International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
Article Received: *25 November 2023* ***Revised:*** *12 December 2023* ***Accepted:*** *30 January 2024*

A Review: Internet of Things with Machine Learning to Develop Intelligent Systems

[1]Vibhor Sharma, [2]Deepak Srivastava, [3]Vinay Avasthi
[1,2,3]Department of Computer Science & Engineering, Himalayan School of Science & Technology, Swami Rama Himalayan University, Dehradun, Uttarakhand, India

Abstract- A fresh era of internet-connected sensing gadgets that bridge the gap between the real and virtual worlds has begun, thanks to the rapid advancements in hardware, software, and communication technologies. About twenty-five and fifty billion internet-enabled gadgets are predicted to be in use worldwide. The term "Internet of Things" is a term used to signify a system of electrical devices that communicate with one another. There is a wide variety of infrastructure, retail, transit, and individual healthcare services and applications made possible by the Internet of Things. IoT is a driving force behind the evolution of the Internet and other forms of modern communication technology. Smart computation and evaluation of massive data are crucial to the growth of Internet of Things applications. IoT applications may benefit from data science tools by discovering new patterns and insights in data. Industry applications of data science with the Internet of Things focus on volume, velocity, and pattern identification. With the help of machine learning's predictive analysis, programs can now anticipate both welcome and unwanted occurrences. Thus, machine learning systems not only identify out-of-the-ordinary conduct but also aid in deducing and predicting broader societal tendencies. Continuing modification and monitoring is necessary for efficacy and effectiveness in data analysis. There are two sections to this article: the first discusses the many uses of the Internet of Things where machine learning plays a role in creating an intelligent system, while the second looks ahead to the potential of IoT and machine learning in the advancement of communication devices. Questions such as "What is the classification of artificial intelligence that can be implemented in IoT?" and "How could machine intelligence be implemented in IoT applications?" will be answered in this article.

Keywords: Machine Learning, Artificial Intelligence, Data Analytics, Internet of Things, Data science.

INTRODUCTION

The Internet of Things (IoT) is the interconnection and use of electronic devices, software, and connections to networks to create a network of physical things endowed with limited computational, storage, and ability to communicate. Authors in [1], described IOT as an integrated and dispersed network that consists of integrated system of interacting via wireless or wired means of communication. Problems may arise in areas like storage, connectivity, and privacy when dealing with devices connected to an IoT network. The extensive study of IoT's architecture, connectivity, computing, security, and privacy was covered in [2].

IoT devices create vast quantity of data which may be utilized further trends, forecasts and assessments. This information opens a new front in the data processing system. To extract value from data produced by IoT devices, a new technique is needed. Machine learning (ML) is the most applicable computing paradigm. With the help of machine learning, IoT devices can learn on the fly and infer information from the data they collect. Machine learning improves smart devices' capacity to adapt to new circumstances or automate previously manual behaviors. Classification, regression analysis, and estimation of density are all possible using ML. Smart services, including fraud detection, virus detection, and voice recognition, may be provided by using ML methods and algorithms in IoT-based systems [3].

PROBLEMS WITH INTERNET OF THINGS SECURITY

- The Internet of Things has considerable sway because it adds a new layer to the online universe. The security and privacy of IoT services and applications are major concerns. Architectural privacy, information safety, communication security, virus analysis, and so on may all play a role in protecting an Internet of Things device. The authors in [4], compared and contrasted the security concerns of IoT and conventional IT systems. They identified software, hardware, networks, and applications as the most often cited motivators. The problems of security and privacy in the IoT can only be solved by employing a cross-layer architecture and an optimized algorithm. To further address security and privacy concerns, a novel class of encryption and other

algorithms may need to be developed for IoT devices. However, as the variety of IoT devices proliferates, so too may the complexity of their security mechanisms. When compared to the state of the art, a comprehensive approach to security and privacy is highly valued. To manage difficulties and vulnerabilities in IoT applications, this fresh strategy is going to offer new intelligent, resilient, adaptive and scalable mechanisms.

- Machine learning (ML) is one of these smart approaches that finds the best answer by learning from examples. Mathematical modelling (ML) use mathematical methods to simulate behavior. ML may also enable devices with sensors to learn without usage of explicitly programmed. Because of its interdisciplinary nature, ML may draw on several fields, such as AI, OT, and CS. In areas like robots, speech recognition, and real-world problems, where human knowledge is not applicable, this property makes ML invaluable. It delivers the answer to IoT wherein the solution for a particular issue varies in time. Despite its overall dependability, the ML approach has to be guided and tweaked so that it doesn't create false positives and genuine negatives. Deep Learning (DL), a more advanced form of ML, helps to solve this problem by automatically estimating the reliability of a prediction. Both [5, 6] concluded that DL's self-service nature makes it ideally suited for forecasting and categorizing tasks in cutting-edge IoT applications.

- The data generated by an IoT network is enormous and may be put to good use in ML and DL applications. Numerous studies have shown that both of these may be utilized in networks of the Internet of Things for study of security, identification and avoidance of attacks, and analysis of malware. Authors in [7], explored the difficulties of deploying such models on low-powered IoT devices. These difficulties arise because it is crucial to lessen the burden of processing and storage on IoT gadgets. Due to their limited resources, IoT devices cannot employ complex security mechanisms to protect themselves from cybercriminals. The assault surface is further enlarged by the widespread use of many technologies. Zigbee, LoRaWAN, z-Wave, and Near Field Communication are only few of the communication protocols used by IoT devices. Security-wise, these communication systems have limits, as authors in [8] pointed out. In addition to the aforementioned difficulties, the Internet of Things (IoT) also faces issues with scalability, complexities, addressing, for instance and inadequate resource utilizations [9, 10].

LITERATURE REVIEW

- The security of the Internet of Things can benefit from the application of a wide range of machine learning algorithms. When a known outcome is desired from a known set of inputs, supervised learning is employed. It is done when both the nature of the input data and the final result are understood in advance. It may be utilized for spectral sense, multichannel calculation, dynamic filtration, and privacy and location challenges. The environment alone serves as input for unsupervised learning, therefore labelled data is unnecessary. Anomaly, fault, and detection of breaches, cell clustering, and load balancing are all areas where it finds use. Where there are no predetermined results, agents can use RL to pick up knowledge via trial and error as they interact with their surroundings and provide feedback. Data analysis is the primary emphasis of both supervised and unsupervised methods, whereas comparability and decision making challenges are best tackled using reinforcement learning approaches. It's employed in the training process, when the computer has to figure out how to make sense of unstructured input. Where labels are missing from many observations, learning that is semi-supervised, a hybrid of supervised and unsupervised methods, can be used to fill in the gaps. Deep learning is best suited for massive amounts of unlabeled, uncategorized, and unsupervised data that need distributed computation, learning, and analysis.

- Since DL is based on ANN, the weights between all pairs of neurons are adjusted iteratively during the learning process [11]. Speech recognition, computer vision, and natural language processing are only few of the ML applications that can benefit from DL's enhanced categorization models, as mentioned by [12]. It solves protection and confidentiality issues associated with IoT by using polynomial approximations, estimate, and learning capabilities. IoT devices have resource limited hence might not be competent to handle complicated computing method. Therefore, DL algorithms outperform more traditional theories and methods while being more efficient in terms of delay and complexities.

- It has been shown that traditional RL is insufficient, and that a hybrid of DL and RL is necessary for determining the optimal policy and action quality for every given situation [13]. There are positive outcomes for both RL and DL. A recent study shown that DL, despite its ability to learn from complicated patterns, is vulnerable to mis-classification. DRL, as proposed by [14], is a hybrid of RL and DL that brings together RL's decision-making

with DL's perceptual abilities. Google's "AlphaGo" programme, which was built with the help of DRL, was described in detail by [15]. The DRL technique is commonly employed in IoT network security and DDOS detection. Authors in [16] offer a technique for adaptive IoT water labelling to detect cyber assaults.

- Data communication between systems is the backbone of many IoT applications. Information obtained from Internet of Things apps is sent into a decision-support system for analysis. These operations receive the same data flow, but their implementation may vary according to the design of the IoT. User or application authentication is necessary whenever data is requested by any user. A request for access will be denied if authentication is not provided. It is also quite difficult to implement network access restrictions. In the Internet of Things, an ML-based authentication and authorization mechanism is used to selectively give and deny access to vital data sets.

CONSTRAINTS OF MACHINERY LEARNING IN THE IoT

However, ML algorithms are not yet effective enough to deal with the substantial modifications necessitated by the inherent uncertainties in IoT data [17]. As a result, there are also certain constraints connected with employing ML in the IoT. Methodology of machine learning includes concerns with memories, and complexity in computation. Due to their inability to scale, ML methods can only be used to problems with low dimensionality. Since ML requires a continuous inflow of data in order to function, it is not always a good fit for intelligent IoT devices that must analyse data in real time. Authors in [18] explained how the more data there is, the less accurate the algorithm becomes. Data from an IoT network exhibits morphological and semantic variability due to differences in semantics and structure [19]. Since ML algorithms are not well-suited for working with semantic and syntactically diverse data, they run into difficulties in applications that operate in real-time where information collected from various sources has been formatted and represented in different ways. Combining an ML algorithm with an already streaming solution increases the method's total complexity [20].

IMPLICATIONS OF IOT AND ML FOR THE FUTURE

Machine learning propels AI forward. The key advantages of adopting ML technology are intuitive learning, and decision trees for core administration and data collecting.ML algorithms are used in every data science-based application there is, including data mining, IR systems, search engines, and large data analysis. It also aids in the search for object recognition software in computer vision [21]. The Internet of Things (IoT) is now the most common and cutting-edge usage of ML. Many academics gave the survey of utilizing IoT with ML in diverse applications and services. IoT and its applications in civil engineering were surveyed in a recent paper by [22]. Using data mining techniques, Authors in [23] conducted a survey of IoT in cyber security systems. The majority of the already suggested solutions are primarily concerned with technical aspects rather than user requirements. Although ML provides users with technology benefits that make their lives easier, it also poses several serious concerns. Scalability, affordability, battery life of sensors that are handling of many sensors, time elapse, and many other difficulties will need to be addressed in the future of ML combined with IoT.

CONCLUSION

ML approaches are being utilized for rendering IoT devices and apps more sophisticated and intelligent. Enhanced processing power and the incorporation of numerous technical discoveries have made this possible, and it aids in lowering computational costs. Models for designing, testing, and training data sets are all products of ML. Although ML algorithms are useful for pattern and similarity detection, a major drawback is that they often require a training dataset before being applied to real data. DL is employed in the business world since it helps to overcome ML's shortcomings. Examples of DL algorithms include the virtual assistants Siri (Apple), Cortana (Microsoft), Alexa (Amazon), and Google Photos (Google). To learn automatic extraction from massive volumes of high-dimensional, unsupervised data, DL, RL, and DRL have emerged as the leading study areas. Although ML and DL are commonly believed to be effective prediction and classification algorithms, they may not be able to meet all of the needs of an IoT network.

REFERENCES

[1] Arora, Jyoti Batra, IoT and Machine Learning - A Technological Combination for Smart Application (February 21, 2020). Proceedings of the 4th International Conference: Innovative Advancement in Engineering & Technology (IAET) 2020, Available at
SSRN: https://ssrn.com/abstract=3548431 or http://dx.doi.org/10.2139/ssrn.3548431

[2] S. K. Jagatheesaperumal, Q. -V. Pham, R. Ruby, Z. Yang, C. Xu and Z. Zhang, "Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions," in IEEE Open Journal of the Communications Society, vol. 3, pp. 2106-2136, 2022, doi: 10.1109/OJCOMS.2022.3215676.

[3] Alsharif MH, Kelechi AH, Yahya K, Chaudhry SA. Machine Learning Algorithms for Smart Data Analysis in Internet of Things Environment: Taxonomies and Research Trends. Symmetry. 2020; 12(1):88. https://doi.org/10.3390/sym12010088

[4] V. Visoottiviseth, P. Sakarin, J. Thongwilai, and T. Choobanjong, "Signature-based and Behavior-Based Attack Detection with Machine Learning for Home IoT Devices," in Proceedings of the 2020 IEEE REGION 10 CONFERENCE (TENCON), pp. 829–834, IEEE, Osaka, Japan, 2020.

[5] Ullah, A., Anwar, S.M., Li, J. et al. Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex Intell. Syst. (2023). https://doi.org/10.1007/s40747-023-01175-4

[6] Xiaocong Chen, Lina Yao, Julian McAuley, Guanglin Zhou, Xianzhi Wang, Deep reinforcement learning in recommender systems: A survey and new perspectives, Knowledge-Based Systems, Volume 264,2023,110335,ISSN 0950-7051,https://doi.org/10.1016/j.knosys.2023.110335.

[7] Chen, Xiaocong, et al. "Knowledge-guided deep reinforcement learning for interactive recommendation." 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020.

[8] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, Ioanna Kantzavelou,IoT: Communication protocols and security threats,Internet of Things and Cyber-Physical Systems,Volume 3,2023,Pages 1-13,ISSN 2667-3452,https://doi.org/10.1016/j.iotcps.2022.12.003.

[9] Saeed Javanmardi, Mohammad Shojafar, Reza Mohammadi, Mamoun Alazab, Antonio M. Caruso,An SDN perspective IoT-Fog security: A survey,Computer Networks,Volume 229,2023,109732,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2023.109732.

[10] Rehmat Ullah, Muhammad Atif Ur Rehman, Muhammad Ali Naeem, Byung-Seo Kim, Spyridon Mastorakis,ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks,Future Generation Computer Systems,Volume 111,2020,Pages 159-174,ISSN 0167-739X,https://doi.org/10.1016/j.future.2020.04.033.

[11] Zhang S, Li Y, Zhang S, Shahabi F, Xia S, Deng Y, Alshurafa N. Deep Learning in Human Activity Recognition with Wearable Sensors: A Review on Advances. *Sensors*. 2022; 22(4):1476. https://doi.org/10.3390/s22041476

[12] Siqi Liu, Tianyu Wang, Shaowei Wang,Toward intelligent wireless communications: Deep learning - based physical layer technologies,Digital Communications and Networks,Volume 7, Issue 4,2021,Pages 589-597,ISSN 2352-8648,https://doi.org/10.1016/j.dcan.2021.09.014.

[13] O'shea, T., & Hoydis, J. (2017). An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4), 563-575.

[14] Rajendran, S., Meert, W., Giustiniano, D., Lenders, V., & Pollin, S. (2018). Deep learning models for wireless signal classification with distributed low-cost spectrum sensors. IEEE Transactions on Cognitive Communications and Networking, 4(3), 433-445.

[15] Kang, J. M., Chun, C. J., & Kim, I. M. (2018). Deep-learning-based channel estimation for wireless energy transfer. IEEE Communications Letters, 22(11), 2310-2313.

[16] Ye, H., Gao, F., Qian, J., Wang, H., & Li, G. Y. (2020). Deep learning-based denoise network for CSI feedback in FDD massive MIMO systems. IEEE Communications Letters, 24(8), 1742-1746.

[17] Li, W., Chai, Y., Khan, F. et al. A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System. Mobile Netw Appl 26, 234–252 (2021). https://doi.org/10.1007/s11036-020-01700-6

[18] S. Athmaja, M. Hanumanthappa and V. Kavitha, "A survey of machine learning algorithms for big data analytics," *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore,

India, 2017, pp. 1-4, doi: 10.1109/ICIIECS.2017.8276028.

[19] Bogale, Tadilo Endeshaw & Wang, Xianbin & Le, Long. (2017). Machine Intelligence Techniques for Next-Generation Context-Aware Wireless Networks. ITU (To appear). 1. 10.

[20] Jingjing Yan, Jing Tian, Hong Yang, Gangfei Han, Yanling Liu, Hangzhi He, Qinghua Han, Yanbo Zhang,A clinical decision support system for predicting coronary artery stenosis in patients with suspected coronary heart disease,Computers in Biology and Medicine,Volume 151, Part A,2022,106300,ISSN 0010-4825,https://doi.org/10.1016/j.compbiomed.2022.106300.

[21] Ayodeji Olalekan Salau, Thomas Kokumo Yesufu, Babatunde Sunday Ogundare,Vehicle plate number localization using a modified GrabCut algorithm,Journal of King Saud University - Computer and Information Sciences,Volume 33, Issue 4,2021,Pages 399-407,ISSN 1319-1578,https://doi.org/10.1016/j.jksuci.2019.01.011.

[22] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile- internet of things (M-IoT): a survey," IEEE Access, vol. 8, pp. 167123–167163, 2020.

[23] Buczak, Anna & Guven, Erhan. (2015). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. 18. 1-1. 10.1109/COMST.2015.2494502.