Journal of Statistics, Computing and Interdisciplinary Research
ISSN (P): 2707-7101

J. Stat. Comp. & Interdis. Rese.
Volume 7(2) (2025), 115-138
http://scir.wum.edu.pk/index.php/ojs

A Machine Learning-Based Framework for Enhancing Data Security in Cloud of Things

Sadia Zahra[1], Afshan Gul[2], Fatima Bukhari[1], Kashia Riaz[3], Muhammad Ahsan Jamil[5]*

[1] Department of Computing, National University of Modern Languages, Multan, 60000, Pakistan.
[2] Faculty of Computing, The Islamia University of Bahawalpur, 63100, Pakistan.
[3] Department of Computer Science, Quaid-e-Azam University Islamabad, 45320, Pakistan.
[4] Institute of Computing, MNS University of Agriculture, Multan, 60000, Pakistan.
***Corresponding Author:** Muhammad Ahsan Jamil, ahsan.jamil@mnsuam.edu.pk

Abstract

Cloud computing has arisen as a progressive model in the field of IoT. It runs on the bases of on-demand services which can be taken in a way that the users of the services can avail them based on their demand, not only this, the user can balance the resources on per demand. Cloud computing comes up with never-ending benefits, but being cost-effective is it's the main merit. Security of cloud is the focused thing in this work. the data generated by IoT is huge in amount that low-power constrained find it difficult to handle, so this is what the clouding computing is here for. The combination of Cloud Computing and IOT is known as Cloud of Things (CoT). This fusion is solving the issues of storage but it also comes up with the challenges of security. To identify the issues of security, many researches has been done. These include the integrity and the confidentiality of data but it also identifies different kinds of CoT attacks, i.e. eavesdropping, forgery, flooding attacks, DOS, insider attacks etc. some researchers have also suggested some solutions, but there is still a need of finding the solutions that are comprehensive, intelligent and detailed. This research work will propose the theoretical framework of data security in CoT based on Machine Learning Techniques. This work will present some solutions

that how can the machine learning techniques can be used to cope up with the threats against CoT.

Keywords: *Cloud Computing, Security issues in cloud system, Cloud of Things, CoT Data Security.*

1. Introduction

An intelligent system that has a global and persistent network of smart devices or sensors which help to physically govern the environment through the process of collecting, processing, and then transmitting the huge data on the internet, this system is termed as IoT [1]. Computational resources in cloud computing are assigned a service to provide a fresh vision high-performance computing system that is based on the internet. IoT produces data in huge amounts, so the low power constrained feel difficult to handle such big data, so to handle such kind of data, cloud computing is used [2]. Cloud of Things (CoT) is the combination of the Internet of Things (IoT) and cloud computing. This combination can solve the issue of security, but it generated some serious security issues. Several researchers have conducted researches on finding out the issue of security that entails different types of attacks i.e. DOS, forgery, flooding attacks, insider attacks, etc, the integrity and confidentiality of data. They have also presented some solutions, but more solutions must be put forward that are effective and comprehensive [3].

Cloud Computing

Cloud computing is the combined term used for the information technology group of innovations that is capable of working together in order to change the method in the way that IT administration has conveyed, entered, or paid. Several publications have presented the importance of cloud computing but clarification about the cloud computing by NIST is globally acknowledged, that says:

It is the model that is used for providing easy, on-request network access to configurable computing resource's shared pool i.e. application, server, storage, and network that can be immediately unconfined with less effort from management or any interaction from the service provider [1]. The networked interconnection of devices that we use in an everyday life are frequently prepared with the global devices is termed as Internet of Things (IoT). IoT is based on the handling of huge amount of data so that the useful service can be provided [4].

Security Requirements of Cloud Computing, IoT, and CoT

With the advancement of any technology its security risks also increase, as cloud computing is evolving model in the field of IT so its security concerns are increasing as well. In cloud

computing, this is the most important issue to be addressed because the customer must feel secure that the data or information presented there is protected by the authority [4,5]. The security challenges and issues in CoT are considered to be linked with areas like heterogeneity, which is instigated by the platforms, different kind of devices, operating system, service available, computation and storage aspects, storage, reliability needed for mission-critical application, processing, performance of communication, access, huge data causing issues of transportation and the monitoring [6,7]. In recent times, learning algorithms are applied by many researchers while practicing their work. if we talk about the recent advancement of learning algorithms, is includes the new algorithm's development, low computation cost of algorithm and big data's availability [8]. The growth of ML has been remarkable as it started from laboratory work and emerged into applying practically by using it extensively with other applications. Traditional machine learning requires the engineered features for transformation for the analysis of patterns; this is what ML refers to. Common ML algorithms such as decision trees (DT), k-nearest neighbor (KNN), and k-means clustering are discussed keeping in mind their merits, demerits, applications in IoT, CoT, and the cloud computing security. Technology advancement has led the world to grow fastly. The data generated from the devices has been so huge in amount that there came the need to hand it in by controlling its challenges and securing the data by using some effective solutions. So, the main motivation of the researcher behind this paper is to propose an effective and intelligent framework in detail which is based on machine learning methods that may help the practitioners in solving the issues that arise in the CoT. This will also help other researchers to add to their knowledge who have the motivation of doing experimental work in the field of Cot using machine learning techniques. To solve the data security issues, the techniques of security must be understood. To minimize the risks of data security in the environment of CoT, the standardized guidelines for the services of cloud users and the cloud suppliers are provided. Some other objectives are as follows:

- To identify data security problems or threats in CoT environment.
- To control security control processes that hurt the CoT must be identified and avoided.
- To suggest theoretical machine intelligent framework or model in which the issues and the demerits of data security in CoT are recognized.

2. Literature Review

The local data can be stored by operators with the usage of cloud facilities, operators in the remote data server where the operators choose the cloud services. The relationship between

public and private objects is improved with the support of using cloud facilities. There is an individual place for cloud computing in the market for having affordable strategies for businesses on small scale and fulfilling the requirements of end-user. The customers of cloud computing environment are provided with a number of benefits on economic level [9]. Therefore, cloud providers are working more analytically under the increasing pressure of innovative developing technologies throughout the world so that all the requirements of the operator can be fulfilled with better and enhanced facilities. There are diverse architectures of environments of cloud computing environments depending on the cloud facilities. In the cloud environment, the information is stored in a server having large size and a large amount of instruction for processing. This is the point where the cloud providers must be trusted by the user in terms of data security [10].

Cloud Computing Architecture

NIST (National Institute of Standards and Technology) have given various innovative emerging ideas, strategies, tools in the field of information technology [11]. In the field of information technology, a very important is played by NIST.

NIST cloud computing architecture says that there have been five actors recognized in the cloud system who perform particular and special cloud computational schemes [11]. The cloud service consumer gains cloud services from the cloud provider and then the consumer is able to use cloud services [8]. Cloud consumers could be a company or organization that is going to use the cloud-based server e.g. a SAAS platform, such as e-mail. Cloud service providers provide the required services to all consumers of the cloud system. CSP also manages the correct allotment of resources to the consumer and controls and maintains cloud services. Cloud broker blend and merge the cloud services to produce better and advance services and also give value-added services to the cloud user. Sometimes it acts like a cloud service provider when communicating with a consumer and sometimes it acts like a consumer when it communicates with the cloud service provider [12]. Check and analyze the cloud services that are provided by the cloud provider to the consumer in order to make sure that the merchant is working according to the expectation and also evaluate whether it is securely performed or not. Furthermore, according to NIST, cloud auditing is very essential in federal agencies, and they should add an authorized section involving third parties in order to manage the security controls of cloud providers.

Cloud carrier provides connections and transits cloud services from cloud providers to the cloud consumer e.g. an internet service provider (ISP). Cloud providers will probably build up a service level agreement (SLAs) with cloud carriers to provide services in accordance with the level of SLAs offered to the cloud consumers. Depending on the services provided by the cloud provider to the consumers, the cloud computing system has been classified into three services delivery models. Following is a brief explanation of each delivery model.

Cloud Deployment Model

A Cloud platform in which public users can participate and register themselves and use the available infrastructure on a commercial basis. It can be easily accessible because it covers a huge organizational area, but security risks are very high in this cloud [13,14]. It exists at the cloud provider's premises. Public cloud provides several benefits to the consumers as customers do not need to do any basic investment on the whole framework.

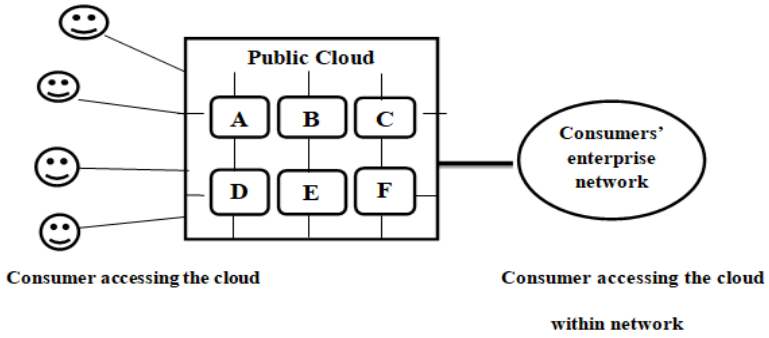

Figure 1: Public Cloud

Private clouds are formulated for the specific organization on a private network, also known as the internal cloud. A private cloud is fully controlled and managed by a specific organization or third party who purchases this cloud. it can be on-site or off site [15,16]. In which the cloud exists on the site of the third party with the hosting facility and is accessible only to the legitimate users. Figure (2) shows the on-site private cloud and Figure (3) shows the Out-source private cloud. Consumers access the private cloud.

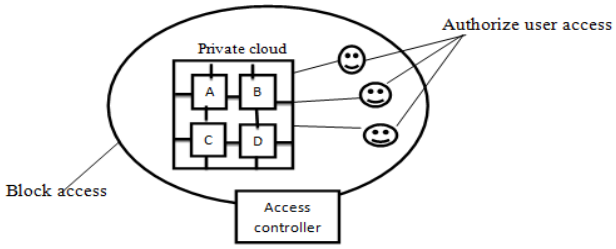

Figure 2: On-Site Private Cloud

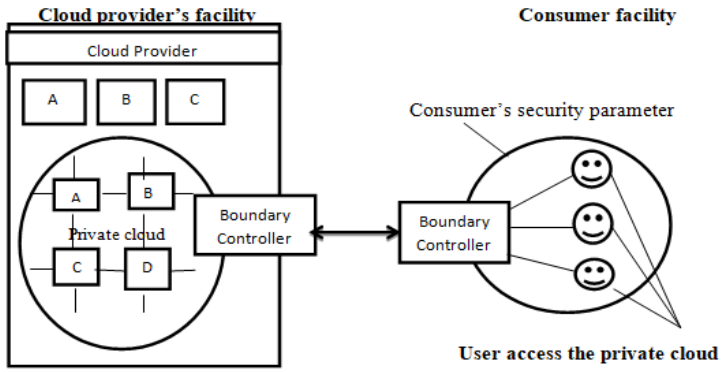

Figure 3: In-Site Private Cloud

A hybrid cloud is a composition of a public and private cloud that attempts to define each approach's application. In the hybrid cloud, part of the service framework performs in the private cloud while another part performs in the public cloud [17,18]. It remains distinct but linked in a standardized way. Hybrid cloud provides more security than public cloud while still providing service and flexibility on demand.

Cloud of Things (CoT)

IoT is booming with the development of information technology. It can connect sensors, controllers, machines, people and other things together with local networks or the internet by using wireless communication which will get the information, exchange it, remote control management and intelligence. This shows that a huge amount of data will be generated. Here sensitive outsourcing data management will be a great challenge. To deal with the big data storage and analysis, clouding will be e feasible method [19,20]. So, integration of cloud computing and IOT makes a new computing paradigm which is called COT.

This combination IoT and cloud computing was required to handle unstructured data efficiently. In the large internet of things environment, clouds of things will play an important role in the future for enabling the service provision. The infrastructure of Internet is highly affected because of the huge amount of data collected by the internet of things which is combined with other big data that is already available. So many corporations are working on solutions to ease the pressure which will resolve the obstacles of data with main part of this solution being cloud computing [21]. Cloud computing means to process the huge amount of data and also enables us to use this characteristic to share and distribute the data which is generated by the IoT devices and other sensors. The way IoT had included the cloud in its architecture by a convenient, scalable and on-demand network access to other devises and sensors and other resources of computing that are IoT configurable.

Cloud and IoT are one of the most important features of upcoming internet. Their combination creates the Cloud of Things. The paradigms of cloud computing is inspired by the paradigms of IoT everything thing particularly 'smart things' are completely connected to the internet and is integrated with the cloud computing [22,23]. All the services which are offered by cloud computing, Cloud of things facilitates to communicate which include the SaaS, IaaS, and PaaS. CoT provides the cheap and guaranteed access to smart things, moreover, being user friendly and doable in a cost-effective way. There is no doubt that paradigms of cloud are different from the IoT, but combination of these will provide the various advantages which are reported in the literature. Cloud computing is considered to be an accessible, efficient and reasonable solution in the era, A phenomenon is provided by the combination of IoT and cloud computing which is known as Cloud of Things and many new possibilities like processing of big data, coverage of security concerns, resource constraints and scalability also enables to some extent though their combination [24]. Other things like new revenue stream, improves customer services and inspired product innovation are created by the CoT [25]. Along with these enablers, middleware which plays a key role in the CoT (similar to IoT), can be seen in the figure, focusing on the technologies of middleware and targeting to study their roles and necessities in the environment of CoT [26,27]. The software layer which sits between the applications and objects. It focusses on finding the solution for the frequently encountered problems such as interoperability, heterogeneity, security and dependability. This layer can be considered as "network oriented" vision. We are observing the growth in the middleware development on a daily basis because this will make it easy to combine the new services, previous technologies to produce the new and more capable service. The main feature possessed by the middleware is transparency [28]. Abstraction is provided by this software layer to the application from different objects. This feature will solve the problem of architecture mismatch. There are also many other features provided by the middleware for desirable performance. Including flexibility, context management, interoperability, reusability, maintainability and other properties. A secure environment in cloud computing reduces the cost that becomes affordable to any consumer. If there is not any security management then there may be chances of whole data to be destroyed or maybe access by an unauthorized user, so in the cloud computing environment, it is necessary to make secure the cloud computing environment [29,30].

As the data stored on the server of the cloud so there are a lot of chances of damaging the data and losing data. In order to protect the data on cloud, there is need to secure the cloud so that cloud works efficiently [31,32].

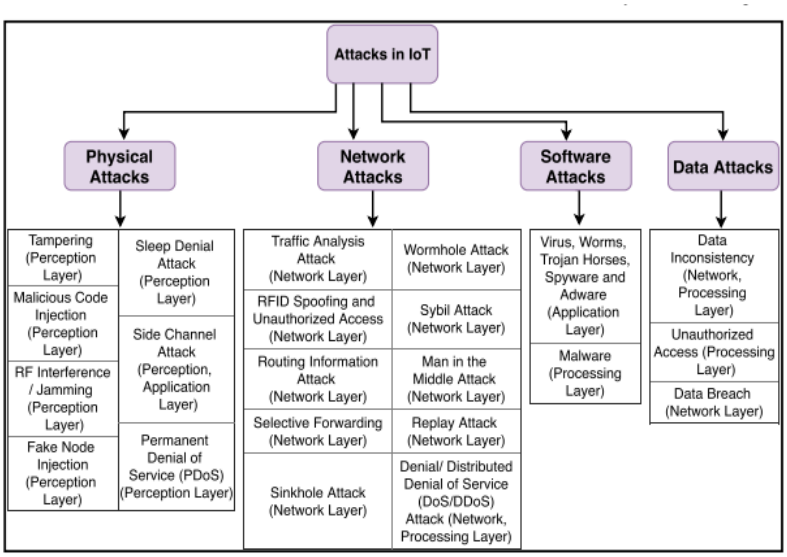

Figure 4 Attacks in IoT

The data processing capabilities can be improved greatly with the help of CoT, but the architecture if it is very much exposed that results in producing the security threats beacsue their wireless transmission channel's nature is open [33]. The International Data Corporation surveyed in 2011 according to which about 74.6% of customers of the corporation suggested that safety is the main challenge that they have encountered. Moreover, Forbes released their report in 2015, that showed there is a focus on spending on CoT's security which will grow by 42%. From such facts, we can reckon that how much security issue is CoT is crucial [34,35]. The most important and the only obstacle that IoT incorporation faces with cloud computing is the factor of trust when it comes to the security and the privacy of data. Furthermore, there are a lot of devices in the IoT which can be at risk of being attacked by an attacker and this leaves them making expose to the threats [36]. Mostly, IoT devices have the function that they store confidential information and the most important infrastructure, that is why privacy and security are the two most important factors that need to be taken into consideration. Heterogeneity is the areas that are caused by the platforms, number of different devices, availability of services, and the operating system [37,38].

- The areas like storage aspects, communication performance, and computation
- For mission-important devices, reliability is needed.

- The issues like storage. Processing, transportation, and access can be caused by big data monitoring.

Table 1: Comparison Supervised ML methods with Conventional security methods

Algorithms	**ML Methods**	**Conventional Methods**
Future Predictability	Can train themselves automatically with new attacks	They are rigid in their approach.
Improvement	They Keep on Improving their accuracy and efficiency	They are rigid in their approach.
Big Data	Can Deal with Huge Amount of increasing data	Can only deal with limited data
Learning Ability	Can easily learn discover specific trends and patterns from huge amount of Data	Do not have learning capability
Automation	Can detect new attacks without human intervention	Cannot automate the process of new attacks
Data Handling	Can handle Multi-dimensional and Multi variety of data	Can only deal with specific type of data
Range of Application	It has wide range of application	Has limited range of application
Time and Space	Require More Time and space	Require less Time and space
Acquisition of Data	Required massive amounts of data for training and it should be unbiased and of good quality	Does not depend on data training
Resources	Require massive resources to function	Require less resources

3. Methodology:

After identification of the research question and subject domain, then the first and foremost thing is to select the research strategy that must be matched with the subject domain and research questions. The research strategy is called the scientific method through which we can answer our research questions. After the proper study of all the methods and then according to the research question, there needs to be an approach to do research.

Method Selection:

The method is a technique to find out the solution to any problem or extract something new regarding that problem. According to the three conditions that should be used to answer the research question is either experimental, case study or survey. Firstly, analyze the conditions then according to the research questions, the method is to be selected. After that, analyze the scope of the researcher's power over real behavioral events and then the level of focus on current events in order to select the strategy for research.

Data Collection:

For data collection, the study of much research that has explained the cloud computing security issues is mandatory. The first and foremost thing is that attempt to identify what sort of contextual analysis that exhibits to present an initial flaw through which the whole security problem rises. To identify which areas of cloud of things need more research, initially CC challenges are found (this is done by searching the literature). Available methods for achieving this are literature review (LR) and systematic literature review (SLR). SLR is used to find all available data relevant to a particular research area. Literature review is also used for collecting information to satisfy 'RQ 1' and 'RQ 2'. Based on the information gathered from literature review, an analysis was employed to develop general explanations. Using search engines and electronic databases to find information. The research questions of this study and the corresponding research methodologies are laid out in a tabular form. As we can see, LR is used to identify security related challenges in clouds of things. Data analysis on LR helps to answer the question 'How can we make a CoT environment more secure by machine learning methods?' Narrative Analysis is used to answer, 'What are architectures of different frameworks for CoT based environments?' Finally, the Narrative and Experimental Analysis answers, "How the proposed design of machine intelligent framework can overcome the data security challenges of a CoT environment?'

Proposed CoT Framework

A broad range of applications are covered by the IoT theoretically. These applications include, smart lightening of streets, smart home systems, traffic controlling, city-wide management, networks of vehicle in a real time, monitoring of nose, and plans of smart city etc. A broad range of technologies integrated by the IoT practically such as servers, sensors/ actuators, and individual devices. In order extract valuable or actionable information to perform the complex and smart services, the data from the different resources may be collected, merged, analyzed and processed. To accomplish this open sharing, the technology helped named cloud computing. This technology is developed to process, store and manage huge amounts of data at remote places. In an IoT architecture, Cloud is a perfect element and integration of both make a new paradigm.

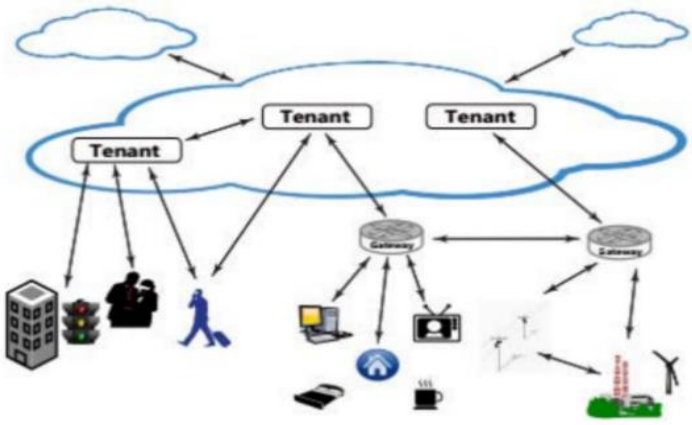

Figure 5: The interactions within Cloud of Things

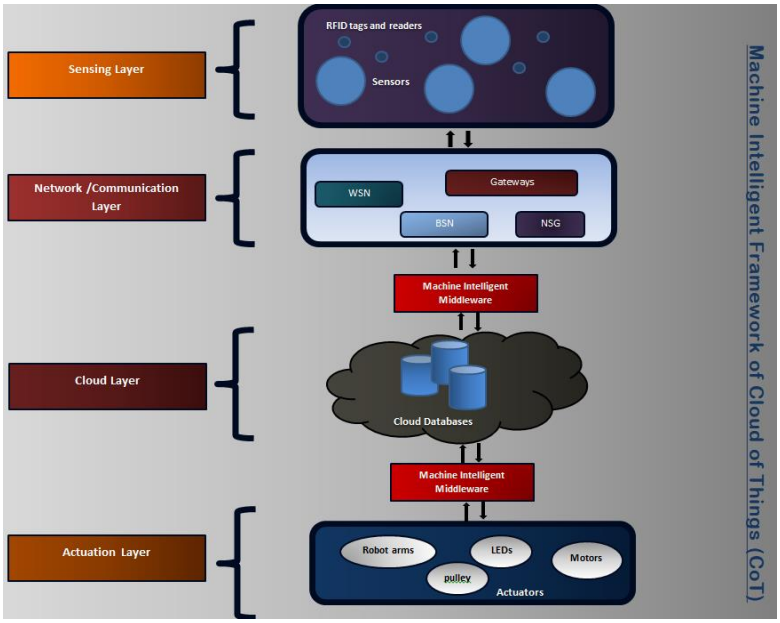

Figure 6: Proposed Framework Architecture

The ability to develop, deploy and manage the applications through the Cloud is what makes the CoT different than the present Internet of Things. So, it is required to protect the outgoing and coming data from any kind of malicious attacks. To ensure the proper implementation of CoT based ecosystem, there is need for robust and scalable architecture. That architecture should be able to deal with the end user's never-ending requirements across with handling the challenge. The first step towards the solution is constructing the architecture. The architecture for the Cloud of Things is proposed in this section which would be present as a blueprint for the described technology and explains the various components that compose it. The detailed description of each layer framework with various actors which concern Cloud of Things.

Sensing Layer

This layer consists of the various sensors whose work is to collect the data from environment and transfer this information to network layer. Sensor here acts as an eye and ear for the system whose work is to detect the events and transmitted the collection information to the network layer. There are basically three parameters based on which sensors can be categorized. These are named Methodology, Sensing and Type. Here Type Defines the type of a sensor i.e. Homo or Heterogeneous sensor, single dimensional or multidimensional sensor. Here methodology tells the pattern which sensors follow to collect the information for example as from MRI, passive sensing is gathering the data (blood pressure) from the data which is collected by the active sensing. There are number of parameters which a sensor is capable of sensing known as sensing parameters. For example, one sensor may only sense the body temperature of one parameter and other may sense numerous parameters like in the case of ECG. This layer may also consist of the RFID readers which collect the information from the RFID tags. These RFID tags can store large amounts of information and can conveniently tag on any object like whether it's an animal, human being or consumer product.

Network /Communication Layer

This layer is also known as communication layer. The maintenance of communication among the many sensors, things and humans is the main purpose of this layer. The communication took place divided into three broad categories. 1) Sensor to Thing, 2) Thing to Thing.3) Human to Thing. This layer gets the information from the sensing layer and transmits it to the control layer. This layer consists of two gateways which work as a collection point to combine the collected information from many sensors and RFID readers. All the form of unstructured information is combined by these gateways which are then transmitted to the control layer. In order to ensure the interaction at many levels, network layer uses many networks. The network which forms the core of network layer is WSN (wireless sensor networks). In the scenario of WSN, sensors are connected in various networks and transmitted their respective information to their respective host the wireless network. BSN (body sensor network) is another type of sensor network which is also used by the network layer.

Cloud Layer

The layer is most important layer in the whole architecture. By performing various computations, this layer drives useful insights over the data it receives from the communication layer. From the technical point of view, control layer can also be called cloud layer because this is the point where all data is stored and processed. This layer also provides the platform to

the service provide for hosting their services, so this is also known and service layer. The data is received form the communication layer which is then stored in the databases. Then n number of computations performed on the collected through using certain algorithms to find interesting patterns. The performed computation will be in accordance with the service to which it belongs. The processing results are sent back to the end user and depicted by the actuators in the form of useful information

Actuation Layer

This layer shows the information collected from the cloud layer. This layer act as an actuator which gets the representation of the useful insights coming from cloud layer into the physical world. The elements upon which this layer consist of are robotic arms, LED screen, motors, pulleys etc. The actuation process can be both manual or automatic. Human intervention is involved in the case of manual actuation and results are also shown by humans based on the recommendation given by the cloud layer and actuators work on their own in the case of automatic actuation, according to the information sent by the control layer. This is the most important part of the proposed framework. This will act as a milestone in achieving data security in CoT. If a strict monitoring mechanism is not considered in storing and retrieving data in cloud, then the attackers could steal the important data stored on some storage devices. As shown in Figure 7 the data and commands coming and going from cloud layer will be monitored by machine intelligent middleware so having the capability to monitor IoT devices and cloud data it can intelligently provide a solution to new or zero-day attacks. In order to learn about the normal and abnormal behavior as per how CoT components will interact with each other within the IoT environment, Machine intelligent middleware will have the various powerful data exploration methods. For each part of CoT system, input data may be collected and checked for the normal behavior pattern of interaction, thereby finding malicious behavior at the early stages. The prediction of new attacks which are mostly mutations of pre-existing attacks can also be done by the machine intelligent middleware by using ML methods in a more convenient way because the coming unknown attacks could be wisely predicted by ML methods from the existing examples.

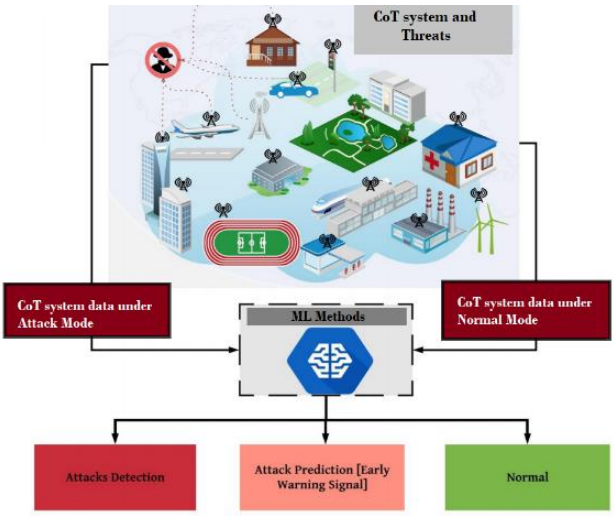

Figure 7: Potential role of Machine Learning middleware in CoT data security

4. Result & Conclusion

In order to perform the experiment to check and compare the efficiency and accuracy of some supervised machine algorithms WEKA (3.8.5) has been used as a simulator in this research work.

Table 2: Machine/Tools used in Experimentation and evaluation of result

Sr	Machine/Tool	Description
1	ENVIRONMENT	Windows 10
2	PROCESSOR	Core i5 ,2.5ghz
3	RAM	4.00 Gb
4	SIMULATOR	Weka 3.8.5

In this research UNSW-NB-15 dataset has been used which was created in ACCS cyber range lab. This dataset consists of 9 types of attacks which are named Backdoor, Dos, Shell code, Fussers, Analysis, Generic, Exploits, Worms and Reconnaissance.

This dataset has total 45 features. It has been divided into two sets, such as Training set and Testing set. The training set has been used to develop machine intelligent models and testing set is used to test the accuracy of developed models.

The statistics of records of both training and testing datasets are given below:

Table 3: Dataset Statistics

Dataset	Total Records	Normal	Attacks
Training Dataset	175341	56000	119341
Testing Dataset	82332	37000	45332
Total	257672	93000	164673
Percentage	100%	36.1%	63.9%

So, the suggested framework middleware is trained by building model/Classifier using machine leaning algorithm on training dataset and after that is it tested using the testing dataset to check the performance and accuracy of anomalous behavior of data and traffic coming and leaving the cloud layer.

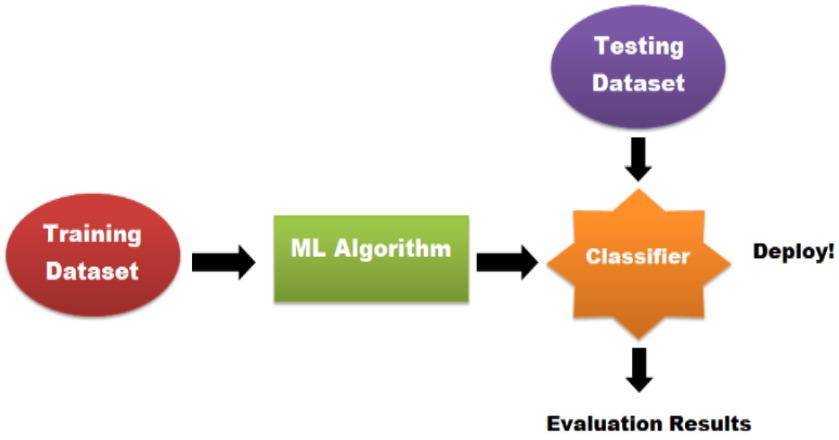

Figure 8: Illustration of how the ML middleware of suggested Framework got Trained & Tested

Techniques used for Model Evaluation

In Weka tool there are 4 Test options for evaluation of models using training and testing of datasets Using Training set, Supplied Test Set, Cross validation, Percentage split. First the model is trained and tested using J48 Classifier and using 2 test Options Cross validations and Supplied Test Set on Weka tool and it has given following results.

Then the model is trained and tested using Bayes Net Classifier and using 2 test Options Cross validations and Supplied Test Set on Weka tool and it has given following results.

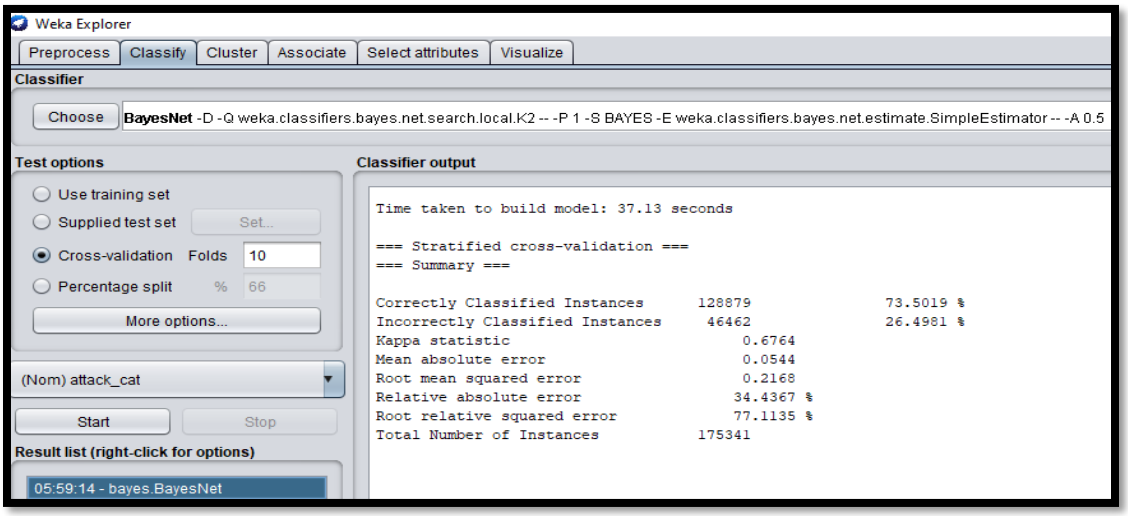

Figure 9: Bayes Net Training set Summary

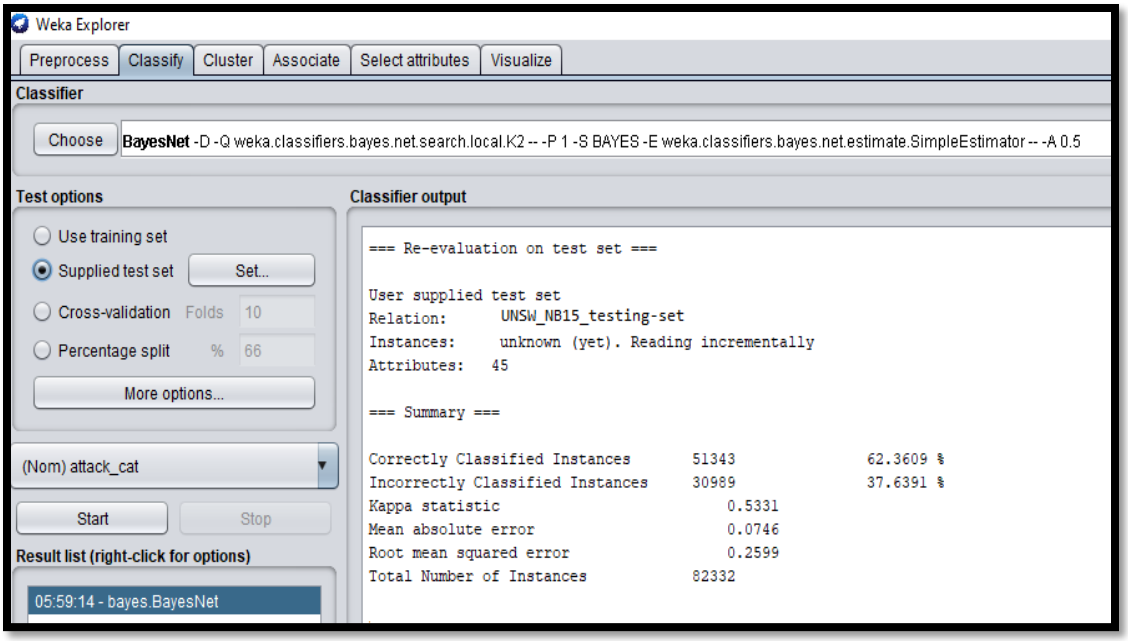

Figure 10: Bayes Net testing set summary

Lastly the model is trained and tested using KNN Classifier and using 2 test Options Cross validations and Supplied Test Set on Weka tool and it has given following results.

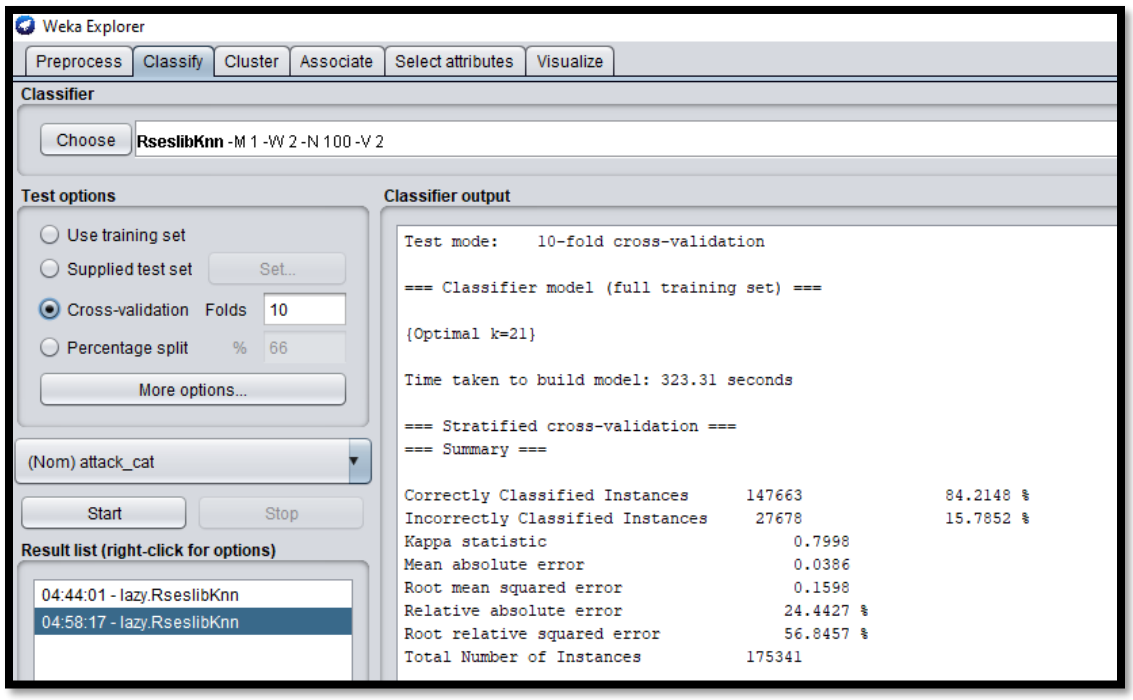

Figure 11: KNN Training set Summary

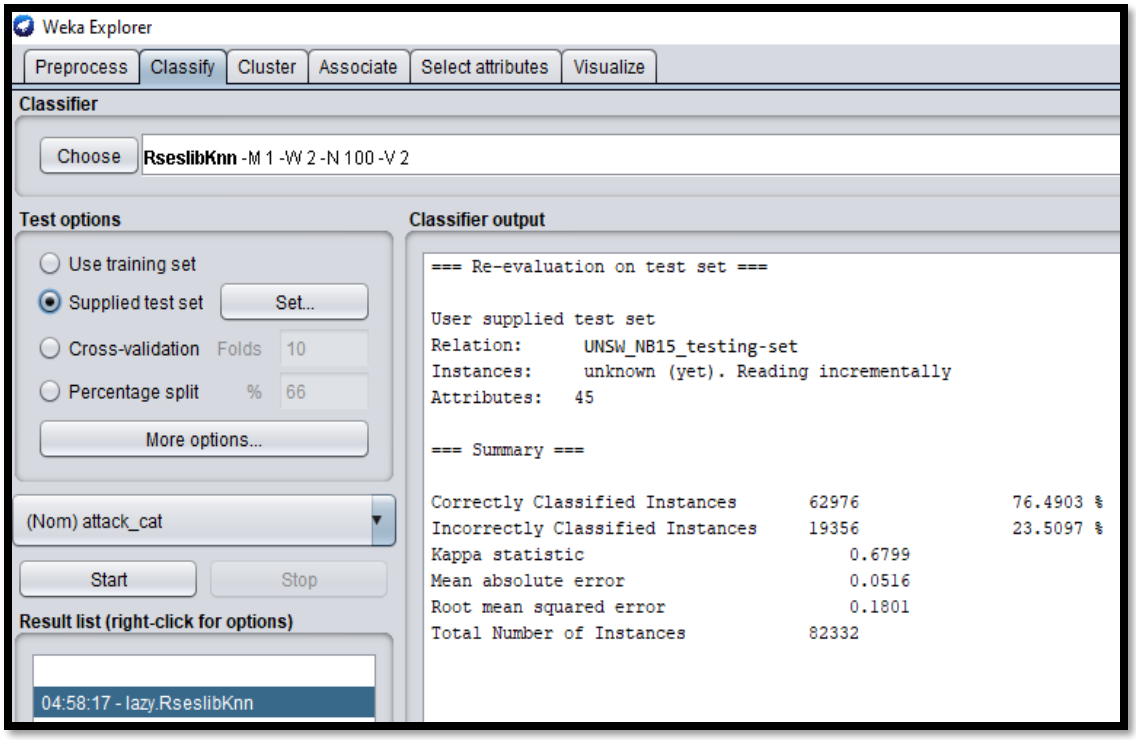

Figure 12: KNN Testing summary

Result Analysis

So, the ML middleware has been trained as mentioned earlier on different supervised ML schemes using training dataset and WEKA tool. Then their performance has been recorded using Test data set. The results are given below:

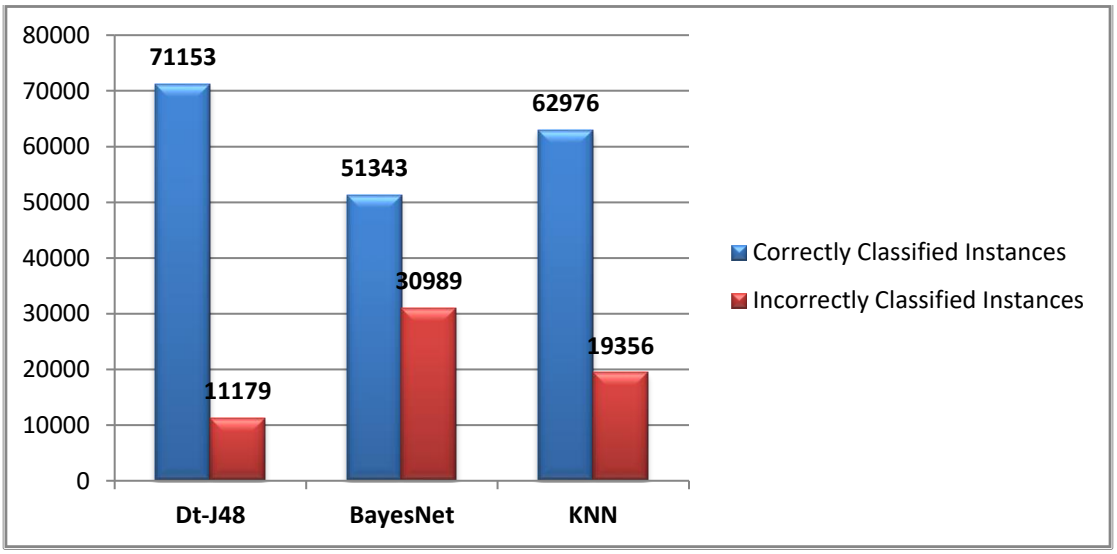

Figure 13: Overall Statistics of Correctly and Incorrectly Classified Instances

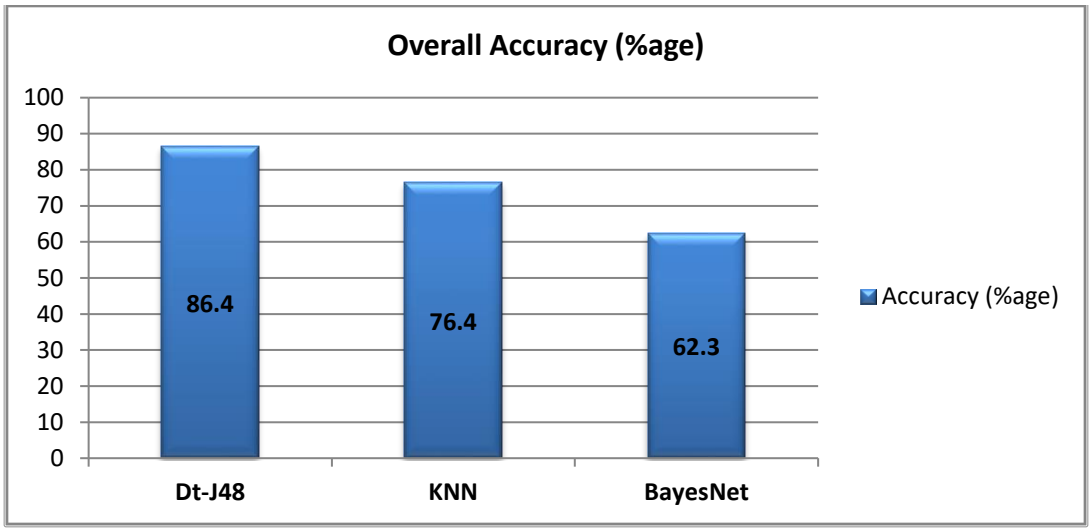

Figure 14: Overall Accuracy (%age) with Testing dataset

Accuracy is one of the measures of evaluating the performance of a model. Accuracy is basically the ratio of correct predictions to total prediction made.

Accuracy = Total Number of Correct Predictions / Total Predictions

Figures 13 and 14 show the overall performance of ML techniques that have been used. So, from results it has been observed that with test datasets J48 has given best result with 86.4% accuracy, followed by KNN with 75.4% accuracy and Bayes Net has given less accuracy of 62.3%.

Table 4: Detailed Accuracy summary of Classifiers

Classifier	**Implemented Algorithm**	**Time taken to build model**	**FP Rate**	**TP Rate (Recall)**	**Precision**	**ROC Area**
Decision Tree	J48	147.6 s	0.01	0.864	0.897	0.947
Bayesian Network	Bayes Net	37.13 s	0.02	0.624	0.831	0.957
K Nearest Neighbor	RsesLibKnn	323.31 s	0.01	0.765	0.833	0.917

If we plot these values in a graph we will get following results:

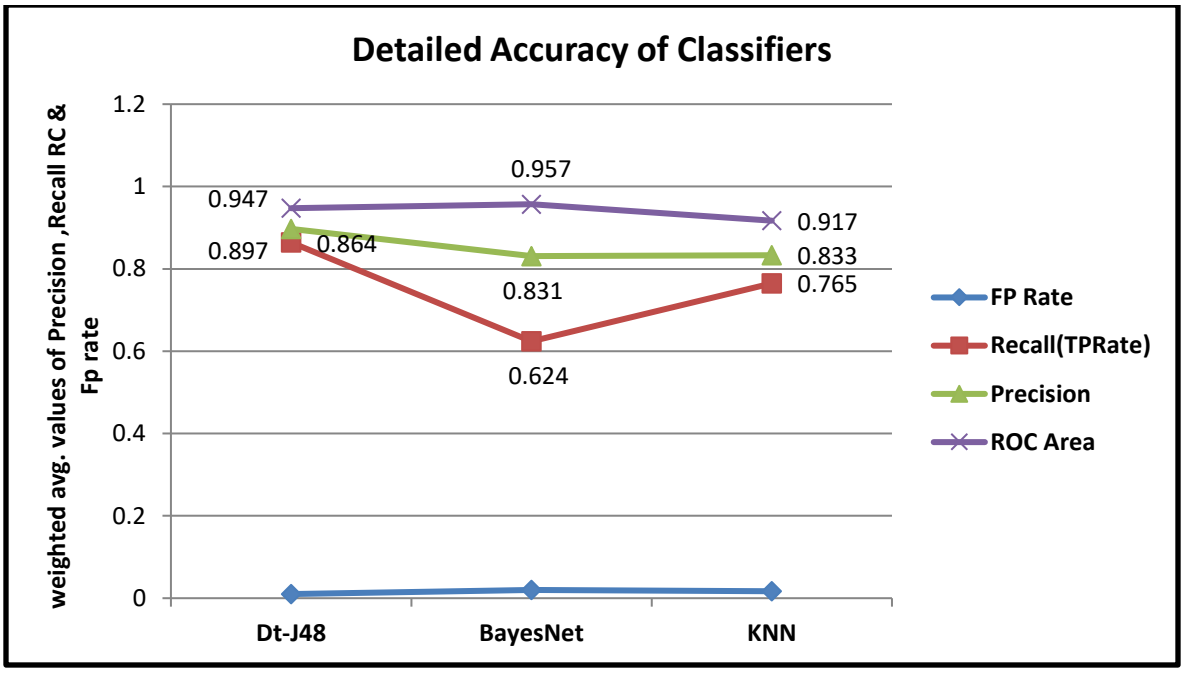

Figure 15: Detailed Accuracy of classifiers with testing dataset

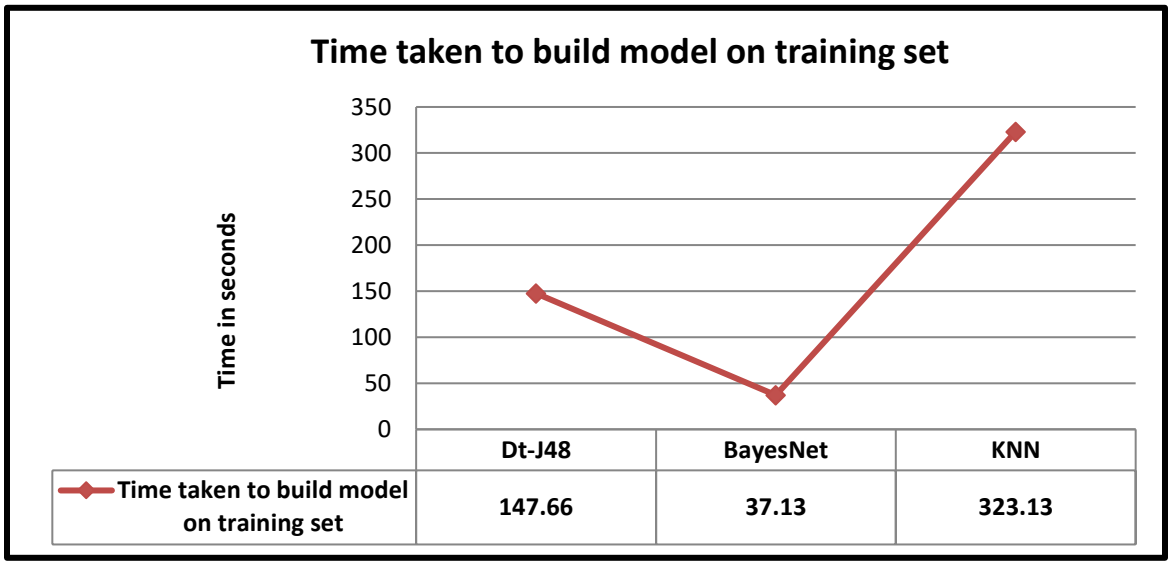

Figure 16: Time taken by Classifiers to build model on training set

Table 5: Comparisons of Classifiers on Time taken to build model on training set

Classifiers	**Training Time**
Dt-J48	Slow
Bayes Net	Fast
KNN	Very Slow

Figure 15, 16 and table 4, 5 help us to give information about metrics that can be considered to analyze or measure the accuracy of a classifier.

Table 6: Detailed Accuracy comparison of Bayes Net Classifiers by Class of Attack

Attacks	**Performance Metrics Values**				**Ranking of each Attack against each Performance Metrics**			
	Precision	**Recall**	**ROC Area**	**Accuracy**	**Precision**	**Recall**	**ROC Area**	**Accuracy**
Backdoor	0.020	0.324	0.864	32.4%	7th	7th	7th	7th
Analysis	0.002	0.003	0.921	0.29%	9th	9th	5th	9th
Fuzzers	0.277	0.587	0.862	58.7%	4th	5th	8th	5th
Shellcode	0.255	0.743	0.989	74.3%	5th	3rd	1st	3rd
Reconnaissance	0.895	0.737	0.963	73.7%	2nd	4th	3rd	4th
Exploits	0.708	0.494	0.875	49.4%	3rd	6th	6th	6th
DoS	0.131	0.138	0.853	13.7%	6th	8th	9th	8th
Worms	0.010	0.864	0.946	86.3	8th	2nd	4th	2nd
Generic	0.962	0.960	0.988	96.0%	1st	1st	2nd	1sr

Table 7: Detailed Accuracy comparison of J48 Classifiers by Class of Attacks

Attacks	**Performance Metrics Values**				**Ranking of each Attack against each Performance Metrics**			
	Precision	**Recall**	**ROC Area**	**Accuracy**	**Precision**	**Recall**	**ROC Area**	**Accuracy**
Backdoor	0.019	0.161	0.894	16.1%	9th	7th	4th	8th
Analysis	0.030	0.007	0.890	26.2%	8th	9th	5th	7th
Fuzzers	0.891	0.675	0.917	67.5%	3rd	5th	3rd	5th
Shellcode	0.423	0.701	0.888	70.1%	7th	4th	6th	4th
Reconnaissance	0.917	0.805	0.922	80.4%	2nd	2nd	2nd	2nd
Exploits	0.653	00.731	0.855	73.0%	4th	3rd	7th	3rd
DoS	0.477	0.127	0.641	12.7%	6th	8th	8th	9th
Worms	0.591	0.591	0.917	59.0%	5th	6th	3rd	6th
Generic	0.997	0.964	0.984	96.4%	1st	1st	1st	1st

Table 8: Detailed Accuracy comparison of KNN Classifiers by Class of Attacks

Attacks	**Performance Metrics Values**				**Ranking of each Attack against each Performance Metrics**			
	Precision	**Recall**	**ROC Area**	**Accuracy**	**Precision**	**Recall**	**ROC Area**	**Accuracy**
Backdoor	0.022	0.118	0.649	11.8%	8th	6th	8th	7th
Analysis	0.014	0.016	0.816	23.9%	9th	9th	4th	5th
Fuzzers	0.656	0.721	0.923	72.0%	2nd	2nd	2nd	2nd
Shellcode	0.493	0.190	0.901	19.0%	5th	5th	3rd	6th
Reconnaissance	0.378	0.667	0.931	66.6%	6th	3rd	1st	3rd
Exploits	0.629	0.730	0.923	72.9%	3rd	1st	2nd	1st
DoS	0.034	0.038	0.718	3.8%	7th	8th	7th	9th
Worms	0.600	0.068	0.781	6.8%	4th	7th	6th	8th
Generic	1.000	0.576	0.802	57.5%	1st	4th	5th	4th

This is the performance analysis of some supervised ML techniques but as the world is moving towards big data and attacks are changing their shapes and modes so suggested middleware

needs to be trained on big datasets with more attack behaviors. With the help of these results it can be said with 80k plus records J48 may give best possible results but it may be possible with huge amount of dataset the behavior of trained models may vary. So, more research needs to be carried out in the ML And CoT security. The research may consist of exploring or discovering Unsupervised ML schemes or clustering for detecting anomalous behaviors.

5. Conclusion

As with the help of facts and figures and results it is discussed that there is rapid development of the Cloud of Things based computing in the world which is not only demanding many tools and techniques to be developed in order to meet the growing demands, but researchers are also facing new data safety issues. In this paper we have done the detailed overview of CoT based computing with machine learning methods for the data security. Moreover, the potential data privacy issues which can affect the system effectiveness and respective solutions to secure the computing have been discussed. Furthermore, several applications are presented to show how data secured CoT-based computing could be implemented in real world applications with machine learning techniques. In an effort to further ease the development of such technologies, this paper provided a clear, comprehensive, framework for data security using machine learning techniques in CoT. Its practical implementation challenges open up an exciting opportunity of extensive research in the future.

References

[1] Alshammari, K., Beach, T. and Rezgui, Y. Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction*, *26*, 159-173, 2021.

[2] Wang, W., Wang, C., Guo, Y., Yuan, M., Luo, X. and Gao, Y. Industrial control malicious traffic anomaly detection system based on deep autoencoder. *Frontiers in Energy Research*, *8*, p.555145, 2021.

[3] Almtrafi, Sara Mutlaq, Bdour Abduallatif Alkhudadi, Hatim Alsuwat, and Emad Alsuwat. "Cloud of Things (CoTs): Security Threats and Attacks." *International Journal of Computer Science & Network Security* 21, no. 8, pp.229-237, 2021.

[4] Okey, O.D., Melgarejo, D.C., Saadi, M., Rosa, R.L., Kleinschmidt, J.H. and Rodríguez, D.Z. Transfer learning approach to IDS on cloud IoT devices using optimized CNN. *IEEE Access*, *11*, pp.1023-1038, 2023.

[5] Suhailam, P., Yerolla, R. and Besta, C.S. 1 Cloud of Things. *Cloud of Things: Foundations, Applications, and Challenges*, p.1, 2024.

[6] T. Mengistu, A. Alahmadi, A. Albuali, Y. Alsenani, and D. Che, "A "No Data Center" Solution to Cloud Computing," pp. 714-717, 2017.

[7] S. Narula, A. Jain, and Prachi, "Cloud Computing Security: Amazon Web Service," pp. 501-505, 2015.

[8] Abuhussein, H. Bedi, and S. Shiva, "Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing," pp. 958-959, 2013.

[9] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia Computer Science, vol. 48, pp. 204-209, 2015.

[10] Sun, G. Gao, T. Ji, and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," pp. 197-201, 2018.

[11] Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," pp. 1081- 1084, 2015.

[12] Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Engineering Science and Technology, an International Journal, vol. 21, pp. 574-588, 2018.

[13] S. Namasudra, P. Roy, and B. Balusamy, "Cloud Computing: Fundamentals and Research Issues," pp. 7-12, 2017. (Namasudra, Roy, &Balusamy, 2017).

[14] Y. Wang and D. Leblanc, "Integrating SaaS and SaaP with Dew Computing," pp. 590-594, 2016. (Wang &Leblanc, 2016)

[15] R. Lin, B. Wu, S. Su, P. Xu, S. Yang, and Y. Zhao, "A Security PaaS Container with a Customized JVM," pp. 960-961, 2014.

[16] Hahn, H. Kwon, and J. Hur, "Toward Trustworthy Delegation: Verifiable Outsourced Decryption with Tamper-Resistance in Public Cloud Storage," pp. 920-923, 2018.

[17] Babar and B. Ramsey, "Tutorial: Building Secure and Scalable Private Cloud Infrastructure with Open Stack," pp. 166-166, 2015.

[18] R. Sahl, P. Dupont, C. Messager, M. Honnorat, and T. Vu La, "High-Resolution Ocean Winds: Hybrid-Cloud Infrastructure for Satellite Imagery Processing," pp. 883-886, 2018.

[19] Rath, Mamata, Jyotirmaya Satpathy, and George S. Oreku. "Artificial intelligence and machine learning applications in cloud computing and Internet of Things." In *Artificial*

intelligence to solve pervasive internet of things issues, pp. 103-123. Academic Press, 2021.

[20] Padyana, Uday Krishna, Hitesh Premshankar Rai, Pavan Ogeti, Narendra Sharad Fadnavis, and Gireesh Bhaulal Patil. "AI and Machine Learning in Cloud-Based Internet of Things (IoT) Solutions: A Comprehensive Review and Analysis." *Integrated Journal for Research in Arts and Humanities* 3, no. 3, pp.121-132, 2023.

[21] Hafiz Muhammad Sanaullah Badar, Nadeem Iqbal Kajla, Jehangir Arshad, Najia Saher, Manal Ahmad, & Muhammad Ahsan Jamil. "Lightweight Intrusion Detection for IoD Infrastructure using Deep Learning". *Journal of Computing & Biomedical Informatics*, 2024.

[22] Bashir, Adil, and Sahil Sholla. "Resource efficient security mechanism for cloud of things." *International Journal of Wireless and Microwave Technologies (IJWMT)* 11, no. 4, pp.41-45, 2021.

[23] Koltyukova, Veronika. "EDGE-CoT: next generation cloud computing and its impact on business." Master's paper, 2021.

[24] Sikandar Ahmad Khan, Muhammad Asad, Haroon Asif, Amjad Ali, & Muhammad Ahsan Jamil. "Author Identification Using Machine Learning". *Journal of Computing & Biomedical Informatics, 2024*.

[25] R. Bharadwaj, A. Bhattacharya, and M. Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution," pp. 95-99, 2018.

[26] W. Nie, X. Xiao, Z. Wu, Y. Wu, F. Shen, and X. Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology," pp. 185-189, 2018.

[27] Abdul Aziz, Uzair Ahmad, Shoaib Saleem, Munahil Khursheed, Arslan Munir, Manal Ahmad, & Muhammad Ahsan Jamil. "IoT Based Smart Vehicular Identification using Machine Learning Techniques". *Journal of Computing & Biomedical Informatics*, *7*(02), 2024.

[28] W. Dworzański and I. A. Lomazova, "CPN tools-assisted simulation and verification of nested Petri nets," Automatic Control and Computer Sciences, vol. 47, pp. 393-402, 2014.

[29] T. Mengistu, A. Alahmadi, A. Albuali, Y. Alsenani, and D. Che, "A "No Data Center" Solution to Cloud Computing," pp. 714-717, 2017.

[30] S. Namasudra, P. Roy, and B. Balusamy, "Cloud Computing: Fundamentals and Research Issues," pp. 7-12, 2017.

[31] B. Shahid, Z. Ahmed, A. Faroqi, and R. M. Navid-ur-Rehman, "Implementation of smart system based on smart grid Smart Meter and smart appliances," in Smart Grids (ICSG), 2012 2nd Iranian Conference on, pp. 1-4, 2012,

[32] Fadi Aloula, A. R. Al-Alia, Rami Al-Dalkya, M. Al-Mardinia, and a. W. El-Hajjb, "Smart Grid Security: Threats, Vulnerabilities and Solutions " Internationa--l Journal of Smart Grid and Clean Energy vol. 1, 2012.

[33] M. Badra and S. Zeadally, "Key management solutions in the smart grid environment," in Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, pp. 1-7, 2013.

[34] L. Nian, C. Jinshan, Z. Lin, Z. Jianhua, and H. Yanling, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," Industrial Electronics, IEEE Transactions on, vol. 60, pp. 4746-4756, 2013.

[35] S. S. Iyengar and R. R. Brooks, Distributed Sensor Networks, Second Edition: Sensor Networking and Applications: Taylor & Francis, 2012.

[36] G. A. Tizazu, H. R. Hussen, and K. Ki-Hyung, "Secure session key exchange scheme for Smart Grid Home Area Networks," in ICT Convergence (ICTC), 2013 International Conference on, pp. 1116-1120, 2013.

[37] E. D. Knapp and R. Samani, "Chapter 1 - What is the Smart Grid?," in Applied Cyber Security and the Smart Grid, ed Boston: Syngress, pp. 1-15, 2013.

[38] P. Stavroulakis and M. Stamp, Handbook of Information and Communication Security: Springer, 2010.