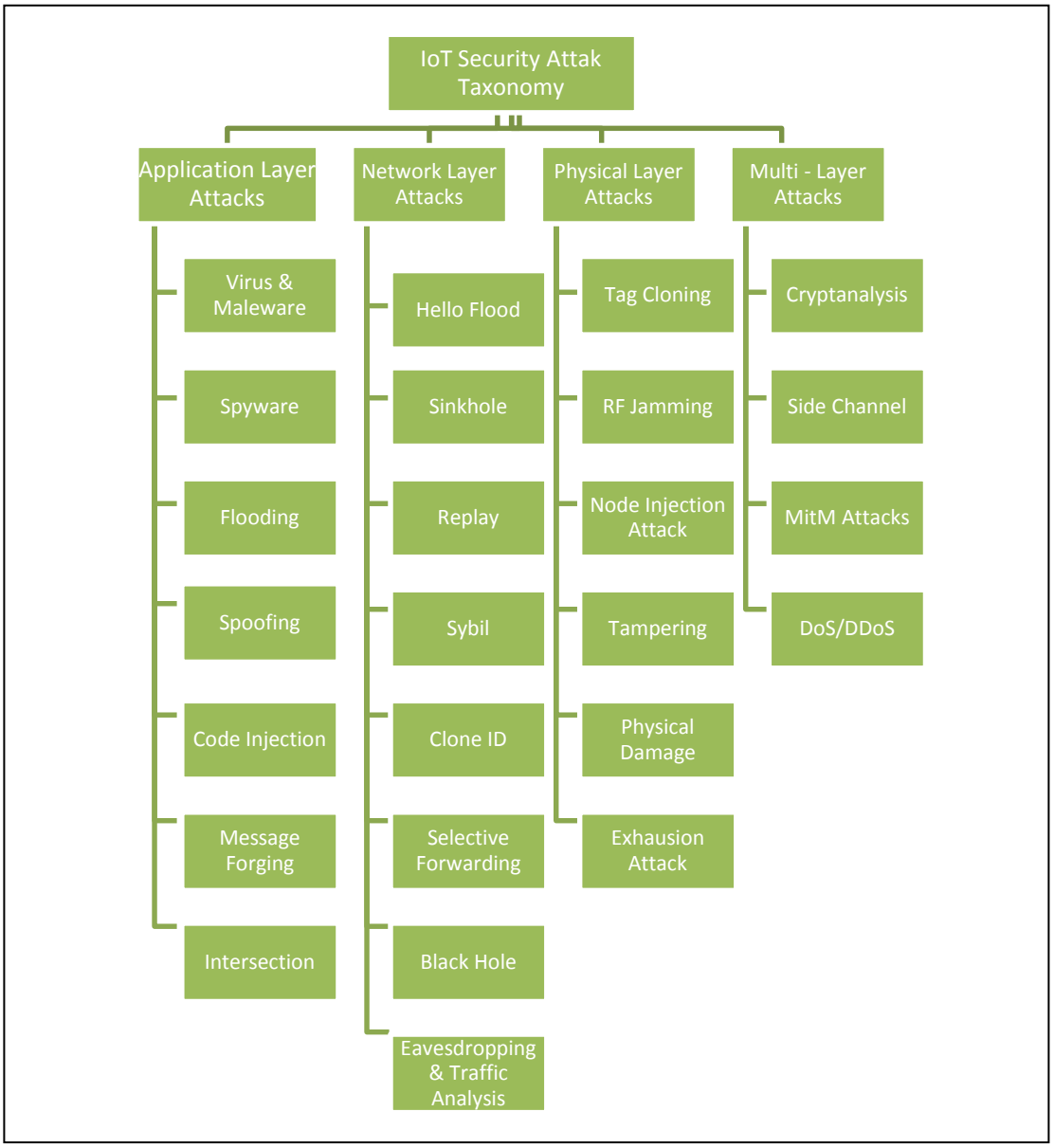

Figure 2.7: Layer-based IoT security attack taxonomy

2.11 MACHINE LEARINIG BASED INTRUSION DETECTION FOR IOT BOTNET

Few detections work on botnets on IoT devices has been done. The developers suggested a one-class host-based detection scheme [74]. For different factors including the fact that we need the IoT vendor to add host-based anomaly detectors on products, detection depending on the host technologies may not be as useful for assaults on IoT botnets. In addition, considering the rapid transmission rate of IoT botnet attacks and the daily complexity [75], Several of these variants

are effective in circumventing established early detection techniques [76]. [77] using the single-class Vector Machine Support designed to detect malicious behaviors through features like CPU and memory consumption. Suggested Botnet Traffic Shark (BoTShark) a deep-learning botnet analyzer to distinct from deep packet inspection approaches in that it utilizes just network transfers [78], relationships to be discovered of the originals and new factors for every cascade - extracted auto encoder layer or CNN. [79] Suggested T-IDS built on a new RDPLM based on a factor set of lightweight networks and a functioning selection system; Simplifying sub-spacing and numerous spontaneous metrics. [80] have studied, in particular with partial knowledge, the efficacy of several group identification algorithms for the detection of P2P botnets. They showed that with just approximately half of the nodes, the solution will disclose their contact charts only with a slight improvement in identification errors. In [81] a method is recommended for detecting infected IoT devices in a botnet. This approach is based on the logistic regression that estimates the likelihood of a bot running a communication device. [84] tests empirically a network anomaly identification approach that obtains snapshots of network traffic activity and uses deep self-encoders to recognize traffic abnormalities on the network from impaired IoT computers. [82] Also provide an excellent overview of IoT glitches, botnets and other malware attacks.

3. DESIGN AND IMPLEMENTATION

Detecting intrusions in three primary ways has become increasingly important in systems of secure data as the number of attacks grows exponentially thanks to advancements in network technology over the years. In the first method, which is referred to as the anomaly detection method, modern intrusions that have been preserved from everyday work are detected. The second technique is known as the signature detection technique, and it involves searching for a specific signature that matches and marks an intrusion. An attacker is revealed when the detection system does not agree with a set of conditions specified by the detection system. This is known as the specification-based method.

Due to time constraints, it is difficult to gather enough information for the preside classifier to design attack patterns. K-nearest neighbors learning was used in this thesis to design an intelligent IDS. This chapter explains the proposed IDS and its architecture, as well as the mobility establishment using the network simulation and the dataset source, and the preprocessing of the mentioned dataset [83].

3.1 THE PROPOSED SYSTEM MAIN CONSTRUCTION

The methodology of our proposed system for IDS based on machine learning such as RF and KNN algorithms illustrate in figure (3.1), we collected data from UNSW-NB15 Dataset, with 45 features with class labels detailed in the UNSW-NB15_features.csv file. 82332 is the total number of records stored in the CSV file, called, UNSW-NB15.csv. we preprocessed data, transform and then normalized data, splitting the dataset in the next phase into test and training with test size = 33% by using standard scalar, then the data become ready for the classifier. We applied two smart techniques such as RF and KNN algorithms to evaluate the performance of models by using many metrics like ER , ACC , Precision , Recall and F1.

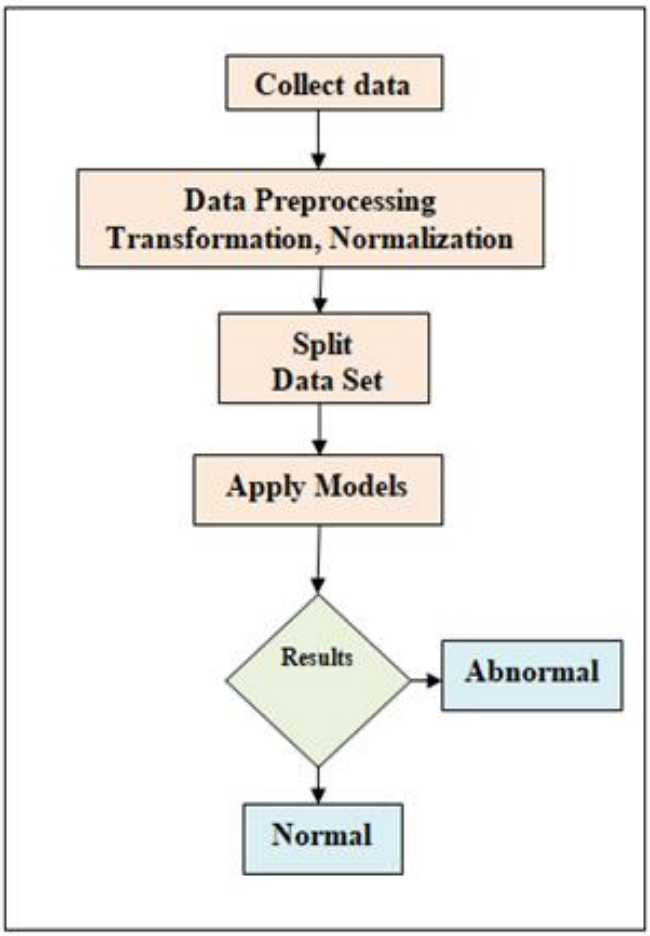

Figure 3.1: Proposed system

According to the results of these operations when it is 0 that means is normal and when the result is 1 is abnormal which mean there is an attack

3.2 DATASET DESCRIPTION

Our dataset has nine types of attacks, namely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. There are argus and Bro-IDS tools, as well as twelve algorithms, utilized to create 49 characteristics with the class label, UNSW-NB15_features.csv file contains the description of these features.

Two million and 540,044 is the total number of records stored in the four CSV files, namely, UNSW-NB151.csv, UNSW-NB152.csv, UNSW-NB153.csv and UNSW-NB154.csv.

The ground truth table is named UNSW-NB15GT.csv and the list of event file is called UNSW-NB15LIST_EVENTS.csv.

The files UNSWNB15training-set.csv and UNSWNB15testing-set.csv, which come from this dataset, are used to train and test the algorithm. The number of records in the training set is 175,341 records and the testing set is 82,332 records from the different types, attack and normal.

3.3 CLASSIFICATION WITH MACHINE LEARNING ALGORITHMS

We suggest a system for IDS of IoT, in this system we used algorithms of ML, these algorithms were RF, DT and KNN and we used UNSW-NB15 Dataset which source was [84]. We used and checked the algorithms of ML by the dependence of this data set after that we evaluate the performances of algorithms by using performance metrics such as Acc and DR, all these operations were done by python language; our methodology went through several stages:

a. Collecting data from Mustafa [84], we collected data from UNSW-NB15 Dataset, with 45 features with class labels. The UNSW-NB15_features.csv file contains the description of these features. 82332 records is the total number of records stored in the CSV file, called, UNSW-NB15.csv.

b. Preprocessing data: we preprocessed data, transformed data which they shown in figure (3.1) and then normalized them.

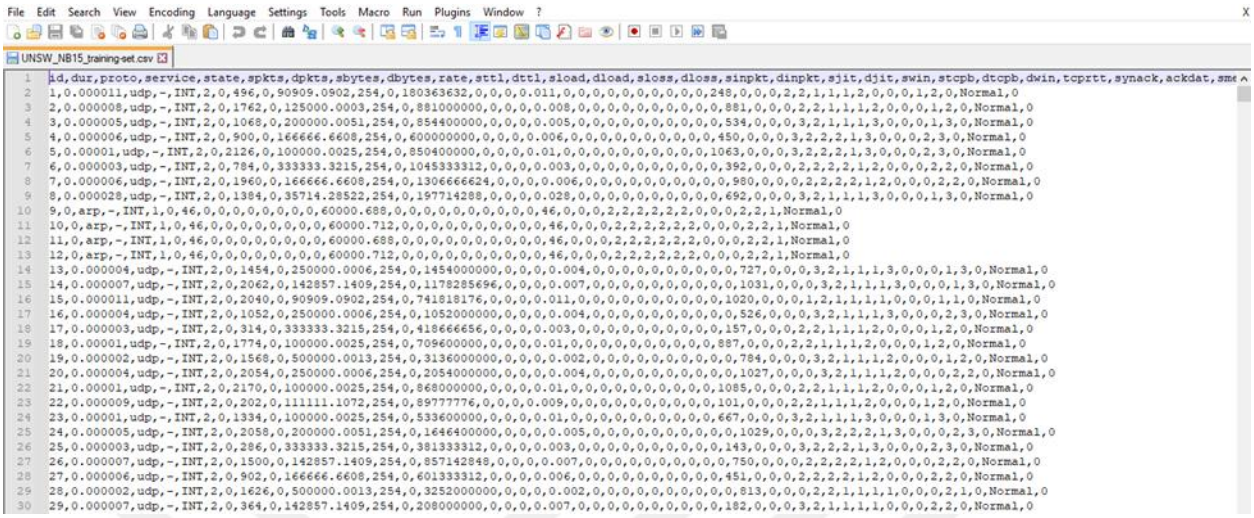

Figure 3.2: Data set

c. Data splitting: splitting dataset into test and training with test size=33% in the next phase by using standard scalar, then the data become ready for the classifier.

d. Applying ML models: We applied two smart techniques such as RF and KNN algorithms to assessing how well models perform by using many metrics like ER, ACC, Precision, Recall and F1. We considered the value of max depth= 2, and the value of Random State= 0 in RF, In KNN we used the Default Parameters.

3.4 PERFORMANCE METRICS

Numerous tests have been conducted on various data sources for malicious events as a means of determining their effectiveness and performance, The evaluation metrics of ACC, DR, FPR and Receiver Operating Characteristic (ROC) curves are used to accomplish this. As a basis for these metrics, we use four terms: True Positive (TP), True Negative (TN), False Negative (FN) and False Positive (FP). TP is the number of actual anomalous records detected as attacks, TN is the number of actual legitimate records detected as normal, FN is the number of actual anomalous records classified as normal and FP is the number of actual legitimate records classified as attacks. The metrics are described as follows.

i. The ACC is the percentage of all legitimate and anomalous records that are correctly detected, that is, ACC =T P + T N/T P + T N + F P + F N

ii. The DR is the percentage of correctly identified anomalous records that is DR = T P/T P + F N

iii. The false positive rate (FPR) is the percentage of incorrectly identified anomalous records that is F P R = F P/F P + T N

iv. The ROC curve represents the relationship between the DR in the y-axis and the FPR in the x-axis, reflecting the overall performance of a system [85].

4. RESULTS AND DISCUSSION

RESULTS AND DISCUSSIONS

The motivation of this thesis is to implement a reliable and robust detection system for protecting data from different attacks. Detection of intrusions is presented as a way to prevent malicious events. Using three ML techniques, RF, KNN and DT, to analyze the impact of these traits and efficiently detect fraudulent events. UNSW-NB15 datasets are utilized to extract and assess the technique's suggested attributes. Experimentation outcomes indicate that the proposed features exhibit traits of both normal and malicious behavior when ER, ACC, precision, recall and F1 are considered.Additionally, the suggested technique has a greater DR and a lower FPR when compared to each of the framework's classification techniques and three other state-of-the-art procedures. The suggested system's detection performance is quantified in terms of ER, ACC, precision, recall and F1. The suggested system is designed in five phases, which are: collecting data, Preprocessing of Data (Transformation, Normalization), Dataset Splitting, Apply Models, training and testing phases. A strategy for detecting intrusions is provided to reduce harmful occurrences. By using three ML approaches, DT, Naive Bayes (NB) and RF, to adequately analyze the impact of these attributes and identify malicious events. The performance metrics used in our work

The performance of a model is often evaluated using performance metrics.. There are many types of metrics. In this study, what interests us is the classification metrics, because the fraud detection problem is considered a classification problem. where some of them were used. As dataset classes are highly unbalanced, common performance metrics such as Confusion Matrix and Accuracy are unable to determine the actual fraud rate. Classification metrics must therefore be appropriately selected. The following lines describe the details of all metrics used.

4.1 SOFTWARE AND TOOLS

Throughout our tests, we have used UNSW-NB15 and DoH20 datasets. Python version 3.8.8 64-bit and KNN, RF, and DT algorithms to conduct an assessment of the proposed system and to

compare the outcomes. An experiment was conducted on a machine with 4GB memory (RAM) and a core i5 processor.

4.2 EVALUATION MEASUREMENT (EVALUATION MEASUREMENT OF CLASSIFICATION PERFORMANCE)

The proposed system performance is evaluated and measured by the confusion matrix calculation; the components of this matrix are shown in table (4.1).

Table 4.1: Confusion Matrix

		Predicated class	
		Positive class (normal)	Negative class (malignant)
	Positive class (normal)	TP	FN
Actual class	TP	FP	TN

i. TN: Indicate the total number of attacks that have been appropriately classified

ii. TP: denotes a normal behaviors that is accurately categorized.

iii. FP: Indicates to wrong detection in which normal activities are an attack that was misclassified or malignant behaviors.

iv. FN: denotes the detection system failure for intrusion detection in which malignant activities are incorrectly classified as normal behaviors.

The confusion matrix able to obtained a various values as follow:

True Positive Rate (TPR) = TP / (TP + FN) *100%. (4.1)

True Negative Rate (TNR) =TN / (TN + FP) *100%. (4.2)

False Positive Rate (FPR) = FP / (FP + TN) *100%. (4.3)

False Negative Rate (FNR) = FN / (FN + TP) *100%. (4.4)

ACC Rate = [(TP + TN)/ (TP + TN + FP + FN)] *100%. (4.5)

The FPR and the DR are both employed as assessment metrics in experiments, and they are both used to determine the success of the experiment. The FPR is referred to as the fall-out too; it can be calculated as (100-TN). The TPR is also called the DR.

4.3 EXPERIMENTAL RESULTS OF KNN-IDS WITHOUT NORMALIZATION

The proposed detection system is configured to detect the attacks; this system can define two activities which are the normal and the malignant activities. The proposed system can be evaluated using the performance metrics for both datasets (UNSW-NB15 and DoH20), which are the four different alarms (that described before) and the DR. The same datasets are used during the training and the testing phases to measure the TP, the TN, the FP, the FN Rates, and the total accuracy.

We used three algorithms for both UNSW-NB15 and DoH20 RF, KNN, DT to evaluate the performance metrics.Tables (4.2) and (4.3) shows ER, ACC, Precision, Recall and F1 values.

Table 4.2: The values of Performance metrics for UNSW-NB15 dataset by using three algorithms

algorithms	ER	ACC	Precision	Recall	F1
RF	0.95693%	99.043 %	98.281 %	100 %	99.133 %
KNN	18.8811 %	81.119 %	83.305 %	81.915 %	82.604 %
DT	0 %	100 %	100 %	100 %	100 %

Table 4.3: The values of Performance metrics for DoH20 dataset by using three algorithms

algorithms	ER	ACC	Precision	Recall	F1
RF	0 %	100 %	100 %	100 %	100 %
KNN	0.2788%	99.721 %	99.746 %	99.671 %	99.708 %
DT	0 %	100 %	100 %	100 %	100 %

The equations (4.1), (4.2), (4.3), and (4.4) are used for calculating the recognition rates for each dataset and their algorithms as shown in tables (4.4) and (4.5)

Table 4.4: The percent of alarms rate for RF, KNN and DT algorithms for UNSW-NB15 dataset

Alarms	RF	KNN	DT
TP	100%	81.92%	100%
TN	97.88%	80.16%	100%
FP	2.114%	19.84%	0
FN	0%	18.08%	0

Table 4.5: Percent of alarms rate for RF, KNN and DT algorithms for DoH20 dataset

Alarms	RF	KNN	DT
TP	100%	99.67%	100%
TN	100%	99.77%	100%
FP	0%	0.23%	0%
FN	0%	0.33%	0%

4.4 EXPERIMENTAL RESULTS OF KNN-IDS WITH NORMALIZATION

The same normalized datasets is used during training and testing phases to measure TP, TN, FP, FN Rates, and total accuracy.

Table 4.6: The values of Performance metrics for UNSW-NB15 dataset after normalization the RF, KNN, DT

algorithms	ER	ACC	Precision	Recall	F1
RF	0.85388 %	99.146 %	98.464 %	100 %	99.226 %
KNN	0 %	100 %	100 %	100 %	100 %
DT	0 %	100 %	100 %	100 %	100 %

Table 4.7: The values of Performance metrics for DoH20 dataset by using three algorithms after normalization

algorithms	ER	ACC	Precision	Recall	F1
RF	0 %	100 %	100 %	100 %	100 %
KNN	0 %	100 %	100 %	100 %	100 %
DT	0 %	100 %	100 %	100 %	100 %

The equations (4.1), (4.2), (4, 3), and (4.4) are used for calculating the recognition rates as shown in the tables (4.12) and (4.13).

Table 4.8: Percent of alarms rate for RF, KNN and DT algorithms for UNSW-NB15 dataset after normalization

Alarms	RF	KNN	DT
TP	100%	100%	100%
TN	98.11%	100%	100%
FP	1.88%	0%	0%
FN	0%	0%	0%

Table 4.9: The percent of alarms rate for RF, KNN and DT algorithms for DoH20 dataset after normalization

Alarms	RF	KNN	DT
TP	100%	100%	100%
TN	100%	100%	100%
FP	0%	0%	0%
FN	0%	0%	0%

4.5 RESULTS COMPARISON BETWEEN USED ALGORITHMS WITH AND WITHOUT NORMALIZATION

When the results of the proposed IDS that use the three algorithms (RF, KNN, DT) for both datasets UNSW-NB15 and DoH20 without normalization compared with the IDS that use with normalization, low error rate, and false alarms rate with higher accuracy rate for the proposed IDS with normalization is obtained as shown in tables (4.9) and (4.10).

Table 4.10: Comparison of accuracy and error rate between IDS with and without normalization for RF, KNN, and DT for UNSW-NB15 dataset

Class	RF		KNN		DT	
	ACC	ER	ACC	ER	ACC	ER
Without Normalization	99.043 %	0.95693%	81.119 %	18.8811 %	100 %	0%
With Normalization	99.146 %	0.85388 %	100 %	0%	100 %	0%

Table 4.11: Comparison of accuracy and error rate between IDS with and without normalization for RF, KNN, and DT for DoH20 dataset

Class	RF		KNN		DT	
	ACC	ER	ACC	ER	ACC	ER
Without Normalization	100 %	0%	99.721 %	0.279%	100 %	0%
With Normalization	100 %	0%	100 %	0%	100 %	0%

According to the results shown in tables (4.10) and (4.11), the proposed IDS that utilize the RF and DT algorithms are not effective considerably with normalization, while we notice the KNN algorithm is effective and efficient than the system that utilizes KNN without normalization.

5. CONCLUSION AND UPCOMING PROJECTS

5.1 CONCLUSIONS

By using UNSW NB15 and DoH20 datasets in IoT networkswere gathered and presented in this work. The datasets are developed with the goal of replication the behaviour and a series of attacks against real-world networks. We treated data with three algorithms as RF, KNN and DT, We discovered that the performance of RF and DT are superior to the KNN performance in both datasets by analyzing the results for both classifiers, The KNN method was then normalized to increase its performance. and we got a worth result in KNN performance and enhanced the performance of KNN against the attacker by increasing the values of Accuracy from 81.119 % to 100% and in UNSW NB15 dataset and 99.721% to 100% in DoH20 dataset, and decreasing the error rate from de 18.8811 % to 0% in UNSW NB15 dataset and from 0.279% to 0% in DoH20 dataset.

5.2 FUTURE WORKS

The primary goal of this project is to uncover intrusions into IoT. To obtain that, three ML techniques have been used over two datasets. This research demonstrates that ML is capable of effectively defending against attacks in the IoT.

An effort to include elements from other IoT protocols into this work is expected to take place in the future to build a dynamic profile of normal and attacking behaviour. Utilizing the proposed method, Existing and zero-day attacks can be detected with the help of a feature database like this one.

5.3 LIMITATIONS

The suggested IDSused in this thesis is not without flaws There are still a couple of potential issues that need to be looked into and rectified before moving forward Because of the limited time available for the thesis project, some of these limitations as follow Time is a significant constraint, The computational overhead of the suggested system, as well as the cost of implementing the proposed IDS.

REFERENCES

[1] P. Singh, "Internet of Things Based Health Monitoring System : Opportunities and Challenges," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 1, pp. 224–228, 2018, doi: 10.26483/ijarcs.v9i1.5308.

[2] H. D. Kotha and V. Mnssvkr Gupta, "IoT application, a survey," *Int. J. Eng. Technol.*, vol. 7, no. May, pp. 891–896, 2018, doi: 10.14419/ijet.v7i2.7.11089.

[3] J. Beavers and S. Pournouri, "Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions," in *Advanced Sciences and Technologies for Security Applications*, Springer, Cham, 2019, pp. 249–267.

[4] Okul, M. A. Aydin, and F. Keleş, "Security problems and attacks on smart cars," in *Lecture Notes in Electrical Engineering*, 2019, vol. 504, pp. 203–213, doi: 10.1007/978-981-13-0408-8_17.

[5] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," *Comput. Law Secur. Rev.*, vol. 32, no. 1, pp. 4–15, Feb. 2016, doi: 10.1016/J.CLSR.2015.12.001.

[6] Y. Liu, T. Liu, H. Sun, K. Zhang, and P. Liu, "Hidden Electricity Theft by Exploiting Multiple-Pricing Scheme in Smart Grids," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2453–2468, 2020, doi: 10.1109/TIFS.2020.2965276.

[7] S. Choudhary and N. Kesswani, "A survey: Intrusion detection techniques for internet of things," *Int. J. Inf. Secur. Priv.*, vol. 13, no. 1, pp. 86–105, 2019, doi: 10.4018/IJISP.2019010107.

[8] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion detection systems in wireless sensor networks: A review,” *International Journal of Distributed Sensor Networks*, vol. 2013. SAGE PublicationsSage UK: London, England, May 19, 2013, doi: 10.1155/2013/167575.

[9] G. Spanos *et al.*, “A Lightweight Cyber-Security Defense Framework for Smart Homes,” *INISTA 2020 - 2020 Int. Conf. Innov. Intell. Syst. Appl. Proc.*, no. 740923, 2020, doi: 10.1109/INISTA49547.2020.9194689.

[10] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. Sanz Rodrigo, “An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets,” *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–15, Jan. 2021, doi: 10.3390/s21020656.

[11] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, “A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks,” *IEEE Internet Things J.*, pp. 1–1, May 2020, doi: 10.1109/jiot.2020.2996590.

[12] S. M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, and M. H. Zavvar, “Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree,” in *2020 6th International Conference on Web Research, ICWR 2020*, Apr. 2020, pp. 152–156, doi: 10.1109/ICWR49608.2020.9122320.

[13] A. Yahyaoui, T. Abdellatif, S. Yangui, and R. Attia, “READ-IoT: Reliable Event and Anomaly Detection Framework for the Internet of Things,” *IEEE Access*, vol. 9, pp. 24168–24186, 2021, doi: 10.1109/ACCESS.2021.3056149.

[14] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning," in *CENIM 2020 - Proceeding: International Conference on Computer Engineering, Network, and Intelligent Multimedia 2020*, Nov. 2020, pp. 303–308, doi: 10.1109/CENIM51130.2020.9297958.

[15] B. Susilo and R. F. Sari, "Intrusion Detection in IoT Networks Using Deep Learning Algorithm," *Information*, vol. 11, no. 5, p. 279, May 2020, doi: 10.3390/info11050279.

[16] I. Ullah and Q. H. Mahmoud, "A Technique for Generating a Botnet Dataset for Anomalous Activity Detection in IoT Networks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Oct. 2020, vol. 2020-Octob, pp. 134–140, doi: 10.1109/SMC42975.2020.9283220.

[17] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," in *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, Jan. 2020, pp. 562–567, doi: 10.1109/CCWC47524.2020.9031206.

[18] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

[19] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2219–2230, Oct. 2020, doi: 10.1109/TNSE.2020.2990984.

[20] I. Ullah and Q. H. Mahmoud, “A two-level flow-based anomalous activity detection system for IoT networks,” *Electron.*, vol. 9, no. 3, p. 530, Mar. 2020, doi: 10.3390/electronics9030530.

[21] A. Verma and V. Ranga, “Machine Learning Based Intrusion Detection Systems for IoT Applications,” *Wirel. Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, 2020, doi: 10.1007/s11277-019-06986-8.

[22] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, “Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges,” *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.

[23] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A Supervised Intrusion Detection System for Smart Home IoT Devices,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, 2019, doi: 10.1109/JIOT.2019.2926365.

[24] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang, “Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network,” *IEEE Access*, vol. 7, pp. 106043–106052, 2019, doi: 10.1109/ACCESS.2019.2929919.

[25] H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: A survey,” *Appl. Sci.*, vol. 9, no. 20, 2019, doi: 10.3390/app9204396.

[26] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, “Toward a Lightweight Intrusion Detection System for the Internet of Things,” *IEEE Access*, vol. 7, pp. 42450–42471, 2019, doi: 10.1109/ACCESS.2019.2907965.

[27] G. Thamilarasu and S. Chawla, “Towards deep-learning-driven intrusion detection for the internet of things,” *Sensors (Switzerland)*, vol. 19, no. 9, p. 1977, Apr. 2019, doi: 10.3390/s19091977.

[28] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks,” *Electron.*, vol. 8, no. 11, 2019, doi: 10.3390/electronics8111210.

[29] L. A. Amaral, F. P. Hessel, E. A. Bezerra, J. C. Corrêa, O. B. Longhi, and T. F. O. Dias, “ECloudRFID - A mobile software framework architecture for pervasive RFID-based applications,” *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 972–979, May 2011, doi: 10.1016/j.jnca.2010.04.005.

[30] G. Svensson, “Auditing the Human Factor as a Part of Setting up an Information Security Management System,” pp. 1–29, 2013, Accessed: May 20, 2021. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-119528.

[31] E. D. Frangopoulos, M. M. Eloff, and L. M. Venter, “Psychosocial risks: Can their effects on the security of information systems really be ignored?,” *Inf. Manag. Comput. Secur.*, vol. 21, no. 1, pp. 53–65, 2013, doi: 10.1108/09685221311314428.

[32] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 1933–1954, Apr. 24, 2014, doi: 10.1109/COMST.2014.2320093.

[33] M. S. Virat, S. M. Bindu, B. Aishwarya, B. N. Dhanush, and M. R. Kounte, “Security and

Privacy Challenges in Internet of Things," in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, Nov. 2018, pp. 454–460, doi: 10.1109/ICOEI.2018.8553919.

[34] J. Colding and S. Barthel, "An urban ecology critique on the 'Smart City' model," *Journal of Cleaner Production*, vol. 164. Elsevier Ltd, pp. 95–101, Oct. 15, 2017, doi: 10.1016/j.jclepro.2017.06.191.

[35] Z. Pang *et al.*, "Mobile and wide area deployable sensor system for networked services," in *Proceedings of IEEE Sensors*, 2009, pp. 1396–1399, doi: 10.1109/ICSENS.2009.5398428.

[36] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5. Institute of Electrical and Electronics Engineers Inc., pp. 26521–26544, Nov. 29, 2017, doi: 10.1109/ACCESS.2017.2775180.

[37] L. Alonso, V. Milanés, C. Torre-Ferrero, J. Godoy, J. P. Oria, and T. de Pedro, "Ultrasonic sensors in urban traffic driving-aid systems," *Sensors*, vol. 11, no. 1, pp. 661–673, Jan. 2011, doi: 10.3390/s110100661.

[38] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54. Elsevier, pp. 1–31, Dec. 01, 2014, doi: 10.1016/j.comcom.2014.09.008.

[39] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*,

vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[40] A. L. Review, “The Use , Benefits and Challenges of using the Internet of Things (IoT) in retail businesses A Literature Review,” pp. 430–436, 2016.

[41] R. Gupta, “ABC of Internet of Things : Advancements , Benefits , Challenges , Enablers and Facilities of IoT,” 2016.

[42] S. Khanam, I. Bin Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, “A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things,” *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/ACCESS.2020.3037359.

[43] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” in *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015*, Aug. 2015, pp. 21–28, doi: 10.1109/SERVICES.2015.12.

[44] S. Li, T. Tryfonas, and H. Li, “The Internet of Things: a security point of view,” *Internet Res.*, vol. 26, no. 2, pp. 337–359, Apr. 2016, doi: 10.1108/IntR-07-2014-0173.

[45] E. R. Naru, H. Saini, and M. Sharma, “A recent review on lightweight cryptography in IoT,” in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, Oct. 2017, pp. 887–890, doi: 10.1109/I-SMAC.2017.8058307.

[46] A. Paranjothi, M. S. Khan, S. Zeadally, A. Pawar, and D. Hicks, “GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model,” *arXiv*, vol. 7. arXiv, p. 100071, Jun. 10, 2019, doi: 10.1016/j.iot.2019.100071.

[47] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, “IoT Middleware: A Survey on Issues and Enabling Technologies,” *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2017, doi: 10.1109/JIOT.2016.2615180.

[48] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, “Advanced internet of things for personalised healthcare systems: A survey,” *Pervasive and Mobile Computing*, vol. 41. Elsevier B.V., pp. 132–149, Oct. 01, 2017, doi: 10.1016/j.pmcj.2017.06.018.

[49] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, “CoAPâ€”Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP,” in *Internet of Things*, Springer International Publishing, 2020, pp. 151–175.

[50] J. Santos, J. J. P. C. Rodrigues, B. M. C. Silva, J. Casal, K. Saleem, and V. Denisov, “An IoT-based mobile gateway for intelligent personal assistants on mobile health environments,” *J. Netw. Comput. Appl.*, vol. 71, pp. 194–204, Aug. 2016, doi: 10.1016/j.jnca.2016.03.014.

[51] D. Minoli and B. Occhiogrosso, “Blockchain mechanisms for IoT security,” *Internet of Things*, vol. 1–2, pp. 1–13, Sep. 2018, doi: 10.1016/j.iot.2018.05.002.

[52] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, “Threats to Networking Cloud and Edge Datacenters in the Internet of Things,” *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May 2016, doi: 10.1109/MCC.2016.63.

[53] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, “Fuzzy pattern tree for edge malware detection and categorization in IoT,” *J.*

Syst. Archit., vol. 97, pp. 1–7, Aug. 2019, doi: 10.1016/j.sysarc.2019.01.017.

[54] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88. Academic Press, pp. 10–28, Jun. 15, 2017, doi: 10.1016/j.jnca.2017.04.002.

[55] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 2013, pp. 663–667, doi: 10.1109/CIS.2013.145.

[56] K. Sha, R. Errabelly, W. Wei, T. A. Yang, and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," in *Proceedings - 2017 IEEE 1st International Conference on Fog and Edge Computing, ICFEC 2017*, Aug. 2017, pp. 81–88, doi: 10.1109/ICFEC.2017.7.

[57] H. Al-Hamadi, I. R. Chen, D. C. Wang, and M. Almashan, "Attack and defense strategies for intrusion detection in autonomous distributed IoT systems," *IEEE Access*, vol. 8, pp. 168994–169009, 2020, doi: 10.1109/ACCESS.2020.3023616.

[58] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," in *Proceedings - IEEE Military Communications Conference MILCOM*, Dec. 2017, vol. 2017-October, pp. 267–272, doi: 10.1109/MILCOM.2017.8170867.

[59] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84. Academic Press, pp. 25–37, Apr. 15, 2017, doi: 10.1016/j.jnca.2017.02.009.

[60] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and

mitigation framework for smart home IoT using OpenFlow," in *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, Dec. 2016, pp. 147–156, doi: 10.1109/ARES.2016.64.

[61] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: Behavior-based malware detection system for android," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2011, pp. 15–25, doi: 10.1145/2046614.2046619.

[62] T. Nandy *et al.*, "Review on Security of Internet of Things Authentication Mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[63] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the era of wireless keys: How the IoT can change authentication paradigm," in *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, 2014, pp. 51–56, doi: 10.1109/WF-IoT.2014.6803116.

[64] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 623–632, 2012, doi: 10.1109/TITB.2012.2194788.

[65] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," *Journal of Network and Computer Applications*, vol. 49. Academic Press, pp. 112–127, Mar. 01, 2015, doi: 10.1016/j.jnca.2014.11.011.

[66] R. Sudirman, N. Tabatabaey-Mashadi, and I. Ariffin, "Aspects of a standardized automated system for screening children's handwriting," in *Proceedings - 1st International Conference on Informatics and Computational Intelligence, ICI 2011*, 2011, pp. 49–54, doi: 10.1109/ICI.2011.19.

[67] A. Ahmed, A. H. Ahmed, N. M. Omar, and H. M. Ibrahim, “Modern IoT Architectures Review: A Security Perspective,” 2017, doi: 10.5176/2251-2136_ICT-BDCS17.30.

[68] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, “Efficient and Secure Anonymous Authentication with Location Privacy for IoT-Based WBANs,” *IEEE Trans. Ind. Informatics*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020, doi: 10.1109/TII.2019.2925071.

[69] L. Garms and A. Lehmann, “Group Signatures with Selective Linkability,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Apr. 2019, vol. 11442 LNCS, pp. 190–220, doi: 10.1007/978-3-030-17253-4_7.

[70] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou, “Improving the Privacy of IoT with Decentralised Identifiers (DIDs),” *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/8706760.

[71] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, “Operating Systems for Low-End Devices in the Internet of Things: A Survey,” *IEEE Internet Things J.*, vol. 3, no. 5, pp. 720–734, Oct. 2016, doi: 10.1109/JIOT.2015.2505901.

[72] A. K. Bairagi, R. Khondoker, and R. Islam, “An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures,” *Inf. Secur. J.*, vol. 25, no. 4–6, pp. 197–212, Dec. 2016, doi: 10.1080/19393555.2016.1206640.

[73] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” in

Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 2012, vol. 3, pp. 648–651, doi: 10.1109/ICCSEE.2012.373.

[74] V. H. Bezerra, V. G. T. da Costa, S. B. Junior, R. S. Miani, and B. B. Zarpelão, "One-class Classification to Detect Botnets in IoT devices ∗," *An. do XVIII Simpósio Bras. em Segurança da Informação e Sist. Comput.*, no. October, pp. 43–56, Oct. 2018, Accessed: May 17, 2021. [Online]. Available: http://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/index.html.

[75] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[76] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer (Long. Beach. Calif).*, vol. 50, no. 2, pp. 76–79, Feb. 2017, doi: 10.1109/MC.2017.62.

[77] A. A. Munshi and Y. A. R. I. Mohamed, "Data Lake Lambda Architecture for Smart Grids Big Data Analytics," *IEEE Access*, vol. 6, pp. 40463–40471, Jul. 2018, doi: 10.1109/ACCESS.2018.2858256.

[78] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "BoTShark: A deep learning approach for botnet traffic detection," in *Advances in Information Security*, vol. 70, Springer New York LLC, 2018, pp. 137–153.

[79] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha, and K. Kim, "Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection," *IEEE Trans. Cybern.*, vol. 46, no. 8, pp. 1796–1806, Aug. 2016, doi:

10.1109/TCYB.2015.2490802.

[80] H. P. Joshi, M. Bennison, and R. Dutta, “Collaborative botnet detection with partial communication graph information,” Oct. 2017, doi: 10.1109/SARNOF.2017.8080397.

[81] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, “A method to detect Internet of Things botnets,” in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, Mar. 2018, vol. 2018-January, pp. 105–108, doi: 10.1109/EIConRus.2018.8317041.

[82] Y. Meidan *et al.*, “N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders,” *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

[83] S. M. Shahooth, “Intelligent Intrusion Detection System for Drones Based on KNN and LDA,” 2020.

[84] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” Dec. 2015, doi: 10.1109/MilCIS.2015.7348942.

[85] N. Moustafa, B. Turnbull, and K. K. R. Choo, “An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, 2019, doi: 10.1109/JIOT.2018.2871719.