INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, ALLAHABAD
VI Semester B.Tech in Information Technology

Mini project- II Report

IOT devices attacks detection using deep learning methods

By :-

Chinmay Shravanbal Tayade (IIT2018138)

Inayat Baig (IIT2018165)

Guide : - Dr.J. Kokila

Table of contents

Abstract: These days IOT devices and their safety is a centre of attraction for researchers and their defects and vulnerabilities are a great point of attraction for hackers too. So application of Hardware security has been considered important, also significant knowledge of Hardware trojan and the techniques to protect it from attack is extremely important , As they are major threats to hardware. Project is focused on the significance of safe and secure IC's and hardware for the safety of IOT devices around the world .Yearly the price at which innovation in our day to day life is actually improving at a rapid rate This fast growth drives the modern technology business to make and also design their circuits in unreliable third party forges to get them designed at efficient and affordable cost hence leaving behind area for a simultaneous kind of virus referred to as Hardware Trojan the developed HTs leak confidential and encrypted details deteriorate device performance or trigger overall devastation To lower the dangers connected with these viruses several methods have been actually cultivated aiming to protect against as well as detect all of them based on traditional or equipment learning approaches Preferably any type of undesirable alteration helped make to an IC must be actually visible through pre silicon simulation and also post silicon screening The contaminated circuit may be put in different steps of the designing process providing finding and detecting these Hardware trojans is challenging method. In this project we compared various different Machine Learning algorithms and Some Deep learning algorithms for Detecting Trojan free and Infected Integrated Circuits . From the results on comparison of various deep learning and Machine learning algorithms we found out that hardware trojan detection using the Gradient Boosting algorithm can reach the highest accuracy and the performance rate.We also compared our model with previous existing projects , we found that our Gradient boosting Model is the most accurate .

1. INTRODUCTION

1.1 Background and Preliminaries

The current Era is known as the era of technical advancement necessity for even more technological suggestions leads to a lot more complicated and stylish software and also equipment also discussed that a substantial explanation for this technical difficulty is the utility of little sensing units to even a lot more gadgets in a mix Data Analyzing as well as Artificial Intelligence Artificial Intelligence To eliminate this complication they outsource the layout as well as extra frequently the construction of their Integrated circuits to creating business thus jeopardizing potential safety and security issues The most up to date example of safety and security problems has HTs In order to conquer this barrier they the design and also extra currently the designing of their Circuits to manufacturing business thus taking the chance of potential security problems is current issue of security concerns is made up a brand new type of infection known as HT As a result of to the complex attributes of contemporary circuits HTs can easily be launched right into every IC progression phase and also stay inactive till induced by a vast variation of account activation devices HTs are connected with unforeseen IC malfunctions circuit devastation also leakage of confidential information irrespective of the file encryption state Yet another example of influenced fields our company can discuss army issues HT strikes is actually a very interested danger for a lot of markets HT has actually been actually the subject matter of scholastic investigation The post and pre silicon periods where IC's verification process and testing process are included need to spot any type of alteration on an IC that is actually contrary to the beneficial health conditions At the post silicon period we can easily confirm the layout of the IC either through contrasting the means the circuit features and also its own qualities with a gold version of the circuit or even by means of de packaging and Reverse Engineering of the production process of the IC The method of detrimental de packaging of the IC for its own design verification can easily not be actually scalable using the existing highest developed strategies The factor can easily be located at the devious attributes of HTs and also extraordinarily extensive sphere of achievable trojan circumstances an opponent can utilize In the ML segment introduce the terms as well as interpretations of Machine Learning The measures need to have to become adhered to in order to create prophecies coming from the first records In Methodology segment our team evaluated the methods our company make use of for the validation and the testing of our designs In the Result and Comparison area our experts present the last end results of our designs and also HTs are actually viruses which are associated with improvements impacting the circuits during the layout and/or manufacture phase and also are typically introduced by an untrusted design shop or design software program because of complex structure of advanced Integrated circuits Hardware trojans may be offered in to every IC growth stage and remain inactive up until set off through a wide selection of activation procedure HTs are affiliated along with unpredicted IC breakdowns circuit destruction as properly as the disclosing of delicate information no matter of the security condition Hardware trojan has been the

target of academic investigation At the post silicon period experts can verify the style of the IC either through matching up the method the circuit features and its own qualities with a golden design of the circuit or by means of de packaging and Reverse Engineering of the production method of the IC The method of devastating de packaging of the IC for its own style proof can easily not be scalable making use of the present highest developed methods.

1.2 PROBLEM STATEMENT

IoT devices attack detection using Deep Learning Methods with emphasis on Hardware Trojan and countermeasures on IOT Hardware Trojan attacks.

1.3 OBJECTIVES

- Emphasize the significance of application of Security in IoT devices and networks. Discussing challenges faced in security of Hardware i.e the Integrated Circuits used in designing of IOT devices.
- Emphasize the damages caused by hardware Trojan and definition of Hardware Trojan.
- introducing the terminology and definitions of Machine Learning (ML) and necessary implementation need to be done to get accurate predictions from the given data.
- Analyzing the approaches we used for the training and testing of the models .
- Presentation of the final results of our models and in comparison, with the existing work.
- concluding ideas of this project and possible future improvements on the current work.

1.4MOTIVATION

In the world of 5G network and Internet of things the safety of IOT hardware is a necessity To make the IOT network and the devices work effectively and efficiently without the hardware security of IOT devices the respective connected objects like machines and operating bots can be hacked easily nce the network/hardware is hacked the hackers can topple the object functionality and could steal the user data also. Being sustainable helps to improve productivity and it eventually saves money.

1.5 APPLICATIONS

These are the following motives for which Hardware security is useful in different types of Industries.

- INDUSTRY : to protect public key infrastructure from cyber attacks. For example, the competitor of a company could infect its network and infrastructure with inserting a virus in the form of a circuit into an IC and trying to confine its market share or reduce its profits and consumers' preference on its products.
- E- HEALTH : to transmit the data of patients to Machines and devices in a secure way and trusted parties.
- AUTOMOTIVE : securing communication between the various control devices of automobiles.
- M2M : to secure the internet-based information flow be- tween the enterprise.
- SMART METERING : serve to store individual, customer- related keys and provide encryption mechanisms for secure data transmission.
- ARMY AND DEFENCE OPERATIONS : many military operations rely on the ICs Manufactured outside the country . To enhance the security of IC's and Defence mechanisms used by armed forces Hardware Trojan detection is used.

1.6 MACHINE LEARNING

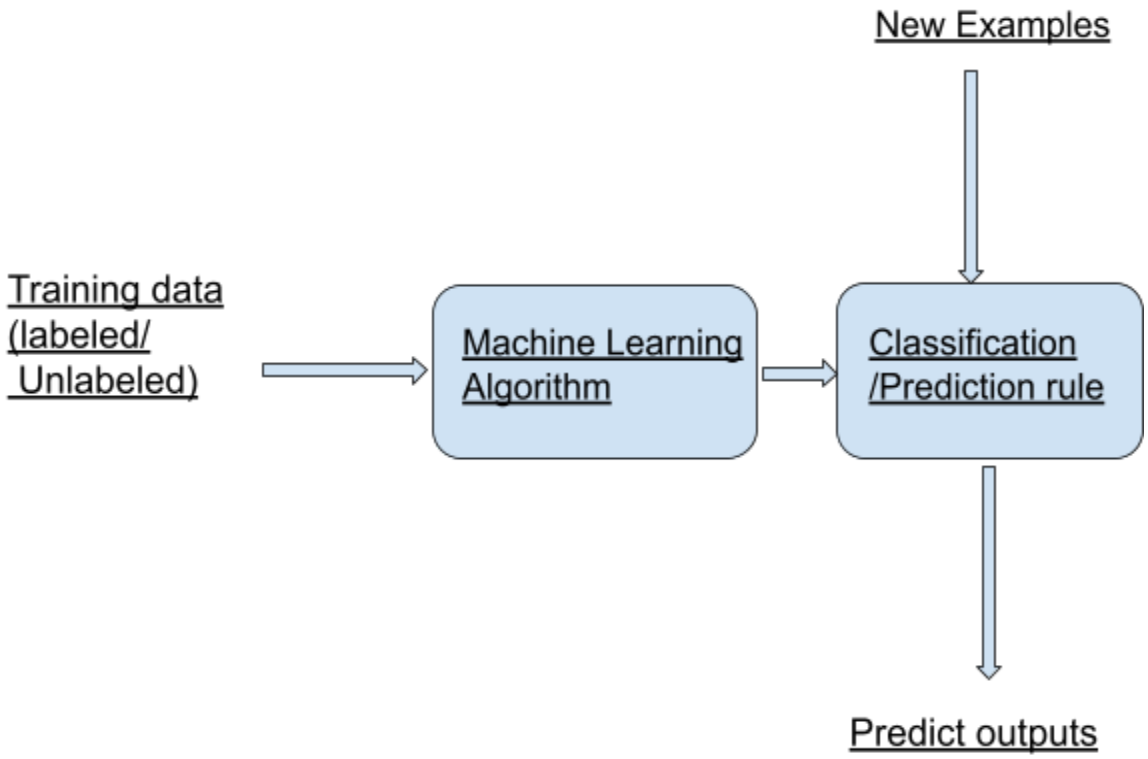
1.6.1 Definition

Computers as well as human beings possess a couple of differences, along with the most crucial found on the first ones' potential to gain from their previous experiences, while machinery systems require to become strictly assisted to the method of carrying out a task. Computer systems are actually makers completely adhering to the reasoning with absence of good sense. Simply put, the system should deliver them with specified, measure- by-step details on exactly what to perform, to do one task.

Our duty is actually to compose scripts as well as plan computer systems to follow those instructions. Below is where the place of ML is available in. Its own concept is actually concentrated on the tip of preparing machines that can learn from previous experiences and records, through using computational formulas and maths.

As a subfield of Artificial Intelligence (Artificial Intelligence), ML makes systems able to pick up from adventures- past data without being clearly configured. It focuses its own concentration on building such computer programs which can use records to learn on their own.

.



The 7 Steps of Machine Learning :-

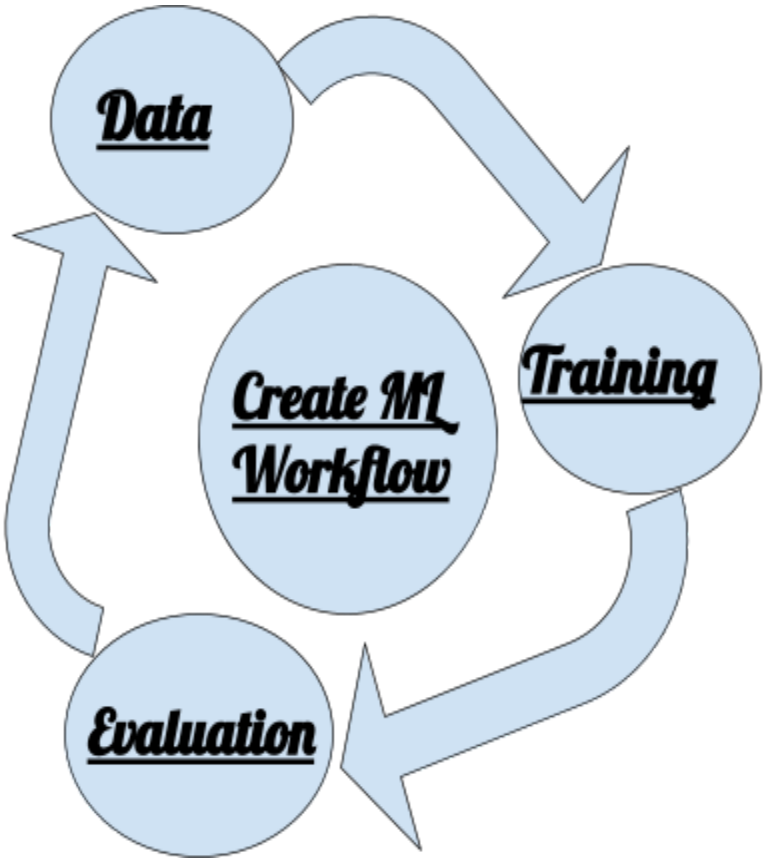
1.Data Collection:

In the Era of quick development of the relevant data ,industries generate data at an unexpected rate. That is actually exactly how the term Big data seems in our day to day lifestyle.
These data could be either numerical values like elevation tem, population or particular like different colors categories of songs. A few of them are identified for supervised learning or otherwise designated as unsupervised learning .

The 1st step of ML is composed of accumulating information that are essential for training the Machine learning model to deliver the precise forecasts Records compilation may be looked at as the procedure of acquiring info from various resources like sites establishments authorities's services etc.

Data collection could be considered as the process of gathering information from different sources, such as websites, institutions

2.Data Preparation:
data is cleaned from the duplicate samples and errors plus bias should be removed. we can visualize the errors and check for outliers and patterns.
3.Choose a Model:
The next step is to choose a model .
factor helpful for choosing a model
i.accuracy
ii.scalability
4.Train the Model.
Training is focused on improving the predictions of the model.Each training step consists of updating the weights and the biases.
The model is created based on labelled data samples – in supervised ML – and trying to leak inferences from not labelled data – in unsupervised ML.



4.1 Supervised Learning

A supervised ML algorithm takes labeled records for input as well as develops a result model which can easily forecast potential events with delivered brand new data. Such an algorithm can be either utilized for a category problem or even a regression issue. It begins examining a recognized training dataset and makes a function to generate forecasts concerning the output worths. Our model separates the input dataset into training and also testing sets.

4.2 Unsupervised Learning

This kind of mothod out manages non-labeled information, or even records that had certainly not been actually arranged into categories. It derives information regarding the attributes from the records and also when it finds new records, it utilizes the actually discovered functions to categorize the brand new samples into a group of market values, called class. The primary areas that unsupervised learning is used are concentration and dimensionality reduction. As for the initial one, a sample of one team will have very same properties to the various other records in its group, so regarding when it is actually contrasted with a sample of another group, they should have considerably various buildings. Component decline compresses the records by merely minimizing the dimension of the feature collection.

5.Evaluate the Model.

Evaluation is a process of testing our model on an unseen dataset and seeing how it performs.

To produce better results, the training and testing data should be also increased , for better results.

6.Parameter Tuning.

For better results we need to modify the weights at regular intervals, which will result in an increase in the count of training steps resulting in more specific results.

prior to getting into the training procedure we should fine-tune the criteria of the design and try out the different results, in order to get the optimal ones.

7.Make Predictions.

here we evaluate the design with best criteria, it is time for using predictions to respond to concerns concerning our dataset.

1.6.2 LEARNING MODELS IN MACHINE LEARNING

The following are the most common learning models used.

a. Logistic Regression

Logistic Regression (LR) is a supervised Machine Learning algorithm utilised in classification issues, and specifically for categorizing observations into a group of discrete classes. Although linear regression assigns observations to a continuous number of values, LR applies on its output a transformation - activation – function, called the logistic sigmoid function.

b. KNN

The K-Nearest Neighbour supervised machine learning algorithm that may be used to uncover regression related classification challenges in an easy and uncomplicated manner The KNN method relies on the premise that in a confined region there are comparable items In other words comparable objects are in close proximity to one another.
he KNN could be a supervised machine learning algorithmic rule helpful for resolution regression associated classification issues in a very easy and straightforward way The KNN algorithm is predicated on the belief that constant things exist in a closed area In different words similar things are on the brink of one another KNN is rely on the concept of similarity also called as the distance proximity or closeness which is used to solve the issue of finding the area between two points on a graph because the human brain has a model of neurons neural networks are created Neural networks are made up of layers of linked neurons or nodes each with its own activation function its thought is to present our network many inputs each input could be a single characteristic Then we have a propensity to move across the network by summing our inputs and assigning weights to them eventually victimization associate activation perform to get the following nodes This method is perennial Before adding a final activation function to produce the output layer our prediction this technique is repeated numerous times via the hidden layers.

c. Support Vector Machines

Support vector machines (SVMs) were designed in the work of the statistical learning theories .SVMs are supervised learning models that are utilised in classification and regression issues for data analysis and pattern identification. SVMs use the kernel trick dot product to change the input feature space into a higher-dimensional feature space, where (x, y) is substituted by k (x, y) = <f(x), f(y)> (f is known as kernel function).The sample distance of each dataset to a specific dividing hyperplane may be determined. The smallest distance between the samples and the hyperplane is referred to as margin. A hyperplane, or dividing curve between various classes, can be used to divide the altered data. The best hyperplane is one that maximises the margin.

d. RF

A decision tree is a graphical representation of data which applies a branching method to describe with illustrations any possible result of a decision. Each tree branch stands for a possible option that is available for taking a decision. The depth of the tree is extended as new decisions need to be made. So, the decision tree as a tree structure, has few components; internal nodes for a test on an attribute, the branches that represent a test result and leaf nodes (terminal nodes) that contain information for the class labels. The outcome of a test
- based on the node's attributes creates a new branch, and as we go from root to the next node and so on, we reach a leaf node that belongs to a unique label (class).

e. GRADIENT BOOSTING

Gradient boosting (GB) is a machine learning (ML) approach for classification and regression issues that tries to build a model for predictions out of a collection of inefficient prediction models known as decision trees. Every new tree is a fit on an updated version of the original data set during the boosting phase. To begin, the GB creates a decision tree and gives equal weight to each observation. We drop the weights for easy-to-classify data and raise the weights for hard-to-classify data after the first tree evaluation. Then, using this weighted data, we create the next tree in an attempt to enhance the previous tree's predictions. Our new model combines tree 1 and tree 2.The classification error from this combination of two-tree models is then computed, and a third model is created to forecast the corrected residuals. This method is repeated for a certain number of iterations. The subsequent trees assist us in classifying the observations that were not adequately classified by the previous trees. The final ensemble model's predictions are the weighted sum of the previous models' forecasts. The final ensemble model's predictions are the weighted sum of the preceding three models' forecasts.

2.LITERATURE SURVEY

2.1 REPORT 1

Title: Deep Transfer Learning for IoT Attack Detection
Name of conference : Vietnam National Foundation for Science and Technology Development, 102.05-2019.05
Purpose : solve the ‘‘lack of labelled information" problem for the training detection model in ubiquitous IoT devices

Methodology :
investigate how effective our proposed model is at transferring knowledge from the source domain to the target domain.

Dataset :Examine the efficacy of our suggested model in transferring information from the source to the target domain.

Results : showed that DTL techniques can improve the AUC score for IoT threat detection

2.2 REPORT 2

Title : Securing IoT Space via Hardware Trojan Detection

Author:
Shize Guo, Jian Wang , Member, IEEE, Zhe Chen, Yubai Li, and Zhonghai Lu , Senior Member, IEEE

Name of conference : IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 11, NOVEMBER 2020.

Purpose : Several Hardware Trojan detection approaches have been presented in the recent decade to reduce the potential hazards of Hardware Trojan assaults in the IC supply chain. They can be done at any time during the semiconductor design process, including runtime.

Dataset : . Datasets Gathering Exp. Returns Security.

Results :elucidate the efficacy of our approach In the Trust-hub benchmarks, it can identify Hardware Trojans that consume just 0.02 percent of the original design's power and accurately pinpoint Trojan sites.

2.3 REPORT 3

Title : Hardware Security in IoT Devices with Emphasis on Hardware Trojans

Name of conference : J. Sens. Actuator Netw. 2019

objectives :
Various data mining approaches were executed on the input data in order to determine

the optimum performance strategy.

Results : Finally, IoT devices will not be truly safe until they are built on a solid foundation of secure hardware. All of the effort and money spent to safeguard these devices might be for naught if they include a Hardware Trojan that may be activated at any time and destroy the entire device.

2.4 PEPORT 4

Title : Hardware Trojans in Chips: A Survey for Detection and Prevention.

Name of conference : Sensors 20, no. 18: 5165. https://doi.org/10.3390/s20185165

objectives :
On the input data, several data mining techniques are used to determine the optimal performance producing strategy.

Results : Hardware Trojan threats have drawn increased attention in academic and industrial research.The authors of this paper focused on the most up-to-date uses of machine learning-based methodologies in Hardware Trojan protection research. Potential difficulties and concerns facing present research are discovered by examining relevant achievements.

2.5 REPORT 5

Title : A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,

International Journal of Advanced Computer Science and Applications,

Name of conference : International Journal of Advanced Computer Science and

Applications,
Vol. 9, No. 3, 2018

ABOUT : presents a four-phase IoT attack model; primarily, it might be utilised to assist in the construction of a secure IoT-related system. Mitigation approaches might be integrated by application designers that want to build safe IoT systems.

Result :presents a four-phase IoT attack model; primarily, it might be utilised to assist in the construction of a secure IoT-related system. Mitigation approaches might be integrated by application designers that want to build safe IoT systems. The goal of this work is to present a complete categorization of IoT attacks based on a unique building-blocked reference model, as well as a set of recommendations.
2.6 REPORT 6

Title : A Multi-Layer Hardware Trojan Protection Framework for IoT Chips

Name of conference : National Natural Science Foundation of China under Grant 61672159, Grant 61872091, Grant U1804263, and Grant 61702105

Purpose : construct a hardware design with several layers The Trojan defence framework RG–Secure addresses the basic security threat provided by IoT devices.
Methodology :
offer RG–Secure, a quick and practical hardware Trojan protection system for third-party IP cores based on RTL and gate-level hardware Trojans.

.

3.PROPOSED WORK

In order to identify the Hardware Trojan Attacks, we proposed an Hardware Trojan detection and classification technique.
The main work is Model Builder for

- data collection
- data categorization/preprocessing
- model training
- feature selection.

For comparison we will use ML and Deep Learning algorithms.

Only used 5 models:-

- Support Vectors Machine(SVM)
- Gradient Boosting(GB)
- K-nearest neighbors (KNN)

- logistic regression (LR)
- random forest (RF))

From deep learning methods we used:-
- MLP
- CNN

For classification of IC’s.

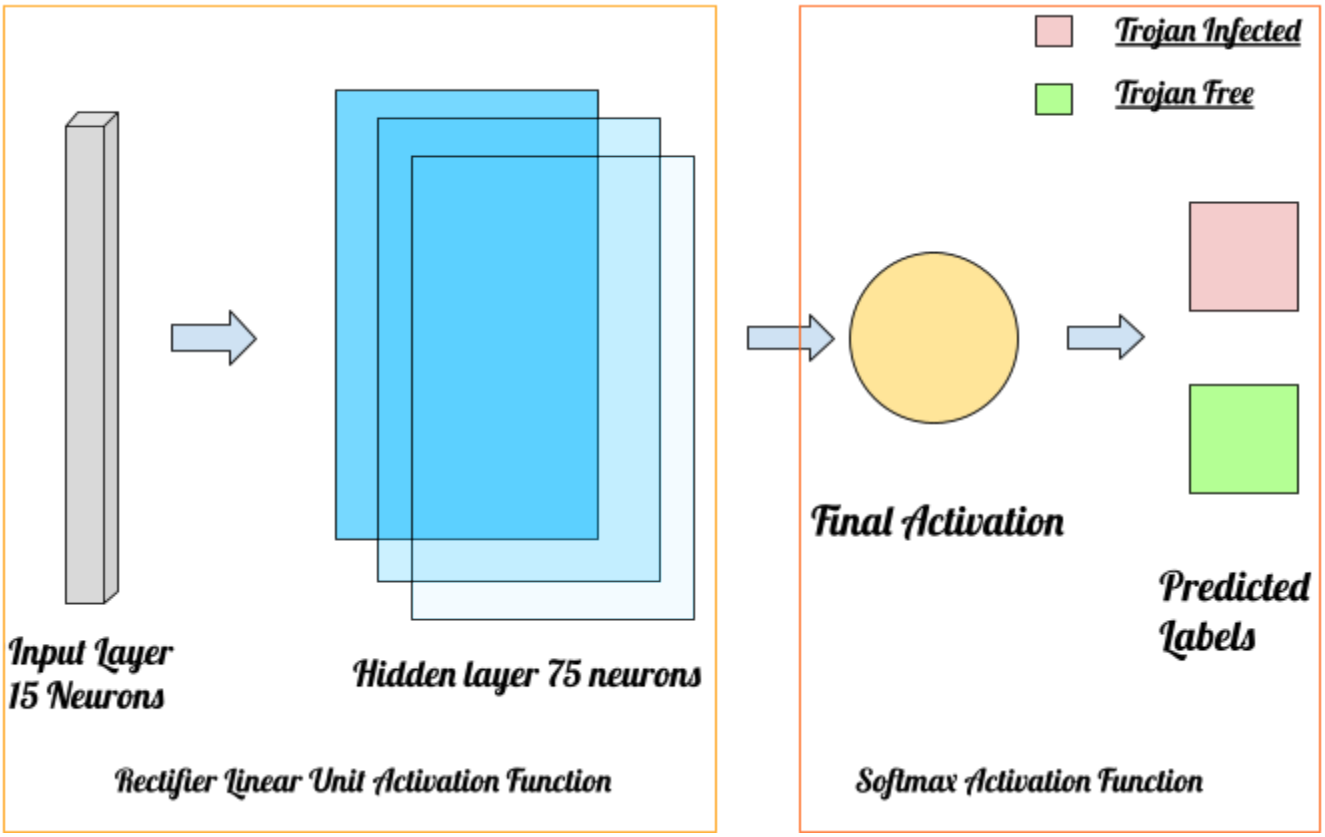
In “Model Training”, we will first create a model using the “Sequential” model class of keras.

An initial input layer is followed by three dense layers in the suggested model. Each layer's output becomes the input for the following layer.
To prevent the system from overheating, a dropout layer is introduced. The output of the dropout layer is given to a fully connected layer, which then feeds input to the dense layer with sigmoid function.

We need to configure the learning process before we can train the model, which we can accomplish with the ‘compile' function. Then, using our training data, we train our model to learn our weights.

Feature Selector module usually chooses the most relevant features for each kind of attack

CNN Architecture :-



4..METHODOLOGY

4.1 Tools used

- Scikit-learn.
- Numpy
- Scipy

4.2 Dataset Construction

Experiments were carried out on a dataset that was created by research benchmarks from Trust-Hub, a certified public library with Trojan free (TF) and Trojan Infected (TI) circuits. For the creation of our dataset we used all the circuits from Trust-Hub, approximately 1.000 circuits. Twenty-one (21) of them refers to TF circuits and all the other refers to TI circuits. The extraction process created the final dataset, consisting of 50 characteristics.

Dataset - link

4.3 Dataset Preprocessing and Feature Extraction

We eliminated several small discrepancies in the dataset, such as missing features, during the dataset cleaning process. It has 50 characteristics, after removing the ones that are strongly associated (at least 95% correlation) to make our method more cost and time efficient. It comprises the 24 characteristics listed below, as well as the feature with the targeted values.

Area	Power (1)	Power (2)	Power (3)
Number of ports	Net Switching Power	Cell Internal Power	Black_Box Total Power
Number of sequential cells	Cell Leakage Power	Memory Switching Power	Clock_Network Internal Power
Number of macros/black boxes	IO_Pad Internal Power	Memory Leakage Power	Clock_Network Switching Power
Number of references	IO_Pad Switching Power	Memory Total Power	Clock_Network Leakage Power
Macro/Black Box area	IO_Pad Leakage Power	Black_Box Internal Power	Sequential Internal Power
	IO_Pad Total Power	Black_Box Switching Power	Sequential Leakage Power
	Memory Internal Power	Black_Box Leakage Power	

There were only 21 out of 1.000 TF labeled instances, with a particular type of circuit. In order to balance the ratio between TF and infection, we used a reproduced technique in order to reproduce each TF multiple times, to match the total number of TI of the same circuit category. This type of technique is not optional, but recommended under unbalanced datasets. As for the features dropping step, when we examine the features of a dataset, some of them might not be useful to make the necessary prediction. So we are dropping the highly correlated features in order to make our algorithm more cost
and time efficient.
Chip-level Trojan Benchmarks link -
https://www.trust-hub.org/#/benchmarks/chip-level-trojan
Downloadable dataset link - https://caslab.e-ce.uth.gr/benchmark/

5.Algorithms used

5.1 MLP(Deep Learning Model)
probability distribution :-

- 0 => Trojan- free,
- 1 => for Trojan-infected

We used a softmax activation function.
The sigmoid function only works with two classes, which isn't what we're looking for. The softmax function, like a sigmoid function, squashes the outputs of each unit to be between 0 and 1. It does, however, split each result so that the entire sum of the outputs equals one.

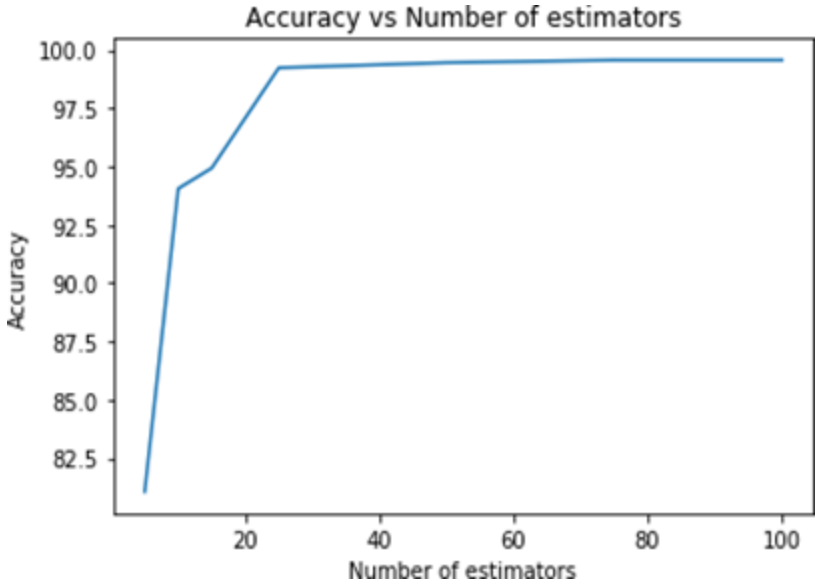
5.2 SVM
A radial basis function (RBF) kernel is employed to train the SVM in our scenario since it is essential to solve this nonlinear problem.
Large value of parameter C should cause a small margin, and the opposite. Small value of parameter C should cause a large margin. There is no rule to choose a C value, it totally depends on our testing data. The only way is to try different values of the parameters and go with those that give the highest classification accuracy on the testing phase. As for the gamma parameter, if its value is low then even the far away points can be taken into consideration when drawing the decision boundary and the opposite. With a high gamma parameter, the hyperplane is dependent on the very close points and ignores the ones that are far away from it. So, parameters are 10 for the C value, and 1 for the gamma value.

5.3 RF

After experimenting with various different factors, we settled on 5 estimators: the number of trees in the forest and 5 as the depth of the tree. The algorithm gave us a high-accuracy answer in a short amount of time, 99.01 percent in 0.01 seconds. In general, we thought the algorithm gave us the greatest results in terms of how easy it was to build and how quickly it could be executed.

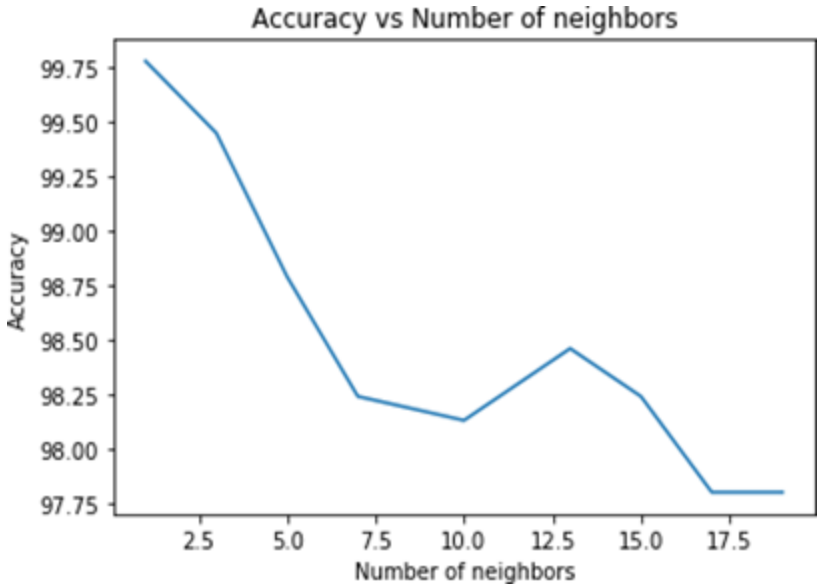
5.4 GB

We changed the values 01 and 75 with least time to execute after testing the rate of learning and estimating the number of boosting stages to perform – respectively and the model was trained at 99% accuracy.



5.5 KNN

In our problem, we choose 3 as the number of neighbors, despite the fact that we achieve the highest accuracy with 1, since we have better execution time.



5.6 LR

In our dataset, we use binary LR since we have 2 discrete classes for our predicted labels. We use Sklearn's 'Logisti- cRegression' classifier class, 'liblinear' solver since we have a small dataset and 'or' since the data is binary. In order for the method to converge we choose 300 as the max iterations number.

6. IMPLEMENTATION

Deep learning Model -

We have created the model stance using the Sequential class of Keras_model = Sequential()

```
model.add(Dense(15,input_dim=train_x.shape[1], activation='relu'))
model.add(Dense(75, activation='relu'))
model.add(Dense(num_classes, activation='softmax'))
model.compile(optimizer='adam', loss='categorical_crossentropy',metrics=['mse',
'accuracy'])
```

SVM -

We have used the SVC function of sklearn with a radial basis function (RBF) kernel with C value as 10 and gamma value as 1.

classifier = SVC(kernel="rbf", C=10, gamma=1)

LR -

We have imported and used the LogisticRegressionfunction of the sklearn library.

LogisticRegression(random_state=0, solver='liblinear', max_iter=300,multi_class='ovr')

GB -

We have imported and used the GradientBoostingClassifier function of the sklearn library.

GradientBoostingClassifier(learning_rate=0.1, n_estimators=75)

KNN -

We have imported and used the KNeighboursClassifier function of the sklearn library.

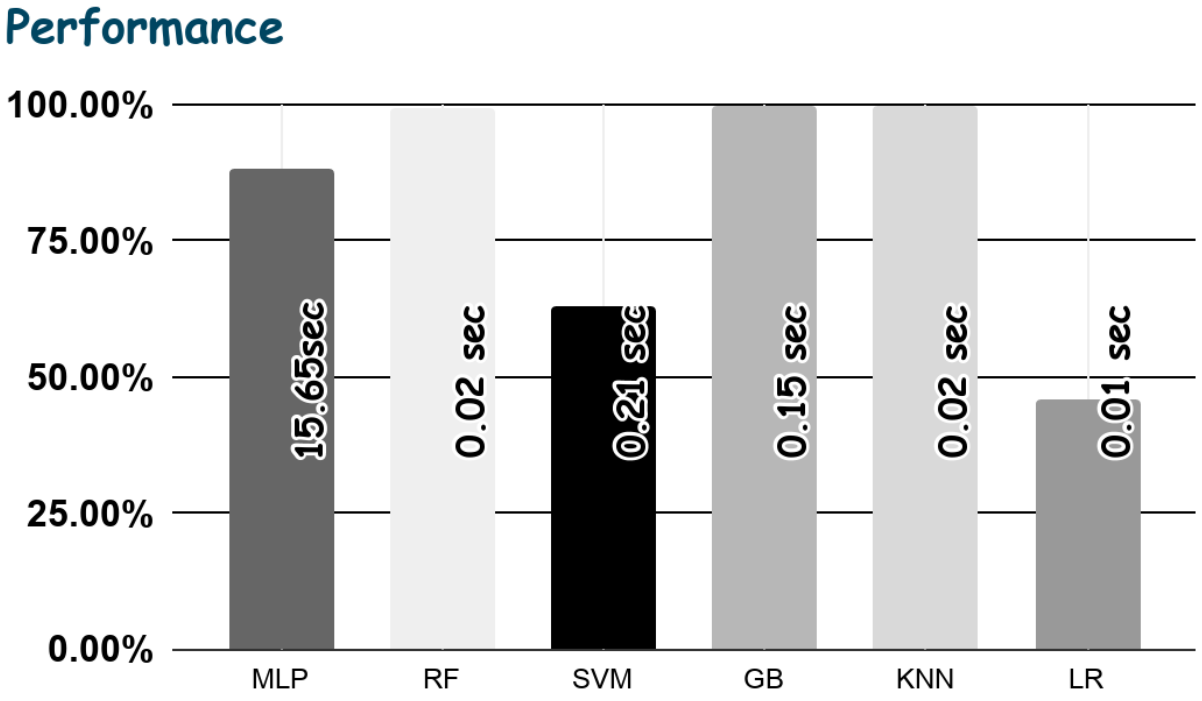
KNeighborsClassifier(n_neighbors=3)

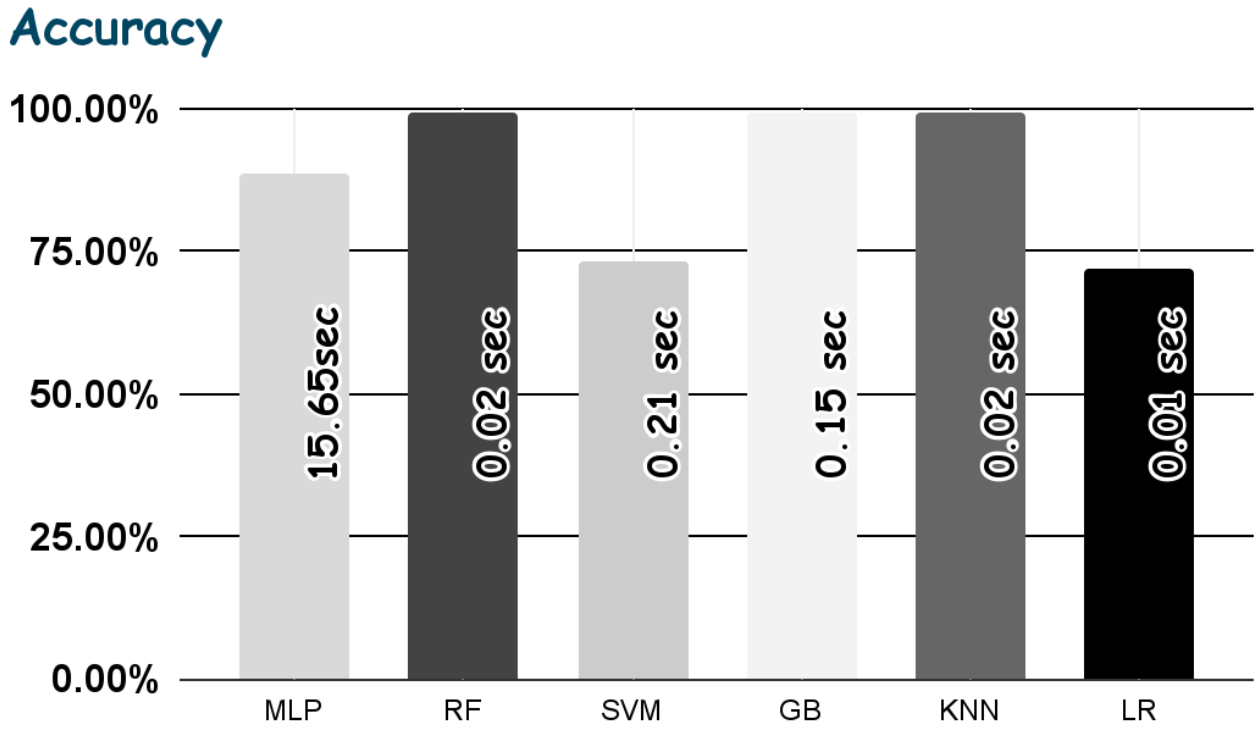
RF -

We have used the RandomForestClassifier function of the sklearn library.

RandomForestClassifier(n_estimators=5, max_depth=5, random_state=1)

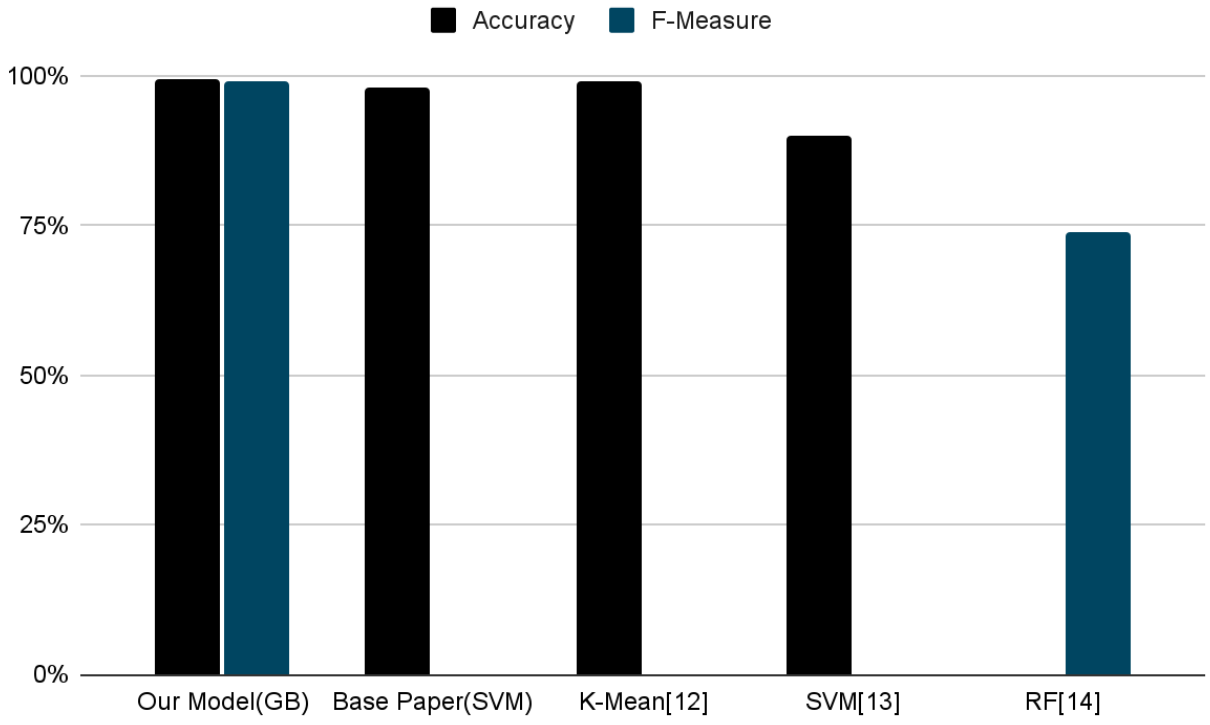
7. RESULTS


Performance
100.00%
75.00%
50.00%
25.00%
0.00%
15.65sec
0.02 sec
0.21 sec
0.15 sec
0.02 sec
0.01 sec
MLP
RF
SVM
GB
KNN
LR


Accuracy
100.00%
75.00%
50.00%
25.00%
0.00%
15.65sec
0.02 sec
0.21 sec
0.15 sec
0.02 sec
0.01 sec
MLP
RF
SVM
GB
KNN
LR

Algorithm	Accuracy	Execution Time	F-measure
MLP	89.54 %	15.65sec	88.28%
RF	99.29 %	0.02 sec	99.15%
SVM	77.31 %	0.21 sec	63.11%
GB	99.56 %	0.15 sec	99.94%
KNN	99.45 %	0.02 sec	99.61%
LR	71.81 %	0.01 sec	45.86%

. COMPARATIVE STUDY (WITH PREVIOUS PAPERS)



Results by	Algorithm	Accuracy	F -Measure
Our Model	GB	99.7%	99.54%
BasePaper[11]	SVM	98%	-
Author [12]	K-Mean	99.4%	-
author [13]	SVM	80 - 100%	-
author [14]	RF	-	74.6%

8. CONCLUSION

Every year, the development speed and complexity of Hardware Trojan grow at an alarming rate. The introduction of very complex strategies for the design of Hardware Trojan continues to infect a wide range of integrated circuits,from basic circuits utilised in most of our daily activities to the most cutting-edge circuits used for military, industrial, and financial applications, even sensitive areas for state-funded research. Hardware Trojans are stealth in nature,Hardware Trojans have various types of formations, and types, and Hardware Trojan attacks cause millions of dollars in damages to global economic and technology companies every year. If not restricted, these intrusion attempts will turn into the biggest obstacle to future technological progress, seriously affecting all aspects of our daily lives. With increasing uncertainties related to the design and manufacturing of safety integrated circuits, there is a natural need for efficient, versatile, and scalable countermeasures.

In order to identify Hardware Trojan, this article proposes a technology for Hardware Trojan detection and classification of the GLN phase of the ASIC circuit through area and power characteristics. First, we use Design Compiler NXT software to design, and all circuits are from the Trust-HUB library. After that, we developed and compared seven ML models, namely MLP, RF, SVM, GB, KNN, LR, and XGB. The GB model we selected yielded the highest precision and the metric F, which was 100%. Finally, we compare our model with existing models from journal and conference research. Our model produced the highest results, with an average accuracy of 99.7 and an F value of 99.5.

9. ACTIVITY SCHEDULE

Steps	Time Required	Predicted Date & Time
Requirement Verify	Done	15th February 2021
Project Planning	Done	28th February 2021
System & Detail Design	Done	20th March 2021
Coding	Done	25th March 2021

Debugging and coding	Done	15th April 2021
Testing	Done	29th April 2021
Documentation and Final	Done	20th May 2021

10. REFERENCES

[1].L. Vu, Q. U. Nguyen, D.
N. Nguyen, D. T. Hoang and E. Dutkiewicz, "Deep Transfer Learning for IoT Attack Detection," in IEEE Access, vol. 8, pp. 107335-107344, 2020, doi: 10.1109/ACCESS.2020.3000476

[2]S. Bhunia et al., “Protection against hardware trojan attacks: Towards a comprehensive solution,” IEEE Des. Test, 2013, doi: 10.1109/MDT.2012.2196252.

[3]Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,Internet of Things,Volume 7,2019,100059,
ISSN 2542-6605.

[4].S. Guo, J. Wang, Z. Chen, Y. Li and Z. Lu, "Securing IoT Space via Hardware Trojan Detection," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11115-11122, Nov. 2020, doi: 10.1109/JIOT.2020.2994627

[5].M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0452-0457, doi: 10.1109/CCWC.2019.8666588

[6].Sidhu, Simranjeet; Mohd, Bassam J.; Hayajneh, Thaier. 2019. "Hardware Security in IoT Devices with Emphasis on Hardware Trojans" J. Sens. Actuator Netw. 8, no. 3: 42. https://doi.org/10.3390/jsan8030042

[7].Dong, Chen; Xu, Yi; Liu, Ximeng; Zhang, Fan; He, Guorong; Chen, Yuzhong. 2020. "Hardware Trojans in Chips: A Survey for Detection and Prevention" Sensors 20, no.

18: 5165. https://doi.org/10.3390/s20185165

[8].A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,
International Journal of Advanced Computer Science and Applications,
Vol. 9, No. 3, 2018.

[9].C. Dong, G. He, X. Liu, Y. Yang and W. Guo, "A Multi-Layer Hardware Trojan Protection Framework for IoT Chips," in IEEE Access, vol. 7, pp. 23628-23639, 2019, doi: 10.1109/ACCESS.2019.2896479.

[10]M. Hossin , M. Sulaiman , A review on evaluation metrics for data classification evaluations, Int. J. Data Mining Knowl. Manag. Process 5 (2) (2015) .

[11].M. Xue, J. Wang, and A. Hux, “An enhanced classification-based golden chips-free hardware Trojan detection technique,” in Proceedings of the 2016 IEEE Asian Hardware Oriented Security and Trust Symposium, AsianHOST 2016, 2017, doi: 10.1109/AsianHOST.2016.7835553.

[12].H. Salmani, “COTD: Reference-Free Hardware Trojan Detection and Recovery Based on Controllability and Observability in Gate-Level Netlist,” IEEE Trans. Inf. Forensics Secur., 2017, doi: 10.1109/TIFS.2016.2613842.

[13].K. Hasegawa, M. Oya, M. Yanagisawa, and N. Togawa, “Hardware Trojans classification for gate-level netlists based on machine learning,” in 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design, IOLTS 2016, 2016, doi: 10.1109/IOLTS.2016.7604700.
[14].K. Hasegawa, M. Yanagisawa, and N. Togawa, “Trojan-feature extraction at gate-level netlists and its application to hardware-Trojan detection using random forest classifier,” in Proceedings - IEEE International Symposium on Circuits and Systems, 2017, doi: 10.1109/ISCAS.2017.8050827.

[15]. Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. Davis Guarnizo, and Y. Elovici, ‘‘Detection of unauthorized IoT devices using machine learning techniques,’’ 2017, arXiv:1709.04647.

[16].I. Ahmed, A. P. Saleel, B. Beheshti, Z. A. Khan, and I. Ahmad, ‘‘SecDeep Transfer Learning for IoT Attack Detection - IEEE Xplore Purity in the Internet of Things (IoT),’’ in Proc. 4th HCT Inf. Technol. Trends (ITT), Oct. 2017, pp. 84–90.

[17].A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, ‘‘From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3369–3388, Jul. 2018.

[18].S. García, A. Zunino, and M. Campo, ‘‘Botnet behavior detection using network synchronism,’’ in Privacy, Intrusion Detection and Response: Technologies for Protecting Networks. Hershey, PA, USA: IGI Global, 2012, pp. 122–144

[19].R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions", Proc. IEEE Int. High Level Design Validation Test Workshop, pp. 166-171, 2009.

[20].M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection", IEEE Design Test Comput., vol. 27, no. 1, pp. 10-25, Jan.–Feb. 2010.