Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 10, October 2020, pg.40 – 44

A Survey of Machine Learning for IoT Networks

Dr. R. Thamaraiselvi[1]; S. Anitha Selva Mary[2]

[1]Head, Department of Computer Applications, Bishop Heber College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India

[2]Department of Computer Applications, Bishop Heber College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India

[1] thams.shakthi@gmail.com; [2] anitavk1995@gmail.com

DOI: 10.47760/IJCSMC.2020.v09i10.006

Abstract— In practice applications like Security Systems, intelligent infrastructure, traffic management and weather systems (among others), internet of things (IoT) is becoming more and more popular. Recently, the Internet of Things (IoT) has become more common because the number of intelligent devices used in everyday human life with minimal network life. The transfer of routing information plays a major role in providing communication between nodes. The IoT produces big data in addition to its increased volume, with a variety of multiple modalities and differing data quality, distinguished by its time and position dependence. Intelligent data processing and analysis are the main elements for the creation of intelligent IoT applications. This paper focuses on IoT network security aspects by exploring the serviceability of machine learning algorithms to identify anomalies in data from these networks. Taxonomy of machine learning algorithms is introduced to illustrate how various methods are applied to the data in order to obtain higher level knowledge. There will also be discussions on the ability and problems of Machine Learning for IoT data processing.

Keywords— Internet of Thinks (IoT), Machine learning, Security Systems

I. INTRODUCTION

Internet of Things (IoT) constitutes a network of heterogeneous devices communicating and exchanging data amongst themselves to provide smarter services to users. The Internet of Things (IoT) is a worldview that has improved better notoriety as of late. At a calculated level, IoT alludes to the interconnectivity among our regular devices, for example, PCs, workstations, tablets, advanced cells, PDAs, and other hand-held installed devices as appeared in fig.1. These devices currently convey sagaciously to each other. Besides, associated devices furnished with sensors or potentially actuators see their environment, comprehend what is happening, and perform likewise. These interconnected gadget systems can prompt an expansive number of clever and self-ruling applications and services that can bring critical individual, professional, and monetary advantages bringing about the rise of more information driven organizations [1][2].

IoT devices need to make their information available to invested individuals, which can be web services, advanced mobile phone, cloud asset, and so forth. Subsequently, IoT can't be viewed as individual frameworks, yet as a basic, incorporated foundation whereupon numerous applications and services can run. A few applications will be customized, for example, digitizing day by day life exercises, others will be citywide, for example, proficient, sans delay transportation, and others will be overall, for example, worldwide conveyance frameworks. The objective of the Internet of Things is to empower things to be associated whenever, wherever,

with anything and anybody in a perfect world utilizing any way/arrange and any service. Internet of Things is another upset of the Internet. Items make themselves unmistakable and they acquire insight by settling on or empowering setting related choices because of the way that they can impart data about themselves and they can get to data that has-been collected by different things, or they can be parts of complex services.

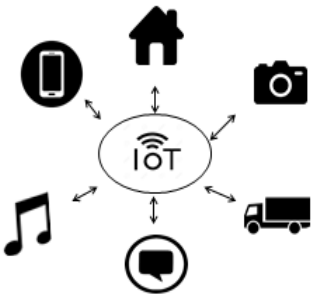

Figure 1. Various platforms connected with IoT

Similarly, IoT has improved the lifestyle of individuals by introducing automated services. However, such an uncontrolled explosion has increased privacy and security challenges. The unconscious use, not changing passwords, and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems' sensitive data. Such inappropriate security practices increase the chances of a data breach and other threats. Most of the security professionals consider IoT as the vulnerable point for cyber-attacks due to weak security protocols and policies. While many protection protocols have been established to defend IoT devices from cyber-attacks, safety standards are not well recorded. [2]. Thereby, end-users could not apply protective measures to avert data attacks. Hackers developed different kinds of malware to infect the IoT devices since the eve of 2008. They designed various phishing techniques to provoke the employees or individuals to share sensitive data [3]. Therefore, corporate workstations and personal devices often face privacy violations due to high-profile attacks. If device manufacturers and security experts assess the cyber threats accurately, they can develop an efficient protective mechanism to prevent or neutralize cyber threats.

IoT enabled devices have been used in industrial applications and for multiple business purposes [4]. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

Every day new technologies emerge, or changes are made to existing ones. Consider the latest advances in the 5G network, for example. 5G is expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions.

II. TAXONOMY OF MACHINE LEARING ALGORITHMS

Machine learning is a computer science sub-field and is a form of intelligence (AI) that enables computers to learn without explicit programming. Machine learning has developed from understanding of patterns and theory in computer education. Some basic concepts of machine learning and the commonly used machine learning algorithms for intelligent data analysis are discussed here. An algorithm for learning takes a set of samples as an input called a training set. Overall, there are three primary learning categories: supervised, unsupervised, and reinforced. In an informal sense, the training set for supervised learning consists of samples of input vectors along with their respective target vectors, also known as marks. No labels are required for training set in

unsupervised learning. Supervised learning transactions with the problem of learning the superlative action or series of actions to be taken to maximize payoff for a given scenario. This paper is based on supervised and unsupervised learning as it has been widely used in IoT intelligent data analysis and still applies. Supervised learning is aimed at learning how to predict the appropriate output vector for a given input vector. Classification activities are called applications in which the target labels consist of a small number of distinct categories. Cases where one or more continuous variables consist of a target mark are called regression functions.

It is difficult to describe the target of unsupervised learning. One of the key aims is to identify significant clusters of such samples, called clustering, within the input data. Furthermore, the target should be that the input data can be found internally in a helpful way by preprocessing the original input variable to move the data into a new variable space. The machine-learning algorithm will greatly boost the outcome of this preprocessing step and is called feature extraction.

The rest of the current paper is organized four parts. The second part presents a Machine learning algorithm in groups based on recent studies on IoT data and machine learning algorithms are studied and summarized the third is devoted for the discussion of metrics and Demetris, and the last part is for the conclusion together with future research trends and open issues are presented in.

III. RELATED WORK

Lo'ai Tawalbeh et al. [5] suggested a new IoT-layered model: generic and expanded with the identification of privacy, protection components and layers. Implementation and evaluation of the proposed IoT framework assisted by cloud/edge. The lower layer of the IoT nodes created as virtual machines from the Amazon Web Service (AWS). The middle layer (edge) was introduced with the Greengrass Edge System in the AWS as a Raspberry Pi 4 hardware package. They use AWS cloud-enabled IoT to deploy the top layer (cloud). The security protocols and essential administration sessions were conducted between the two layers to guarantee the protection of user information. Security certificates were implemented to allow data transmission among the layers of the IoT powered cloud / edge model proposed. It can be used, along with the best safety technologies, to address cybersecurity threats to any layer, cloud, edge and IoT, not just to remove potential security vulnerabilities.

Asthana et al. [6] have put forward a recommendation framework advising every person of wearable IoT and wearable devices. This device first gathers available user health data from medical and fitness devices, including health history, demographics, and previously collected IoT data. The framework also makes predictions about diseases with classification models such as decision tree, logistic regression and LibSVM. Could condition has to do with certain attributes to be controlled. Finally, the best IoT solution or wearable devices is recommended through a mathematical optimization model.

Walinjkar et al. [7] proposed a prognostic approach based on real-time Electrocardiograph (ECG) analysis. The scheme first analyses ECG waveforms with a K-NN or other classifier with real-time data from continuously monitoring ECG devices. Arrhythmia and other disorders can be predicted by the system. The authors have set up an IoT tracking network in the NHS (National Health Services, UK) cloud for real-time transportation of data. The test results show that precision will hit 99.4 percent when K-NN is used, including two classifiers like the bagged tree and K-NN.

In the medical sector, Nguyen et al. [8] explored the IoT application and proposed an IoT tiered architecture which collects, analyses and transforms sensor data into clinical feedback. The architecture is divided into three levels. (1) the sensing layer, which uses sensors, drives and wearable devices, can collect data; (2) the transmitting layer where communications mechanisms such as Wi-Fi, Bluetooth, Zig-bee and LTE can be used for transmitting data to a server. If required, after processing, notifications and alerts could be generated; 4) storage layers where data can be stored in clouded or hosted servers; 5) mining and learning layer that converts information to decisions or predictions using mining or machine learning algorithms.

Pandey [9] used single heart beat to determine whether a person is in stress or not on an IoT network. A Wi-Fi board was developed by the author, which can detect pulse waves. The board will move the data on to the server. The server will assemble a fingerprint of the data over time through various periods of the day. The server will make predictions about stress using either SVM or logistic regression. The results show that, if suitable models are used, the precision will exceed 68 per cent.

Siryani et al. [10] used machine learning to progress the competence of smart meter operation. Administrative must guarantee the cost efficiency of their activities with the massive rise in the number of smart meters. The authors used various methods of master learning in this paper to assess if a technician should be assigned to a client. The device will eliminate a lot of travel and human capital with increased precision. The models have been validated with commercial network data. Various classification algorithms were tested including the Bayesian network, naive bays, decision tree and random forest. Finally, the results show that the most accurate random forest, which is 96.69%, and the expected cost saved for the commercial network is around US$ 1 million.

Ling et al. [11] developed an IoT device that can automatically detect occupancy of the car park. First the captured images are uploaded by the system. Then you can learn the parking spot using a car recognition tool. After that, the most commonly parked locations are identified in a function clustering algorithm based on Mean-shift. A Raspberry Pi 3 model is evaluated by the scientists. Camera information is gathered on a local street near Washington Campus University. For restoration and observation, the Raspberry Pi board is linked to AWS IoT. The findings suggest that 97 percent can be done in real time.

Amit Sagu et al. [12] concentrated on all the problems related to IoT security and how computer teaching would help resolve these security concerns. The paper also explores the methods, criteria, features and techniques proposed and examines which technique could be more efficient.

Uwagbol et al. [13] obtainable a pattern driven corpus to expect SQL injection attack. Although SQL injector attacks are well known, the problem arises again as IoT and SDN networks offer the assailants new opportunities and the advocates lack machine learning capabilities which could detect new attacks. The authors proposed a framework for the generation of finite State automatics powered by a pattern. The developed corpus could be used to train a new model with machine learning methods. Finally, the method can be tested by publicly using two data sets, and the results demonstrate that it is possible to obtain a high degree of precision.

Ahmed et al. [14] made use of machine learning methods to identify DNS query-based attack. DNS query-based attack. In comparison to a DDoS attack, the DNS query-based attack could be initiated with just a small number of packets. The SDN controller in the proposed framework will collect network traffic data and classify machine-based query-based attack traffic. The authors eventually introduce a prototype based on the Dirichlet mixing model and perform real world track simulation. The results of the simulation show that the machine learning system exceeds conventional average shift method.

IV. RECENT MACHINE LEARNING BASED IOT APPLICATION WORKS

Work Year	Problem	Technique used	Data/ Signal	Accuracy
2020[5]	lack of efficient and robust security protocols	new IoT layered model	(AWS)	None
2017[6]	Recommoned IoT solutions and wearable devices	Decision tree, logistic regression,LibSVM	Health history	None
2017[7]	Prognostic based on ECG	Bagged tree, K-NN	ECG waveform	99.4
2017[8]	IoT health architecture	None	Sensor data	None
2017[9]	Human stress detection	SVM, logistic regression	Pulse waveform	68
2017[10]	Smart meter operation	Bayesian network, naive bayes, decision tree, random forest	Smart meter data	99.69
2017[11]	Parking space detection	Clustering algorithm	Camera data	97
2020[12]	Numerous kinds of risks	Support Vector Machine Regression, Random Forest and Linear Regression	Steal critical data from people as well as organizat-ion	None
2017[13]	SQL injection attack detection	SVM	Traffic data	96.4
2017[14]	DNS query-based attack detection	Bayesian	Traffic data	75

V. CONCLUSION

The main technology for IoT is machine learning with a major potential. Trends in machine learning to test IoT applications. In spite of the recent wave of success in computer network learning, machine learning literature on its IoT services and systems implementations is scarce, and the purpose of this survey is to address them. We have written this paper in order to emphasize the implementation of the computer training for IoT and its analysis of recent developments which are very different from the previously published survey papers in terms of emphasis, reach which width. Because of IoT's flexibility and changing existence, each application cannot be protected. However, the present paper aims to cover key machine learning applications for IOT and related techniques, including traffic profiling, identification of IoT devices, security, cutting-edge computing infrastructures, SDN-based network management and typical IoT applications. A systematic research on the use of IoT machine learnings, its technological developments and its application fields was presented in recent studies. We have also addressed succinct research problems and open issues that are important for the implementation of IoT machine learning.

REFERENCES

[1]. Wu, Dapeng, Hang Shi, Honggang Wang, Ruyan Wang, and Hua Fang. "A Feature-based Learning System for Internet of Things Applications." IEEE Internet of Things Journal (2018).

[2]. Elijah, Olakunle, Tharek Abdul Rahman, Igbafe Orikumhi, Chee Yen Leow, and MHD Nour Hindia. "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges." IEEE Internet of Things Journal (2018).

[3]. Chhabra, Anshuman, Vidushi Vashishth, Anirudh Khanna, Deepak Kumar Sharma, and Jyotsna Singh. "An Energy Efficient Routing Protocol for Wireless Internet-of-Things Sensor Networks." arXiv preprint arXiv:1808.01039 (2018).

[4]. Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on, pp. 10-pp. IEEE, 2000.

[5]. Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." Applied Sciences 10, no. 12, 2020.

[6]. Asthana, Shubhi, Aly Megahed, and Ray Strong. "A recommendation system for proactive health monitoring using IoT and wearable technologies." In 2017 IEEE International Conference on AI & Mobile Services (AIMS), pp. 14-21. IEEE, 2017.

[7]. Walinjkar, Amit, and John Woods. "ECG classification and prognostic approach towards personalized healthcare." In 2017 International Conference On Social Media, Wearable And Web Analytics (Social Media), pp. 1-8. IEEE, 2017.

[8]. Nguyen, Hoa Hong, Farhaan Mirza, M. Asif Naeem, and Minh Nguyen. "A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback." In 2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 257-262. IEEE, 2017.

[9]. Pandey, Purnendu Shekhar. "Machine learning and IoT for prediction and detection of stress." In 2017 17th International Conference on Computational Science and Its Applications (ICCSA), pp. 1-5. IEEE, 2017.

[10]. Siryani, Joseph, Bereket Tanju, and Timothy J. Eveleigh. "A machine learning decision-support system improves the internet of things' smart meter operations." IEEE Internet of Things Journal 4, no. 4, 2017.

[11]. Ling, Xiao, Jie Sheng, Orlando Baiocchi, Xing Liu, and Matthew E. Tolentino. "Identifying parking spaces & detecting occupancy using vision-based IoT devices." In 2017 Global Internet of Things Summit (GIoTS), pp. 1-6. IEEE, 2017.

[12]. Amit Sagu, Nasib Singh Gill, "Machine Learning Techniques for Securing IoT Environment", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020.

[13]. Uwagbole, Solomon Ogbomon, William J. Buchanan, and Lu Fan. "An applied pattern-driven corpus to predictive analytics in mitigating SQL injection attack." In 2017 Seventh International Conference on Emerging Security Technologies (EST), pp. 12-17. IEEE, 2017.

[14]. Ahmed, Muhammad Ejaz, Hyoungshick Kim, and Moosung Park. "Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking." In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 11-16. IEEE, 2017.

