T.C.

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

AN EFFICIENT IOTS SECURITY METHOD BASED ON OPTIMIZED MACHINE LEARNING TECHNIQUE AND OPTIMIZATION ALGORITHM

Taif Ayad Khaleel KHALEEL

Master's Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2020

A NEW METHOD BASED DATA MINING TECHNIQUES TO DETECT DISTRIBUTED DENIALS OF SERVICE (DDOS) ATTACKS IN CLOUD COMPUTING

by

Taif Ayad Khaleel KHALEEL

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2020

The thesis titled “A NEW METHOD BASED DATA MINING TECHNIQUES TO DETECT DISTRIBUTED DENIALS OF SERVICE (DDOS) ATTACKS IN CLOUD COMPUTING” prepared and presented by “TAIF AYAD KHALEEL KHALEEL” was accepted as a Master of Science Thesis in Electrical and Computer Engineering.

Asst. Prof. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

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

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

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.

Taif Ayad Khaleel KHALEEL

DEDICATION

I dedicate my dissertation work to my family. A special feeling of gratitude to my loving parents, Ayad and Buthainah who's words of encouragement and push for tenacity ring in my ears. My brother Mohammed, my sister Haneen and my uncle Alauldeen who have never left my side and supported me throughout the process.

ACKNOWLEDGEMENTS

I would like to thank my thesis supervisor Asst. Prof. Dr**.** Sefer Kurnaz from the Electrical and Computer Engineering at Altınbaş University. He always supported and steered me in the right direction whenever he thought I needed it.

Finally, I must express my very profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

ABSTRACT

AN EFFICIENT IOTS SECURITY METHOD BASED ON OPTIMIZED MACHINE LEARNING TECHNIQUE AND OPTIMIZATION ALGORITHM

Khaleel, Taif Ayad Khaleel

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

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: October, 2020

Pages: 45

In the study, new method presented to detect IDS attacks in IoTs using machine larning techniques. In the first stage, the GWO applied to the input data to select effective features of IDS dataset. The GWO is one of the common used optimization algorithms in the last years which applied in several fields such as: computer security, feature selection, image recognition, and optimization problems. The KNN applied as classifiers to classify the selected features by GWO. We developed the framework which is presented high detection rate in IoTs security issue. The aim of this study to assist the growing of IoTs which huge problem of this field is security problem. Then, the presented framework compared with numerous studies proposed to detect attack in IoTs.

Keywords: IDS, machine learning, computer security, IoTs.

ÖZET

OPTİMİZE MAKİNE ÖĞRENME TEKNİĞİ VE OPTİMİZASYON ALGORİTMASINA DAYALI VERİMLİ GÜVENLİK YÖNTEM

Khaleel, Taıf Ayad Khaleel

Yüksek Lisans, Elektrik Ve Bilgisayar Mühendisliği, Altınbaş Üniversitesi,

Danışman: Dr. Öğr. Üyesi Sefer KURNAZ

Tarih: Ekim, 2020

Sayfa Sayısı: 45

Bu Çalışmada, makine larning teknikleri kullanılarak IoT'lerde IDS saldırılarını tespit etmek için yeni bir yöntem sunulmuştur. İlk aşamada GWO, IDS veri kümesinin etkili özelliklerini seçmek için giriş verilerine uygulandı. GWO, son yıllarda bilgisayar güvenliği, özellik seçimi, görüntü tanıma ve optimizasyon sorunları gibi çeşitli alanlarda uygulanan yaygın kullanılan optimizasyon algoritmalarından biridir. KNN, seçilen özellikleri GWO'ya göre sınıflandırmak için sınıflandırıcılar olarak uygulanmıştır. IoT'lerin güvenlik konusunda yüksek tespit oranı sunan çerçeveyi geliştirdik. Bu çalışmanın amacı, bu alandaki büyük problemin güvenlik sorunu olan IoT'lerin büyümesine yardımcı olmaktır. Daha sonra sunulan çerçeve, IoT'lerde saldırıyı tespit etmek için önerilen çok sayıda çalışma ile karşılaştırıldı.

Anahtar Kelimeler: IDS, makine öğrenimi, bilgisayar güvenliği, IoTs.

TABLE OF CONTENTS

Pages

ABSTRACT……vii

ÖZET……viii

LIST OF TABLES...……viii

LIST OF FIGURES xii

LIST OF ABBREVIATIONS xiii

1. INTRODUCTION 1

1.1 CONTRIBUTION 3

1.2 PROBLEM STATEMENT 3

1.3 QUESTIONS OF THE RESEARCH 3

1.4 THE PURPOSE OF THESIS 3

2. OVERVIEW 4

2.1 SURVEY 4

2.2 CHALENGES OF IOTS 5

2.3 BENEFITS OF IOTS 6

2.4 DISADVANTAGES OF IOTS 8

2.5 IOTS SECURITY 8

2.6 ATTACKS IN IOTS 9

2.7 AN INTRUSION DETECTION SYSTEM (IDS) 11

2.7.1 Signature Based (Misuse) IDS 12

2.7.2 Anomaly Based IDS 13

2.7.3 Hybrid IDS 14

2.7.4 P2P Network……15

2.7.5 P2P Traffic Detection 15

3. MATERIAL AND METHODS 17

3.1 MACHINE LEARNING 17
3.1.1 Feature Extraction 18
3.1.1.1 PCA 18
3.1.1.2 K-means clustering 19
3.1.2 Classification 19
3.1.2.1 Neural Network 20
3.2 DEEP NEURAL NETWORK (DNN) 20
3.2.1 Convolutional Neural Network (CNN) 22
3.2.2 Recurrent Neural Network (RNN) 23
3.2.4 Deep Belief Network (DBN) 25
3.3 OUR FRAMEWORK GWO BASED KNN 26
4. EXPERIMENTS AND DISSCUSION 27
4.1 MATLAB TOOLBOX 27
4.2 VALIDATION TECHNIQUES 27
4.2.1 k-Cross Validation 27
4.1.3 LEAVE-ONE-OUT CROSS 28
4.2 DATASET 29
4.3 RESULTS 31
5. CONCLUSION 33
REFERENCES 34

LIST OF TABLES

Pages

Table 4.1: DDoS dataset features [39] 30

Table 4.2: KNN 31

Table 4.3: GWO+KNN 32

Table 4.4: Results GWO+KNN 32

LIST OF FIGURES

Pages

Figure 1.1: Security Services Architecture [3]. 2

Figure 2.1:The Architecture of the SDN-based WSN clusters for IoT [12] 6

Figure 3.1: Shallow Neural Network [28]. 20

Figure 3.2: Recurrent Neural Network (RNN) [34] 22

Figure 3.3: Convolutional Neural Network (CNN) [34] 23

Figure 3.4: Simple RNN, 3 input and 1 output [34]. 23

Figure 3.5: Simple Series Time RNN [34]. 24

Figure 3.6: RNN 3 Input and 3 Outputs [34] 25

Figure 3.7: RBM in DBNs 26

Figure 4.1: k-Cross Validation [36] 28

Figure 4.2: Leave-one-out cross [38] 29

Figure 4.3: Results of Our Method 32

LIST OF ABBREVIATIONS

SVM	:	Support vector machine
NN	:	Neural Network
RBF	:	Radial Basis Function
DBN	:	Deep Belief Network
DDoS	:	A distributed denial-of-service (DDoS)

1. INTRODUCTION

The Internet of Things (IoT) has increased the number of devices on the internet, largely because of the need to obtain information from these devices for various IoT applications, so that the number of these devices is expected to continue to rise [1]. Cisco expects that the number of Internet-connected devices will rise to approximately 50 billion by next year. Nowadays, wireless sensor and actuator networks (WSANs) play a significantrole in data transfer from several systems through their various applications. Applications include environmental monitoring data such as air temperature, humidity, smog-like gasses and precision agriculture. WSAN networks have become very important and preferred for several applications due to characteristics such as their low cost, small size, low power consumption, mobility, and multifunctional sensors. For these reasons, integration of WSAN and IoT networks is useful for IoT applications, but there are also challenges to meet IoT application requirements such as energy efficiency, flexible management, and network reconfiguration after deployment. The most important design constraints when constructing a WSAN is energy efficiency, because each device operates with limited power resources. These devices consume more power when they send or receive data depending on the routing protocol used [2]. Therefore, the routing mechanism has to take in energy consumption parameters to be controlled. Thus, a smart and flexible network is needed for forwarding data among those devices. Moreover, the routing protocol must be designed in such a way as to maximize the lifetime of the network by saving energy. The routing decision used in traditional wireless network sensors does not take into account energy consumption during communication, which results in unmeasured energy consumption, unwanted delays and a great deal of overhead traffic. These results are required for some IoT applications, since IoT applications' performance relies on the forwarding and routing methods. Therefore, IoT applications need to make appropriate decisions based on the lowest possible path cost to send data through WSN nodes from the source to the target. This challenge requires an intelligent network energy administration for WSAN devices. Network management and control design form the key part of the solution, the software-defined networking (SDN) architecture, which aims to provide solutions such as security and network privacy reconfiguration after deployment to IoTs. Since Security of the IoTs is the most important task of an IoTs, as we will see in the literature, there are many different proposals for this purpose. The

research interest of this thesis is to integrate the concept of SDN for IoT technologies and perform better flexible network energy management for WSAN devices.

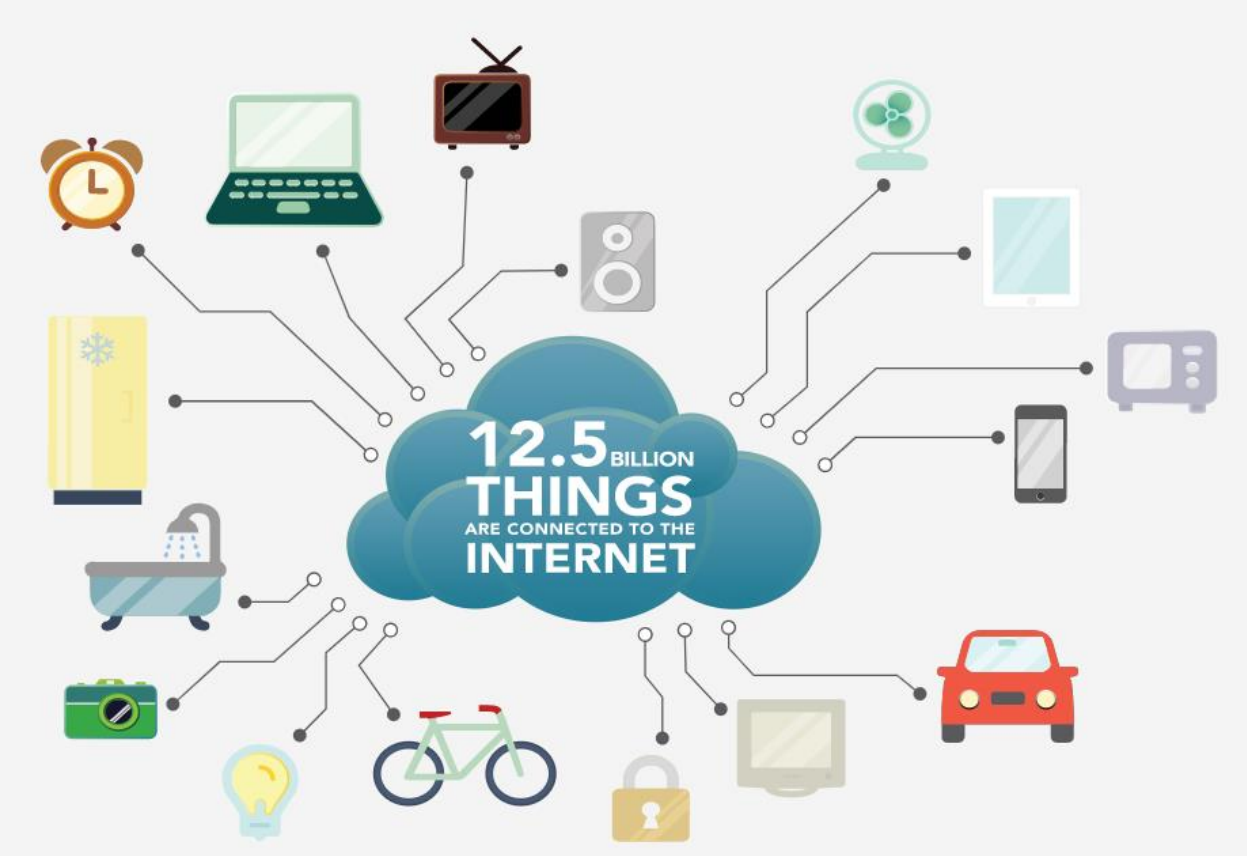

Figure 1.1: Security Services Architecture [3].

Recently, Software Defined Networks (SDN) are a new solution to reconfigure and manage networks according to application needs, increasing interest in the computer network community. SDN Architecture to separate data and control layers, all network management functions are performed by a central device called the SDN controller (SDNC). During this time, the network devices in the data level are only responsible for data transmission using the corresponding entries in the flow table. The advantage of using the SDNC is that the applications' data relies on the forwarding and routing method's performance. Besides that, the SDNC device should make an appropriate decision based on the lowest cost path from the source to the destination, since paths with higher costs make devices consume a great deal of energy in a short time.

Software-defined networking developed as an intelligent solution to many wired network issues: troubleshooting, traffic management, and resources on the network deployed in cloud data centers.

Despite these developments, SDN is creating tremendous enhancements in network programming that do not require any hardware replacement. Although the SDN concept was built on wired networks, it was not planned to implement the SDN concept in a WSAN. Many researchers have recently discussed the issues with integrating SDN into a WSAN network structure [4].

1.1 CONTRIBUTION

Established software to detect IDS attacks in IoTs by using ML based optimization algorithms. Use ML techniques the optimized using optimization algorithms and compare the results. Several supervised ML techniques are applied to this problem, but KNN presented the remarkable results.

1.2 PROBLEM STATEMENT

How to developed new ML based frameworks to detect the IDS in IoTs. How use ML methods to IDS attacks in IoTs in effective form accurate and fast model.

1.3 QUESTIONS OF THE RESEARCH

What is internet of things (IoTs). What are the advantages and disadvantages of IoTs. What is the security issue in IoTs. How can developed new and active IDS attacks recognition system. How can we use ML and DL techniques to avoid the security problems in IoTs.

1.4 THE PURPOSE OF THESIS

It is well understood that today IoTs security is crucial for any group or institution and henceforth the need for IDS. Though, there have been fairly an insufficient study works in the arena of distributed calculating traffic nursing. There has continuously been the need to recover dispensation competences of these schemes more and rise the storage size to grip to contest with always rising network traffic.

Practically, all of the investigation work we have absented through on dispersed setting, have applied MATLAB systems to identify threats in the network. However, MATLAB multiple reads and write actions on the disk creates a huge bottleneck in the performance.

2. OVERVIEW

2.1 SURVEY

The IoTs is already known today and is a fascinating term. Support people in everyday life, as various types of systems and sensors are becoming increasingly important. The number of linked plans lasts to produce worldwide. Variety and actual application is an attractive manufacturing industry for measuring tons. Many organizations and companies are actively and enthusiastically working on modern devices and new solutions that should be implemented in the rapidly growing industry of connected devices. This can destroy the environment, such as transportation, plantations, industrialization, smart homes and big cities. The association and the company are working on developing new devices and improving communication and security protocols for all possible scenarios. As costs continue to decrease and demand increases, about 1 billion devices will be connected in 2015, and from 2 to 3 billion devices in 2020. Thanks to the current technological progress, it was developed not only to solve other accessibility problems, but also for careful monitoring and interaction with the system. The functionality of this system is based on the use of unmanned surface vehicles (UPS) to support maritime surveillance operations using a herd with several drones to solve the extended space. For example, the system can be used to detect oil spills or for general monitoring of environmental conditions.

The Internet of things can help solve many problems in various fields. The implementation of IoT is associated with noise, parking problems, traffic, lighting monitoring [5], earthquake response systems and detailed agricultural applications for optimizing cultural values . The Internet of Things (IoT) is used to transmit information about sensors and actuators. In the close future, thousands of unmanned midair cars, also recognized as buzzes, are predictable to quickly establish themselves in various areas of everyday life. They will have significant power from transporting the package to immersion in water for certain underwater operations. The use of drones can be divided into military and urban models. The above cases are for non-governmental and governmental purposes. For example, rescue operations and the use of drones to recover from serious disasters, like the Abundant East Japan Earthquake, Natural Tragedies in Indonesia, the Earthquake in Nepal ”” Drone, it is used not only for general disaster relief and rescue operations, but also for many other civilians. Intelligence and surveillance and public services, Department of Homeland Security, General Security, Environmental Supervision, Forest Fire Surveillance,

Security and Border Surveillance, Culture, “Internet transfer”, Building monitoring, “Freight”, “Amazon Prime Air”; the company sends a security package to customers ready to do this using a small drone every 30 minutes ns. The drone in many deployments should have a direct impact on our lives and integrate the same important technologies as modern smartphones. From a technical point of view, drones can be an important part of a highly developed IoT-cyber-physical ecosystem [6].

IoT qualification is that the goal is to be able to ideally use any network to connect and provide services anytime, anywhere. Thanks to the IoT concept, drones can form an additional part of the IoT infrastructure. This is because drones have personal characteristics. It is easy to manage, dynamic, easily reprogrammed on the go, and you can measure anything anywhere. “Flying in a skillful territory with high independence”[7].

2.2 CHALENGES OF IOTS

There are many challenges involved in gathering extensive data in real time from IoT technologies in order to analyse this data and make appropriate decisions on a large scale. Software-defined networking is proposed as a flexible network architecture to face these challenges for IoT requirements. The authors in [8] discuss the challenges of SDN integration with IoT in terms of security and scalability. SDN-SPS designed a gateway node (SITL) to transfer the data from OPNET simulator nodes to an IoT data center using UDP protocol. In this work, the SDN controls the time, frequency and data types. The routing method of RPL and TinySDN protocols uses a collection tree protocol to perform routing and operates based on DODAG control messages. RPL works to improve TinySDN by supporting point-to-point and point-to-multipoint traffic patterns for IoT. Each child node determines its parent node to find a way to the coordinator node to forward its packets, and subsequently will not send DIO messages. The SDN model is used in this work to improve WSN and IoT deployment through its flexible management and control on the sharing resource. The paper in [9] presented SDN controller for WSNs as a floodlight controller in the Mininet network emulator tool. The sensor nodes of the WSNs are implemented in NS2, another simulation network, and both systems are connected via port-to-port communication. In this research, the packet routing processes are achieved through multi pipeline stages; for routing commands, it uses the command line interface to pass the flow rules[10,11].

The SDN structure is designed in three planes, as shown in Figure 2.1.: the application, control, and data plane. The application plane is the place of the IoT applications need without knowing the basic infrastructure of the network. The data flat is accountable for packet forwarding using the IoT devices based on the IEEE 802.15 protocol. The control plane is the place to control routing decisions for each network device.

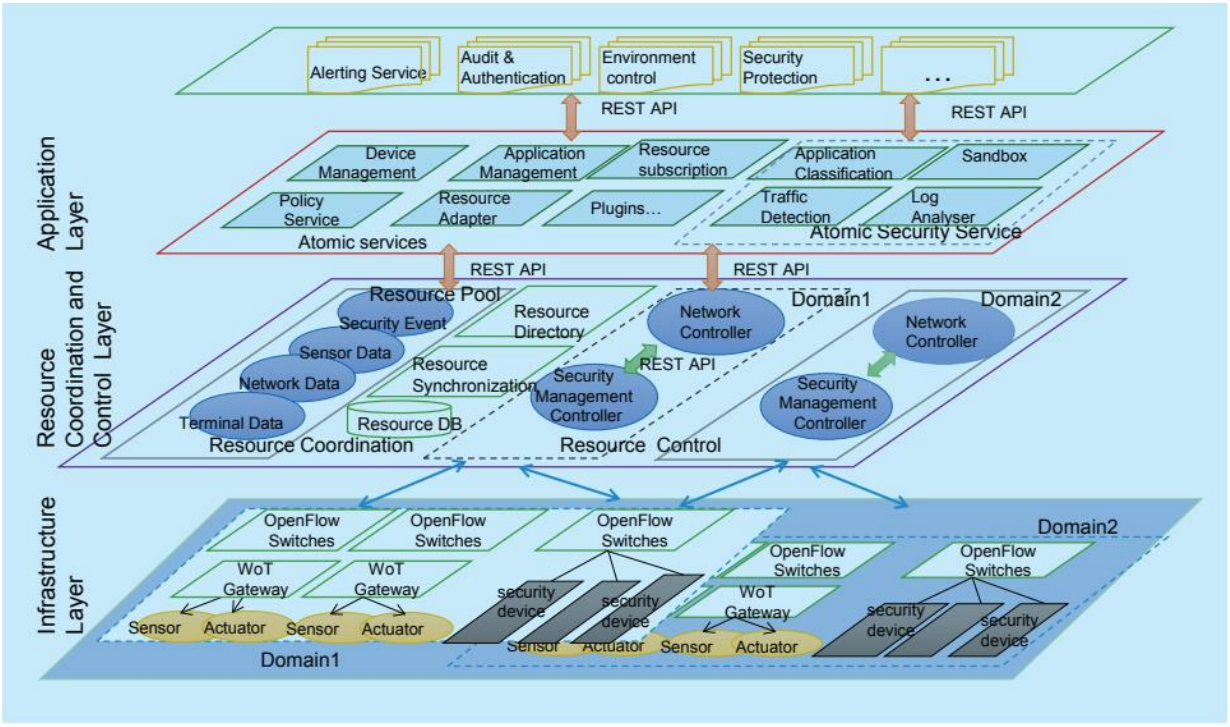

Figure 2.1: The Architecture of the SDN-based WSN clusters for IoT [12]

As shown in Figure 2.1., the proposal framework has three layers, including IEEE 802.15.4 used by IoT sensor nodes to collect data, and SDNC as a flexible network to meet IoT applications' requirements.

2.3 BENEFITS OF IOTS

2.3.1 Cost Savings

If you're concerned about the cost that could result from the move to cloud computing, you're not the only 20% of companies to worry about the early price of applying a cloud waiter. However, if you are trying to weigh the pros and cons of using the cloud, you need to reflect additional issues than the initial price you need to factor in the return on investment. Once in the cloud, easy

admission to your business data saves period and currency when you start the project. And for those who fear disbursing for topographies they neither essential nor poverty, most cloud services are paid on the go. This incomes that at least you don't have to lose money if you don't use the cloud.

2.3.2 Competitive Edge

Not all companies will migrate to the cloud, at least not yet. However, companies that use the cloud are discovering that many of the benefits of the cloud have a positive impact on their business. Adoption of the cloud is increasing every year when companies realize they have access to world-class business technologies. And if you implement a cloud solution now, you will be ahead of the competition.

2.3.3 Flexible Costs:

Cloud computing(CC) prices are ample additional flexible than outdated approaches. Businesses only have to operate the server capacity and infrastructure as needed and therefore only have to pay. It can provide more capacity at peak times and then when you no longer need it. Conventional processing requires sufficient purchasing power at peak times and allows you to remain idle the rest of the time.

2.3.3.1 Flexibility for growth

The cloud is effortlessly scalable so businesses can add or remove possessions as needed. As companies grow, so does their system.

2.3.3.2 Efficient recovery

CC enables quicker and additional precise recovery of requests and data. By less stoppage, this is the most effectual retrieval strategy.

2.3.3.3 Security

CC proposals countless security when intimate data is lost. Because the data is stowed in the scheme, it can be effortlessly retrieved even if somewhat occurs to your PC. You can even delete data from remote machines remotely to prevent it from falling into the wrong hands [13].

2.4 DISADVANTAGES OF IOTS

2.4.1 Risk of Data Confidentiality

There is continuously jeopardy that other people may access user data. Therefore, data and cloud defense must be decent, since if this is not dangerous for data privacy.

2.4.2 Vendor Lock-in

When migrating from one cloud stage to additional, a business can face thoughtful contests due to the changes between vendor stages. Holding and consecutively applications from the present cloud stage on another platform can cause provision subjects, shape difficulty, and additional expense. Corporate data can also be vulnerable to security attacks due to tradeoffs that may have been made during migrations.

2.4.3 Security Issues

Is your data safe? CC is processed on the Internet. Therefore, you should not use cloud computing applications that use or store unwanted data on the Internet. Existing cloud service providers want to do business and understand that data security is a serious problem. Therefore, they are determined to promote the idea of using the latest modern data protection systems. In this regard, however, his authority was badly affected by the NSA's spy scandal. You can also access cloud data from anywhere on the Internet. In other words, hacking that mercilessly protects a disgruntled employee or username and password can damage business data if the data is hacked [14].

2.5 IOTS SECURITY

Cloud computing gives offerings that use the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models. two Cloud customers have get admission to to servers and digital machines thru the IaaS carrier model. Hypervisors run on servers to

virtualize bodily resources. Similarly, the usage of the PaaS provider model, the cloud platform helps working systems, runtime systems, databases, or internet servers. The variety of these carrier shipping fashions makes cloud computing structures extra prone to assault than any different computing platform. Its vulnerability can be uncovered thru one of its most important components: network, digital machines, storage and applications, which are used as the groundwork for classifying assaults and their implications [15]. In the easiest concept, cloud entities signify humans or businesses who remain in touch to operate duties in the cloud. Their coexistence and interplay enable cloud functions, though they are feasible sources of safety problems. Responsibility for implementing, operating, and managing protection is considered in a different way from one cloud mannequin to another. Therefore, it is necessary to make clear these obligations for each the client and the CSP. This consists of readability for the purchaser related to security worries that may also be past their control. Without this, it is not going that vulnerabilities will be recognized in time and records breaches will occur. The significance of cloud computing safety troubles is evident in facts breaches stated given that 2010, some of which continue to be pretty labeled for their relevance to cloud security. For example, fast-growing literature shows that digital computing device vulnerabilities to aspect channel assaults expose IaaS (Infrastructure to Service), PaaS (Platform as Service) and SaaS (Software as Service) to violations. Speculates that there are at least sixty viable safety domains in the cloud structure, with possibly greater rising domains as new implementations introduce new elements to the cloud [16].

2.6 ATTACKS IN IOTS

2.6.1 Cloud Malware Injection Attack

With Cloud Malware Injection Attack, an attacker tries to inject a malicious provider or digital computing device into the cloud. In this kind of attack, the attacker creates his very own malicious carrier shipping shape (SaaS or PaaS) or a digital desktop occasion (IaaS) and tries to add it to the cloud system. Therefore, the attacker need to behave in such a way that it is a legitimate provider for the cloud system. It is a new provider transport occasion amongst legitimate instances. If the attacker succeeds, the cloud routinely forwards legitimate person requests to the deployment of the malicious carrier and the attacker's code is executed. The predominant state of affairs at the back of the Cloud Malware Injection assault is that an attacker transfers an instance of a malicious

carrier to the cloud so that the victim's provider can get right of entry to provider requests. To do this, the attacker should test the victim's statistics in the cloud. According to the classification, this assault is the predominant consultant for the exploitation of the assault floor of the cloud service. The goal of a malware injection assault in the cloud may additionally be of hobby to an attacker. It may additionally incorporate facts changes, adjustments in full performance / reversal or impasse [17].

2.6.2 A side channel attack

A facet channel assault solves CAPTCHA, however now not the underlying synthetic talent problem, and consequently does now not enhance the kingdom of the artwork in contrast to synthetic intelligence. It's known as a facet channel due to the fact it solves the hassle with a approach that would not comply with the deliberate assault route. Side channel assaults can be stated to contain random hypotheses and direct assaults due to the fact they do no longer strive to clear up the underlying AI problem. However, this area solely examines assaults supposed to enforce CAPTCHA. The ASIRRA task by way of the usage of a publicly handy statistical device to method the snap shots (not virtually appreciation whether or not they got here from puppies or cats), then a variety of computer gaining knowledge of classifiers. Implementation of a CAPTCHA provider is primarily based on a server (which affords the venture and validates the response) and a customer (the user's browser, which shows the mission and lets in you to enter the response). The easiest vulnerability in a CAPTCHA is to ship the validation code without delay to the user [18].

2.6.3 An intrusion detection system (IDS)

Cloud computing and grid are the most inclined ambitions Intrusion assault with the aid of disbursed environment. In such environments, intrusion detection structures (IDS) can be used to enhance safety measures through. Systematic manage of registers, configurations and networks traffic. Traditional IDs are no longer appropriate for the cloud Environment for now not recognizing network-based IDS (NIDS) Encrypted node communication, host-based IDS (HIDS) No hidden assault direction found. Gluten Shoulder etc. Proposal of IDS cloud provider the middleware degree at which the audit gadget used to be developed this consists of assaults that NIDS and HIDS can't detect. Include The IDS provider structure consists of nodes, services, Check

occasions and memory. The node includes resources. Accessed by using described middleware Access manipulate policy. Service makes it effortless Communication by using middleware. Event reviewer Network facts monitoring, recording and evaluation what policies / recommendations are violated? Memory continues working (based on contrast of current person movements and frequent movements Behavior) and information base (previously recognized clues) Attack) database. Checked information will be despatched to IDS provider a core that intrudes and analyzes statistics and alarms. The writer examined the IDS prototype with the following help: The simulation effects confirmed adequate overall performance for real-time deployment in the cloud environment. Even if you we did no longer talk about safety coverage compliance evaluations Cloud carrier company and related reporting procedure Cloud consumer [19].

2.6.4 DDoS Attacks

DDoS attacks target all levels of the cloud system (IaaS, PaaS, SaaS) and can take place inside or outwardly. Cloud-based external DDoS attacks start outdoor the cloud setting and board cloud-based facilities. This kind of attack touches the obtainability of the service. The heights most pretentious by external DDoS attacks in cloud systems are the SaaS and PaaS levels. Internal cloud-based DDoS attacks occur in cloud systems mainly at the PaaS and IaaS level and can occur in different ways. For example, an attacker could exploit the test phase of cloud services from certain providers. As a result, authorized users in the cloud environment can initiate DoS attacks internally on the victim's computer. On the other hand, releasing an image of an infected virtual machine can allow an attacker to control and use the infected virtual machine to perform an internal DDoS attack against a target machine in the same cloud computing system. . . DDoS encompasses different types of attacks. The following sections describe these attacks and the practical defense mechanism recommended for cloud systems [20].

2.7 AN INTRUSION DETECTION SYSTEM (IDS)

IDS can be defined as the procedure of classifying malicious comportment that targets a network and its assets [21]. IDS are groups of software, hardware and rules which periodically monitor the network elements and generate an alarm incase of an intrusion. The network element under inspection can be an application running on a computer, the operating system on the computer, a group of computers or all of the computers in a network. According to the type of the inspected

element, IDS analyze the related logs such as access logs and error logs and compare them to the previously defined rules. If a match to an intrusion rule occurs, an alarm is generated. The alarm can be in several forms such as a line in the logs, an email to the system administrator or a Short Message Service (SMS) to the Network Operating Center (NOC) members' cellular phone. The wide range of elements brings a variety to IDS applications. On the other hand, all intrusion detection systems can be grouped into three according to the rule formation procedure.

2.7.1 Signature Based (Misuse) IDS

Signature-based detection analyzes events to detect predefined intrusion patterns. Using well-known intrusion techniques, signatures are generated for each type of attack. Then we verify that the registration and monitoring results are consistent with the attack signature. The logs can belong to the network traffic, to the operating system or to an application. For example a Smurf attack is described as: icmp number (receive( )) ≥m and addr ( ) = (host,broadcast) which means, the number of packets that a host received with "network broadcast address" as the destination address is equal or more than a threshold m. The known attack types are converted into signatures such as the one of Smurf attack and then the related logs are investigated in the signature based IDS. To detect a Smurf, the IDS has a rule for logging the traffic hits to the network broadcast address and then compares the lines in the log to a threshold. Another example of signature involves Common Gateway Interface (CGI) scripts. A popular open source IDS SNORT is used to inspect the packet payloads of the network traffic and search for specific strings. An exploit is used by hackers that probe the target Web server for known CGI bugs. For example, the phf exploit allows an attacker to return any file instead of the proper web page. This is achieved by a request which includes the following string in packets: GET /cgi-bin/phf? If the network hosting the target web server includes a SNORT IDS, the request of the attacker will be detected by the IDS and the preprogrammed actions (dropping he packets, generating an alarm …) will be taken. A similar CGI attack signature in the packet payloads is as follows: cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd . This attack becomes dangerous if the following line is appended to the web server's access log. GET /cgi-bin/phf?Qalias x%0a/bin/cat%20/etc/passwd HTTP/1.0" 200 267 Another example of the signature based IDS is the spam filtering programs. They use header and text analysis, DNS block lists, and collaborative filtering databases. Most of them issue a scaling for an email to identify it as spam or not. Every

hit for the predefined signatures in the header and text analysis advances the score of the mail. The signatures in this phase can be the usage of words such as Viagra, free, download, etc. and including an HTTP link in the mail body. The signatures are both preprogrammed and also learned from the email that the users mark as spam. The signature-based IDS function is the minimum number of false alarms that are obtained by describing the entire malicious behavior. On the other hand, whether the inspected element is a network or a host, this technique is not useful for the undiscovered attacks. Since this technique is not an adaptable one by its nature, the number of false negatives is high because of the undiscovered attacks [22].

2.7.2 Anomaly Based IDS

Failures take a completely different approach to abuse detection technology. This technology is based on the formation of models or characteristics of "normal use". In this normal use, it may belong to users, applications, or network resources of the system. When creating a profile, each use is compared with this profile, and deviations are recorded in the attack. Similar concepts are used to detect communication and credit card fraud. Examples of common usage profiles are available. A regular user profile is created using separate dimensions. Access to files, connection using a processor. Monitoring individual scale values using several test reports and selecting the appropriate time period form a classification called frequency distribution. All individual indicators are calculated and compared with the redistribution of audit data. Compare the difference with the threshold to determine whether the event is normal or abnormal. Instructions for general use of the software are classified. These programs include programs executed and not executed by the controller, other programs of much larger size and complexity, as well as various types of interventions (Trojan horse, denial of service, and memory stream processing programs Buffer). Check only with authorized personnel, there is a risk of damage to the system. Tracing is defined as a list of system calls that one process made from start to finish. For example, Inetd is selected. Inetd supports manual clicks on various well-known ports. When creating a new connection, Inetd launches the program to manage the connection according to the configuration schedule. Thus, the program can manage incoming connections to various services. It starts as a foreground process, starts with a hidden process that runs in the background, and then ends. The hidden process starts the child process and is initialized. This supporting process is almost the same. Inetd uses a data set that includes the effects of the boot process, the daemon process, and

the analog assistant process. An Inetd intervention is a denial of service attack that links network connection resources. Other entries consist of the same track during the attack. The result of comparing both data records is simply an invisible deviation from the process path. For this reason, Inetd attack signatures are created that look for the invisible parts of process variables. When W32.Blaster was detected, an error-based IDS collision occurred. As a result of studying the source ports and the destination of network traffic, the activity of Windows ports increased. An alarm was triggered due to this unusual activity. Further study of network protocols showed that many Internet Protocol (IP) addresses are connected externally through port 135. This IP address sends SYN packets to the same traffic scheme as many other hosts. Observed towards the internal host. W32. Blaster worm definitions, such as IDS, capture anomalies, and network traffic is posted on the security forum. Based on the foregoing, adaptive IDS operation IDS is able to detect undetected attacks, as in the case of W32.Blaster. However, normal use is difficult to explain, and many false positives occur. Using multiple default fonts when creating a general purpose profile causes problems adding results. This summary is mainly obtained by summing up. Comparing the results of this combination with a threshold may produce incorrect results. This procedure is the main reason for the positive results. If one of the measurements is significantly different, the other measurements remain unchanged, and the event may lead to a decision on penetration, and not to actual intervention. Bayesian networks are used to add model output to reduce false positives, rather than use more. IDS are provided based on Bayesian networks. The various symptoms of invasion are analyzed in separate models found in the Bayesian network [23].

2.7.3 Hybrid IDS

The hybrid IDS include both signature based and anomaly based IDS characteristics. Currently some proposed hybrid systems exist, but they are still in the research and development phase. Checking signatures as well as the variations from normal profile, results in a more robust defense of the network. In this manner, both the already known type and the undiscovered attacks will be able to be detected, so hybrid models can be much more successful than its counterparts. On the other hand, they bring the excessive investigation burdens by issuing the two techniques together. More research efforts are needed on hybrid IDS.

2.7.4 P2P Network

Contrary to popular belief, P2P is not a new form of technology. In fact, places have been created using the messaging protocol since the arrival of the Internet. A P2P system is a network of computers, each responsible for data processing. They differ from client-server network systems in that some devices process and provide data together, while other computers consume the data processed by the server. P2P networks were originally introduced for commercial purposes in the early 1980s. Before using P2P networks, I used a mini-frame, like a VS system, to store files on a central hard drive. B. Word processing. However, in order for the computer to work, I had to connect it to the mainframe. As you can imagine, it was ineffective and caused a lot of cable confusion. Today, technological advancements have freed up employees and enabled them to develop PCs that can operate remotely without a permanent mainframe connection. Additionally, P2P networks allow employees to share files and connect printers. It is very common for P2P network systems to be found on local networks such as home networks. In this case, devices can sync files and share files with each other. These systems can be built as wired or wireless networks that perform their functions using the same network protocols and software. Schools and small businesses take the opportunity to regularly create P2P network systems to share and access files with all users. In homes, schools, and businesses where broadband routers are used, the networks created are called hybrid P2P networks and client / server networks. Lambda is fully compatible with hybrid networks and has the resources to ensure the addressing capability of the network layer. Lambda also has functionality for clustered systems with multiple databases, allowing unlimited storage of encrypted data, making it ideal for businesses that need secure data storage solutions. A hybrid network environment consists of routers that act as a centralized publishing tool for Internet connections. However, the local computer connected to the network manages the file sharing. In addition to files, you can share printers and other resources between networked devices.

2.7.5 P2P Traffic Detection

Efforts to detect P2P traffic continued to develop P2P applications. Legal action has been taken to arrest Napster. You can also find P2P members easily by simply checking the traffic connection to the Napster server. Although the second generation P2P network suddenly ended with an

ineffective discovery, the idea of using a distributed topology is adopted by the next generation. After the introduction of the hybrid topology into the P2P network, the P2P communication packet exchange was seen as the definition of the P2P packets. These studies extracted detection methods based on the port number of the transport layer. All management packets and some data packets flow to some of the STL ports (Table I). P2P users are identified by specifying these ports. Most firewalls have rules that block traffic from certain P2P ports. P2P client developers have responded by adding dynamic port functionality to the new version and making port-based discovery necessary. When the user starts the P2P client in the new version, I want to connect to the super node via the standard port. If a connection is not established, the client changes the ports at random. In addition, users can configure the work port manually. When the connection speed reaches 10 Gbps, it is difficult to check and ineffective. At this rate, the packet and buffering capabilities of current packet analysis programs at packets per second (pps) are very high. Significant delays can occur. This is a problem for lag-free applications like Voice over IP. For example, Cisco includes the NBAR (Network Application Recognition) for peer-to-peer peer detection, but not the default router. Another problem with using signature-based detection methods is actually the most threatening, but start-to-end encryption is used for P2P connections. The success of signature-based detection methods in terminal applications forced P2P application developers to hide P2P packets from proxies. The BitTorrent Azureus client has a beta version that contains end-to-end BitTorrent link encryption to look for performance issues. As the programmer Azureus found, the results are critical. They also announced that version 2.4 of the program will continue to use encryption to avoid signature-based detection. Another way to determine P2P traffic is to collect information about the P2P network through client connections using a scanner, a computer with P2P clients. Since some popular files are downloaded and shared on Android, many P2P network clients download files to a specific computer. You can easily record the customer's IP address by checking the traffic flow. This method has very few false alarms, but cannot identify all P2P users on the network. The client cannot find users on non-Android peer-to-peer networks and users who do not download files from Android. You can also improve performance by combining the data collected by Art Locker in different ways [24].

3. MATERIAL AND METHODS

3.1 MACHINE LEARNING

If the ML model is trained, it will be trained in any subset of the available quantities supplemented by observed training data. We define this training mode as manual training (PL). Books (students) in PL learning mode are not transmitted interactively to teachers. Passive students create the following books or models that receive a random world record. Therefore, PL is easy to implement. Machine Learning (AML) is a common area of research in the field of OD. You can search for the encoding manually in the field, specifying the most useful instance of the record. AML's goal is to create extremely accurate books in as few cases as possible requiring specific data at a low cost. An AML workbook consists of a first set of small instances that identifies instances of information from an unrecognized dataset and asks for an expert or Oracle tag that can provide a tag for each instance. Several studies suggest algorithms to combat money laundering and their application to various computer applications. They have shown that AML use of ML models significantly reduces the training data required and works well without losing accuracy. Unlike machines, students are tired of answering questions. Hence review (i.e. sign up) if you know that the concept is often expensive. As a result, you can use AML to teach people, make learning more effective, and reduce training costs. There are many studies on the use of L in human education. The first survey was not conducted and tried to answer the question: "In addition to the data presented for the study class, do people use undisplayed data?" Has been completed. It should also assess whether the student is sensitive to the distribution of unrated classification samples. The results showed that human behavior is consistent with the predictions of the Gaussian blend model of anti-management education. Castro et al. (2009) examine what they call active human learning. They show that users can learn faster and more productively by actively selecting instances of information from an unmarked record instead of random samples. However, human AML is not sensitive to noise, and the selection of queries from a 3D data set without artificial visual stimuli was not as good as the device. There are other empirical studies on money laundering for people that focus on examining two categories of problems in a one-dimensional entry space. Circular had errors. For multi-dimensional classification. The problem in general, the AML curriculum repeatedly selects the least marked examples and recreates the workbook. Even the simplest form can take some time to document again. Therefore, multiple cases were selected in this study each

time a separate active learning strategy was selected. Settles (2010) offers various strategies for selecting AML queries. 1) Confirm the uncertainty. This is the easiest and most popular strategy. The uncertainty example focuses on the selection of cases that the compiler tries to identify with the greatest uncertainty. 2) Reduction of the expected errors. The goal is to request examples to reduce expected classification errors. E 3) The Communications Request Committee (CBQ). The most useful example is that the classification committee found the greatest deviation. Bag and Boosting is used to create a classification committee with one record. You are trying to combine some weak compilations into one strong compiler. Each base workbook is written individually in a package. However, these workbooks can improve the learning process for everyone and influence each other. Contracting is an iterative process in which each training package is first assigned the same weights and then the weights change according to the classifier error rate [25].

3.1.1 Feature Extraction

Feature Extraction goals to decrease the variety of elements in a dataset via growing new facets from the current ones (and then discarding the authentic features). These new decreased set of aspects must then be in a position to summarize most of the data contained in the unique set of features. In this way, a summarised model of the unique elements can be created from a aggregate of the authentic set.

3.1.1.1 PCA

This approach is additionally known as Karhunen Lo`eve transformation. It is one of the linear transformation method that is used to reap points from records or to decompress the data It is used to take world buildings from the high-dimensional information set as nicely as it is utilized to decompose dimensionality of the facts and take special facets from the faces picture. This method can be used additionally to distinguish patterns in information and specific the statistics so as in order to spotlight their differences and similarities between them. This method additionally offers a successful way for dimensional decomposition of the data. The picture of the face picture is required to be represented in a low dimension subspace. This is carried out with the aid of the use of one of the discrimination methods such as the Principal Component Analysis. This subspace is created by using the use of the eigenvectors or principal elements of the array that created from the photo of the face picture in the dataset. Mathematically, eigenfaces characterize the

eigenvectors that derived from the covariance matrix of the picture dataset and the eigenvectors symbolize the significant editions thru the faces in the dataset and each picture of the face in the coaching dataset has a special role in the subspace. In this technique, every image will be examined projected onto this characteristic space. The version of faces picture resulted from a extraordinary stage of illumination is much more than the variant that generated from the identification of the person. Therefore Eigen face technique is utilized to minimize the dimension of the image. Where PCA gives directions of projection that goal to maximize the whole scatter throughout all faces image in the dataset [26].

3.1.1.2 K-means clustering

K-means clustering is one of the simplest and famous unsupervised laptop getting to know algorithms. Typically, unsupervised algorithms make inferences from datasets the use of solely enter vectors except referring to known, or labelled, outcomes. Andrey Bu, who has extra than 5 years of laptop gaining knowledge of journey and presently teaches humans his skills, says that "the goal of K-means is simple: team comparable information factors collectively and find out underlying patterns. To obtain this objective, K-means appears for a constant quantity (k) of clusters in a dataset." The group specifies a number of factual factors grouped for positive similarity. Describes an overview of the full type k, which represents the number of target centers in the data set. The center is a virtual region or real space that represents the center of the group. Each registration operator is assigned to each group by reducing the sum of the squares in the group. In other words, the tolerance range for the center of the K algorithm algorithm is determined, then each factor is distributed to the closest group to reduce the center. Average "K" means average data. In other words, the center revealed [27].

3.1.2 Classification

Classification is the method of discovering a mannequin (or function) that describes and distinguishes facts training or concepts. The mannequin is derived based totally on the evaluation of a set of education facts (i.e., information objects for which the category labels are known). The mannequin is used to predict the classification label of objects for which the category label is unknown.

3.1.2.1 Neural Network

NNs are collected of basic computational devices identified as neurons blended in accordance to special buildings. For instance, they can be organized in layers (multi-layer network), or they may additionally have a connection topology. The feedforward structure, except comments connections (signals go solely to the next layer's neurons). See Figure 3.1.

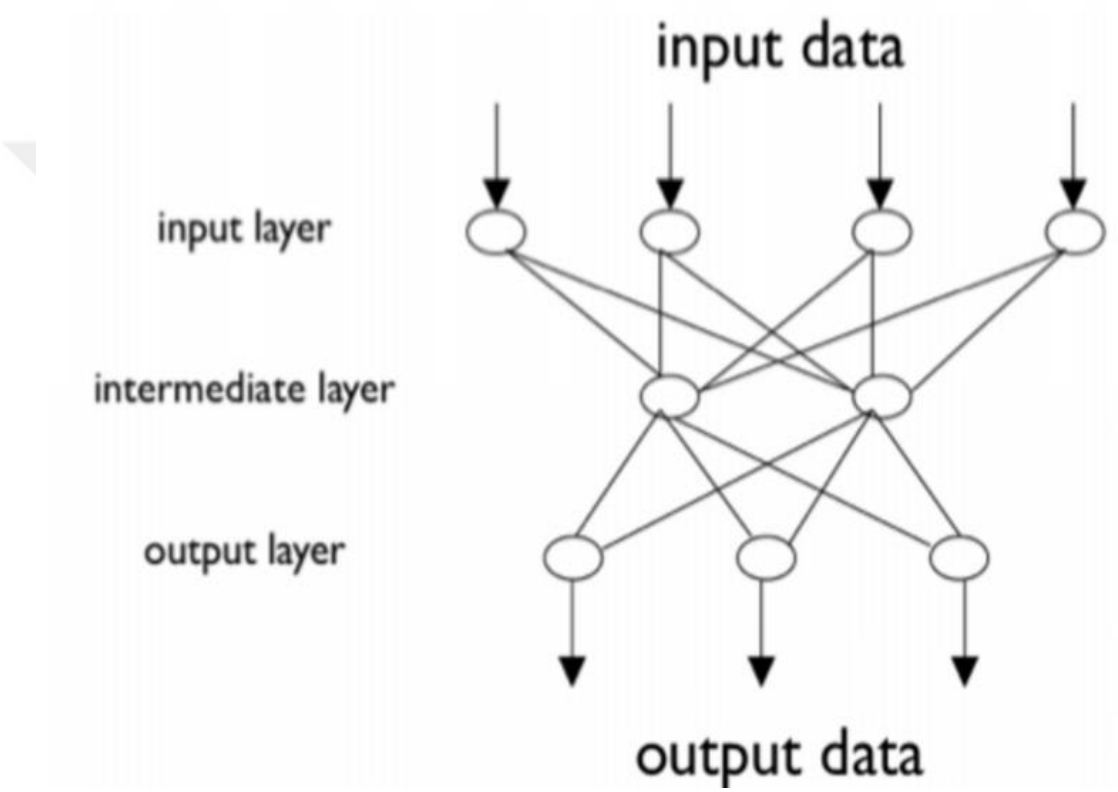

Figure 3.1: Shallow Neural Network [28].

3.2 DEEP NEURAL NETWORK (DNN)

The concept of several levels and levels is called the Deep Neural Network, and the previous topic, Deep Learning (DL), focuses on finding excessive hierarchical explanations for "deep" systems. These deep-mode intersections are common to machine learning (ML) problems that require deliberate manipulation and statistical preprocessing to obtain applicable aspects suitable for a "flat" mode and good performance. Use previously provided by sync. Process. As a result, in order to extract the corresponding vector input parameters, it was necessary to analyze statistics with an unusual amount of information on the tape, and efforts increased when the size of the data set

increased significantly. The index causes some problems, and its effect is difficult to formulate. Recognition of z poetry or facial recognition, etc. These deep learning strategies provide complex and objective learning that can identify recent operations in the input area. By working with raw data, we demonstrate the ability to extract the most important aspects using a simple system that establishes principles with particularly complex concepts. The engineering structure of the effects of deep learning is the result of studying mapping systems to determine symmetrical effects to such an extent that the totality of problems can be generalized in complex terms. For many slides, the system repeats with sufficient likelihood of restoring suitable work for the desired operation. Deep Learning today is a useful tool for many scientific and technological tasks, in particular for laptops (CV), robots, voice processors, language hub processors (NLP) and incredibly promising engines. Research, finance. Deep learning structures can be used in all supervised and unconfirmed educational environments to improve learning. After it is known that the vector of all information receives already preferred output values that are already recognized as predefined, and when calculating SGD, a search method is implemented. Backpropagation algorithm All recording devices can contain tagged and tagged samples, while other recordings can only record a few, so education is called learning with half-control. The stack of unidentified disk drive locations really needs to be learned using implicit mappings and some actions that can be applied to characters. An error occurred while achieving the overall performance indicator. The promotion cycle consists in changing the meaning of the “directive” of the Community, in which the value of the network is safe, taking into account the costs of logical or digital feedback from the network after performing certain actions to measure the overall performance of the network. template. By the way. The region that defines a specific activity. Deep learning networks can be divided into two categories, but here the predictive calculations vary from the level of entry into the account to the level of exit and are called direct flow structures. In addition to pre-powered connections, the tool can communicate with the device itself or with the device at the previous level. These connections provide a similar memory mechanism by transforming the structure into a recurrent neural network (RNN). The post-delivery structure allows any hidden level device to connect to any device on the next hidden level. This structure is called "fully connected." Another architectural variant that ignores mathematical processes, in particular, to reduce the computational complexity of image processing, uses planning, which is a convolutional neural network (CNN). Widespread use for

computer imagination, analysis and image processing, significant performance improvements and relatively simple implementation [29, 30, 31, 32, 33].

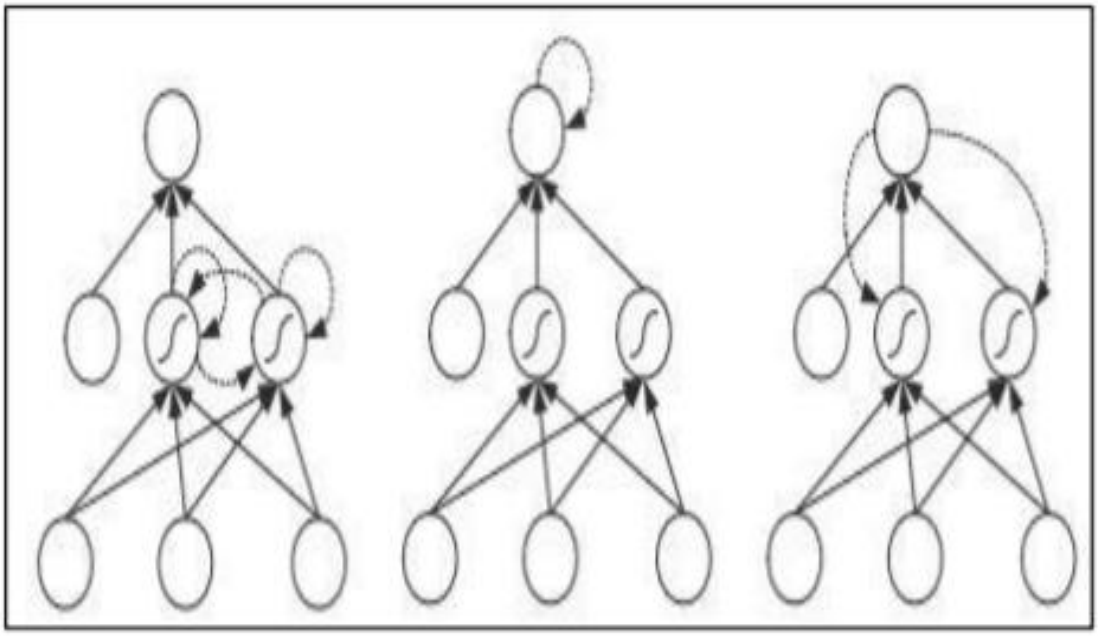

Figure 3.2: Recurrent Neural Network (RNN) [34].

3.2.1 Convolutional Neural Network (CNN)

In this section, an easy preface of deep mastering and CNNs will be given. Today, in many issues deep getting to know and CNNs consequences provide the satisfactory solutions. These can be beneficial to a number of fields like speech recognition, photo cognizance and herbal language processing and so on. Deep getting to know is a section of desktop learning, the reason of which is to create a higher-level illustration of information the use of many layers of nonlinear tactics. These procedures have a exceptional gain for consciousness and classification, hereafter the fundamental features. In the literature there are severa of deep architectures, CNNs viewed the vital one between them. The CNN entails many numbers of convolutional layers, completely linked layers and the pooling layers of direction with the tied weights. In 1998 LeCun gave the universal shape of the deep CNN. In the following Figure 3.3 can be considered the LeNet-5 with the entire implementation.

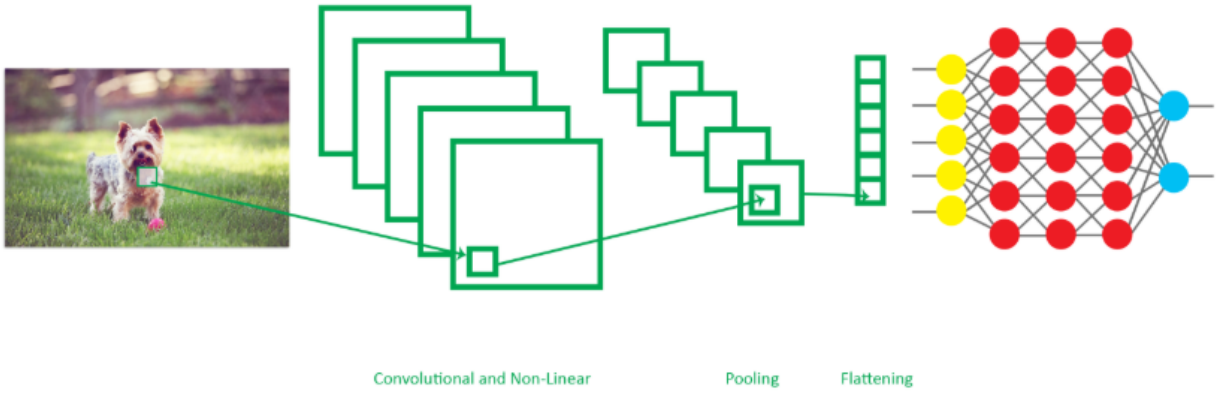

Figure 3.3: Convolutional Neural Network (CNN) [34]

3.2.2 Recurrent Neural Network (RNN)

RNNs add a motivating rotation to simple neural networks. A vanilla neural network takes in a fixed scope course as input which bounds its practice in circumstances that include a 'series' kind contribution with no prearranged scope.

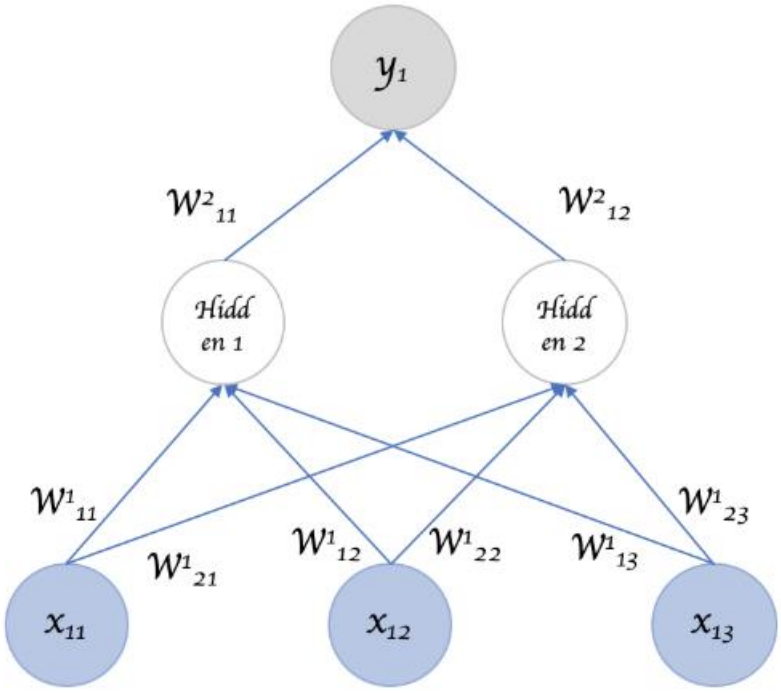

Figure 3.4: Simple RNN, 3 input and 1 output [34].

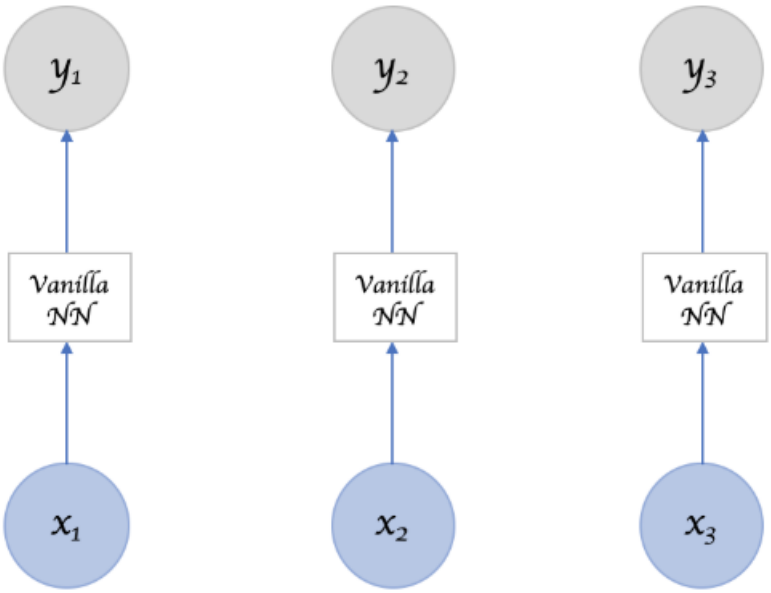

Figure 3.5: Simple Series Time RNN [34].

RNN recalls the past and it's choices are influenced by way of what it has educated from the past. Note: Basic feed ahead networks "remember" matters too, however they be aware matters they learnt throughout training. For example, a photograph classifier learns what a "1" appears like all through coaching and then makes use of that know-how to classify matters in production. While RNNs Do the same during the training, achieving results based on the lessons learned from previous contributions. This is the network phase. RNNs can use multiple input vectors to generate multiple output vectors, and output (output) is no longer affected by the weights used for inputs such as NN every day and across the country. The context in the "hidden" vector primarily indicates the previous input / output, so the same article can provide excellent output based on the previous element in the series. Thus, an input vector for a fixed measurement is converted to an output vector for a fixed measurement in a vanilla neural network. These communities "repeat" when they iteratively perform transformations for a specific set of input data, creating a set of output vectors. Remote operators do not have major barriers. Besides creating the output that characterizes the hidden element and state, depending on the element, it overrides the same hidden state and uses it to process the element.

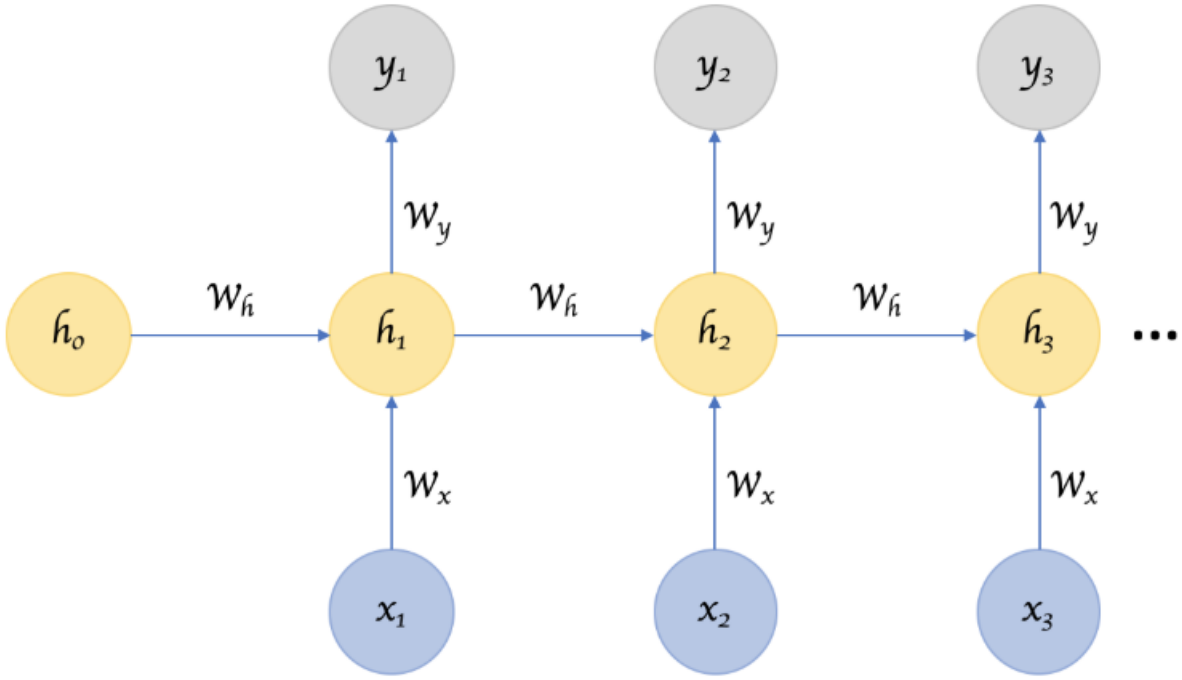

Figure 3.6: RNN 3 Input and 3 Outputs [34]

There is an important difference between Figure 3.4 and Figure 3.5. In the past, one or more unique scales on a particular component of the input object were used to create hidden neurons that use similar scales to obtain results. There seems to be a lot of weight. Figure 3.6 shows that the same weights are repeatedly used for some instruments in the Enter series.

3.2.4 Deep Belief Network (DBN)

Deep Belief Networks (DBN) is production models with many layers of causal variables. Each level of a DBN is made up of an RBM. Hinton et al. He found a way to learn DBNs quickly and greedily, one layer at a time [35]. When an RBM is detected, the function activations are used as "data" to train the next RBM in DBNs.

An important part of a level-based learning process is that the minimum probability of a data day increases with each additional level. However, the number of objects in each level does not decrease. You can repeat this hierarchical guide several times to take a closer look at your hierarchical data model. Each vector level captures a strong correlation between the actions of the next object level. It is more efficient than using the same hidden layer on many devices. With this

greedy algorithm you can find a suitable hierarchical representation of your data. However, this is not optimal. In fact, the weight of each layer is independent of the weight of the subsequent layers. Therefore, the expression in the greedy learning algorithm can be developed using an algorithm that controls weights.

3.3 OUR FRAMEWORK GWO BASED KNN

In this study, new method combined GWO with KNN for IDS problem in IoTs. In the first stage, the GWO applied for feature selection part. This can be by applying GWO for optimizing feature selection objective function see equation 3.1.

$$Objective = \alpha * ErrorRate + (1 - \alpha) * \frac{\#SF}{\#All\_F} \quad (3.1)$$

where ErrorRate represented the error rate of the classification model KNN. $\#SF$ Represented the number of selected features and $\#All\_F$ represented the whole number of the features (total features amont).

Then, the selected features wired to the KNN that used for classifying the selected features. The KNN is robust techniques which used in classification and regression problems. In this study, we applied KNN as classifier because the output of our model is discrete and not continues. The block diagram of our method presented in Figure 3.7.

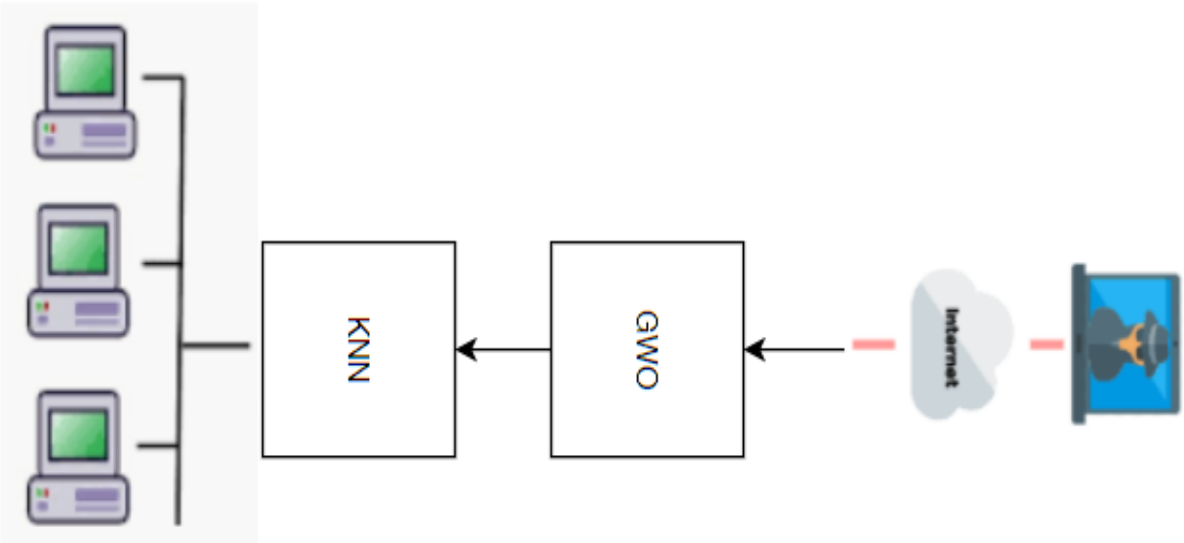

Figure 3.7: RBM in DBNs

4. EXPERIMENTS AND DISSCUSION

4.1 MATLAB TOOLBOX

Perform and evaluate experiments the proposed mechanism is the MATLAB R2015a software. Neural Network Toolbox version, statistics and Machine Learning Toolbox version, Classification tips: In the first step, the time series data extracted in the previous step it is processed by the window processing method the proposed system alone provides a system together with an observation window. The window size is set to 60 sampling periods, with a 1-minute slide 30 sampling.

Then a new technique called RBM is used to reduce the size of the window collected. This technique summarizes 60 feed samples from the current window by extracting the potential energy at level 10 using the symlets4 or sym4 wavelet. This means that instead of feeding the entire window, only the summarized observations are taken to the next step. This planned step improves the performance of the proposed system by reducing the processing time when the model is finally decided.

4.2 VALIDATION TECHNIQUES

It is a decision-making process that quantifies a virtual relationship between variables accepted as written data, called validation. Typically, after training, the model is evaluated as an error. This process does a numerical assessment of the difference between the expected response and the initial response, but only gives an idea of how the model performs Sadin. The model may be inadequate or exceed the data.

4.2.1 k-Cross Validation

Cross validation is similar to the iterative random sampling method, but sampling is performed in such a way that the two sets of tests do not overlap. Using k cross validations, the available training set is divided into k disjoint subsets of approximately the same size. Where is the fold between the subsets of the result This separation is done randomly by selecting training cases without replacement. A model is formed using the subsets k-1, which together represent a learning set.

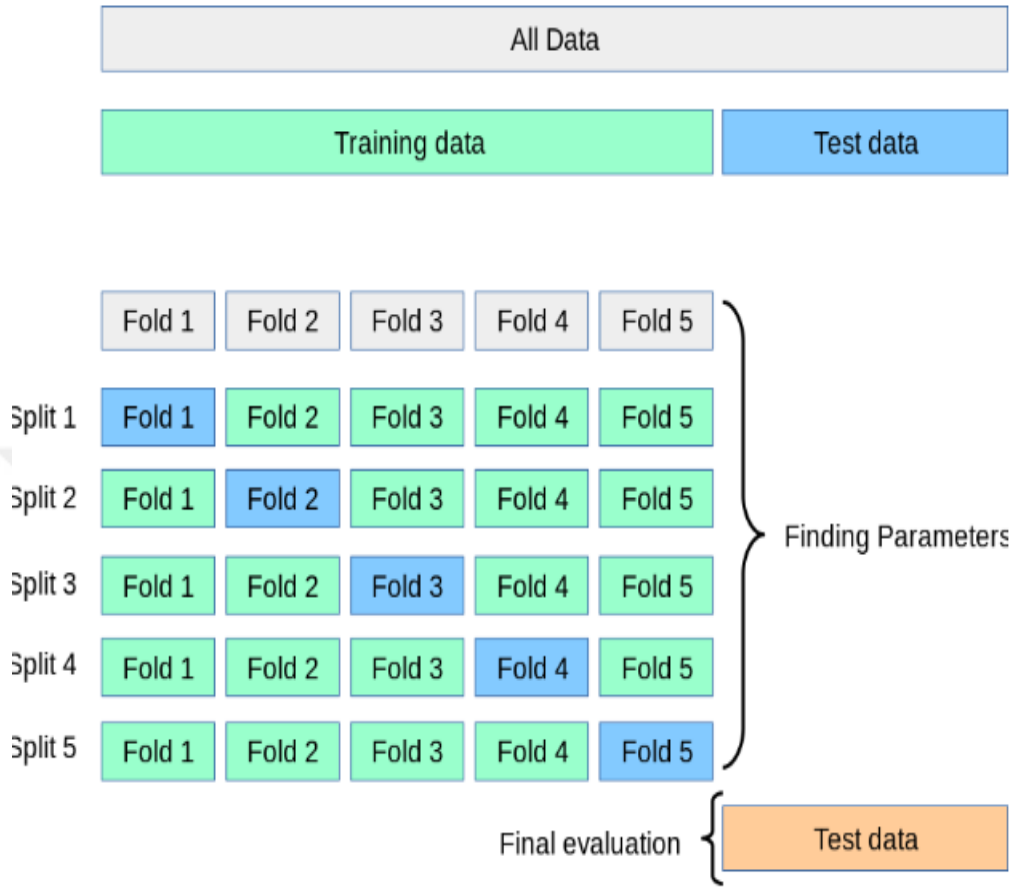

Figure 4.1: k-Cross Validation [36]

4.1.3 LEAVE-ONE-OUT CROSS

A unique cross check is a cross check K multiplied by its logical edge, where K is N, the amount of feature opinions in the set. This incomes that the approximation function for all data except the point is trained N times from each other and a forecast is made for this point. The regular mistake is however calculated and applied to estimate the method. A one-to-one cross-validation error assessment (LOO-XVE) is good, but initially the calculation seems very expensive. Fortunately, local overweight students can make LOO predictions just as simply on a regular basis. This means that the calculation of LOO-XVE does not take longer than the calculation of the residual error and is a greatly well method to estimate the models. We will soon see that Vizier relies deeply on LOO-XVE to select its compatible codes [37].

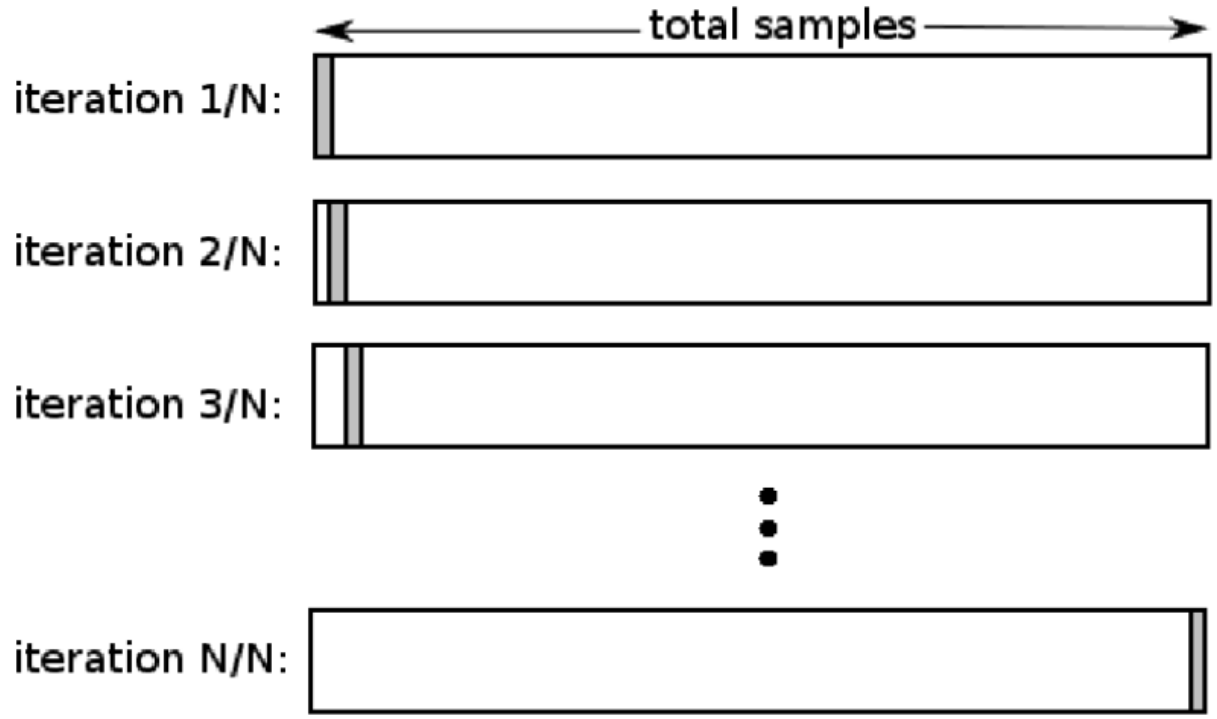

Figure 4.2: Leave-one-out cross [38]

4.2 DATASET

Although the KDD99 dataset and its advanced type NSL-KDD are the two largest known intrusion detection datasets, they are relatively old datasets, and many normal and offensive constructs have changed over the previous period. To solve this problem, the creation of a complete system should be completed in 2015, which depends on a data set that reproduces the traffic scenario of a modern system with many interventions with a reduced area and complexity of traffic data. organized. System. IDS UNSW-NB15 is a group of approximately 100 GB of system data traffic modeled by the ACCS Lab of the Australian Cybersecurity Center (ACCS). This logbook contains actual parallel routine actions and the collaboration of man-made attacks. This dataset contains 48 data and approximately 2,540,044 examples, including normal annals and 9 attack reports such as Fizzers, Examination, Entors, DoS, Feats, General, Investigation, Shell Code and Worms. Researchers created a subsection from a regular series of trainings and tests that spanned 175.341 and 82.332 years, respectively. In this study, to estimate the accuracy of our model, we used a subsection of 20% of the UNSW-NB15 dataset.

Table 4.1: DDoS dataset features [39]

Variable No.	Description	Type
1	SRC ADD	Continuous
2	DES ADD	Continuous
3	PKT ID	Continuous
4	FROM NODE	Continuous
5	TO NODE	Continuous
6	PKT TYPE	Continuous
7	PKT SIZE	Continuous
8	FLAGS	Symbolic
9	FID	Continuous
10	SEQ NUMBER	Continuous
11	NUMBER OF PKT	Continuous
12	NUMBER OF BYTE	Continuous
13	NODE NAME FROM	Symbolic
14	NODE NAME TO	Symbolic
15	PKT IN	Continuous
16	PKT OUT	Continuous
17	PKTR	Continuous
18	PKT DELAY NODE	Continuous
19	PKT RATE	Continuous
20	BYTE RATE	Continuous
21	PKT AVG SIZE	Continuous
22	UTILIZATION	Continuous
23	PKT DELAY	Continuous
24	PKT SEND TIME	Continuous
25	PKT RESEVED TIME	Continuous
26	FIRST PKT SENT	Continuous
27	LAST PKT RESEVED	Continuous

4.3 RESULTS

Numerous experiments is performed in several settings, the test and the outcome were measured applying several measurements, the performance of several experiments were related and the outcomes were highlighted.

The experimental applied by using MATLAB2020 as tool. The dataset features that clarified in the 4.3 used as input to the planned model that written by using MATLAB2020. Several parameters are calculated and presented to evaluate our method:

$$TPR = \frac{TP}{(TP + FN)} \tag{4.1}$$

$$SPC = \frac{TN}{(FP + TN)} \tag{4.2}$$

$$ACC = \frac{(TP + TN)}{(P + N)} \tag{4.3}$$

The results of the KNN presented in the Table 4.2, this experiment applied KNN to the dataset directly.

Table 4.2: KNN

Results	Our Method
Sensitivity	0.8400
Specificity	0.8260
Accuracy	0.8590

On the other hand, GWO combined with the KNN, which lead to optimize the performance of the detection system.

The GWO assist KNN to speed up the processing time and increase the detection accuracy because it's extracted important features and remove unaffected features.

The Table 4.3 calculated by using random sampling techniques and the experiments repeated 10 times and the average of 10 experiments are presented in Table 4.3.

Table 4.3: GWO+KNN

Results	Our Method
Sensitivity	0.9800
Specificity	1.0
Accuracy	0.9667

The results of our method with shallow neural network presented in figure 4.4 for evaluating.

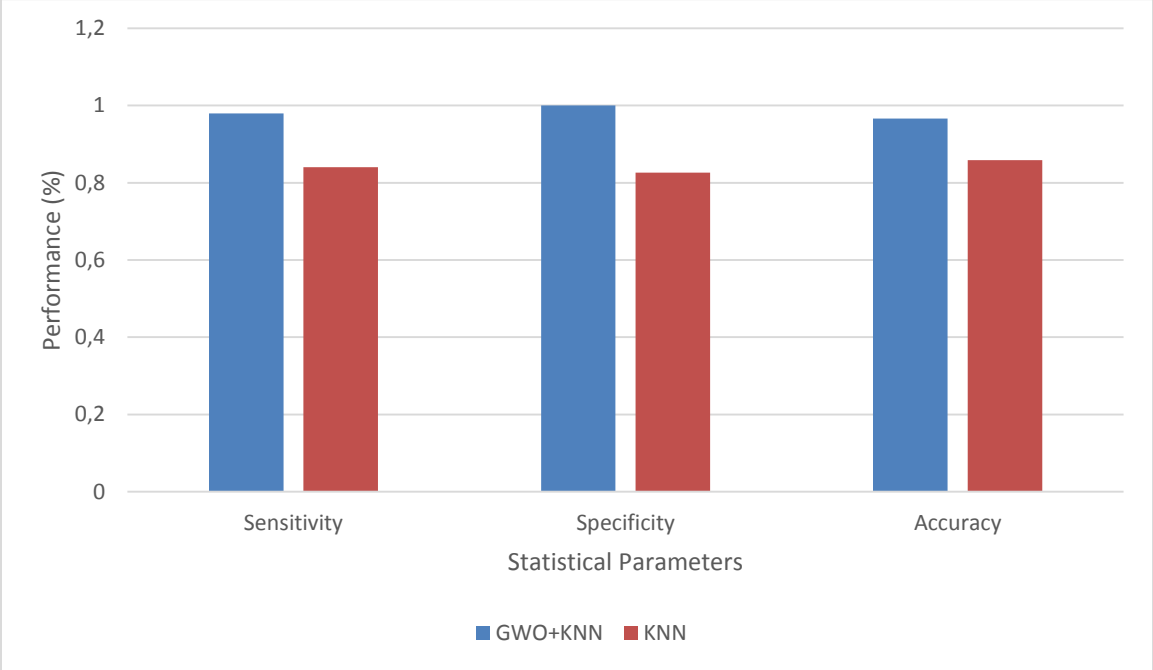

Figure 4.3: Results of Our Method

Furthermore, our method compared with several studies used data mining and machine learning techniques to detect IDS in IoTs. The compression shown in Table 4.4.

Table 4.4: Results GWO+KNN

Ref	**Acc (%)**
[40]	98
[41]	97.79
Our Framework	**99.67**

5. CONCLUSION

We presented new method presented to detect IDS attacks in IoTs using machine larning techniques. In the first stage, the GWO applied to the input data to select effective features of IDS dataset. The GWO is one of the commonly used optimization algorithms in the last years which applied in several fields such as: computer security, feature selection, image recognition, and optimization problems.

The presented method is new idea which combine the GWO with KNN. The aim of this study selects high level features by using GWO to obtain high accuracy results. The selected features wired to the KNN which trained in supervised learning to detect the IDS problem form selected features.

Furthermore, in the first experiment the KNN applied alone without using any feature selection techniques, and presented Sensitivity 0.8400%, Specificity 0.8260%, and Accuracy 0.8590. besides the presented GWO+KNN presented best results than when apply KNN alone, which presented Sensitivity 0.9800, Specificity 1.0, and Accuracy 0.9667.

The proposed method can easily apply to various classification problems such as EEG signal classification, EGC signal classification, face recognition, fingerprint recognition and disease detection by modifying only number of parameters like input features, hidden nodes and output classes.

REFERENCES

[1] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. Chan, “Cost-based modeling for fraud and intrusion detection: results from the jam project, in: DARPA Information Survivability Conference and Exposition,” *DISCEX’00, Proc.*, vol. 2, no. IEEE, 2000, pp. 130–144, 2000.

[2] M. Alkasassbeh, A. B. A. Hassanat, and G. Al-naymat, “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,” vol. 7, no. 1, pp. 436–445, 2016.

[3] A. Abraham, C. Grosan, and C. Martin-Vide, “Evolutionary design of intrusion detection programs,” *Int. J. Netw. Secur.*, vol. 4, no. 3, pp. 328–339, 2007.

[4] 1. L. Zhou, V. Varadharajan and M. Hitchens, "Cryptographic role-based access control for secure cloud data storage systems", IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2381-2395, Nov. 2015.

[5] F. Chen, T. Xiang, Y. Yang and S. S. M. Chow, "Secure cloud storage meets with secure network coding", Proc. IEEE Conf. Comput. Commun., pp. 673-681, 2014.

[6] D. He, S. Zeadally and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks", IEEE Syst. J., vol. PP, no. 99, pp. 1-10, 2015.

[7] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[8] J. Shen, H. Tan, S. Moh, I. Chung and J. Wang, "An efficient RFID authentication protocol providing strong privacy and security", J. Internet Technol., vol. 17, no. 3, 2016.

[9] R. Prodan and S. Ostermann, "A survey and taxonomy of infrastructure as a service and web hosting cloud providers", Grid Computing 2009 10th IEEE/ACM Int'l Conference on.

[10] N. Bhensook and T. Senivongse, "An assessment of security requirements compliance of cloud providers", Cloud Computing Technology and Science (CloudCom) 2012 IEEE 4th Int'l conf.

[11] Guidelines on Security and Privacy in Public Cloud Computing", NITS, Feb 2013, [online] Available: http://csrc.nist.gov/publications/nistpubs/800144/SP800-144.pdf.

[12] Q. Xiaofeng, L. Wenmao, G. Teng, H. Xinxin, W. Xutao and C. Pengcheng, "WoT/SDN : web of things architecture using SDN," in China Communications, vol. 12, no. 11, pp. 1-11, November 2015, doi: 10.1109/CC.2015.7366240.

[13] V. Marbukh, "On systemic risk in the cloud computing model", 26th International Teletraffic Congress (ITC), 2014.

[14] V. Marbukh, "Perron-Frobenius measure of systemic risk of cascading overload in complex clouds: work in progress", IFIP/IEEE International Symposium on Integrated Network Management, 2013.

[15] The top 10 DDoS attack trends", [online] Available: http://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf.

[16] L. Colace, G. Masini, V. Cencelli, F. Denotaristefani and G. Assanto, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Computing Surveys, vol. 39, no. 3, pp. 273-302, 2007.

[17] M. L. Sang, S. K. Dong, J. H. Lee and J. S. Park, "Detection of DDoS attacks using optimized traffic matrix", Computers & Mathematics with Applications, vol. 63, no. 2, pp. 501-510, 2012.

[18] T. Thapngam, S. Yu, W. Zhou and S. K. Makki, "Distributed denial of service (DDoS) detection by traffic pattern analysis", Peer-to-Peer Networking and Applications, vol. 7, no. 4, pp. 346-358, 2014.

[19] M. H. Bhuyan, A. Kalwar, A. Goswami and D. K. Bhattacharyya, "Low-rate and high-rate distributed DoS attack detection using partial rank correlation", Fifth International Conference on Communication Systems and Network Technologies, 2015.

[20] H. J. Kashyap and D. K. Bhattacharyya, "A DDoS attack detection mechanism based on protocol specific traffic features", International Conference on Computational Science Engineering and Information Technology, pp. 194-200, 2012.

[21] P. Xiao, W. Qu, H. Qi and Z. Li, "Detecting DDoS attacks against data center with correlation analysis", Computer Communications, vol. 67, no. C, pp. 66-74, 2015.

[22] S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using novel information theory metrics", Computer Networks, vol. 116, pp. 96-110, 2017.

[23] A. Shiravi, H. Shiravi, M. Tavallaee and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection", Computers & Security, vol. 31, no. 3, pp. 357-374, 2012.

[24] Ahmad Shawahna, Marwan Abu-Amara, S. Ashraf, H. Mahmoud and Yahya Osais, "EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability EDoS Attacks", IEEE Transactions On Cloud Computing, Feb. 2018.

[25] N. Reamaroon, M. W. Sjoding, K. Lin, T. J. Iwashyna and K. Najarian, "Accounting for Label Uncertainty in Machine Learning for Detection of Acute Respiratory Distress Syndrome," in IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 1, pp. 407-415, Jan. 2019, doi: 10.1109/JBHI.2018.2810820.

[26] D. Peng and Z. Yi, "Dynamics of Generalized PCA and MCA Learning Algorithms," in IEEE Transactions on Neural Networks, vol. 18, no. 6, pp. 1777-1784, Nov. 2007, doi: 10.1109/TNN.2007.895821.

[27] K. P. Sinaga and M. Yang, "Unsupervised K-Means Clustering Algorithm," in IEEE Access, vol. 8, pp. 80716-80727, 2020, doi: 10.1109/ACCESS.2020.2988796.

[28] C. Chang, "Deep and Shallow Architecture of Multilayer Neural Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 26, no. 10, pp. 2477-2486, Oct. 2015, doi: 10.1109/TNNLS.2014.2387439.

[29] A. M. Karim, F. V. Çelebi, and A. S. Mohammed, "Software Development for Blood Disease Expert System," Lecture Notes on Empirical Software Engineering, vol. 4, no. 3, pp. 179–183, 2016.

[30] A. M. Karim, O. Karal, and F. C¸ elebi, "A new automatic epilepsy ¨ serious detection method by using deep learning based on discrete wavelet transform," no, vol. 4, pp. 15–18, 2018.

[31] Karim, A.M.; Kaya, H.; Güzel, M.S.; Tolun, M.R.; Çelebi, F.V.; Mishra, A. A Novel Framework Using Deep Auto-Encoders Based Linear Model for Data Classification.

Sensors 2020, 20, 6378.

[32] A. M. Karim, M. S. Guzel, M. R. Tolun, H. Kaya, and F. V. Celebi, ¨"A new generalized deep learning framework combining sparse autoencoder and taguchi method for novel data classification and processing," Mathematical Problems in Engineering, vol. 2018, 2018.

[33] A. M. Karim, M. S. Guzel, M. R. Tolun, H. Kaya, and F. V. C¸ elebi, "A new framework using deep auto-encoder and energy spectral density for medical waveform data classification and processing," Biocybernetics and Biomedical Engineering, vol. 39, no. 1, pp. 148–159, 2019.

[34] A. M. Karim, "A New Framework by Using Deep Learning Techniques for Data Processing," Ph.D. dissertation, Computer Engineering Dept.,. Ankara Yildirim Beyazit Univ., Ankara., Turkey, 2018.

[35] S. N. Tran and A. S. d'Avila Garcez, "Deep Logic Networks: Inserting and Extracting Knowledge From Deep Belief Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 2, pp. 246-258, Feb. 2018, doi: 10.1109/TNNLS.2016.2603784.

[36] S. S. S. Rawat, V. A. Polavarapu, V. Kumar, E. Aruna and V. Sumathi, "Anomaly detection in smart grid using rough set theory and K cross validation," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, 2014, pp. 479-483, doi: 10.1109/ICCPCT.2014.7054882.

[37] C. Yang, X. Zhu, Z. Ahmad, L. Wang and J. Qiao, "Design of Incremental Echo State Network Using Leave-One-Out Cross-Validation," in IEEE Access, vol. 6, pp. 74874-74884, 2018, doi: 10.1109/ACCESS.2018.2883114.

[38] Z. Shao, M. J. Er and N. Wang, "An Efficient Leave-One-Out Cross-Validation-Based Extreme Learning Machine (ELOO-ELM) With Minimal User Intervention," in IEEE Transactions on Cybernetics, vol. 46, no. 8, pp. 1939-1951, Aug. 2016, doi: 10.1109/TCYB.2015.2458177.

[39] N. Moustafa, B. Turnbull and K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of

Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4815-4830, June 2019, doi: 10.1109/JIOT.2018.2871719.

[40] Meng Wang, Yiqin Lu, Jiancheng Qin, A dynamic MLP-based DDoS attack detection method using feature selection and feedback, Computers & Security, Volume 88, 2020, 101645, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101645..

[41] N. R. Sabar, X. Yi and A. Song, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," in *IEEE Access*, vol. 6, pp. 10421-10431, 2018, doi: 10.1109/ACCESS.2018.2801792.