

Pilot Study of Machine Learning In Iot Security and Challenges

Ramanand S. Samdekar¹, S. M. Ghosh², Konda Srinivas³, Rohit Miri⁴

¹PhD Scholar, ^{2,3}Professor, ⁴Associate Professor
^{1,2,3,4}Dr. C. V Raman University, Kota, Bilaspur, India

Article Info

Volume 82

Page Number: 16941 - 16946

Publication Issue:

January - February 2020

Article History

Article Received: 18 May 2019

Revised: 14 July 2019

Accepted: 22 December 2019

Publication: 29 February 2020

Abstract

Internet of Things is a combination of various devices that connect to each other and it uses the various types of sensors over the wireless and wired media. Since the last two decades the development in IOT has been increasing rapidly over the million of IOT devices has been interconnected together. During the development of IOT technology, security challenges has been distinguished as probably come up in IoT. In additional the expanded volume of data, the IoT makes a huge amount of data by its to speed similar to time and region, with the combination of different things and class in data has been changed. The handling and examination of this huge amount of information are the way to creating IoT applications.

Keywords; IOT, Network Security, Sensors, Machine Learning

I. INTRODUCTION

Recent Developing advancements and significant improvements over the Internet and conventions and processing frameworks, have made correspondence between various enabled devices simpler than at any other time.

The devices in IoT allude to the items from our day by day life extending from brilliant house-hold appliances for example, bulb, energy saving meter, humidity/temperature sensor, fire alarm, IP camera, to increasingly complex appliances for example, Radio Frequency Identifier (RFID), sensors in parking service, and a scope of different sensors in cars and so forth. (Hussain et. al. 2017). Although the IOT has a plenty of utilizations and services extending the basic foundation in healthcare, defense system, smarthomes & agriculture services. (A. Al-Fuqaha et. al. 2015). Moreover, the spaces secured by the IoT services incorporate, yet not constrained to, power, retail, transportation, production etc. The enormous size of IoT systems brings new difficulties, for example, device

management, sheer measure of information, network communication, processing and privacy & protection. There have been broad looks into covering these changed parts of IoT (A. Al-Fuqaha et. al. 2015, Mohamad Noor et. al. 2018). The commercial product of IoT innovation is the privacy & protection ensure just user fulfillment. The way that IoT uses empowering advancements, for example, distributed computing and Cloud Computing etc.

The IOT devices make a large volume of data so at that moment conventional methods for data collection, processing and data storage will be failed. In this context we are used more powerful and suitable paradigms to provide the high computational power and intelligences to Internet of Things Gadgets (devices). The machine learning is one of the powerful paradigms for embedded system intelligence in IoT enabled devices. The number of machine learning algorithm have been used for intelligence that is support vector machine, Linear Classifier, Bayes decision, Neural Networks, and

reinforcement learning etc. This machine learning algorithm can be used in various applications like cyber attack detection, voice recognition, image processing, object detection and classification, healthcare system, automobile industries, manufacturing unit, authentication etc.

IOT security Approach: To present the study on current requirement of IOT security, attacks and high level security solution for IOT network (Fatima Hussain et. al. 2019). To propose the high security mechanism based on the machine learning and artificial neural network within the IOT gateway (J. Cañedo et. al. 2016). To input the some valid and invalid data for anomalies detection; proposed model has accurately detected the invalid data in network. Developed an android based security application for monitoring and controlling the campus using the electronics and electrical devices based on the IOT enabled smart services for increasing the security and saves the power consumption (R. Sarmah et. al. 2019). Another technique for security is based on the single password mechanism to authenticate the IOT

devices and the IOT server (T. Shah et. al. 2018). Many security solutions were proposed for cloud based on the IOT. Author proposed an middleware security solution for cloud for proving secure communication between the user and cloud application (H. Garg et. al. 2019)

Machine Learning Approach: In this section conduct the study in different aspects of machine learning techniques used in IOT security. Proposed an Artificial neural network to verifying the valid attribute and to detect the valid and invalid data in network (J. Cañedo et. al. 2016). The use of machine learning approach for collecting the large amount of data from different sources and to provide the security for data (A. Roukounaki et. al. 2019). And hybrid CNN/LSTM model is used to detect the DDos attack in network and to evaluate the trusted nodes in network based on the deep learning (M. Roopak et. al. 2019; E. Eziamma et. al. 2018). Support vector machine is used for providing the difference between the original codes and mutated codes based on edge computing (S. Hou et.al.2019)

II. RECENT WORK OF IDS IN IOT

Sr. No	Authors	Methods/Techniques Used	Security Threats	Limitation
1	Elvin Eziamma et. al.	Naive Bayes, Decision Tree, Linear & Radial SVM, KNearest Neighbor, and Random Forest	Injection Attacks, Ballot Stuffing, Bad Mouthing	If two matrices used individually then performance will be degraded.
2	Size Hou et. al.	RBF, SVM	Code Mutation	System does not detect all types of attack. Only mutated code will be find out during the IOT operation.
3	Monika Roopak et. al.	Convolution neural network and Multilayer Perceptron	DDoS	If dataset are changed then accuracy of attack detection might be change.
4	Janice Canedo et. al.	Artificial Neural Networks	Man in the Middle and (DoS)	The Model gives alternate input of valid and invalid data to detect the anomalies in an IoT.
5	Nathezhtha.Ta	Recurrent Neural Network	Conventional	When new node is joined to

	t. al.			network; the malicious node detection rate is low.
6	M. Aldairi et. al.	Isolation Forest and One-class SVM	Conventional	The honest user is required to recall the model for weekend's activity markup to detecting the insider threats.

Table1: Comparative Study

II. APPLICATION AREAS OF ML AND IOT

Embedded system: The recent work on this area is to develop a cryptographic model of secured communication for embedded system based on the internet on things (P. Peniak et. al. 2015). To propose a security mechanism of employee authentication based on the embedded system. Employee Authentication is done by the adhaar verification to validate the data of peoples in India (A. Joshy et. al. 2018). To build up an arrangement based approach for authorizing the guideline of some benefit, from equipment Security model that effectively screens correspondence uses and framework assets. The approach is based on embedded hardware and software security policies and relief of dangers forced by obscure vulnerabilities of implanted applications and conventions. (F. Siddiqui et. al. 2018)

Smart Homes: This class incorporates customary home gadgets, for example, coolers, clothes washers, or on the other hand lights, that has been created and can speak with one another or with approved clients by means of web, offering a superior checking and the executives of the gadgets just as vitality utilization enhancement (FotiosZantalis et. al. 2019). To develop a highly secured system for smart home to use different devices like motion sensors, cloud server object detection etc. The system is controlled by the authenticate user. (R. Sarmah et. al. 2019).

Transportation: Day by day IoT technology grows and new applications are made so as to improve people life style. (FotiosZantalis et. al. 2019). Understanding the setting of IoT in transportation is

critical, however what are these advancements going to resemble? Where would it be advisable for us to hope to discover them? We've just begun to see the joining of IoT in transportation. They can be as little scale as a vehicle-to-individual correspondence. To distinguish the flow pattern in the utilization of Machine Learning and IoT in transportation, and look at the examination inclusion in every last one of the transportation classifications (FotiosZantalis et. al. 2019).

Health-care System: IOT and machine learning has been used in healthcare system for collecting the patient data like health improvement of patient, habits, daily routine, sleeping and diet (F. Ahamed et. al. 2018) and gives the security for healthcare system from cyber attacks (A. K. Alharam et. al. 2017). In fact, various IOT based framework has been developed to monitor the patient health problems. To proposed a frame work; ease to interaction between the patient and doctor based on the inter-iot scenario (P. Pace et al. 2019).

Privacy and Monitoring Systems: CCTV can get video contribution over the roads. The ongoing visual item acknowledgment, security frameworks can distinguish suspects or anticipate dangerous circumstances.

III. CHALLENGES OF MACHINE LEARNING IN IOT

Good Technique/algorithm Selection: There are several different algorithms and techniques used to implement in machine learning. In spite of the fact that calculations can work in any conventional conditions, there are some rules accessible about

which techniques and algorithm would be used under any conditions. So that good technique and algorithm selection are crucial steps in machine learning in IOT, improper selection causes the wrong output and wastage of time, money and entire efforts.

Data set selection: If you input the wrong data to system; system will gives you wrong output, The appropriate data set selection based on the quality, size of data set, data preparation etc. It is essential to maintain a strategic distance from determination predisposition and select the information which is altogether illustrative of the cases.

Data Preprocessing: There are number of step taken for data processing such as parsing cleaning and preprocessing. It is very difficult task for data processing because of data may contain null values or some missing values. To highlight properties and worth reaches need to studies and methods like component scaling should be applied to keep certain highlights from overwhelming the whole model.

Data Labeling: In Supervised Machine Learning simple and very efficient algorithm are used for data processing. It is very difficult job to select which algorithm/techniques or carried out the algorithm. it may be very long and difficult process sometimes it requires the many ineffective steps. The Supervised Machine Learning needs the data labeling. Frameworks need to comprehend what is appeared on a Image, said in a voice recording, or written in a book, among numerous different things. By data labeling, machines can improve their learning and AI continues advancing.

Security concerns: Now IoT device has been interconnected to each other because of the technology has been growing day by day and also internet giving availability between the physical devices to web world. The large amount of data has been produces s exceptionally flexible but on the other hand is the reason for significant security concerns. Actually, about half of associations

engaged with IoT consider security the greatest deterrent to IoT arrangements. Also, taking into account that around 66% of IoT gadgets are in the buyer space, and how close to home a portion of the common information can be, it is straightforward why. These worries, combined with the normal dangers connected to visit information moves onto the cloud, clarify why clients are requesting assurances in regards to the security of their personal information.

IV. CONCLUSION

The Internet of Things becomes the privacy and security protection is of principal significance and assumes an urgent job in the commercial of the IoT innovation. Conventional privacy protection arrangements experience the ill effects of various problems has been identified with idea of Internet of Things systems. Machine Learning and explicitly Deep Learning methods has been utilized to empower the Internet of Things gadgets to adjust the condition. These learning procedures are bolster self-arranging action and the general model for processing by inputting the measurable data from the surrounding. The very few times datasets requirement for Machine and deep learning. In this paper, we have thought about the recent advancement on machine learning in the IoT environment from privacy point of view. We have examined the privacy and protection challenges of Internet of Things and also security necessities. We have portrayed diverse Machine and Deep Learning strategies and their security application in IoT environment.

V. REFERENCES

- [1] Fatima Hussainet. al., "Machine Learning for Resource Management in Cellular and IoT Networks: Potentials", Current Solutions, and Open Challenges" ArXiv, 2019.
- [2] J. Cañedoet. al., "Using machine learning to secure IoT systems", 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, Pg. 219-222, 2016.doi: 10.1109/PST.2016.7906930

- [3] R. Sarmah, et. al. , "SURE-H: A Secure IoT Enabled Smart Home System", IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, pg. 59-63, 2019. doi: 10.1109/WF-IoT.2019.8767229
- [4] Hussainet. al. "Internet of Things; Building Blocks and Business Modles", Springer, 2017.
- [5] A. Al-Fuqaha, et. al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourth quarter 2015. doi: 10.1109/COMST.2015.2444095.
- [6] Mohamad Noor et. al. "Current research on Internet of Things (IoT) security: A survey", Computer Networks.148, 2018. doi: 10.1016/j.comnet.2018.11.025.
- [7] T. Shah et. al., "Authentication of IoT Device and IoT Server Using Secure Vaults", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/Big DataSE), New York, NY, pg. 819-824, 2018. doi: 10.1109/TrustCom/BigDataSE.2018.00117
- [8] H. Garget. al., "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware", 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, pg. 1-6, 2019. doi: 10.1109/IoT-SIU.2019.8777334
- [9] A. Joshyet. al., "Design and implementation of an IoT based secure biometric authentication system", IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kollam, pg. 1-13, 2017. doi: 10.1109/SPICES.2017.8091360
- [10] M. Singh, et. al., "Blockchain: A game changer for securing IoT data", IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, pg. 51-55, 2018. doi: 10.1109/WF-IoT.2018.8355182
- [11] F. Siddiquiet. al. "Embedded policing and policy enforcement approach for future secure IoTtechnologies", Living in the Internet of Things: Cyber security of the IoT - London, pg. 1-10, 2018. doi: 10.1049/cp.2018.0010
- [12] J. Han et. al, "Security considerations for secure and trustworthy smart home system in the IoT environment", International Conference on Information and Communication Technology Convergence (ICTC), Jeju, pg. 1116-1118, 2015. doi: 10.1109/ICTC.2015.7354752
- [13] P. Peniaket. al., "Extended Model of Secure Communication for Embedded Systems with IoT and MQTT", International Conference on Applied Electronics (AE), Pilsen, pg. 1-4, 2018.doi: 10.23919/AE.2018.8501434
- [14] J. Shahpureet. al., "IoT Based System for Passenger Service in Railways with Secure ICN Architecture", 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, pg. 819-821, 2018. doi: 10.1109/ICOEI.2018.8553938
- [15] M. Hagan et. al., "Enforcing Policy-Based Security Models for Embedded SoCs within the Internet of Things", IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, pg. 1-8, 2018.doi: 10.1109/DESEC.2018.8625140
- [16] M. Son et. al, "Blockchain-based secure firmware management system in IoT environment", 21st International Conference on Advanced Communication Technology (ICACT), PyeongChangKwangwoon_Do, Korea (South), pg. 142-146, 2019. doi: 10.23919/ICACT.2019.8701959
- [17] Fotioet. al. "A Review of Machine Learning and IoT in Smart Transportation", Future Internet, pg 11, 94, 2019; doi:10.3390/fi11040094.
- [18] A. Roukounakiet. al. "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems", Global IoT Summit (GIoTS), Aarhus, Denmark, pg. 1-6, 2019. doi: 10.1109/GIOTS.2019.8766407.
- [19] M. Roopak, et. al., "Deep Learning Models for Cyber Security in IoT Networks", IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pg. 0452-0457. doi: 10.1109/CCWC.2019.8666588
- [20] S. Houet. al., "Use of Machine Learning in Detecting Network Security of Edge Computing System", IEEE 4th International Conference on

- Big Data Analytics (ICBDA), Suzhou, China, pg. 252-256, 2019. doi: 10.1109/ICBDA.2019.8713237
- [21] E. Eziam, et. al., "Machine learning-based recommendation trust model for machine-to-machine communication", IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Louisville, KY, USA, pg. 1-6, 2018. doi: 10.1109/ISSPIT.2018.8705147
- [22] F. Ahamedet. al., "Applying Internet of Things and Machine-Learning for Personalized Healthcare: Issues and Challenges", International Conference on Machine Learning and Data Engineering (iCMLDE), Sydney, Australia, pg. 19-21, 2018. doi: 10.1109/iCMLDE.2018.00014
- [23] P. Pace et al., "INTER-Health: An Interoperable IoT Solution for Active and Assisted Living Healthcare Services", IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, pg. 81-86, 2019. doi: 10.1109/WF-IoT.2019.8767332
- [24] A. K. Alharamet. al., "Complexity of Cyber Security Architecture for IoT Healthcare Industry: A Comparative Study", 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, pg. 246-250, 2017. doi: 10.1109/FiCloudW.2017.100
- [25] T. Nathezhthaet. al., "Cloud Insider Attack Detection Using Machine Learning", International Conference on Recent Trends in Advance Computing (ICRTAC), Chennai, India, Pg. 60-65, 2018. doi: 10.1109/ICRTAC.2018.8679338.
- [26] M. Aldairiet. al., "A Trust Aware Unsupervised Learning Approach for Insider Threat Detection", IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), Los Angeles, CA, USA, 2019, pg. 89-98, 2019. doi: 10.1109/IRI.2019.00027