A Cloud Based Framework for Identification of IoT Devices at Smart Home Using Supervised Machine Intelligence Model

Sourav Kumar Bhoi [1*]& Krishna Prasad K. [2]

[1] Post-Doctoral Fellow, Institute of Computer Science and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India,
Orcid ID: 0000-0002-5173-3453; E-mail: skbhoi300@gmail.com

[2] Associate Professor, Institute of Computer Science and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India,
Orcid ID: 0000-0001-5282-9038; E-mail: krishnaprasadkcci@srinivasuniversity.edu.in

Subject Area: Computer Science.
Type of the Paper: Conceptual Research.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.7053965
Google Scholar Citation: IJAEML

How to Cite this Paper:
Bhoi, Sourav Kumar, & Krishna Prasad, K., (2022). A Cloud Based Framework for Identification of IoT Devices at Smart Home Using Supervised Machine Intelligence Model. *International Journal of Applied Engineering and Management Letters (IJAEML), 6*(2), 104-116. DOI: https://doi.org/10.5281/zenodo.7053965

International Journal of Applied Engineering and Management Letters (IJAEML)
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJAEML.2581.7000.0148

Received on: 14/07/2022
Published on: 31/08/2022

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Cloud Based Framework for Identification of IoT Devices at Smart Home Using Supervised Machine Intelligence Model

Sourav Kumar Bhoi [1]*& Krishna Prasad K. [2]

[1] Post-Doctoral Fellow, Institute of Computer Science and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India,
Orcid ID: 0000-0002-5173-3453; E-mail: skbhoi300@gmail.com

[2] Associate Professor, Institute of Computer Science and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India,
Orcid ID: 0000-0001-5282-9038; E-mail: krishnaprasadkcci@srinivasuniversity.edu.in

ABSTRACT

Purpose: *Identification of Internet of Thing (IoT) devices in smart home is the most important function for a local server/controller to administer and control the home smoothly. The IoT devices continuously send and receive requests, acknowledgments, packets, etc. for efficient data communication and these communication patterns need to be classified.*

Design/Methodology/Approach: *Therefore, to run the smart home smoothly, in this work a framework using cloud computing is proposed to identify the correct IoT device communicating with the local server based on supervised machine learning. The best supervised machine intelligence model will be installed at the local server to classify the devices on the basis of data communication patterns.*

Findings/Result: *Simulation is performed using Orange 3.26 data analytics tool by considering an IoT devices data communication dataset collected from Kaggle data repository. From the simulation results it is observed that Random Forest (RF) shows better performance than existing supervised machine learning models in terms of classification accuracy (CA) to classify the IoT devices with high accuracy.*

Originality/Value: *A cloud based framework is proposed for a smart home to identify the correct IoT device communicating with the local server based on supervised machine learning. Based on the data communication pattern of the IoT devices, an IoT device is accurately identified.*

Paper Type: *Methodology Paper*.

Keywords: IoT, Smart Home, Device Identification, Supervised Machine Learning, CA

1. INTRODUCTION :

IoT is currently a widely accepted technology in the field of wireless/wired communication, where any smart device/hardware can be connected in the world to perform a set of tasks to provide a better service to the requested user [1, 2]. IoT network mainly depends on the standard communication protocols [3] AMQT (advanced message queuing protocol), Bluetooth, cellular, MQTT, Wi-Fi, Zigbee, Z-Wave, CAP (constrained application protocol), DDS (data distribution service), EMPP (extensible messaging and presence protocol), LoRa, LoRaWAN, etc. IoT also mainly focuses on OSI seven layers architecture, however, it can be expressed in multilayer such as three layers, four layers, and five layers architecture [3].

IoT has wide applications [1,2], they are used in smart homes, smart city, self-driving cars, farming, agriculture, IoT retail shops, wearables, smart grid, industrial IoT, smart supply chain management, waste management, pollution monitoring, traffic management, telehealth, smart health, healthcare technology, disaster management, robotics technology, defence, education, etc. IoT makes life of people easier and smooth. Nowadays, IoT uses many new methodologies, techniques, protocols, models, systems, architecture, etc. to reduce the burden on the device itself by offloading the tasks and processing it in other devices such as cloud or fog or local server. Also, to solve new types of problems and provide error free services in less time, IoT is now using the AI (artificial intelligence) which mainly uses machine learning models or deep learning models to deal with the relevant problems or services. One such type of problem in IoT is device identification, where the devices connected to the main controller or local server need to correctly identify or classify the IoT device else the performance of the system reduces. For correctly identifying or classifying the IoT devices machine learning will be a good solution to this type of problem. So, in this work, we have designed a framework by considering a smart home case where the devices connected to a local server should be identified correctly with higher accuracy. For the classification of devices, we have installed the best supervised machine learning model at the local server for doing all identification activities.

The main contributions are discussed as follows:

(1) In this paper, a framework is proposed using cloud computing for a smart home to identify the correct IoT device communicating with the local server based on supervised machine intelligence model.

(2) The best supervised machine intelligence model is installed at the local server to identify the devices based on the data communication patterns.

(3) Simulation is performed using python based Orange 3.26 tool by considering the IoT devices data communication dataset from Kaggle [4] to select the best model and classify the IoT devices with high CA.

(4) Results show that RF performs better than kNN, NN, SVM, Tree, NB, AB, and LR in terms of CA.

The rest of the work is presented as follows. Section 2 presents the related work. Section 3 and section 4 presents the research gap and research agenda respectively. Section 5 presents the objective of the work. Section 6 and Section 7 presents the methodology and results respectively. Section 8 presents the conclusion section. Section 9 presents the recommendation.

2. RELATED WORKS :

Many research works are conducted in this area to identify devices or sensors using machine intelligence models. Some research papers are discussed as follows. Cvitic et al. [5] proposed an ensemble learning based method to identify the IoT devices in smart home. Meidan et al. [6] detects sensors or devices using machine intelligence model by network traffic analysis. Meidan et al. [7] detected IoT devices performing unauthorized access in the system using machine intelligence models. Makkar et al. [8] detected spam for IoT devices using a machine learning approach. Liu et al. [9] surveyed on the identification of IoT devices using machine learning. Salman et al. [10] proposed an abnormal traffic detection framework using a machine learning approach. Alrashdi et al. [11] proposed a method to detect anomalies IoT based smart city application using the machine intelligence. Hasan et al. [12] detected anomalies and attacks in IoT sensors in IoT sites using a machine intelligence. Choi et al. [13] identified faulty IoT devices in a smart home using context extraction. Table 1 shows some related research works in this IoT device identification using machine learning.

Table 1: Review of articles related to IoT device identification Source: [5-13]

S. No.	Field of Research	Focus	Outcome	Reference
1	Smart Home Based IoT Device Identification	The authors proposed an ensemble learning based method to identify smart home based IoT devices.	The smart home based devices are detected well.	Cvitic et al. (2021) [5]
2	IoT Device Identification	The authors detected IoT devices based on machine learning by analyzing traffic in the network.	IoT device are able to be detected.	Meidan et al. (2017) [6]
3	IoT Device Identification for Unauthorized Access	The authors detected devices performing unauthorized access using a machine learning based approach.	The devices performing unauthorized access are detected.	Meidan et al. (2017) [7]
4	Spam Detection	The authors detected spam for IoT devices using a	The spam is detected well in	Makkar et al. (2020) [8]

		machine learning approach.	IoT.	
5	IoT Device Identification	The authors surveyed on the identification of IoT devices using machine learning.	Survey has been done well on identification of IoT devices.	Liu et al. (2021) [9]
6	Abnormal Traffic Detection	The authors proposed an abnormal traffic detection framework using a machine learning approach.	The abnormal traffic is detected.	Salman et al. (2022) [10]
7	Anomaly Detection in IoT Based Smart City.	The authors proposed a model to detect the anomaly in IoT based smart city.	The anomaly is detected in IoT based smart city.	Alrashdi et al. (2019) [11]
8	Anomaly Detection in IoT	The authors proposed a method to detect the anomaly and attack in IoT sites.	Anomaly and attack in IoT sites are detected well.	Hasan et al. (2019) [12]
9	Faulty IoT Devices Identification	The authors identified faulty IoT devices in smart home using context extraction.	Faulty IoT devices in smart home are identified.	Choi et al. (2018) [13]

3. RESEARCH GAP :

From the above study, many research papers focus on the identification of malicious, abnormal, and faulty IoT devices only, as per our knowledge no such work is done above in individually categorizing an IoT device connected to the network. So, in this paper, a cloud based framework is proposed that identifies the IoT device category as a security camera, TV, watch, etc. using a supervised machine learning approach.

4. RESEARCH AGENDA :

The main agenda of research is based on design of a framework for categorizing the individual IoT devices using machine learning approach that is connected to a network. The research agenda is presented as follows. Section 5 defines the objective of the work. Section 6 presents the methodology of the whole work. The simulation and result of the work is presented in section 7. The conclusion of the whole work is presented in section 8. The recommendation of the work is presented in section 9. Then at last the references related to the work is presented.

5. OBJECTIVES :

The objectives of this work are presented as follows:
(1) To design a cloud based framework for a smart home to identify the correct IoT device communicating with the local server based on a supervised machine intelligence model.
(2) To select the best supervised machine intelligent model for the local server for IoT device recognition more accurately.
(3) To simulate the machine intelligence part using python based Orange 3.26 data analytics tool using an IoT device communication dataset for measuring the performance of the models based on CA.

6. METHODOLOGY :

The methodology mainly describes the system architecture framework and process flow of the whole functions that are run for smooth execution of the processes. The system architecture mainly consists of two-layer such as the device layer and the cloud layer. The device layer consists of a smart home that consists of many types of IoT devices that are connected to a local server using wireless/wired links. The local server can identify the IoT devices by the data communication patterns using the machine intelligence model. The local server is connected to a cloud API, where the smart home administrator is also connected through this cloud API. Here, the cloud layer consists of a cloud device that stores the current identities of the IoT devices. This is updated from time to time when some new data communication pattern is generated. The smart home administrator can access the results of device identification through the cloud API. The system architecture framework is shown in Fig. 1 as follows.

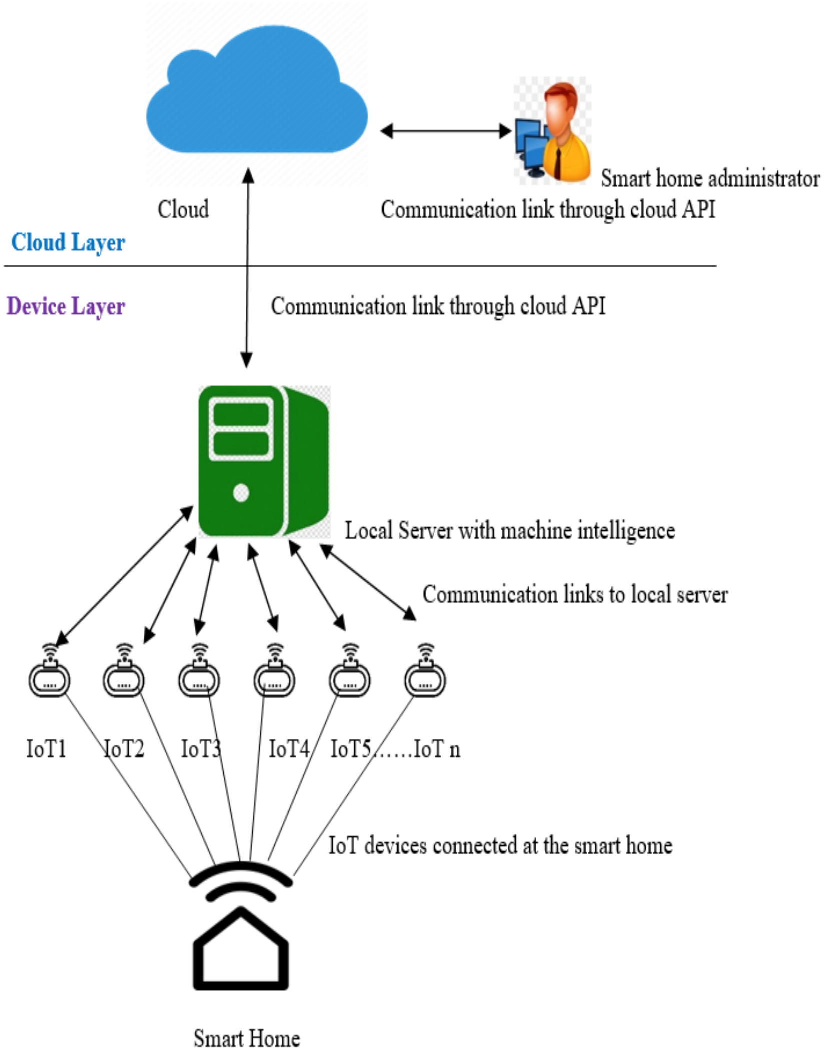

Smart home administrator
Cloud
Communication link through cloud API
Cloud Layer
Device Layer
Communication link through cloud API
Local Server with machine intelligence
Communication links to local server
IoT1
IoT2
IoT3
IoT4
IoT5……IoT n
IoT devices connected at the smart home
Smart Home

Fig. 1: System architecture framework.

Source: Author

The process flow of the proposed framework is discussed in Fig. 2 as follows. The process starts with a connection of IoT devices at the smart home with a local server using Internet. Before that, the best machine intelligence model is selected for the local server to identify the correct devices. For this, the standard/ previous communication history is fed as input to the supervised machine intelligence models at the local server for classifying the devices. The model which has the highest accuracy is selected as the model which will be installed at the local server for identifying the new devices as per the new communication pattern generated. Then the device information is updated by the local server to the cloud using the cloud API. This information is also accessed by the smart home administrator using the same cloud API. Algorithm 1 shows the step-by-step process of the proposed framework.

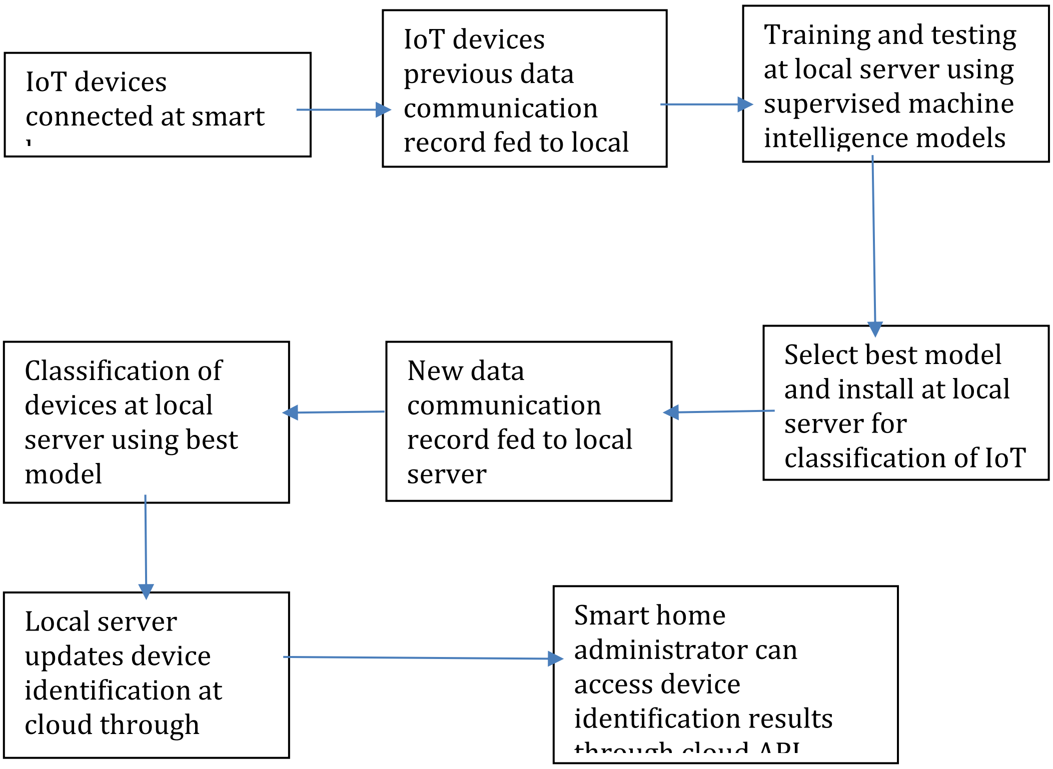

IoT devices connected at smart
IoT devices previous data communication record fed to local
Training and testing at local server using supervised machine intelligence models
Select best model and install at local server for classification of IoT
New data communication record fed to local server
Classification of devices at local server using best model
Local server updates device identification at cloud through
Smart home administrator can access device identification results through cloud API

Fig. 2: Process flow diagram for the proposed framework. Source: Author

Algorithm 1: Device identification in smart home cloud infrastructure
Input: Training and Testing Dataset
Output: Device Identity

(1) Connect devices at smart home to local server
(2) Training and testing at the local server using supervised machine learning models
(3) Best Model = maximum(CA1, CA2, CA3,…,CAn) //classification accuracies of n different models
(4) New dataset is fed into the best model for device identification
(5) Device identification information updated at cloud using cloud API
(6) Smart home administrator can access the device identification result using cloud API
(7) Steps 4-7 continue with new data generated

7. RESULTS :

The simulation is performed in Orange data analytics tool [14] on a machine of 8GB RAM and a Core-i3 processor. The supervised models considered for this simulation are RF, kNN, NN, SVM, Tree, NB, AB, and LR [15-30] for the selection of the best model using the performance metrics like AUC, CA, F1, precision and recall. The performance metrics can also be referred from [15-30]. However, we mainly focus on the CA of the models for selecting the best model for the proposed system to classify the device category.

The dataset considered for this is collected from Kaggle data repository [4]. The dataset has 8 categories of IoT devices and there are 1000 communication instances or rows and there are 298 communication attributes or columns such as ack_A, bytes, http_GET, duration, etc. The 8 categories of IoT devices as per communication instances are security camera, TV, smoke_detector, thermostat, etc. Each category has 100 instances in the dataset.

The simulation is set as per Fig. 3 where supervised machine learning models are taken with the dataset file is given for training and testing. Here the sampling used for training and testing is k-fold, where k is set to 10. Then the results can be found using the test and score as represented in Fig. 3. The results are shown in Table 2.

From Table 2, it is observed that RF show better performance than other models with a classification accuracy of 83.30%. Therefore, it will be better if we prefer RF as the model for installing the local server for classifying the IoT devices with higher accuracy. Other performance metric results are also shown in Table 2 like AUC, F1, precision and recall, however, we mainly focus on CA. The confusion matrix of all 8 models is represented in Fig. 4 - Fig. 11. From this confusion matrix from diagonal elements, it can be observed how many actuals are correctly predicted. Fig. 12 shows the comparison of different supervised machine intelligence models in terms of AUC, CA, precision, recall, and F1.

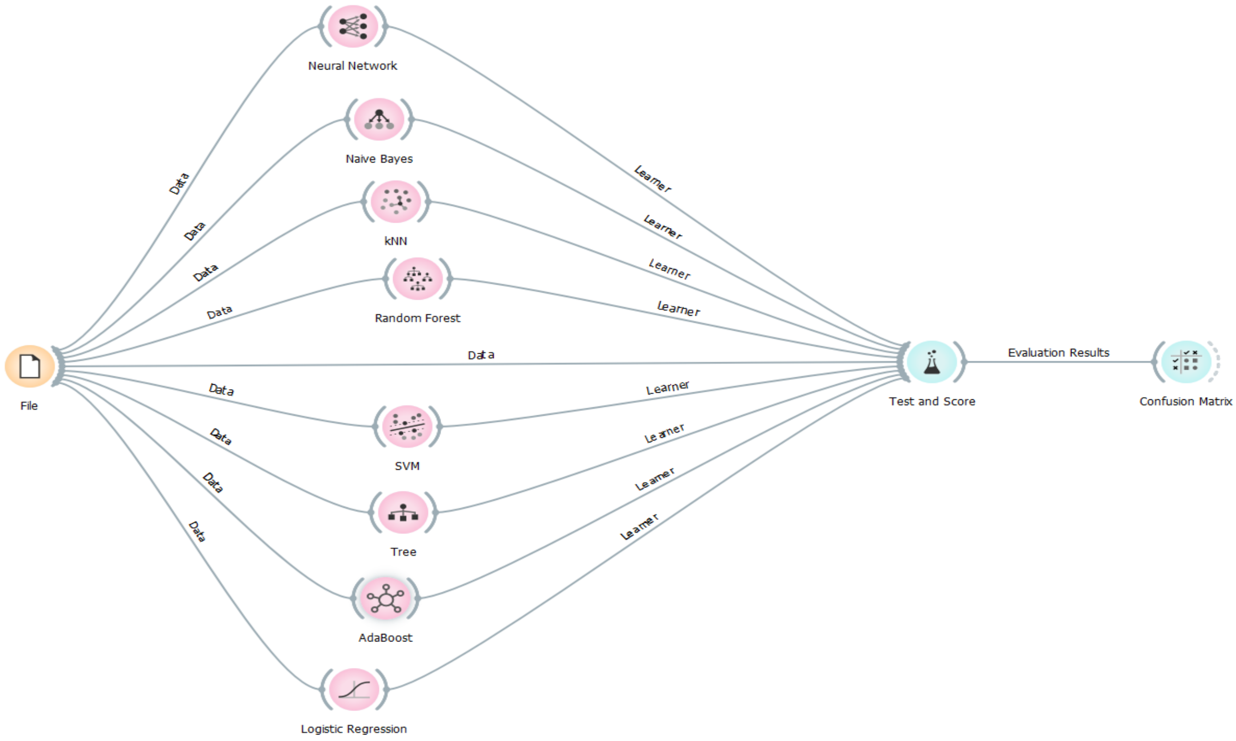
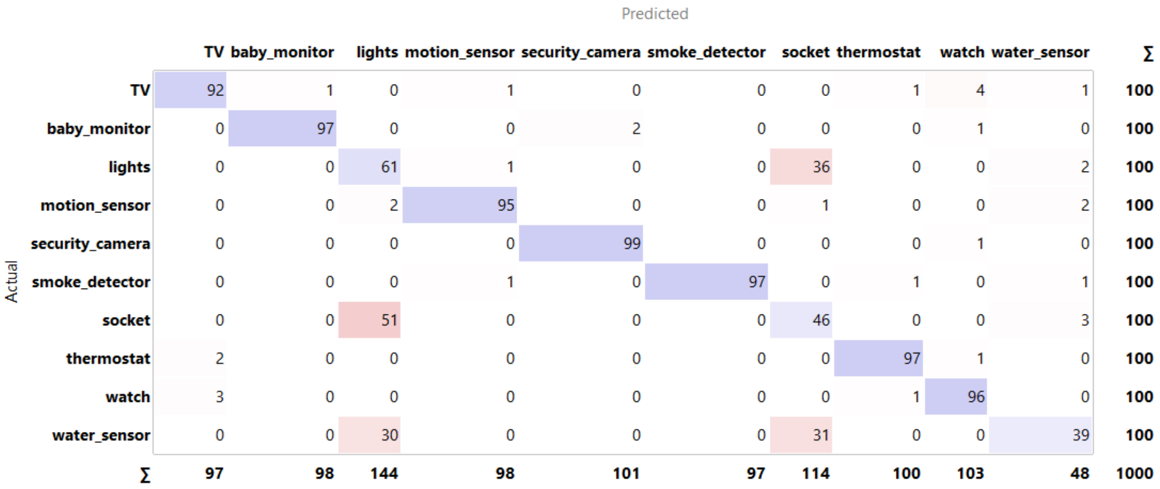


Fig. 3: Orange workflow set for training and testing.

Source: Author

Table 2: Comparison of performance metrics for different supervised machine intelligence models. Source: Author

Models	AUC	CA	F1	Precision	Recall
kNN	0.945	0.767	0.767	0.774	0.767
Tree	0.913	0.813	0.814	0.815	0.813
SVM	0.970	0.786	0.770	0.844	0.786
RF	0.974	**0.833**	0.834	0.836	0.833
NN	0.972	0.819	0.822	0.843	0.819
NB	0.961	0.743	0.731	0.762	0.743
LR	0.660	0.206	0.150	0.185	0.206
AB	0.891	0.804	0.805	0.807	0.804

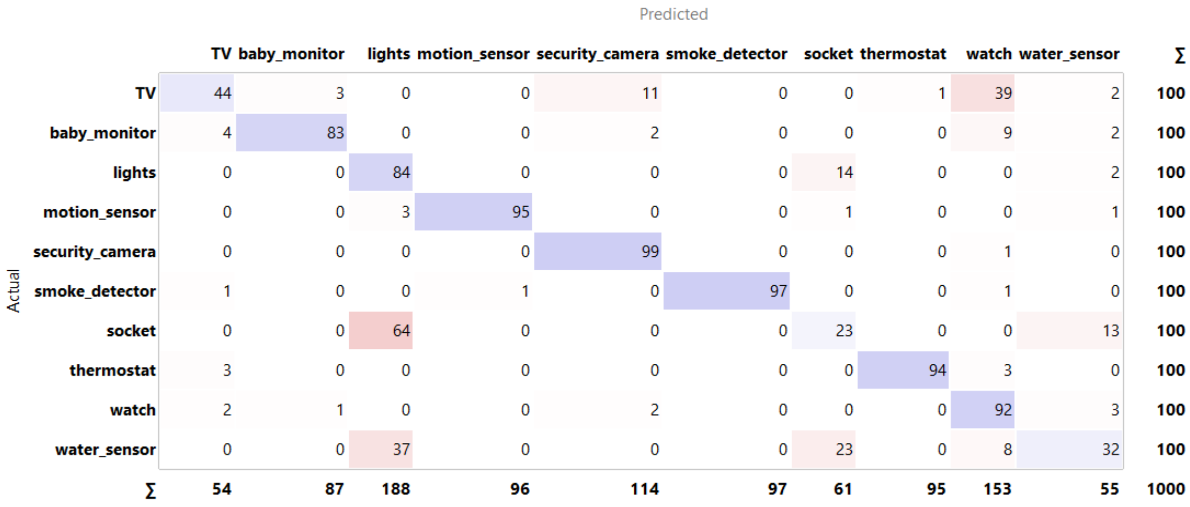


Predicted

Actual	TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	Σ
TV	92	1	0	1	0	0	0	1	4	1	100
baby_monitor	0	97	0	0	2	0	0	0	1	0	100
lights	0	0	61	1	0	0	36	0	0	2	100
motion_sensor	0	0	2	95	0	0	1	0	0	2	100
security_camera	0	0	0	0	99	0	0	0	1	0	100
smoke_detector	0	0	0	1	0	97	0	1	0	1	100
socket	0	0	51	0	0	0	46	0	0	3	100
thermostat	2	0	0	0	0	0	0	97	1	0	100
watch	3	0	0	0	0	0	0	1	96	0	100
water_sensor	0	0	30	0	0	0	31	0	0	39	100
Σ	97	98	144	98	101	97	114	100	103	48	1000

Fig. 4: Confusion matrix of NN.

Source: Author

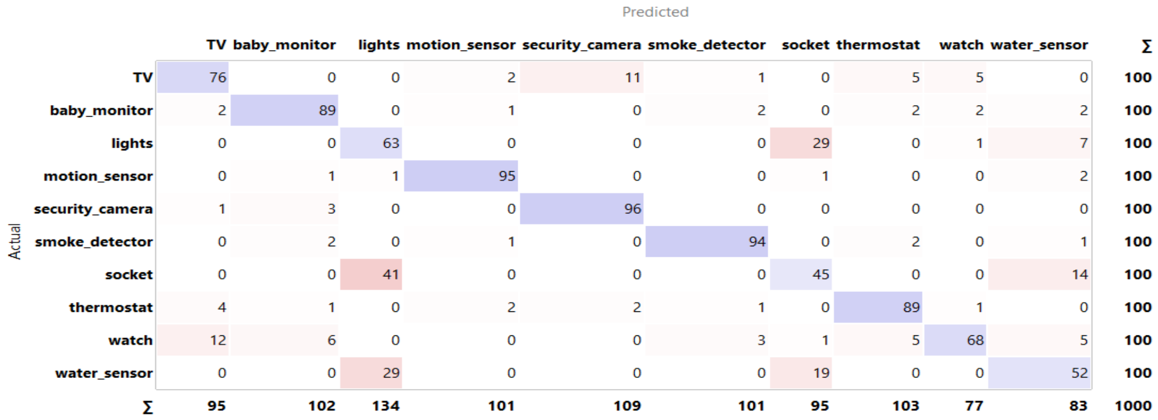


Predicted

Actual	TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	Σ
TV	44	3	0	0	11	0	0	1	39	2	100
baby_monitor	4	83	0	0	2	0	0	0	9	2	100
lights	0	0	84	0	0	0	14	0	0	2	100
motion_sensor	0	0	3	95	0	0	1	0	0	1	100
security_camera	0	0	0	0	99	0	0	0	1	0	100
smoke_detector	1	0	0	1	0	97	0	0	1	0	100
socket	0	0	64	0	0	0	23	0	0	13	100
thermostat	3	0	0	0	0	0	0	94	3	0	100
watch	2	1	0	0	2	0	0	0	92	3	100
water_sensor	0	0	37	0	0	0	23	0	8	32	100
Σ	54	87	188	96	114	97	61	95	153	55	1000

Fig. 5: Confusion matrix of NB.

Source: Author

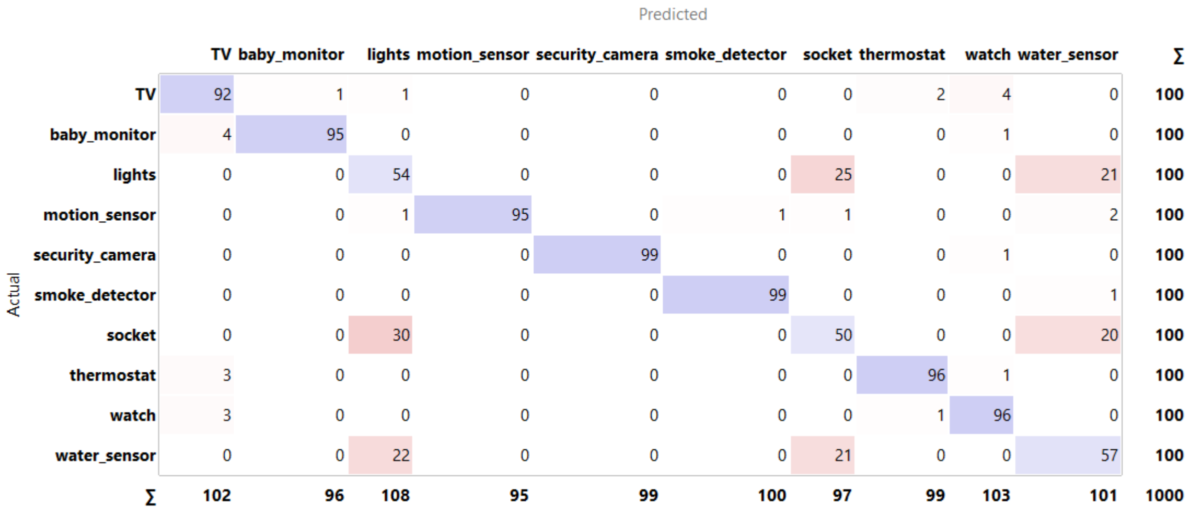


Predicted

Actual	TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	Σ
TV	76	0	0	2	11	1	0	5	5	0	100
baby_monitor	2	89	0	1	0	2	0	2	2	2	100
lights	0	0	63	0	0	0	29	0	1	7	100
motion_sensor	0	1	1	95	0	0	1	0	0	2	100
security_camera	1	3	0	0	96	0	0	0	0	0	100
smoke_detector	0	2	0	1	0	94	0	2	0	1	100
socket	0	0	41	0	0	0	45	0	0	14	100
thermostat	4	1	0	2	2	1	0	89	1	0	100
watch	12	6	0	0	0	3	1	5	68	5	100
water_sensor	0	0	29	0	0	0	19	0	0	52	100
Σ	95	102	134	101	109	101	95	103	77	83	1000

Fig. 6: Confusion matrix of Knn.

Source: Author

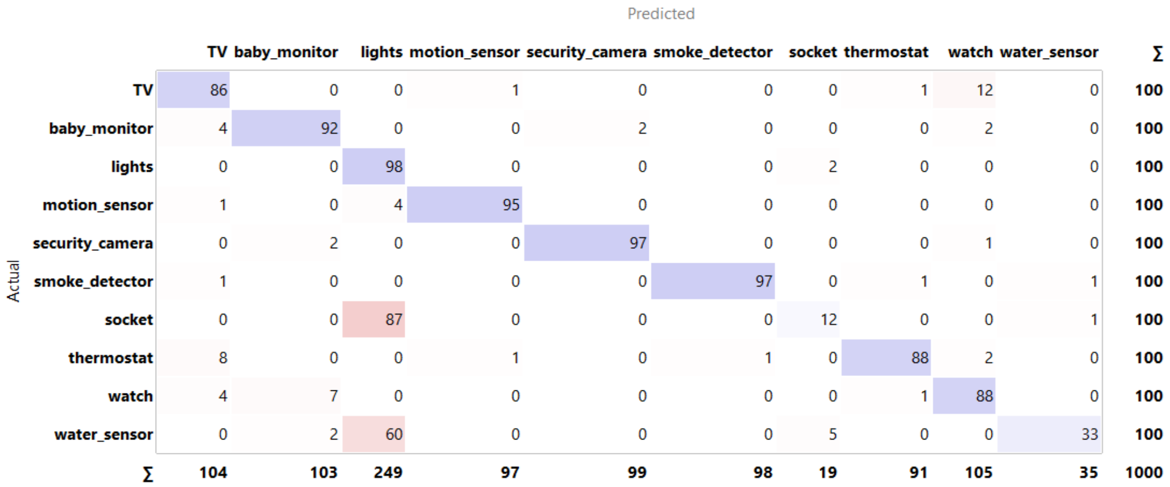


Predicted

		TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	∑
Actual	TV	92	1	1	0	0	0	0	2	4	0	100
	baby_monitor	4	95	0	0	0	0	0	0	1	0	100
	lights	0	0	54	0	0	0	25	0	0	21	100
	motion_sensor	0	0	1	95	0	1	1	0	0	2	100
	security_camera	0	0	0	0	99	0	0	0	1	0	100
	smoke_detector	0	0	0	0	0	99	0	0	0	1	100
	socket	0	0	30	0	0	0	50	0	0	20	100
	thermostat	3	0	0	0	0	0	0	96	1	0	100
	watch	3	0	0	0	0	0	0	1	96	0	100
	water_sensor	0	0	22	0	0	0	21	0	0	57	100
	∑	102	96	108	95	99	100	97	99	103	101	1000

Fig. 7: Confusion matrix of RF.

Source: Author

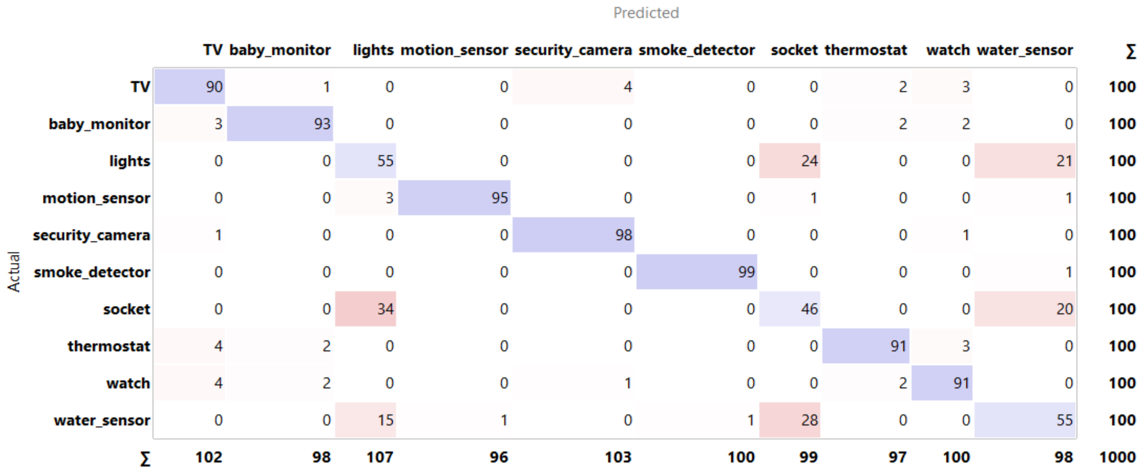


Predicted

		TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	∑
Actual	TV	86	0	0	1	0	0	0	1	12	0	100
	baby_monitor	4	92	0	0	2	0	0	0	2	0	100
	lights	0	0	98	0	0	0	2	0	0	0	100
	motion_sensor	1	0	4	95	0	0	0	0	0	0	100
	security_camera	0	2	0	0	97	0	0	0	1	0	100
	smoke_detector	1	0	0	0	0	97	0	1	0	1	100
	socket	0	0	87	0	0	0	12	0	0	1	100
	thermostat	8	0	0	1	0	1	0	88	2	0	100
	watch	4	7	0	0	0	0	0	1	88	0	100
	water_sensor	0	2	60	0	0	0	5	0	0	33	100
	∑	104	103	249	97	99	98	19	91	105	35	1000

Fig. 8: Confusion matrix of SVM.

Source: Author

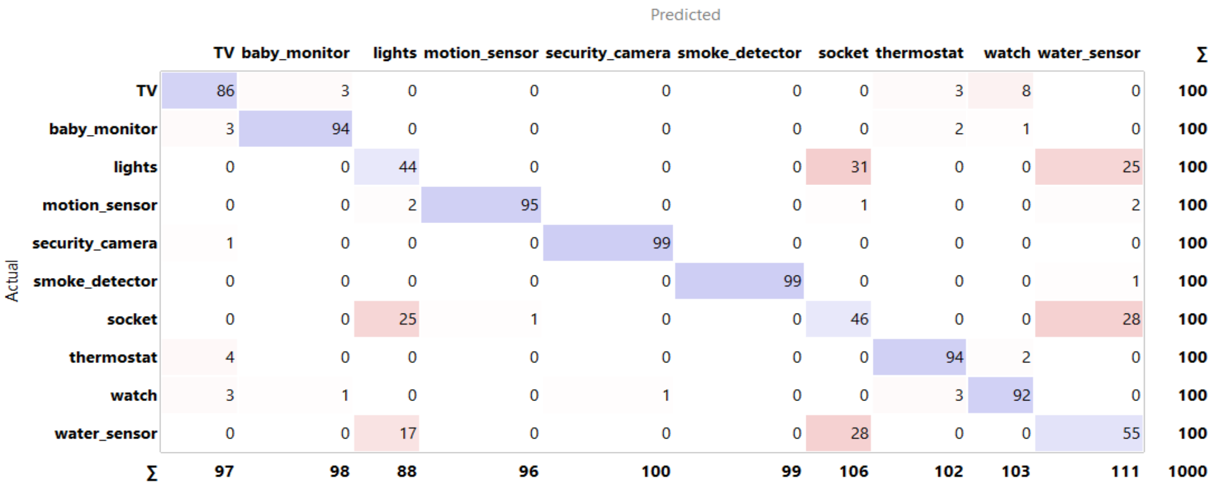


Predicted

		TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	∑
Actual	TV	90	1	0	0	4	0	0	2	3	0	100
	baby_monitor	3	93	0	0	0	0	0	2	2	0	100
	lights	0	0	55	0	0	0	24	0	0	21	100
	motion_sensor	0	0	3	95	0	0	1	0	0	1	100
	security_camera	1	0	0	0	98	0	0	0	1	0	100
	smoke_detector	0	0	0	0	0	99	0	0	0	1	100
	socket	0	0	34	0	0	0	46	0	0	20	100
	thermostat	4	2	0	0	0	0	0	91	3	0	100
	watch	4	2	0	0	1	0	0	2	91	0	100
	water_sensor	0	0	15	1	0	1	28	0	0	55	100
	∑	102	98	107	96	103	100	99	97	100	98	1000

Fig. 9: Confusion matrix of Tree.

Source: Author



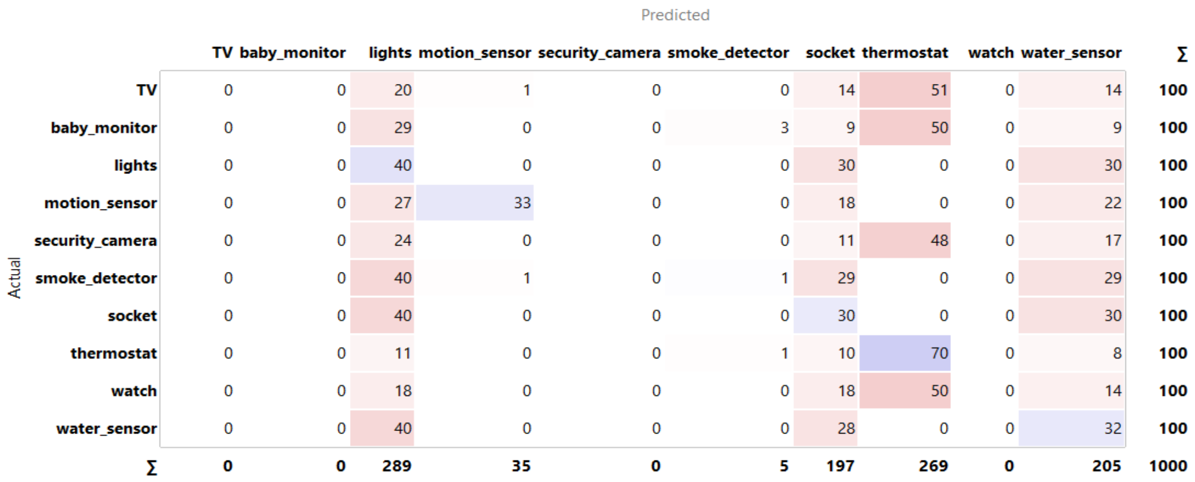
Predicted

Actual

	TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	Σ
TV	86	3	0	0	0	0	0	3	8	0	100
baby_monitor	3	94	0	0	0	0	0	2	1	0	100
lights	0	0	44	0	0	0	31	0	0	25	100
motion_sensor	0	0	2	95	0	0	1	0	0	2	100
security_camera	1	0	0	0	99	0	0	0	0	0	100
smoke_detector	0	0	0	0	0	99	0	0	0	1	100
socket	0	0	25	1	0	0	46	0	0	28	100
thermostat	4	0	0	0	0	0	0	94	2	0	100
watch	3	1	0	0	1	0	0	3	92	0	100
water_sensor	0	0	17	0	0	0	28	0	0	55	100
Σ	97	98	88	96	100	99	106	102	103	111	1000

Fig. 10: Confusion matrix of AB.

Source: Author



Predicted

Actual

	TV	baby_monitor	lights	motion_sensor	security_camera	smoke_detector	socket	thermostat	watch	water_sensor	Σ
TV	0	0	20	1	0	0	14	51	0	14	100
baby_monitor	0	0	29	0	0	3	9	50	0	9	100
lights	0	0	40	0	0	0	30	0	0	30	100
motion_sensor	0	0	27	33	0	0	18	0	0	22	100
security_camera	0	0	24	0	0	0	11	48	0	17	100
smoke_detector	0	0	40	1	0	1	29	0	0	29	100
socket	0	0	40	0	0	0	30	0	0	30	100
thermostat	0	0	11	0	0	1	10	70	0	8	100
watch	0	0	18	0	0	0	18	50	0	14	100
water_sensor	0	0	40	0	0	0	28	0	0	32	100
Σ	0	0	289	35	0	5	197	269	0	205	1000

Fig. 11: Confusion matrix of AB.

Source: Author

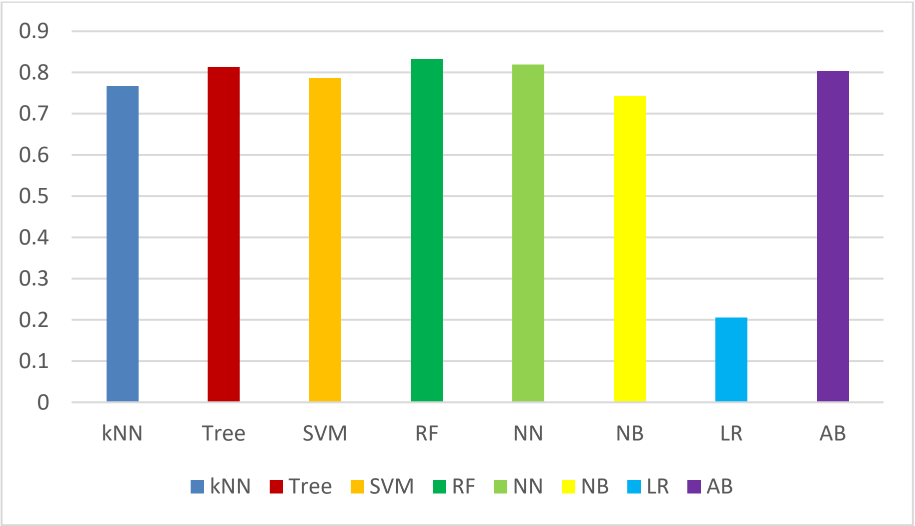


Fig. 12: CA of different supervised machine intelligence models [14]

8. CONCLUSION :

In this work, a cloud based framework is proposed for a smart home to identify the correct IoT device communicating with the local server based on a supervised machine intelligence model. From the results, it is observed that RF show better performance than other models with a classification accuracy of 83.30%. Therefore, it will be better if we prefer RF as the model for installing the local server for classifying the IoT devices with higher accuracy. The confusion matrix of all 8 models is also represented above. In future, we will consider a larger dataset for increasing the classification accuracy of the model. This framework will be a better model for IoT technology for the identification of devices.

9. RECOMMENDATION :

Future work of this system can be focused on the new machine intelligent models or hybrid models, to improve classification accuracy. In the system, new experimental settings can be performed to evaluate the performance.

REFERENCES :

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805. Google Scholar↗

[2] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*(1), 1-50. Google Scholar↗

[3] *Top 12 most commonly used IoT protocols and standards.* Retrieved June 24, 2022, from https://www.techtarget.com/iotagenda/tip/Top-12-most-commonly-used-IoT-protocols-and-standards

[4] *IoT device identification.* Retrieved June 24, 2022, from https://www.kaggle.com/datasets/fanbyprinciple/iot-device-identification?resource=download

[5] Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3179-3202. Google Scholar↗

[6] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017, April). ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the symposium on applied computing* (pp. 506-509). Google Scholar↗

[7] Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*, *1*(1), 1-13. Google Scholar↗

[8] Makkar, A., Garg, S., Kumar, N., Hossain, M. S., Ghoneim, A., & Alrashoud, M. (2020). An efficient spam detection technique for IoT devices using machine learning. *IEEE Transactions on Industrial Informatics*, *17*(2), 903-912. Google Scholar↗

[9] Liu, Y., Wang, J., Li, J., Niu, S., & Song, H. (2021). Machine learning for the detection and identification of internet of things devices: A survey. *IEEE Internet of Things Journal*, *9*(1), 298-320. Google Scholar↗

[10] Salman, O., Elhajj, I. H., Chehab, A., & Kayssi, A. (2022). A machine learning based framework for IoT device identification and abnormal traffic detection. *Transactions on Emerging Telecommunications Technologies*, *33*(3), 1-15. Google Scholar↗

[11] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0305-0310). IEEE. Google Scholar↗

[12] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*(1),

100059. Google Scholar↗

[13] Choi, J., Jeoung, H., Kim, J., Ko, Y., Jung, W., Kim, H., & Kim, J. (2018, June). Detecting and identifying faulty IoT devices in smart home with context extraction. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 610-621). IEEE. Google Scholar↗

[14] *Orange*. Retrieved June 24, 2022, from https://orangedatamining.com/

[15] Bhoi, S. K. (2021). Prediction of diabetes in females of pima Indian heritage: a complete supervised learning approach. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 3074-3084. Google Scholar↗

[16] Bhoi, S. K., Mallick, C., Mohanty, C. R., & Nayak, R. S. (2022). Analysis of Noise Pollution during Dussehra Festival in Bhubaneswar Smart City in India: A Study Using Machine Intelligence Models. *Applied Computational Intelligence and Soft Computing*, *2022*(1), 1-10. Google Scholar↗

[17] Bhoi, S. K., Mallick, C., Nayak, R. P., Mohapatra, D., & Jena, K. K. (2022). Estimating the Category of Districts in a State Based on COVID Test Positivity Rate (TPR): A Study Using Supervised Machine Learning Approach. In *Advances in Distributed Computing and Machine Learning* (pp. 469-478). Springer, Singapore. Google Scholar↗

[18] Nayak, R. P., Sethi, S., Bhoi, S. K., Sahoo, K. S., & Nayyar, A. (2022). ML-MDS: Machine Learning based Misbehavior Detection System for Cognitive Software-defined Multimedia VANETs (CSDMV) in smart cities. *Multimedia Tools and Applications*, *1*(1), 1-21. Google Scholar↗

[19] Bhoi, S. K., Mallick, C., & Mohanty, C. R. (2022). Estimating the Water Quality Class of a Major Irrigation Canal in Odisha, India: A Supervised Machine Learning Approach. *Nature Environment and Pollution Technology*, *21*(2), 433-446. Google Scholar↗

[20] Thomas, L., & Bhat, S. (2021). Machine Learning and Deep Learning Techniques for IoT-based Intrusion Detection Systems: A Literature Review. *International Journal of Management, Technology and Social Sciences (IJMTS)*, *6*(2), 296-314. Google Scholar↗

[21] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686-1721. Google Scholar↗

[22] Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet*, *11*(4), 94; 1-23. Google Scholar↗

[23] Khattab, A., & Youssry, N. (2020). Machine learning for IoT systems. *Internet of Things (IoT)*, 105-127. Google Scholar↗

[24] Firouzi, F., Farahani, B., Ye, F., & Barzegari, M. (2020). Machine learning for iot. In *Intelligent Internet of Things* (pp. 243-313). Springer, Cham. Google Scholar↗

[25] Mitchell, T., Buchanan, B., DeJong, G., Dietterich, T., Rosenbloom, P., & Waibel, A. (1990). Machine learning. *Annual review of computer science*, *4*(1), 417-433. Google Scholar↗

[26] Mitchell, T. M., & Mitchell, T. M. (1997). *Machine learning*. New York: McGraw-hill, *1*(9), 1-20. Google Scholar↗

[27] Jindal, M., Gupta, J., & Bhushan, B. (2019, October). Machine learning methods for IoT and their Future Applications. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 430-434). IEEE. Google Scholar↗

[28] Adi, E., Anwar, A., Baig, Z., & Zeadally, S. (2020). Machine learning and data analytics for the IoT. *Neural Computing and Applications*, *32*(20), 16205-16233. Google Scholar↗

[29] Merenda, M., Porcaro, C., & Iero, D. (2020). Edge machine learning for ai-enabled iot devices: A review. *Sensors*, *20*(9), 1-34. Google Scholar↗

[30] Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, *14*(1), 1-42. Google Scholar↗

****