University of Ibadan
Journal of Science and Logics in ICT Research

Internet of Things (IoT), Internet of Robotic Things (IoRT), IoT Security (IoTS) and Machine Learning Algorithms: A Review Perspective

[1] Odirichukwu, J . C., [2]Ndigwe, C., [3]Njoku, O . A.

[1,3]Federal University of Technology, Owerri
[2]Odumegwu Ojukwu University, Uli (OOU)
jacinta.odirichukwu@futo.edu.ng; chiomajaco6@gmail.com

Abstract

The purpose of this article is to critically review existing studies on the Intelligent systems (IoT), IoT and Robotics (IoRT), IoT Security (IoTS), and Machine Learning Algorithms in order to establish the foundation for a future study. A systematic literature review was conducted with 29 papers from different database sources collected. Intelligent homes, offices, buildings, cities, intelligent agriculture, and intelligent environment monitoring are just a few of the sectors that can benefit from IoT and IoRT applications that are currently available. The research, however, demonstrates that the major challenge of these cutting-edge technologies is the security issue. Therefore, for maximum security in an IoT network, effective and efficient security and privacy protocols like confidentiality, authentication, access control, and integrity are needed. This study presents insight into IoT, IoRT, IoTS, and machine learning algorithms to academics, researchers, and students. Given the ongoing development and interest in IoT technologies, IoRT, and machine learning, this paper aims at contributing to extending knowledge in IoT, IoRT, IoT, and machine learning.

Keywords: Ambient Intelligence**,** Internet of things, Internet of Robotic things, IoT Security, Machine Learning.

1. INTRODUCTION

Robotics is the area of artificial intelligence that deals with designing, planning, building, and controlling robots. The robotics industry's objective is to create Smart machines that can assist human in a variety of ways [10]. Robots are intelligent agents, typically electromechanical devices with intelligent firmware that can be remotely or independently operated by a Personal Computer (PC). With artificial intelligence built in, an autonomous robot can complete duties independently. Robotics, a sub-field of artificial intelligence, is one of the few topics that can be covered in depth due to the variety of scientific technologies it incorporates [20]. The Internet of Things enables the collection, sharing, storing, processing, and analysis of data by connecting collectively embedded systems with external entities such as intelligent objects and communication protocols built on Internet Protocols. The IoRT combines robotics and IoT [14]. The communication between machines, people, and other devices is known as the Internet of Things. Cloud computing and data analytics are now included in this concept [17].

IoRT is the merger of IoT and Robotics, merges intelligent systems, gathers sensor data from numerous sources, keeps track of activities, and monitors the environment. It makes decisions by using both on-board and cloud intelligence and by navigating its surroundings [2]. In an IoT system, edge devices and hubs are referred to as robots, machines that perform tasks similar to those performed by humans. Thin (such as sensors), intelligent (such as microcontroller/ processor), and actuated edge devices that can be static or dynamic (such as robots) are the three different kinds of edge devices [7]. The three primary IoT focus areas are sensing, monitoring, and tracking support services. Data gathering, analytics, communication, and the cloud all make use of the mainly

Odirichukwu, J .C., Ndigwe, C.. Njoku, O. A. (2023). Internet of Things (IoT), Internet of Robotic Things (IoRT), IoT Security (IoTS) and Machine Learning Algorithms: A Review Perspective, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 9 No. 1, pp. 74 - 81

passive sensor data. On the other side, robotics places a strong emphasis on activity, interaction, and autonomous behavior [22]. IoRT applications currently being used include ambient intelligent cities, homes and buildings, agriculture, environment tracking, exploration, disaster rescue, and healthcare. Machine Learning is an Artificial Intelligence methods or algorithms that computers uses in learning and decisions making or predictions [21].

1.1 Internet of Things (IoT) and Its Architecture

The IoT is a network that allows data transmission and reception and is made possible by computing components built into everyday items. The IoT efficiently handles the enormous quantity of data generated by physical objects on the internet at large. A novel technology enables objects to identify one another and communicate with one another [15]. The three major layer of the IoT are the Perception layer, Network layer, and Application Layer [6].

1.1.1 Perception layer of IoT

The Internet of Things (IoT) perception layer connects sensors with the ability to sense the environment in order to collect data from it. IoT sensing technologies include radio frequency identity (RFID), GPS, and sensors for alcohol, gas, humidity, and other variables [1].

1.1.2 Network Layer

The network layer acts as a communication link between the application and perception levels. Several communication methods enable this [1].

1.1.3 Application layer

For storing, visualizing, analyzing, and making decisions, this layer collects data from the perception layer that was transmitted via the network layer [1].

1.2 *Application areas of the Internet of Things and IoRT.*

IoT and IoRT applications include but are not limited to Intelligent healthcare services, Intelligent cities, Intelligent homes and buildings, Intelligent agriculture, Intelligent environment monitoring, Intelligent exploration, Intelligent disaster rescue, Intelligent Retail, and Intelligent Supply Chains [12].

1.3 *Major IoT challenges*

The following are the main obstacles faced when applying embedded electronics to IoT applications:

1.3.1 Security

New, highly developed nodes being added to networks and the internet give malicious individuals many new entry points through which they can take advantage of systemic weaknesses. IoT-enabled appliance hacking has emerged as a security issue that has drawn the attention of prominent governments and technology companies globally [5].

1.3.2 Connectivity

Due to the modifications made to the existing communication models and infrastructures as more devices become interconnected, the IoT will face significant challenges in the future [5].

1.3.3 Standard

Standards such as network protocols, communication protocols, and data aggregation standards facilitate the handling, processing, and storing of data obtained from the sensors. The volume, breadth, and frequency of the data are increased through this aggregation [5].

1.4 IoT Security

As more IoT devices are being deployed, more security flaws become apparent in IoT networks. In order to protect these devices cyber security techniques such as confidentiality, authentication, access control, and integrity, must be put in place [18]. Often, IoT devices are the focus of hackers and intruders. According to a number of studies, 70% of IoT devices are especially susceptible to attacks. Although IoT services are accessible when people and devices are connected, the majority of internet-connected devices are not fully equipped with adequate security procedures, making them susceptible to various security and privacy issues. The IoT must meet specific security standards in order to prevent intrusive network attacks and hacker attacks [23, 24]. A secure network

must have the following characteristics, among others:

1.4.1 Attack resistance
If the Internet of Things device malfunctions while transferring data, it must be able to restart by itself. A server running in a multi-user setting, for instance, needs to be intelligent and able to secure itself from malicious attacks. Every time it crashed, it would instantly recover without notifying the users.

1.4.2 Client privacy
There should be more security around the sharing and transfer of information. Only people with permission should have access to confidential data in order to protect client privacy. Nobody or any unauthorized means can access the client's confidential information.

1.4.3 Access control
Access is only granted to those who meet these conditions. In this instance, the system administrator restricts user access by carefully monitoring each user's login and password in addition to setting access rights so that each user is allowed to view a particular section of the database or program.

1.4.4 Data Authentication
The use of only legitimate devices for data transmission is made possible by authentication processes. Therefore, IoT devices need to be connected to real data [16]. The overwhelming security risks, however, are information eavesdropping and the loss of essential services. The threat to physical security is impacted by these security threats. In addition, user privacy is important because many types of technology share a lot of sensitive data. Consequently, a secure technique is required for protecting personal data [28,24]. IoT also needs the Confidentiality-Integrity-Availability (CIA) triad of protection. Common IoT risks include the HELLO deluge, Sybil attack, wormhole assault, sinkhole attack, and acknowledgment spoofing [28, 4, 25].

1.5 *Machine Learning optimization tools for the Internet of Robotic Things*

Machine Learning is basically a branch of AI (Artificial Intelligence) that works with developing techniques or algorithms that allow computers learn and form perceptions or predictions on its own. It comes from methods used in data mining. Machine learning and statistics are related in many ways. By developing machine learning algorithms, it is possible for the computer to learn without being expressly programmed [21].

Machine learning can be divided into four categories. Algorithms for semi-supervised learning, reinforcement learning, supervised machine learning, and autonomous machine learning are among them. In supervised learning algorithms, a target/outcome variable (or dependent variable) is present and needs to be predicted from a set of predictors (independent variables). These sets of factors are used to construct a function that transforms inputs into desired outputs. The training procedure is repeated until the accuracy of the model on the training data gets the desired level. The teaching examples are made up of features and labels. Examples of supervised learning algorithms include linear regression, decision trees, random forests, K-Nearest Neighbor (KNN), logistic regression, and others.

Algorithms for unsupervised learning do not have a target or outcome variable to forecast or estimate. Users are frequently divided into various groups for targeted activities, and populations are frequently categorized into different groups. Examples of autonomous learning algorithms include the Apriori algorithm, K-means, and others. Semi-supervised learning algorithms combine supervised (labeled data) and unsupervised learning (unlabeled data) to interpret data for decision-making [13]. Finally, a reinforcement learning algorithm instructs the machine to make specific decisions. The machine is placed in a setting where it constantly learns through trial and error. This system learns from experience and tries to collect the most data to make accurate business decisions [3].

1.6 *Steps of Machine Learning Analysis*
There are seven steps of Machine Learning Analysis.

1.6.1 Data Gathering
One of the challenging issues in machine learning is collecting data. How to get a lot of data is one issue with research. One of the challenges of machine learning is having access to labeled data; as opposed to traditional machine learning, in the case of deep learning techniques, features are generated automatically, saving on feature engineering costs. However, it requires larger amounts of labeled data. [19].

1.6.2 Preparing Data
a) The primary objective of machine learning is to predict potential outcomes by using recent data to train your model. We, therefore need an adequate amount of data to train the model. As a consequence, in real life, we are not always equipped with the necessary knowledge. We need to organize the data if it has not been correctly processed before we are able to train our model. Examining the method used to transform our initial data into Training and Test data step-by-step. It uses Python tools like sci-kit Learn, NumPy, and pandas. The following are the stages for data preparation:
a) Get the dataset.
b) Handle Missing Data.
c) Encode categorical data.
d) Split the dataset into Training Set and Test Set.
e) Feature Scaling, if all the columns are not scaled correctly [9].

1.6.3 Choosing a Model
a) First approach to predicting continuous values
In general, linear regression is an appropriate for forecasting continuous quantities like prices.

b) Binary Classification
Support Vector Machine (SVM), another excellent choice for two-class classification, can be used to implement binary classification in an efficient manner.

c) Multi-class classification
Random forest is a choice for multi-class classification.

d) Exists a starter model category that is the simplest or most straightforward?
It's common knowledge that decision trees are simple to use and understand. Decision trees are implemented by models such as Random Forest or Gradient boosting [11].

1.6.4 Training
To train your model, split the data into training and testing sets. Machine learning operates by establishing a relationship between a label and its features. This procedure is known as training a model [27].

1.6.5 Evaluation
A model is evaluated to see how accurate the training set was. Following the conclusion of training with the training dataset, the model's performance is assessed. This makes use of the test dataset that has been set away. Typically, the training and testing sets are split 80:20 or 70:30, indicating that 80 or 70 percent of the training set will be used for training and the remaining 20 or 30 percent will be kept for testing [27].

1.6.6 Hyperparameter Tuning
While the hyperparameter demonstrates the model's structure, the model parameters demonstrate how the data that comes into it is transformed into an expected output. Depending on the selection and value of the hyperparameters, the efficacy of the machine learning model will inevitably rise or fall. For instance, "tree_depth" is a hyperparameter for the decision tree method. If a moderate value is given to the hyperparameter, a decent result can be obtained from the model, but a high value can affect how well the algorithm performs. As a result, hyperparameters need to be cautiously chosen. There are numerous ways to set hyperparameters depending on the particular dataset as well. Manually setting the number is the first option. A further suggested technique is to select the preset hyperparameter values provided by the software applications used in the implementation. For some datasets, these default values perform well, but that does not necessarily imply that they provide the highest accuracy. Additionally, we can employ hyperparameter tuning techniques. These optimization techniques rely on the kind of dataset that is available. The generalization mistake of a machine-learning model is, however, decreased [8].

1.6.7 Prediction

To provide answers, machine learning uses data. Thus, prediction or inference makes use of data to provide a response or make a future inference. The importance of machine learning is now understood [26].

2. METHODOLOGY

This paper adopted PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) methodology. The sources for this paper were taken from the database as indicated in Table 1. The researcher accesses 14 databases, including Elsevier, IEEE Xplore, Springer, and So on. The keyword searched includes "Internet of Things", "Internet of Robotics Things", "Internet of Things security", and "Machine Learning Algorithms". Table 1 enlisted the number of databases selected according to sources. Article selection (inclusion) and exclusion criteria include the following:

1. The researcher considered original articles published in journals and conferences.
2. The papers have to be written entirely in English.
3. The researcher excluded the papers whose databases had access restrictions, because the authors could not access them.

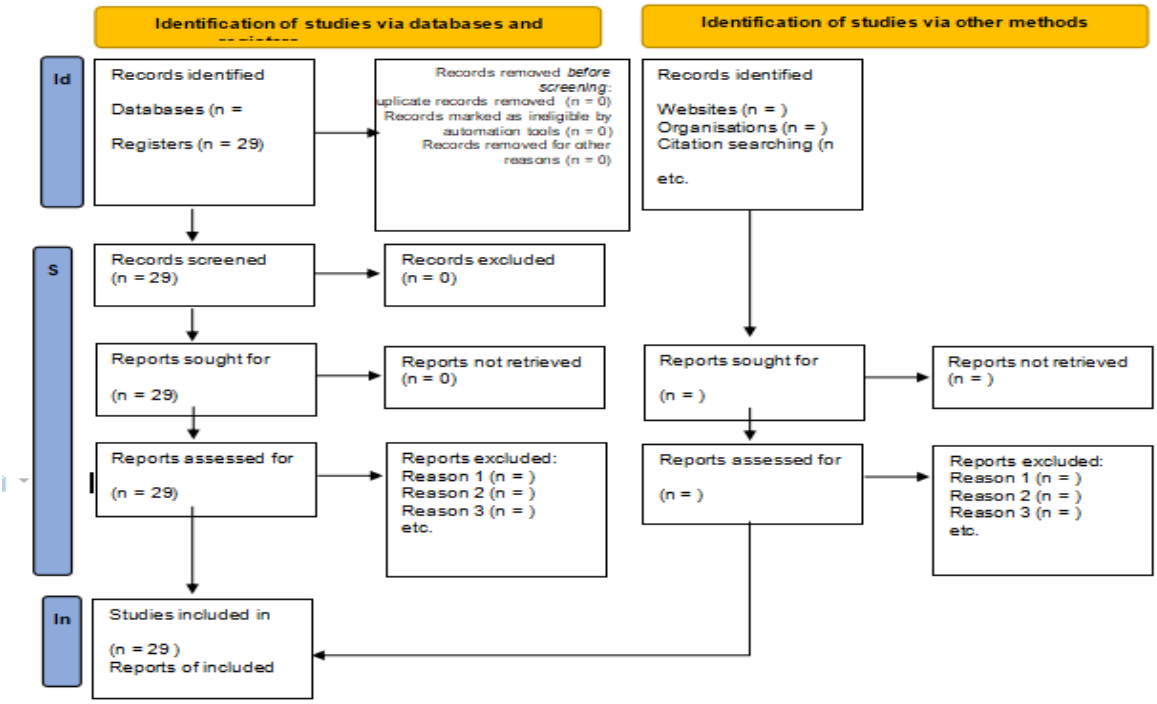

Figure 1: Preferred Reporting Items for Systematic Reviews and Meta-Analysis flow diagram for new systematic reviews which included searches of databases, registers and other sources

Table 1: Source of articles used in the study.

Database source	No. of documents
International Journal of Engineering Science and Computing	1
Other sources	14
IEEE Access	2
preprints	1
International Journal Enginearing and Computer Science	2

Communications on Applied Electronics (CAE), Foundation of Computer Science	1
Elsevierr	1
Springer	1
IOSR Journal of Computer Engineering	1
International Journal of Advanced Computer Science and Application	1
International Journal of Circuits, Systems and Signal Processing	1
Computer Law and Security Review	1
International Journal of Computer and Electrical Engineering	1
Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks	1
Total	29

3. RESULTS AND DISCUSSION

In this study, 15 out of the paper reviewed are empirical papers published in reputable journal, whereas 14 were published in other sources. One-third of all reviewed papers are published in IEEE Access, International Journal of Engineering and Computer Science. The two journal on IoT, IoRT, as well as Machine learning algorithms. However, other percentages of the journals contributed immensely to this study. Moreover, about 45% of the reviewed papers were obtained from other sources such as google, blog articles, conference papers, etc. The first main topic focuses on the concept of IoT and its architecture. Bilal [6] discussed that the IoT architecture includes the Perception Layer, Network Layer, and Application Layer. Concerning the application areas of IoT and IoRT,

Jha [12] presented smart cities, smart homes, smart healthcare, etc. Regarding the challenges of IoT. Archana and Vinodhini [5] proposed that the major challenges encountered by IoT applications are security, connectivity, and standards. Razzaq *et. al.* [18] identified that a growing number of security flaws exist in IoT networks. They then found out that the optimum solution to these flaws is effective and strong security protocols such as confidentiality, authentication, access control, and integrity. Andrea *et. al.* [4], Wood *et. al.* [25] and Karlof Wagner [28] presented some of the essential capabilities of a secured IoT network. An overview of machine learning was presented in Talwar and Kumar [21], while Analytics [3] presented the commonly used machine learning algorithms. However, Grunal [9], Jaokar [11], Roh *et. al.* [19] and Yung [27] did justice to the steps involved in machine learning.

4. CONCLUSION

This paper reviewed Internet of Things, Internet of Robotics Things, Internet of Things Security, and Machine Learning Techniques. Discussed herein also is IoT and Its Architecture. The fusion of robotics technologies and the internet of things give birth to the Internet of Robotics Things. In furtherance, the application areas of IoT and IoRT and their major challenges were pointed out. Meanwhile, the major challenge of this technology is security. Hence, effective and strong security and privacy protocols such as confidentiality, authentication, access control, and integrity are shown to be required in an IoT network to avoid attackers from intruding into the networks. Also, the research discussed machine learning, which is an artificial intelligence technique for making predictions. The types of Machine Learning Techniques; Supervised Learning, Unsupervised Learning, Semi-Supervised and Reinforcement learning. Finally, the steps of Machine Learning analysis were elucidated.

References

[1] Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I. (2015). Architecture of the Internet of Things: State of the Art. Springer, 9.

[2] SABI Research (2015). Internet of Robotics Things. https://www.abiresearch.com/marketresearch/product/1019712-the-internetofrobotic-things.

[3] Analytics vidhya. (2017). Commonly used Machine Learning Algorithms (with Python and R Codes). https://www.analyticsvidhya.com/blog/2017/09/common-machine- learning-algorithms/.

[4] Andrea, I., Chrysostomou, C., Hadjichristofi, G. (2015). Internet of things: Security vulnerabilities and challenges. In 2015 IEEE Symposium on Computers and Communication (ISCC), 180- 187.

[5] Archana,V., and Vinodhini, S. (2017). Fundamentals and Applications of IoT. IOSR. Journal of Computer Engineering (IOSR-JCE), 6(5), 20-23.

[6] Bilal, M. (2017). A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers, Elsevier,

[7] Chowdhury, A. R. (2017). IoT and Robotics: A Synergy. https://peerj.com/preprints/2760.pdf.

[8] Elgeldawi, E., Sayed, A., Galal, A.R., Zaki, A.M.(2021). Hyperparameter Tuning for Machine Learning Algorithms Used for Arabic Sentiment Analysis Informatics 2021, 8, 79. https://doi.org/10.3390/ informatics8040079.

[9] Grunal, L. (2019). How to Prepare Your Dataset for Machine Learning in Python. https://appdividend.com/2018/07/23/prepare-dataset-for-machine-learning-in-pyt hon/.

[10] Hanna, K.T. (2022). Robotics. https://www.techtarget.com/whatis/definition/robotics#:~:text=Robotics%20is%20a%20branch%20of,on%20a%20number%20of%20forms.

[11] Jaokar, A. (2008). How to Choose a Machine Learning Model-Some Guidelines. https://www.datasciencecentral.com/profiles/blogs/how-to-choose-a-machine-learning-model-some-guidelines.

[12] Jha, A.K. (2018). IoT (Internet of Things). Retrieved from https://www.linkedin.com/pulse/iot-internet-things-amit-kumar-jha.

[13] Nasteski, V. (2017). An overview of the supervised machine learning methods. https://www.researchgate.net/publication/328146111_An_overview_of_the_supervised_machine_learning_method s.

[14] Patel, K.K., and Patel, S. M. (2016). Internet of Things IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, 6(5), 6122.

[15] Perwej , Y., Kerim, B., AbouGhaly, M.A., Harb, H.A.M. (2019). An Extended Review on Internet of Things (IoT) and its Promising Applications. Communications on Applied Electronics (CAE), Foundation of Computer Science FCS, 7(26), 1-16.

[16] Qureshi, M.A., Aziz, A., Ahmed, B., Khalid, A., Munir, H. (2012). Comparative analysis and implementation of efficient digital image water-marking schemes. International Journal of Computer and Electrical Engineering, 4(4), 558.

[17] Ray, P. P. (2017). Internet of Robotic Things: Concept, Technologies, and Challenges, IEEE Access, 4, 9489-9500.

[18] Razzaq, M.A., Gill, S.H., Qureshi, M.A., Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications, 8(6), 383-388.

[19] Roh,Y., Heo, G., and Whang, S. E. (2019). A Survey on Data Collection for Machine Learning A Big Data - AI Integration Perspective.

[20] Sharakhatreh, F. (2011). The Basics of Robotics. Lahti University of Applied Sciences Machine- and production technology, 1-122.

[21] Talwar, A., Kumar, Y. (2013). Machine Learning: An artificial intelligence methodology. In International Journal of Engineering and Computer Science.

[22] Tiwari, V. (2020). What is IoRT (Internet of Robotic Things). https://iot4beginners.com/what-is-iortinternet-of-robotic-things/.

[23] Turcu, C., Turcu, C. and Gaitan, V., (2012). Integrating robots into the Internet of Things, International Journal of

Circuits, Systems and Signal Processing, 6(6), 430-437.

[24] Weber, R.H. (2010). Internet of things-new security and privacy challenges. Computer law & security review, 26(1), 23-3.

[25] Wood, A.D., Fang, L., Stankovic, J.A., He, T. (2006). Sigf: A family of configurable, secure routing protocols for wireless sensor networks. In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks, 35-48. https://doi.org/10.1145/1180345.1180351.

[26] Yufeng G. (2017). The 7 Steps of Machine Learning. https://towardsdatascience.com/the-7-steps-of-machine-learning- 2877d7e5548e.

[27] Yung, I. (2018). A beginner to training and deploying Machine Learning Models in python. https://www.freecodecamp.org/news/a-beginners-guide-to-training-and-deploying-machine-learning-models-using-python-48a313502e5a/.

[28] Karlof, C., Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 113-127.