iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43026

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Application of Machine Learning in Internet of Things (IoTs)

Yoginder Kumar
Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur

Abstract: ***Machine learning is a subset of artificial intelligence in which machines learn through real data rather than being explicitly taught to do so. With the growing number of devices on business networks, IT teams are finding it difficult to design adequate security procedures. IoT security is crucial for corporate survival and success, but it comes with its own set of issues. Some of these issues can be addressed using a machine learning (ML) strategy to IoT security. It eliminates the problem of recognizing unknown devices on a network, ensures that they are included in the current security framework, and simplifies IoT management for busy IT teams. In this paper, application of the Machine Learning algorithms in IoT sectors are explored.***
Keywords: Machine Learning; Internet of Things (IoT); Algorithms; Applications

I. WHAT IS MACHINE LEARNING?

Machine learning is a branch of computer science that enables computers to learn without even being explicitly programmed. One of the most intriguing technologies that one has ever encountered is machine learning. As the name suggests, it offers the computer the ability to learn, which makes it more human-like [1-5]. Machine learning is currently in use, possibly in far more locations than one might imagine.

Machine learning is extremely complicated, and its operation differs based on the goal and the algorithm employed to complete it. A machine learning model, on the other hand, is a computer that analyzes data for patterns and then uses those insights that can help fulfill its assigned task [6-9]. Machine learning can automate any operation that relies on a set of points or rules, including more complicated tasks like answering calls from customers and analyzing resumes.

Machine learning algorithms use more or less human involvement depending on the situation. supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning are the four major machine learning models. Machine learning is a large group of algorithms that can take a set of data and recognize patterns, uncover insights, and/or generate predictions using it. Deep learning is a subset of machine learning that goes beyond the capabilities of traditional machine learning [10-14].

Engineers can analyze an algorithm's outputs and make improvements based on their correctness, therefore there is some human participation with machine learning in general. This review has no bearing on deep learning. Instead, a deep learning system checks the accuracy of its results using its own neural network before learning from them.

The neural network of a deep learning algorithm is a layered structure of algorithms that mimics the components of the human brain. Training and inference are the two major steps in the formation of a neural network [15-20]. The deep learning algorithm is presented a data set and is tasked with deciphering what that data set signifies during the training stage. Engineers then provide feedback on the correctness of the neural network's interpretation, and it adjusts accordingly. This method may go through several iterations. When a neural network is used for inference, it may take a data set this has never seen elsewhere predict outcomes about what it symbolizes.

II. APPLICATION OF MACHINE IN VARIOUS SECTORS

Machine learning is the engine that drives a robust, adaptable, and resilient business. Smart businesses use machine learning to boost revenue, staff efficiency, and customer happiness.

Many businesses find achievement with a few machine learning use cases, but that's only the beginning. Experimenting with machine learning may come first, but the integration of ML models into enterprise applications and processes must come next so that they can be scaled across the enterprise. Many businesses lack the necessary expertise, processes, and technologies to achieve this level of enterprise integration. Firms should take investing in MLOps, which comprises the methodology, tools, and technologies that expedite and regulate each phase of the ML lifecycle, from model development through operationalization, in order to achieve ML at scale. MLOps is a new profession that strives to bring agility and speed to the ML lifecycle. It's comparable to what DevOps has accomplished in the software development process. ML technology and methodologies are being successfully adopted throughout vertical industries, giving enterprises with tangible, real-world benefits.

Banks, for example, are adopting machine learning prediction models to better comprehend and address consumer needs by looking at a large number of interconnected metrics. Machine learning predictive models can also detect and reduce risk exposure. Banks can better estimate risk for new products by identifying cyber risks, tracking and documenting fraudulent consumer activity. Fraud prevention and prevention, personal financial counselor services, and credit scoring and loan analysis are some of the most common use cases for machine learning in banking [21-26].

Organizations have integrated automation in manufacturing and are now performance tuning both equipment and processes. They utilize machine learning to restructure and enhance the productivity in a way that is responsive to current demand while also anticipating future change. As a result, a production process that is both agile and resilient has emerged. Yield enhancements, root cause analysis, and supply chain and stock management are the top three ML use cases in manufacturing. Machine learning algorithms produce models that can detect flaws in parts, for example. Surface flaws in manufacturing, painting, and other processes They can also be used to monitor quality in an assembly operation, such as the inclusion or exclusion of pieces, inspect welds, and so on [27-36].

III. MACHINE LEARNING IN INTERNET OF THINGS (IOT)

While serving enormous machine-type communication (mMTC) applications, current random access (RA) allocation approaches suffer from congestion and excessive signaling overhead. In order to minimize latency and boost dependability for smart Internet of Things (IoT) programs with rigorous Quality-of-Service limitations, the third-generation partnership project presented the requirement to adopt fast uplink grant (FUG) allocation. Eldeeb et al. [37] suggested a support vector machine-based FUG allocation method (SVM). First, an SVM classifier is used to prioritize machine-type communication (MTC) devices. Second, to counteract prediction mistakes, a long short-term memory design is used for traffic flow prediction and correction approaches. Both results are utilized to create a resource scheduler that is efficient in terms of average delay and total throughput. To compare the proposed FUG allocation to other existing allocation approaches, a coupled Markov modulated Poisson process (CMMPP) traffic model with combined alert and regular traffic is used. In their study, they try to forecast the condition of each device, such as silent or active, and also the related traffic priority. Following that, the serving BS schedules the active devices in order of priority. They developed the system model using CMMPP, an efficient traffic model. The M-CMMPP model, which comprises of numerous background CMMPP processes, is then used to enhance the baseline model to account for a more dense scenario. The system model is shown in Figure 1.

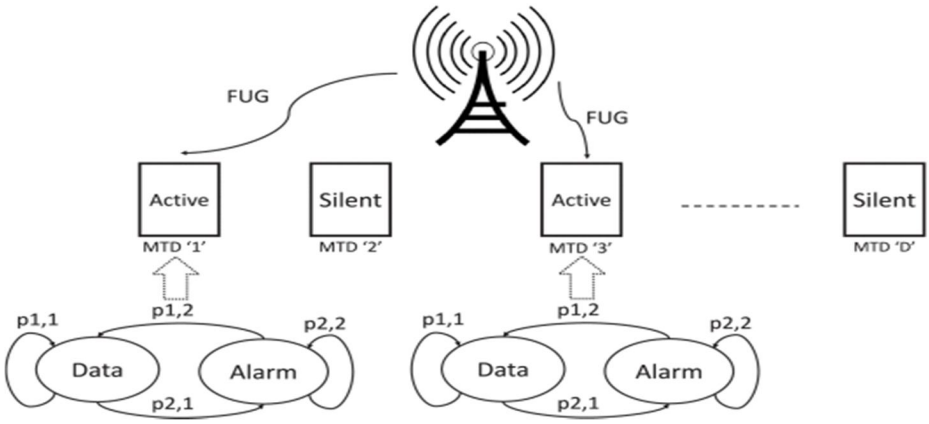


Figure 1: A system model has been considered. A group of D devices that can be active or inactive. Active devices might be in one of two states: data or alarm [37].

By evaluating RSSs using a combination of supervised, unsupervised, and ensemble machine learning approaches, Bhatti et al. [38] developed an outlier detection system called iF Ensemble for Wi-Fi indoor localisation. Isolation forest (iForest) is employed as an unsupervised learning strategy in their study. Support vector machine (SVM), K-nearest neighbor (KNN), and random forest (RF) classifiers with stacking are included in the supervised learning technique. The accuracy, precision, recall, F-score, and ROC-AUC curve are employed in the evaluation. With proposed outlier identification approaches, the accuracy of the localization process in an indoor setting improves by about 2% after eliminating outliers, according to the evaluation of the utilized machine learning method. Because of the potentially devastating effects of an attack, it is vital to secure Industrial Internet of Things (IIoT) equipment. Machine learning (ML) and big data analytics are two of the most effective tools for assessing and safeguarding IoT devices.

These strategies, by extension, can assist improve the security of IIoT systems. A common IIoT protocol and its associated vulnerabilities were disclosed by Zolanvari et al. [39]. They then conducted a cyber-vulnerability assessment and discussed the use of machine learning to mitigate these risks.

The Internet of Things (IoT) generates massive amounts of data in real time. Temporal study of all these data series to uncover behavioural trends could lead to qualified information that impacts a variety of businesses. As a result, using machine learning (ML) algorithms to IoT data has the potential to improve essential process safety, economy, and performance. Developing ML workflows at scale, on the other hand, is a difficult endeavor that requires both production and specialist abilities. Such tasks necessitate the analysis, comprehension, selection, and deployment of unique machine learning workflows, which frequently result in bottlenecks, production challenges, and code management complexity, and may not even produce a final desirable result. The Machine Learning Framework for IoT Data (ML4IoT) was proposed by Alves et al. [40], and it is developed to orchestrate ML workflows, particularly on massive volumes of data series. The ML4IoT framework enables the construction of a variety of machine learning models, each with its own workflow. A simple pipeline can be used to configure and use these models. ML4IoT was built with container-based components in mind, allowing for simultaneous training and deployment of many machine learning models. According to the findings, the suggested framework can effectively integrate IoT heterogeneous data by offering flexibility, resilience, and performance.

Figure 2 shows how the proposed ML4IoT framework leverages containerized microservices to automate the implementation described in machine learning workflows. The orchestrator and scheduler manage and design each container using a REST API-based component. Because ML4IoT is implementation-agnostic, it can simply be expanded to accommodate new components including data pretreatment jobs, algorithm types, and machine learning frameworks. To achieve this, the microservices architecture and container-based virtualization were integrated to address issues such as the large number of available machine learning frameworks and the concurrent execution of ML operations. The framework's Core, in particular, creates and manages containers for training and deploying machine learning models. Each model is converted into a docker image and made available for use. The workflow designer is in charge of creating batch workflow jobs. The specification of dataset linkages, preprocessing data treatments, and the setup of a given accessible ML model are all required for each workflow job. The Orchestrator reads the workflow batch tasks and generates a docker container microservice for each workflow using the Container Management System (CMS). Furthermore, each microservice uses the Distributed Data Processing Engine to complete its job.

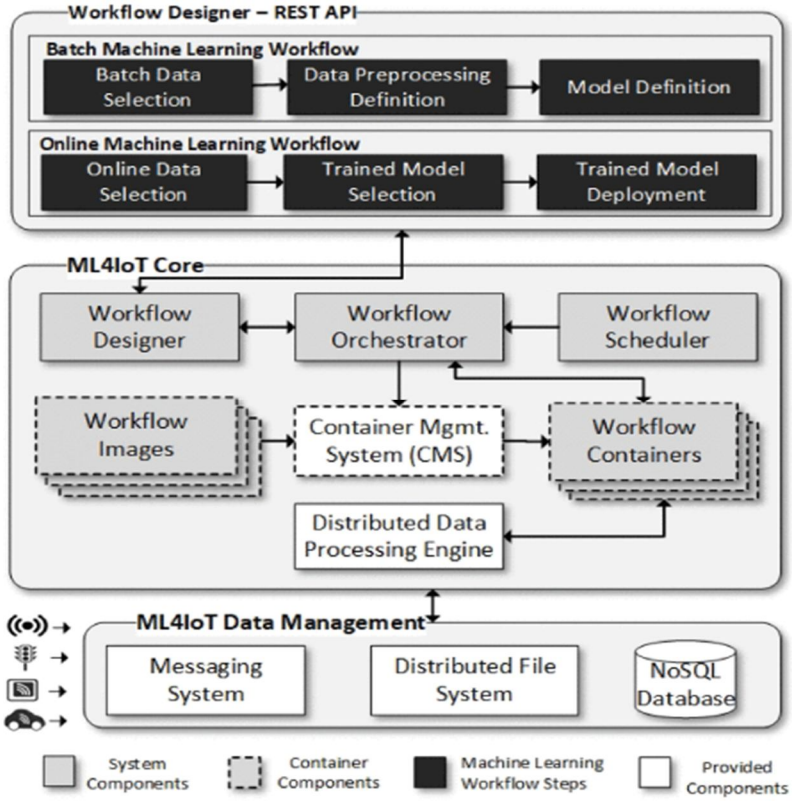


Figure 2: Machine learning framework for IoT data - ML4IoT [40].

The ML4IoT Data Management (DM) component ingests and stores the IoT data utilized by the containers. A Messaging System, a Distributed File System, and a NoSQL database are the three sub-components of the DM. Finally, the DM allows for the temporary storage of preprocessed data as well as the preservation of trained models and forecasted data.

This design allows for the separation of software components into discrete, specialized services, giving the framework more flexibility, reusability, and extensibility.

The Industrial Internet of Things (IIoT) connects a wide range of sensors, machines, industrial uses, databases, services, and workers. Smarter cities, agriculture, and e-healthcare are just a few of the ways the IIoT is enhancing our lives. Although the IIoT and consumer IoT share some aspects, the two networks use different cybersecurity measures. IIoT solutions, unlike client IoT solutions that are utilized by a single user for a single purpose, are usually incorporated into larger operational data. As a consequence, IIoT security solutions necessitate more preparation and awareness in order to ensure the system's security and privacy. Machine learning approaches are used to forecast various cybersecurity attacks such as denial of service (DoS), malicious activity, hostile control, data type probing, surveillance, scan, and incorrect setup. Latif et al. [41] proposed an unique lightweight random neural network (RaNN)-based prediction model to forecast the aforementioned attacks. Several evaluation criteria such as reliability, precision, recall, and F1 score were calculated and compared with the classic artificial neural network (ANN), support vector machine (SVM), and decision tree to evaluate the performance of the RaNN-based prediction model (DT). The suggested RaNN model achieves an accuracy of 99.20 percent with a learning rate of 0.01, with a prediction time of 34.51 milliseconds, according to the evaluation findings. Precision, recall, and F1 score were all 99.11 percent, 99.13 percent, and 99.20 percent, respectively. When compared to state-of-the-art machine learning approaches for IoT security, the proposed scheme enhances threat detection accuracy by an average of 5.65%.

A four-layered architecture can be used to define the IIoT. As shown in Figure 3, this architecture in the industrial sector consists of physical, network, middleware, and application layers. A large number of connected physical equipment, sensors, mobile and computer devices, and other observation and automated objects make up the physical layer. Several communication networks, such as wireless sensor networks, wireless connections, and machine-to-machine interfaces, are included in the network layer. The middleware layer connects the network and application layers and includes cloud storage, an application programming interface, and web services. The application layer is the top layer of an IIoT architecture, and it enables a variety of industrial processes and services, such as smart factories, building automation, smart healthcare, smart vehicles, automation, and so on.

The IIoT is a full architecture that may be used by a variety of people and businesses. However, technology poses numerous additional security, privacy, legal, and social challenges. Solving these problems necessitates highly scalable solutions. IoT devices are resource-constrained devices that require security solutions that can meet their storage, power, and cost requirements. Standard communication protocols must be compatible with these solutions. During industrial operations, IoT devices create massive amounts of data, making an IIoT system a tempting target for hackers. Conventional data processing methods are not applicable for IoT and IIoT applications due to the massive amount of data. As a result, one of the most concept of cognitive paradigms for providing embedded intelligence is machine learning (ML).

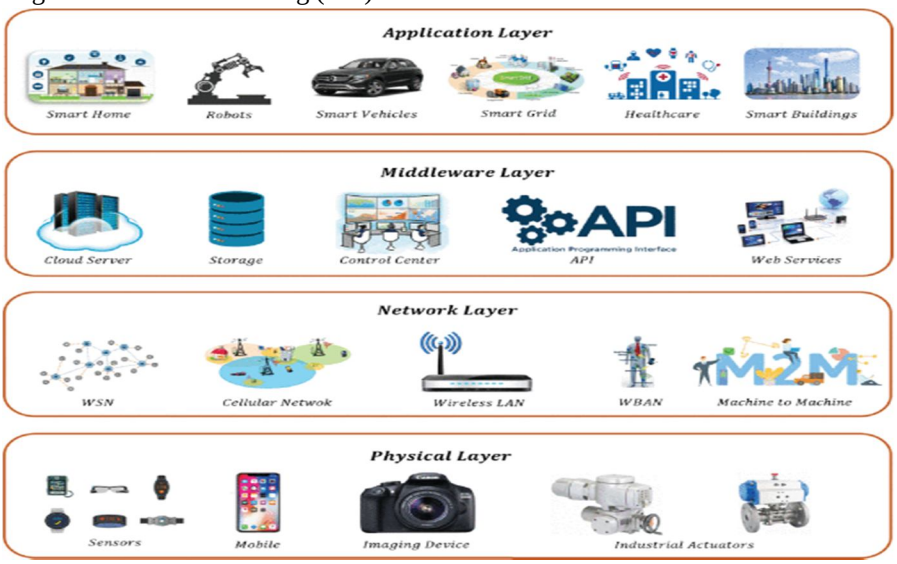


Figure 3: Industrial IoT system architecture [41].

The infrastructure for detecting attacks is made up of numerous operations. Figure 4 depicts the attack detection technique. The dataset collection and observation are the first steps in this architecture. The dataset collected and evaluated according to the data type at this point. The dataset was then subjected to preprocessing, which included data cleansing, visualization, feature engineering, and vectorization. The data features are retrieved using all of these approaches. These feature vectors were divided into two sets, one for training and one for testing, using an 80/20 ratio. With the suggested random neural network, the training set was used for the learning process.

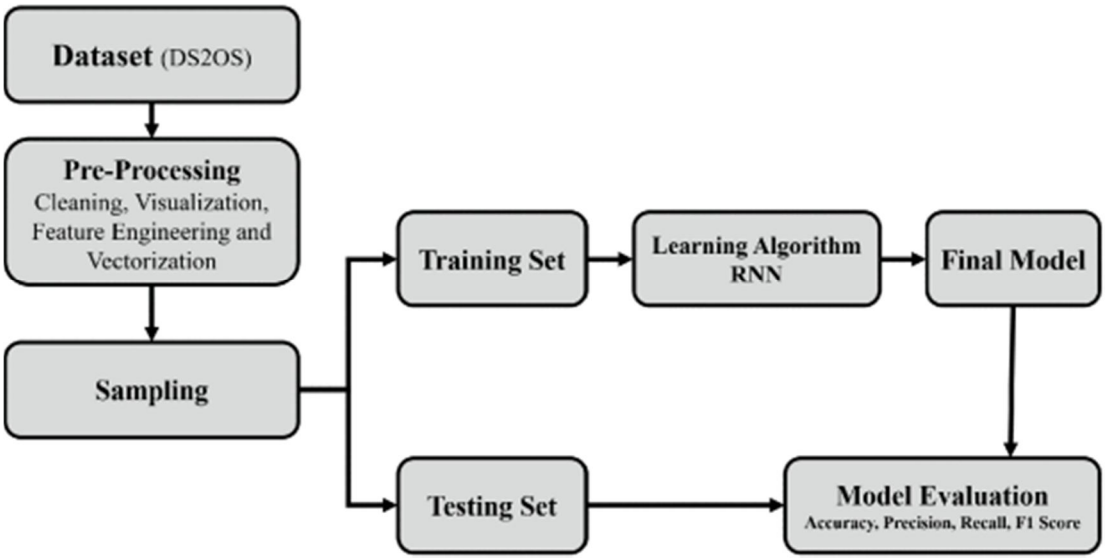


Figure 4: The assault detection technique is depicted as a block diagram [41].

IV. CONCLUSION

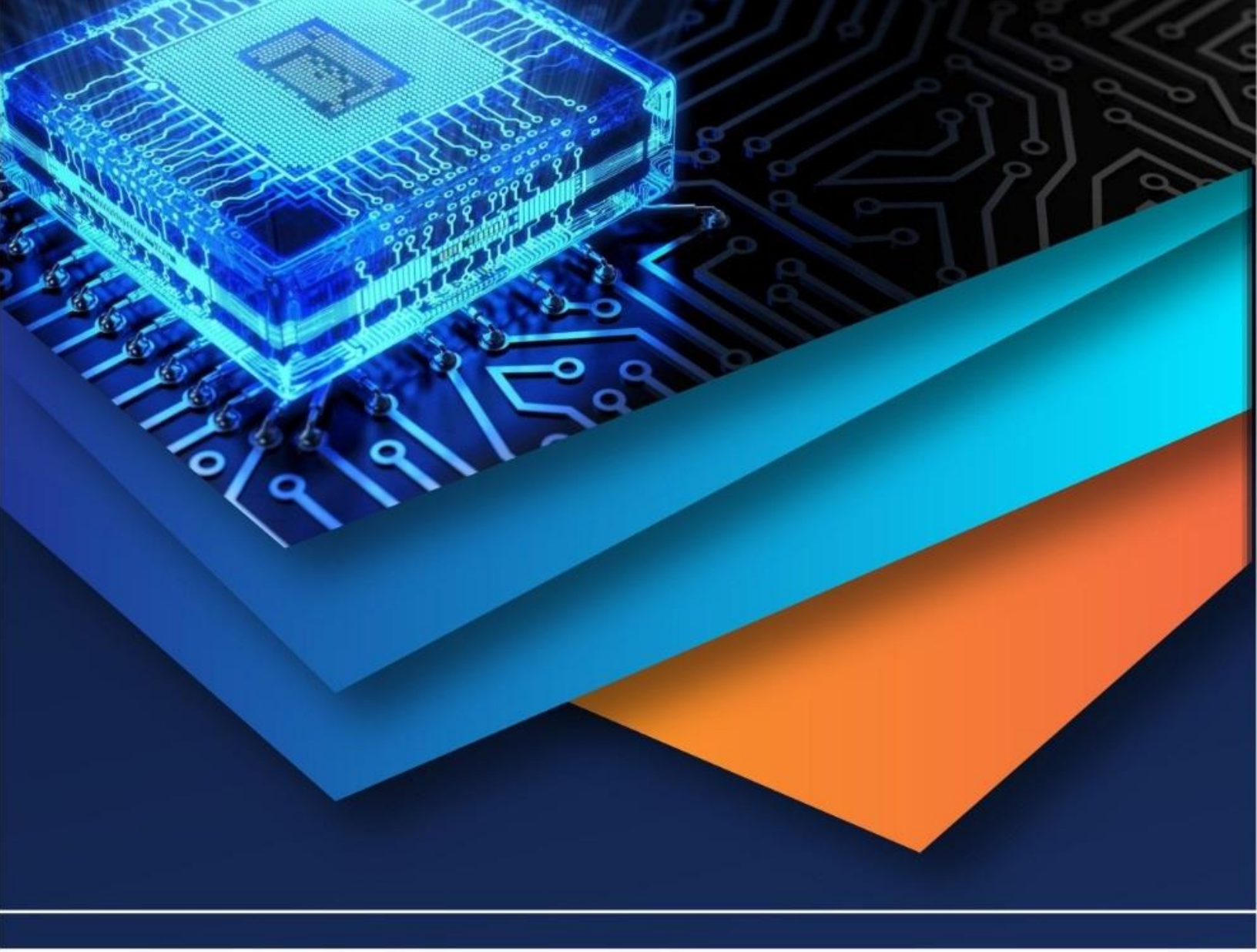
To make cognitive decisions, machine learning employs supervised learning algorithms on historical data. The algorithm's decision-making capabilities improve as the amount of historical data increases. Because the data collected by the devices is typically relatively frequent, this concept makes IoT a great use scenario for machine learning. The following are some examples of how machine learning and IoT work together to enable business optimizations:

1) *Anomaly Monitoring:* Azure machine learning could be used to identify anomalies in time series data, such as data streams sent by IoT devices. A machine learning algorithm watching the live streaming of device data can detect anomalies such as spikes and dips, favourable and unfavourable trends.
2) *Predictive Maintenance:* As one of the most popular machine learning solutions, predictive maintenance has a direct impact on an organization's costs. Machine learning algorithms' capacity to predict the likelihood of a device failing, the remaining life of an instrument, and the causes of failure can help a corporation reduce operational costs by minimizing maintenance.

REFERENCES

[1] Jordan, M.I. and Mitchell, T.M., 2015. Machine learning: Trends, perspectives, and prospects. Science, 349(6245), pp.255-260.
[2] Carleo, G., Cirac, I., Cranmer, K., Daudet, L., Schuld, M., Tishby, N., Vogt-Maranto, L. and Zdeborová, L., 2019. Machine learning and the physical sciences. Reviews of Modern Physics, 91(4), p.045002.
[3] El Naqa, I. and Murphy, M.J., 2015. What is machine learning?. In machine learning in radiation oncology (pp. 3-11). Springer, Cham.
[4] Wang, H., Lei, Z., Zhang, X., Zhou, B. and Peng, J., 2016. Machine learning basics. Deep learning, pp.98-164.
[5] Sammut, C. and Webb, G.I. eds., 2011. Encyclopedia of machine learning. Springer Science & Business Media.
[6] Harrington, P., 2012. Machine learning in action. Simon and Schuster.
[7] Wagstaff, K., 2012. Machine learning that matters. arXiv preprint arXiv:1206.4656.
[8] Bonaccorso, G., 2017. Machine learning algorithms. Packt Publishing Ltd.
[9] Mahesh, B., 2020. Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9, pp.381-386.
[10] Natarajan, B.K., 1991. Machine learning: A theoretical approach. Morgan Kaufmann Publishers Inc..
[11] Wang, H., Ma, C. and Zhou, L., 2009, December. A brief review of machine learning and its application. In 2009 international conference on information engineering and computer science (pp. 1-4). IEEE.
[12] Witten, I.H., Frank, E., Hall, M.A., Pal, C.J. and DATA, M., 2005. Practical machine learning tools and techniques. In DATA MINING (Vol. 2, p. 4).
[13] Alpaydin, E., 2020. Introduction to machine learning. MIT press.
[14] Ij, H., 2018. Statistics versus machine learning. Nat Methods, 15(4), p.233.

[15] Mitchell, T.M., 1997. Does machine learning really work?. AI magazine, 18(3), pp.11-11.
[16] Ray, S., 2019, February. A quick review of machine learning algorithms. In 2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 35-39). IEEE.
[17] Bashar, A., 2019. Survey on evolving deep learning neural network architectures. Journal of Artificial Intelligence, 1(02), pp.73-82.
[18] Bui, D.T., Tsangaratos, P., Nguyen, V.T., Van Liem, N. and Trinh, P.T., 2020. Comparing the prediction performance of a Deep Learning Neural Network model with conventional machine learning models in landslide susceptibility assessment. Catena, 188, p.104426.
[19] Schütt, K.T., Gastegger, M., Tkatchenko, A., Müller, K.R. and Maurer, R.J., 2019. Unifying machine learning and quantum chemistry with a deep neural network for molecular wavefunctions. Nature communications, 10(1), pp.1-10.
[20] Mishra, A. and Patti, A., 2021. Deep Convolutional Neural Network Modeling and Laplace Transformation Algorithm for the Analysis of Surface Quality of Friction Stir Welded Joints.
[21] Leo, M., Sharma, S. and Maddulety, K., 2019. Machine learning in banking risk management: A literature review. Risks, 7(1), p.29.
[22] Donepudi, P.K., 2017. AI and machine learning in banking: a systematic literature review. Asian Journal of Applied Science and Engineering, 6(3), pp.157-162.
[23] Patil, P.S. and Dharwadkar, N.V., 2017, February. Analysis of banking data using machine learning. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 876-881). IEEE.
[24] Beutel, J., List, S. and von Schweinitz, G., 2019. Does machine learning help us predict banking crises?. Journal of financial Stability, 45, p.100693.
[25] Donepudi, P.K., 2017. Machine learning and artificial intelligence in banking. Engineering International, 5(2), pp.83-86.
[26] Mirmozaffari, M., Boskabadi, A., Azeem, G., Massah, R., Boskabadi, E., Dolatsara, H.A. and Liravian, A., 2020. Machine learning clustering algorithms based on the DEA optimization approach for banking system in developing countries. European Journal of Engineering and Technology Research, 5(6), pp.651-658.
[27] Mishra, A. and Pathak, T., 2021. Estimation of Grain Size Distribution of Friction Stir Welded Joint by using Machine Learning Approach. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 10(1), pp.99-110.
[28] Mishra, A. and Dixit, D., 2021. Brain Inspired Computing Approach for the Optimization of the Thin Film Thickness of Polystyrene on the Glass Substrates. arXiv preprint arXiv:2107.12156.
[29] Mishra, A., 2020. Local binary pattern for the evaluation of surface quality of dissimilar Friction Stir Welded Ultrafine Grained 1050 and 6061-T6 Aluminium Alloys.
[30] Mishra, A., 2020. Artificial intelligence algorithms for the analysis of mechanical property of friction stir welded joints by using python programming. Welding Technology Review, 92.
[31] Mishra, A., 2020. Discrete wavelet transformation approach for surface defects detection in friction stir welded joints. Fatigue of Aircraft Structures.
[32] Mishra, A. and Morisetty, R., 2022. Determination of the Ultimate Tensile Strength (UTS) of Friction Stir Welded Similar AA6061 Joints by using Supervised Machine Learning based Algorithms. Manufacturing Letters.
[33] Mishra, A., Sefene, E.M. and Tsegaw, A.A., 2021. Process parameter optimization of Friction Stir Welding on 6061AA using Supervised Machine Learning Regression-based Algorithms. arXiv preprint arXiv:2109.00570.
[34] Mishra, A. and Nagpal, K., 2019. Convolutional Neural Network for Image Processing of Friction Stir Welded and Conventional Welded Joints Texture. Int. J. Hum. Comp. Inter. Data Min, 2(1&2), pp.5-9.
[35] Mishra, A., Suman, A. and Dixit, D., 2022. Computer Vision Algorithm for Predicting the Welding Efficiency of Friction Stir Welded Copper Joints from its Microstructures. arXiv preprint arXiv:2203.09479.
[36] Mishra, A. and Pathak, T., 2021. Deep Convolutional Generative Modeling for Artificial Microstructure Development of Aluminum-Silicon Alloy. arXiv preprint arXiv:2109.06635.
[37] E. Eldeeb, M. Shehab and H. Alves, "A Learning-Based Fast Uplink Grant for Massive IoT via Support Vector Machines and Long Short-Term Memory," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3889-3898, 1 March1, 2022, doi: 10.1109/JIOT.2021.3101978.
[38] M. A. Bhatti, R. Riaz, S. S. Rizvi, S. Shokat, F. Riaz and S. J. Kwon, "Outlier detection in indoor localization and Internet of Things (IoT) using machine learning," in Journal of Communications and Networks, vol. 22, no. 3, pp. 236-243, June 2020, doi: 10.1109/JCN.2020.000018.
[39] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.
[40] J. M. Alves, L. M. Honório and M. A. M. Capretz, "ML4IoT: A Framework to Orchestrate Machine Learning Workflows on Internet of Things Data," in IEEE Access, vol. 7, pp. 152953-152967, 2019, doi: 10.1109/ACCESS.2019.2948160.
[41] S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network," in IEEE Access, vol. 8, pp. 89337-89350, 2020, doi: 10.1109/ACCESS.2020.2994079.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY