International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 247-251 www.ijaem.net ISSN: 2395-5252

"Machine learning Technique for Internet of Things: A Review"

Pragya, Mr. Nitesh Gupta, Mr. Anurag Srivastava
MTech Scholar Department of CSE NIIST Bhopal
Associate Professor Department of CSE NIIST Bhopal
HOD Department of CSE NIIST Bhopal

Date of Submission: 10-10-2020 Date of Acceptance: 27-10-2020

ABSTRACT—Internet of Things (IoT) combines hundreds of millions of devices which are capable of interaction with each other with minimum user interaction. Now internet of things is become the fastest-growing areas of computing with rapid developments in communication technologieshave allowed the Internet-connected sensory devices that provideobservation and data measurement from the physical world. Internet-connected devices being used willbe increased rapidly. In addition to increased volume, the IoT generates Big Datacharacterized by velocity in terms of time and location dependency.This paper assesses the machine learning techniques that deal with the challenges in IoT. Paper also reviews the machine learningalgorithms and its application in IOT.

Keywords—Internet of Things (IOT), Classification, Machine Learning

I. INTRODUCTION

IoT is an umbrella term that covers all the devices over the internet which has ability to transfer the data. The Internet of Things (IoT) [3] is a network of sensing devices with limited resources and capable of wired/wireless communications with cloud services. There are numerous applications from smart device to smart industries. Smart home is popular application in which all appliances in home can be controlled and managed by smart devices for instance smart air conditioner can be switched on/off from any place, one can surveillance on their house by camera from remote location over internet and many more. There is a prediction statement by CISCO which state that there will be over 50 billion connected devices by 2020 [1]. In Health care many devices are being proposed for monitor human health, they detect condition of patient and send collected data. With the help of IOT nodes a city can be facilitate from traffic control to water distribution. Wearable devices, smart grid, industrial internet, connected car, smart farming are few more popular applications of IOT now a days.

This paper aims to review the machine learning techniques which is used by the Internet of Things. This paper will help the researchers to know about the concept of machine learning and IOT with its technology and application in detail. Research in this area has recently gained lots of attention, of course lots of money, and is supported by the collaboration from academia, industry, and standardization bodies in several communities such as telecommunication, health insurance companies, semantic Web, and informatics. This leads to lots of venture capitals go with the tide.

IoT Components:

IoT components primarily include the following: Sensor- It is physical entity which senses the environment data, e.g - temperature, air speed, humidity, movements. Actuator – it is responsible of movement in device when it get any control signal. For instance rotate the CCTV Camera in any direction. Network – IoT objects are tied up with networks by various wireless standards. 802.15 standard are using for wearable device, Zigbee or 802.11 used for home automation. Power efficient network standards have preferred mostly. User – people control the object via some user interface. User interface application provides facility to people to interact with devices. [2]

IoT devices cannot support complex security structures given their limited computation and power resources. Complex security structures of the IoT are due to not only limited computation, communication and power resources but also trustworthy interaction with a physical domain, particularly the behavior of a physical environment in unanticipated and unpredictable modes, because the IoT system is also part of a cyber-physical system; autonomously, IoT systems must constantly adapt and survive in a precise and

predictable manner with safety as a key priority, particularly in settings where threatening conditions, such as in health systems, might occur. Moreover, new attack surfaces are introduced by the IoT environment. Such attack surfaces are caused by the interdependent and interconnected environments of the IoT. Consequently, the security is at higher risk in IoT systems than in other computing systems, and the traditional solution may be ineffective for such systems. IoT systems are accessible worldwide, consist mainly of Constrained resources and constructed by lossy links. Therefore, crucial modifications of existing security concepts for information and wireless networks should be implemented to provide effective IoT security methods.

The rest of this paper is organized as follows. Related articles in thisfield are reviewed and reported in Section2. Overview of the machine learning, its type and machine learning algorithms are discussed in section 3. Section 4 concludes the paper.

1. Literature Review

In view of the fact that IoT represents a new concept for the Internet and smart data, itis a challenging area in thefield of computer science. The importantchallenges for researchers with respect to IoT consist of preparing andprocessing data and discovering knowledge.

In this research paper [2] the authors have used machine learning techniques, approaches or methods for securing things in IOT environment. This paper attempts to review the related research on machine learning approaches to secure IOT devices.

In this research [4] the various machine learningmethods that deal with the challenges presented by IOT data by considering smart cities as the main use case. Thekey contribution of this study is the presentation of taxonomy of machine learning algorithms explaining howdifferent techniques are applied to the data in order to extract higher level information. The potential andchallenges of machine learning for IOT data analytics will also be discussed. A use case of applying a SupportVector Machine (SVM) to Aarhus smart city traffic data is presented for a more detailed exploration.

In this research paper [5] authorsaims to provide a brief overview of machine learning methods for internet of things (IOT). Authors present some of the applications of machine learning in IOT and have tried to provide an overview of the types of ML, ML task and its applications as related to IoT. In conclusion, it is needful to mention that ML provides higher precision in calculations and for prediction, it is highly effective and is able to look at a lot of information in smaller interims of time.

In the research paper [8] authors review ML/DLmethods for IoT security and present the opportunities,advantages and shortcomings of each method. Authors discuss theopportunities and challenges involved in applying ML/DL to IoTsecurity. These opportunities and challenges can serve as potentialfuture research directions.

This research paper [9] addresses the comparison of severalfrequently used ML classifiers from the group of SVMlike classifiers, namely SMO and C-SMV algorithm, and arange of ensemble algorithms on the other side, namelyLADTree, REPTree, RF and MultiBoost. The analysis isbased on a range of testing procedures in Weka, with agoal to estimate a set of selected performance metrics andmake classifier comparison. As the analysed UNSWNB15dataset belongs to a unbalanced dataset category,for the proper examination of the classifiers we haveassumed the need for calculating the precision, recall,ROC and necessary time for classification.

2. Machine learning

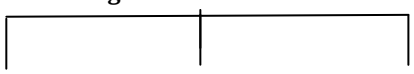
Machine learning is a type of artificial intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can teach themselves to grow and change when exposed to new data. Machine learning techniques have ability to implement a system that can learn from data. For example, a machine learning system could be trained on incoming packets to learn to distinguish between intrusive and normal packet. After learning, it can then be used to classify new incoming packets into intrusive and normal packets. In machine learning, computer algorithms (learners) attempt to automatically distill knowledge from example data. This knowledge can be used to make predictions about novel data in the future and to provide insight into the nature of the target concepts applied to the research at hand, this means that a computer would learn to classify alerts into incidents and non-incidents task. A possible performance measure (P) for this task would be the Accuracy with which the machine learning program classifies the instances correctly. Machine learning often included in the category of predictive analytics as it helps to predict the future analysis.

ML mainlydivided into three categories. Supervised and unsupervised arewidely used

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 247-251 www.ijaem.net ISSN: 2395-5252

categories. In supervised machine algorithm,training data has input and its corresponding output.Unsupervised machine learning, we do not have any output.In reinforcement machine learning a software agentautomatic take action to maximize the performance or award. For active learning type, a PC can simply get information for a confined game plan of cases. Exactly when used instinctively, this information can be shown to the customer.

Machine Learning



Supervised Unsupervised Reinforcement

Figure 1: Types of Machine Learning

Machine Learning Algorithms:-

K-NN Algorithms: K-Nearest Neighbors (K-NN)

K nearest neighbors is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure (e.g., distance functions). KNN has been used in statistical estimation and pattern recognition already in the beginning of 1970's as a non-parametric technique. KNN is a non parametric lazy learning algorithm. The k-Nearest Neighbor algorithm is based on learning by analogy. The k-nearest neighbor algorithm is amongst the simplest of all machine learning algorithms.

Genetic Algorithm: Genetic Algorithms, first proposed by Holland in 1975, are a class of computational models that mimic natural evolution to solve problems in wide variety of domains. Genetic algorithms are particularly it is suitable for solving complex optimization problems and for applications that require adaptive problem-solving strategies .It is based on the mechanics of natural genetics, ie.,operations existing in nature. A genetic algorithm operates on a set of individual elements (the population) and there is a set of biologically inspired operators that can change these individuals .In computing terms, genetic algorithms map strings of numbers to each potential solution .Each solution becomes an individual in the population ,and each string becomes a representation of an individual. There should be a way to derive each individual from its string representation. The genetic algorithm then manipulates the most promising string in its search for an improved solution. The algorithm operates through a simple cycle:Creation of a population of strings, Evaluation of each string, Selection of the best strings, Genetic manipulation to create a new population of strings.

Decision Tree:-

A decision tree is a classification scheme which generates a tree and a set of rules, representing the model of deferent classes, from a given data set. The set of records available for developing classification methods is generally divided into two disjoint subsets –a training set and a test set. Attributes whose domain is numerical are called the numerical attributes, and the attributes whose domain is not numerical are called the categorical attributes. There is one distinguished attribute called the class label.

IOT Applications:

IoT has several applications. The commonly knownapplications include smart healthcare, smart transportation,smart grid and smart building. These applications are brieflydiscussed in the following subsections.

Smart healthcare: IoT devices have become popular in health applications inrecent years. IoT devices are used in healthcaresectors to closely observe and record patient conditions andsend warnings to the concerned healthcare system in criticalcircumstances to provide a rapid and timely treatment topatients.

Smart transportation: Smart or intelligent transport systems have become attainable with the help of IoT systems. The main objective of smart transport is to manage daily traffic in cities intelligently byanalyzing data from well-connected sensors located in different places and implementing data fusion (data from CCTV, mobile devices, GPS, accelerometers, gyroscope-based applicationsand weather sensors).

Smart governance:

IoT can facilitate smart governance. Integrating data fromdifferent governmental sectors can provide authorities withabundant information from a wide range of sensor data (from weather-related data to security-related data).

Smart agriculture

IoT systems can be applied to improve the agriculture sector.IoT sensors can be implemented to enable real-time monitoringof the agriculture sector. IoT sensors can collect useful data onhumidity level, temperature level, weather conditions andmoisture level.The collected data can then be analyzed toprovide important real-time mechanisms, such as automaticirrigation, water quality monitoring, soil constituent monitoringand disease and pest monitoring.

Smart homes

IoT components are used to realize smart homes. Home IoTbasedmachines and systems (e.g. fridge, TV, doors, airconditioner, heating systems and so on) are now easy to observeand control remotely [28, 57]. A smart home system canunderstand and respond to surrounding changes, such asautomatically switching on air conditioners based on weatherpredictions and opening the door based on face recognition.

Smart supply chain

An important application of IoT technology in real life is thedevelopment of easier and more flexible business processesthan before. The development in IoT-embedded sensors, suchas RFID and NFCE, enables the interaction between IoTsensors embedded on the products and business supervisors.Therefore, these goods can be tracked throughout productionand transportation processes until they reach the consumer.

II. CONCLUSION

The main focus of machine learning (ML) technique is to outline more productive in terms of time and space learning strategies that can perform better in various applications to save time and cost. In this paper, we have tried to provide areview of the types of ML, ML task and its applications as related to IoT. It is needful to mention that ML provides higher precision in calculations and for prediction, it is highly effective and is able to look at a lot of information in smaller interims of time. This paper will helpful for the researchers who want to explorer the machine learning technology and ML algorithms with its application in real world. This paper also helpful for the understand the concept of internet of things.

REFERENCES

[1]. D. Evans, "The Internet of Things How the Next Evolution of the Internet is Changing Everything," CISCO, 2011.

[2]. AmitSagu, Nasib Singh Gill “Securing IoT Environment using Machine Learning Techniques” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-3, February, 2020

[3]. Chao Liang1, Bharanidharan Shanmugam1, Sami Azam1, Mirjam Jonkman1, Friso De Boer1, Ganthan Narayansamy2 "Intrusion Detection System for Internet of Things based on a Machine Learning approach" 978-1-5386-9353-7/19/$31.00 ©2019 IEEE

[4]. YueXu “Recent Machine Learning Applications to Internet of Things (IoT)” Recent Machine Learning Applications to Internet of Things (IoT) Recent Machine Learning Applications to Internet of Things (IoT)

[5]. Mohammad Saeid Mahdavinejad Mohammadreza Rezvan Mohammadamin Barekatain Peyman AdibiPayam Barnaghi Amit P. Sheth[1,2][3][4] “Machine learning for internet of things data analysis: a survey” http:// www.keaipublishing.com/en/journals/digital-communications-and-networks/

[6]. Arun Kumar Rana1, AyodejiOlalekan Salau2, Swati Gupta3, Sandeep Arora4 “A Survey of Machine Learning Methods for IoT and their Future Applications”

[7]. Amity Journal of Computational Sciences (AJCS) Volume 2 Issue 2 ISSN: 2456-6616 (Online)

[8]. Fei Wu, Limin Xiao, Jinbin Zhu "Bayesian Model Updating Method Based Android Malware Detection for IoT Services " 978-1-5386-7747-6/19/$31.00 ©2019 IEEE

[9]. Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani “A Survey of machine and deep learning methods for internet of things (IoT) Security”

[10]. ValentinaTimcenko, SlavkoGajin "Machine learning based network anomaly detection for IoT environments" ieee explorer

[11]. Jadel Alsamiri1, Khalid Alsubhi2 "Internet of Things Cyber Attacks Detection using Machine Learning" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, 2019

[12]. GiampaoloCasolla,SalvatoreCuomo,VincenzoSchiano di Cola , and Francesco Piccialli "Exploring Unsupervised Learning Techniques for the Internet of Things " 1551-3203 © 2019 IEEE

[13]. YU-XIN MENG “The Practice on Using Machine Learning For Network Anomaly Intrusion Detection” 2011 IEEE

[14]. Chi Cheng, Wee PengTay and Guang-Bin Huang “Extreme Learning Machines for Intrusion Detection” - WCCI 2012 IEEE World Congress on Computational Intelligence June, 10-15, 2012 - Brisbane, Australia

[15]. NaeemSeliya, Taghi M. Khoshgoftaar “Active Learning with Neural Networks for Intrusion Detection” IEEE IRI 2010, August

4-6, 2010, Las Vegas, Nevada, USA 978-1-4244-8099-9/10/$26.00 ©2010 IEEE

[16]. Kamarularifin Abd Jalill, Mohamad Noorman Masrek "Comparison of Machine Learning Algorithms Performance in Detecting Network Intrusion" 201O International Conference on Networking and Information Technology 978-1-4244-7578-0/$26.00 © 2010 IEEE

[17]. Shingo Mabu, Member, IEEE, Ci Chen, Nannan Lu, Kaoru Shimada, and Kotaro Hirasawa, Member, IEEE "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming" IEEE, JANUARY 2011

[18]. Liu Hui, CAO Yonghui "Research Intrusion Detection Techniques from the Perspective of Machine Learning" - 2010 Second International Conference on MultiMedia and Information Technology 978-0-7695-4008-5/10 $26.00 © 2010 IEEE

[19]. Jingbo Yuan , Haixiao Li, Shunli Ding , Limin Cao "Intrusion Detection Model based on Improved Support Vector Machine" Third International Symposium on Intelligent Information Technology and Security Informatics 978-0-7695-4020-7/10 $26.00 © 2010 IEEE

[20]. Maria Muntean, HonoriuVălean, LiviuMiclea, Arpad Incze "A Novel Intrusion Detection Method Based on Support Vector Machines" IEEE 2010.

[21]. W. Yassin, Z. Muda, M.N. Sulaiman, N.I.Udzir, "Intrusion Detection based on K-Means Clustering and One R Classification" IEEE 2011.

[22]. MohammadrezaEktefa, Sara Memar, Fatimah Sidi, Lilly SurianiAffendey "Intrusion Detection Using Data Mining Techniques" IEEE 2010.

[23]. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php

[24]. Hanwen Wang,Biao Han, Jinshu Su," Biao Han, Jinshu S" 978-1-5386-9380-3/18/$31.00 ©2018 IEEE

[25]. IbraheemAljamal, Ali Tekeoglu Korkut Bekiroglu, Sangupta "Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environment" 978-1-7281-0798-1/19/$31.00 ©2019 IEEE SERA 2019, May 29-31, 2019, Honolulu, Hawai