ISSN 2347 - 3983
Volume 9. No. 5, May 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter03952021.pdf
https://doi.org/10.30534/ijeter/2021/03952021

An Evaluation of Machine Learning Classifiers for Prediction of Attacks to Secure Green IoT Infrastructure

Hassan Adegbola Afolabi[1], Abdurazzag Aburas[2]
[1]School of Electrical, Electronic and Computer Engineering
University of Kwazulu-Natal South Africa, 219048801@stu.ukzn.ac.za
[2]School of Electrical, Electronic and Computer Engineering
University of Kwazulu-Natal South Africa,aburasa@ukzn.ac.za

ABSTRACT

Internet of things is an emerging technology that allows many devices to be connected in an unparalleled way. Despite having many beneficial applications, IoT technology presents significant emission risks due to the large number of devices used in the applications. Therefore, to gain maximum benefit from IoT, we must step towards green IT. On the other hand, cloud computing has been successfully used to provide limitless computational storage and other resources for a variety of IoT devices across the internet. Unfortunately, security concerns in cloud computing for IoT are still a concern. Motivated by the goal of creating a better atmosphere for IoT and ensuring its resilience to risks and attacks, this report reveals ways to decrease the impact of energy use by IoT on the environment. Additionally, it addresses research concerns for IoT security and reflects on how to protect green IoT networks through the use of an effective machine learning intrusion detection technology to deter attacks on IoT platforms. To do that, we first evaluated some existing ML classifiers such Artificial Neural Network (ANN), Support Vector Machine (SVM), Gaussian Naïve Bayes (NB), Decision Tree (DT) and Random Forest (RF) with the old KDD'99 datasets. The accuracy was extremely high for all classifiers except Gaussian NB whose accuracy was < 90%. The SVM is the highest at 99.24% accuracy with a loss of 4.68% in the last epoch of training. However, using a more recent dataset (ISCX1DS2012) on these same ML classifiers, we observed some discrepancies, all the classifiers dropped in their predictive accuracy even after altering the hyper-parameters.The ANN was at its lowest accuracy at 85.92% and the SVM which was relatively accurate dropped to 90.02%. NB algorithm produced approximately 67.9% accuracy which made it less accurate for both datasets. Based on these findings, we proceeded to propose an efficient model with enough hidden layers and nodes to increase the detection accuracy and to outperform the existing ML classifiers when evaluated with a more recent dataset.

Key Words: Cloud-computing, Energy efficiency, E-waste, IoT, Intrusion detection system, Machine Learning

1. INTRODUCTION

Recent IoT and cloud computing developments have changed our work and daily life styles [1]. According to earlier predictions, IoT is destined to invade every single facet of our lives, particularly through the interconnection of millions of smart devices and IoT control system. They include, but are not limited to the next generation electric grid, intelligent transportation systems, and intelligent health technologies. Although it's touted as a helpful technology for several purposes, it is also criticized for several threats because it makes use of an increasing amount of energy resources, thereby embracing both pollution and e-waste. On this account, the green IoT reflects its effect on the climate and it's widely believed to be the future of IoT [2]. As such, moving toward green IoT is essential to capitalize on the benefits of IoT's disruptive potential. In Internet of Things (IoT) systems, cloud computing is depended on for both data and applications processing and storage. Various implementations of IoT technologies may lead to many security weaknesses, particularly if not well monitored and secured. This presents a major security issue for cloud computing on the Internet of Things. Thus, if there are no appropriate security protocols are in place, the security and credibility of data and information could be undermined [3].Although, cybersecurity is an ongoing issue, these security weaknesses can be largely reduced by using advanced security measures during the IoT deployment to take advantage of these new technologies to their fullest extent. Extra effort

should be devoted in the research all anticipated security problems, to ensure that we are prepared to address any possible risks should they occur.

2.INTERNET OF THINGS

Internet of Things (IoT) is an evolving technology that connects billions of devices together regardless of where they are located. Radio frequency identification (RFID) and wireless sensor networks (WSNs) can be regarded as the fundamental technologies for IoT.

Using RFID technology, microchips can transmit an object's identification information to a reader through wireless communication. These readers make it possible to automatically identify, control, and track objects equipped with RFID tags [4]. RFID technology is well-known for its widespread use in manufacturing, retail, and logistics. For sensing and monitoring, (WSNs) primarily depend on interconnected smart sensors. It is commonly used in environmental, traffic and health care monitoring [5]-[6]. Both RFID and WSN developments have made a major contribution to the growth of IoT.

As the use of IoT continues to grow and expand, our everyday lives and lifestyles have been revolutionized and enhanced by this technology, which has been embraced in a variety of realms which includes Smart Homes, Smart Supply Chains, Smart Cities [7]-[9]. Other applications of IoT includes Smart Grid, Wearables, Smart Health Care (Digital Health and Telemedicine) etc.The Internet of Things provides users with a plethora of technical capabilities all under one roof, posing many obstacles for researchers.

3.GREEN INTERNET OF THINGS

By 2025, there will be billions of mobile smartphones connected to the internet. However, the most important obstacle to IoT deployment would be energy. Regardless of their numerous benefits, the energy consumption of these devices can serve as a deterrent to their widespread adoption. This is a major concern, as carbon emissions and E-Waste produced by ICT products can rapidly increase. This would have a detrimental effect on our environment if effective interventions are not implemented [10]. To fix this problem, it is important to transition to green IoT, which is environmentally friendly. Green IoT are energy-efficient methods in IoT that either minimize or eliminate the greenhouse effect caused by the current applications [11]. It is mostly concerned with the energy conservation of IoT. In a green IoT, every move should be environmentally friendly; it should prioritize green construction, green manufacturing, green use, and green disposal or recycling in order to have a negligible or no impact on the environment. A variety of methods should be implemented in order to introduce the Green IoT. Authors in [12] suggested a method for optimizing the energy efficiency of IoT systems. Green RFIDs, Green Data Centers, Green Wireless Sensor Networks, Green Machine to Machine (M2M), and Green Cloud Computing are only a couple of the techniques discussed in this article.

3.1 Green RFIDs

The RFID tag is a small microchip with a unique identifier connected to a radio (which is used to receive and transmit the signal). RFID tags are used to store data about the items to which they are connected. RFIDs may be active or passive; in order to achieve more environmentally friendly RFID devices, it would be necessary to reduce the size of RFID tags in order to reduce the amount of non-biodegradable content used in their manufacture. Additionally, projects such as printable RFID tags [13], biodegradable RFID tags, and RFID tags made of paper should be considered.

3.2Green Data Center

A data center's primary function is to store, maintain, process, and distribute all forms of data and applications generated by users, objects, and systems. Data centers use enormous quantities of resources to manage a variety of data and applications, resulting in high operating costs and significant CO_2 emissions. Hence, in order to achieve a green DC, the techniques discussed in [14]-[18] should be considered, such as implementing more renewable and efficient energy sources like wind, water and solar energy. the design of more energy-efficient hardware, the use of efficient dynamic power-management technologies, the design of a novel energy-efficient data center architecture to achieve power conservation, should be implemented.

3.3 Green Wireless Sensor Networks

A WSN consists of a huge distributed sensor node and a base station (BS) known as the sink. These sensor nodes collectively monitor physical and environmental factors such as temperature, sound, motion etc. Green solutions are needed to optimally utilize WSNs. This can be accomplished by ensuring that data transmission occurs at low-power, as described in [11], [19]-[20].

3.4 Green Cloud Computing

Cloud computing provides consumers with a variety of resources based on their requirements. These resources are categorized as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) (Software as a Service). As a

result of more systems and applications migrating to the cloud, more energy and resources are used, resulting in increased environmental challenges and CO2 emissions. As a result, a more environmentally friendly approach to cloud computing is important to reduce energy usage. This can be accomplished by using cloud resources efficiently.

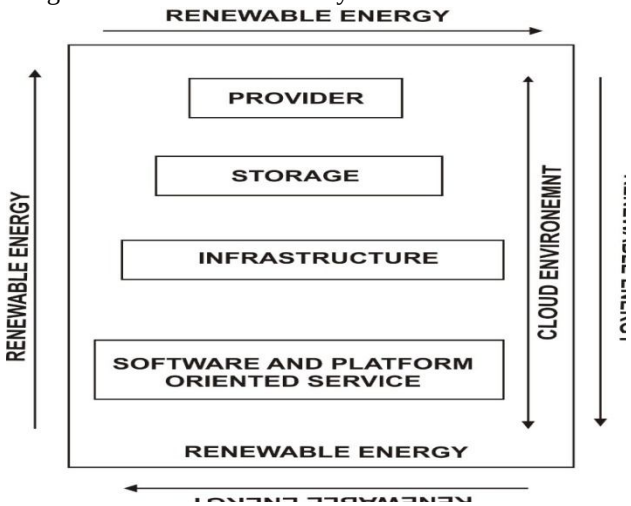

Figure 1: Green Cloud Computing Architecture

As depicted in the illustration above, the green cloud computing platform is entirely cloud-based with an emphasis on sustainable energy use and effective resource use, as well as a reduction in carbon emissions from both vendors and users. Once carbon emissions are reduced, the green cloud computing target is achieved.

3.5 Green Machine to Machine

M2M is a system that enables the communication of both wireless and wired devices with other devices of the same kind. M2M interactions require large machines, which allows them to consume a great deal of energy. As discussed in [21]-[25], energy efficiency can be increased to achieve a green M2M by (but not limited to) the following techniques: intelligently adjusting transmission power to the bare minimum required level, designing efficient communication routing protocols by the use of algorithmic and distributed computing techniques, activity scheduling (switching certain nodes to idle 'low-power' mode to enable only a few other perform needed tasks).

4. GREEN CLOUD COMPUTING AND INTERNET OF THINGS

Cloud computing provide computing power, storage space, utilities, and applications over the internet. On the other hand, the Internet of Things is a new technology that enables the connection of billions of physical objects for the purpose of data collection and sharing. Both concepts have developed independently over time in terms of hardware and software. Researchers discovered that cloud computing could be able to solve the IoT dilemmas of processing capability, storage space, and energy efficiency. As a result, the need for integrating CC and IoT technology becomes apparent, and the idea of Cloud of Things (CoT) was founded [26], [27]. Its integration has resulted in several benefits for both technologies, as CC is often engaged in the analysis of data provided by IoT devices. As a result of the growth of CoT, there is an increase in energy demand from the billions of devices linked together due to exchange of massive amounts of data and information. According to a Gartner survey [28], the global ICT industry contributed nearly 2% of global CO2 emissions. Therefore, it is important to transition to green cloud infrastructure and green IoT in order to maximize the advantages of CoT. Liu et al. [29] proposed a green cloud architecture with the aim of reducing data center energy consumption. This would be economically prudent and an important strategy for environmental protection. Green computing is not limited to the use of IoT devices alone, it encompasses all other environmental concerns as well, including CO2 pollution, (e-)waste disposal, and natural resource use. The evolution of this study was influenced by a growing interest in environmental safety and the widespread use of cloud computing.

5. IMPLEMENTATION OF GREEN IOT INFASTRUCTURE

The green processes include both green computing technologies and green communication. Green computing is more concerned about the environmentally sustainable application of ICT infrastructure. This can be accomplished by reducing energy consumption and greenhouse gas emissions, decreasing the number of devices used by servers and data centers, improving storage capacity and cost effectiveness, enhancing time utilization and recycling equipment effectively. Green communication is more concerned with the reduction of CO2 emissions during communication, making it a more difficult problem to address.

This segment discusses how to apply green IoT. Apart from ensuring that the IoT enablers mentioned previously are environmentally friendly, several literatures have discussed various strategies for implementing green IoT. Among them are the following:

5.1 Software Based Techniques

The energy efficiency of an IoT network is largely determined by the data center's energy management.

Authors in [21] proposes an e-policy focused on Orchestration Agent (OA) that intelligently chooses servers based on their energy usage. After that, the chosen servers handle the data and return it to their clients.

5.2 Hardware Based Techniques

Changes to the hardware components used in IoT can be made to obtain a green IoT. In [22] Core LH was presented, it is a dual core processor designed with CoreL and CoreH for low and high computing tasks in the IoT. This system conserves energy by allocating various activities to the CoreL and CoreH based on their resource requirements.

5.3 Policy Based Techniques

Numerous policies and plans for energy saving may be implemented. These approaches include energy usage monitoring in a variety of situations.

5.4 Awareness Based Techniques

Numerous awareness can be conducted to educate IoT consumers about their energy use; this strategy can save nearly 10% of energy [23], i.e. providing homeowners with Smart Metering Technology would notify them of their energy consumption in real-time and allow them to monitor and reduce it.

5.5 Changing Habits Towards Green IoT

Users can change their behaviors and routines in order to save energy resources. Energy can be conserved by monitoring its use through a variety of automation systems, as described in [24],[25], and [30]. As insignificant as its effect can seem on an individual basis, it can have a significant effect when seen collectively.

5.6 Recycling for Green IoT

Environmentally sustainable and recyclable components may be used to build devices for the IoT network. For example, some non-biodegradable materials are used in the manufacture of cell phones, and when recycled, they accumulate in billions, contributing to the greenhouse effect. If recyclable materials are used, substantial progress will be made in lowering the carbon footprint. [31] discusses some strategies for optimizing the efficiency of mobile phones and reclaiming electrical and electronic equipment's.

Due to the fact that the solutions discussed above could have certain limitations, it is necessary to seek out more practical and feasible methods of energy conservation. We suggest the following methods for achieving a green IoT infrastructure, based on the approaches discussed previously:

i. *Reducing the size of the IoT network by the use of optimal routing strategies and effective node placement*
ii. *Sensing data selectively in a given scenario by gathering only the information that is needed*
iii. *Developing appropriate energy-efficient plans and regulations for Internet of Things infrastructure, i.e. smart buildings.*
iv. *The use of architectures with both passive and active sensors for discrete functions*
v. *Selecting trade-offs intelligently and allocating communication and/or expense resources appropriately.*

6.SECURITY AND PRIVACY THREATS IN GREEN CLOUD OF THINGS

Green IoT, like IoT, is dependent on cloud infrastructure for data and device storage. The billions of connected devices in IoT technologies could cause several security flaws and expose the system to cyber threats. As a result, making security a major challenge. A threat is described as an adversary's potential to compromise a system's asset with the intent of compromising the privacy of system users or the system's overall protection [32]. The aim of this section is to recognize potential security and privacy risks. The term "security" refers to the processes that are used to protect the integrity, availability, and confidentiality of data at various points in a system. Whereas privacy refers to the right to manage privileged access to data that may contain extremely sensitive information about a person inside a device [33]. The figure 2 below illustrates a number of security and privacy risks that may affect any CoT device.

6.1 Security Threats

This group includes threats that can jeopardize the security of an IoT system, such as communication threats, physical threats, data threats, service provisioning threats, and other threats. Each of these sub-categories is discussed in detail below, along with the listed risks [32].

A. Communication Threats

In communication threats, an attacker mayexploit a communication channel to launch a variety of threats. A common example is denial of service (DoS) attacks. DoS can cause hardware failures, resource depletion, program glitches, and malicious broadcasting of high-energy signals, this attack will significantly reduce or eliminate a network's capacity to perform its intended operation. Due to the device limitations, CoT is susceptible to Dos attacks. [33] [34].

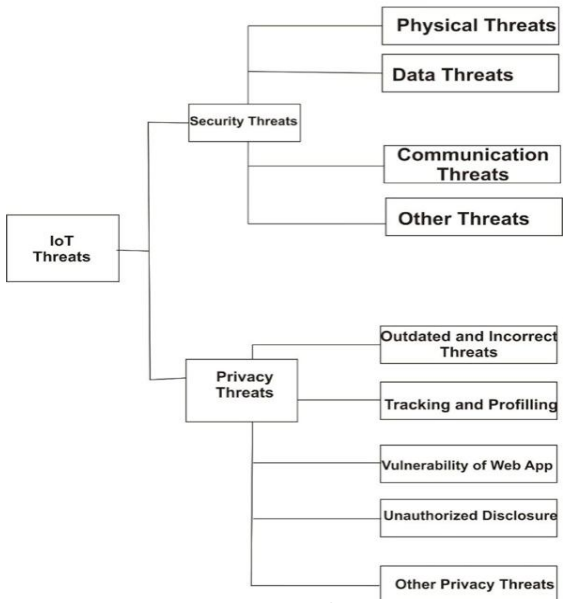

FIGURE 2: Taxonomy of Threats in IoT.

B. Physical Threats

These kinds of threats are numerous. They are incidents that can result in physical damage or destruction of connected IoT devices. These threats can either be Internal (fire, unreliable electricity supplies, etc.), external threats (lightning, earthquakes, etc.), and human threats (theft, arson, deliberate or unintended mistakes, etc.) [35].

C. Data Breaches

are one of the most prevalent types of cybersecurity threats. This category includes spamming, disabling security settings, and stealing and/or corrupting data. Data leaks, data destruction and leakage, and fake data injection are all examples of threats that rely on CoT data.

Other significant risks that are unrelated to either of the above examples include malicious insiders, shared infrastructure bugs, cloud server misuse and nefarious use [36], [37].

6.2 Privacy Threats

Since privacy concerns mostly the users of a system, privacy risks are more based on compromising and invading the privacy of the CoT system's users. Numerous attacks may be used to compromise the privacy of some users of a CoT environment [35].

7. INTRUSION DETECTION SYSTEM

Intrusion detection systems are a well-known strategy for defending against network attacks. An IDS's task is to detect anomalous behavior that may indicate potential attacks or malicious activity. It is capable of performing two primary roles.

7.1 Alarm Generation

Alarms are produced by Ids to notify the system administrator of discovered abnormalities. The efficacy of an IDS can be evaluated by examining its false alarm rate.

7.2 InformationGathering

An IDS can track the network and its systems and collect data on a local level. The collected data will then be forwarded to other applications for review. There are several styles and classes of IDS, each of which uses a unique identification strategy for detecting various types of attacks/malicious activity. The primary emphasis of this research paper is on IDS based on machine learning.

8. EXPERIMENTATION AND SIMULATION RESULT OF EXISTING ML IDS

In this section, we simulated some existing ML classifiers with two sets of data which are KDD'99 and CIC 2012 datasets

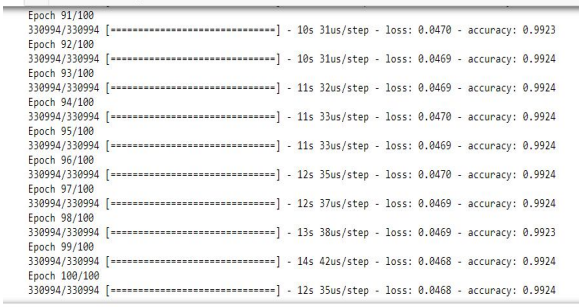

Figure 3: Final Epoch Output of the Training Process using KDD'99

Using a Network Intrusion Detection Model with the KDD'99 datasets the accuracy was extremely high as the loss was at a very low value of 0.0468 and accuracy at 0.9924 at the final epoch (100) during the training process. Epoch is the process of passing an entire dataset through a model.

There is different attack recorded in every dataset. The distribution of the various attack type in the KDD99 datasets is shown in the table below

Table 1: Attack Distribution in KDD'99 dataset

TYPES	SIZES.
DOS	391458
Normal	97278
Probe	4107
r2l	1126
u2r	52

The graphical illustration of the network during the testing phase to check its prediction and accuracy is shown below. The bar graph is the result from the Artificial Neural Network, Support Vector Machine, Gaussian Naïve Bayes, Decision Tree and Random Forest.

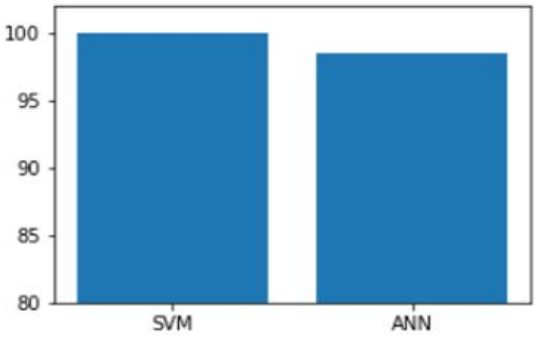

Figure 4: Output of SVM and ANN Algorithms on KDD'99 Dataset.

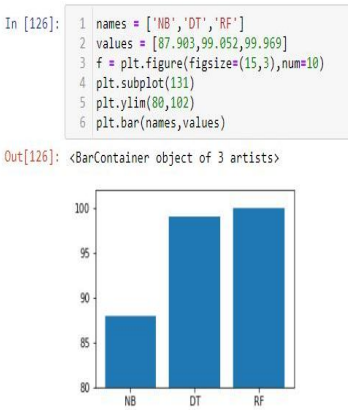

Figure 5: Output of Gaussian Naïve Bayes, Decision Tree and Random Forest Algorithms on KDD'99 Dataset

Using the 2012 intrusion dataset from the Canadian Institute of Cybersecurity on the ML algorithms – Artificial Neural Network, Support Vector Machine, Gaussian Naïve Bayes, Decision Tree and Random Forest using the same model as above.

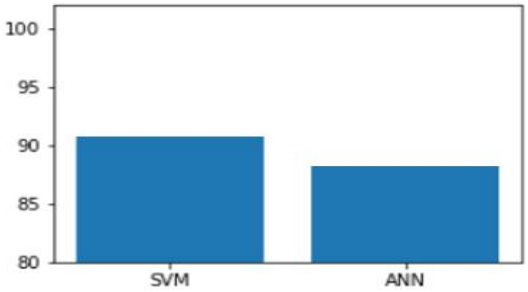

Figure 6: Output of SVM and ANN Algorithms on ISCX1DS2012 Dataset.

From the above bar graph on ANN and SVM using the same model, it was observed that the discrepancy due to its low predictive accuracy in the result was a little different even after altering the hyper-parameters. The ANN was at its lowest accuracy level with an accuracy of 0.8592 and the SVM which was relatively accurate was at 0.9002. The network model depth was a little bit too shallow to detect most of our new datasets and there were not enough hidden layers and nodes to increase the accuracy and depth of the model structure.

From the bar graph on NB, DT and RF using the same model and a different dataset, it was observed that the accuracy was relatively high except for the Naïve Bayes algorithm which was 67.903% on the testing dataset. Hence, NB should have been avoided due to its relatively low accuracy. The Decision Tree (DT) Algorithm was set at a maximum depth of 4 which affected the accuracy and the outcome of the prediction. For the Random Forest (RF) Algorithm, the n estimators (the number of decision trees) was set to 30. Although high but a little tweaking, probably lowering it would have generalized the algorithm to suit different datasets.

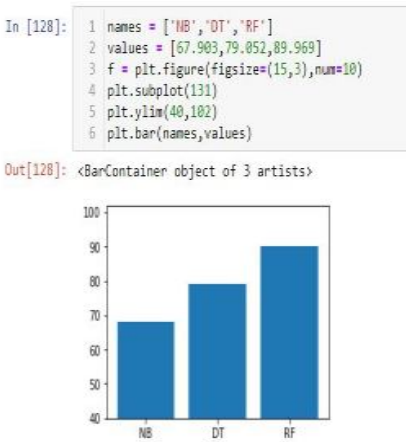

Figure 7: Output of Gaussian Naïve Bayes, Decision Tree and Random Forest Algorithms onISCX1DS2012 Dataset.

9. PROPOSED MODEL

The proposed model will use Deep Neural Networkto solve the challenges of the various flaws and limitations of the simulated existing models and to enhance the predictability of the network when pitched against other recent datasets.

The choice of deep learning methods is because of its effectiveness in dealing with big data and its ability to automatically learn feature representations from raw data.Major focus will be on 4 network-based datasets which are old KDD'99, NSL-KDD, ISCX1DS2012 and CIC-IDS2017.

The proposed Deep Neural Network will be based on back propagation with 3 hidden layers.

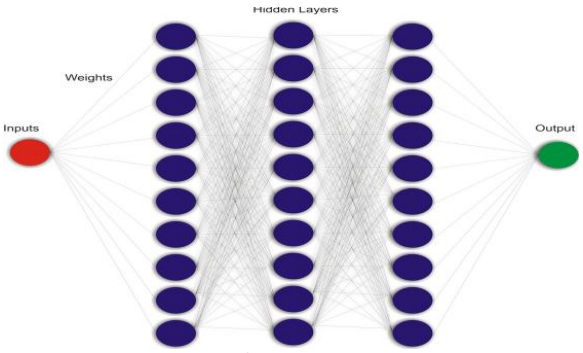

Figure 8: Diagram of the Proposed BP-DNN Model

The DNN will be based on the formula below:

$$y = Wx + b \quad (1)$$

In the above equations y = output, W = weight, x = inputs and b = bias.

Certainly, the prediction outcome (of segmenting a normal packet and an abnormal one using unsupervised learning) should be more accurate and greatly increased if all these suggested techniques are adopted to build the proposed model.

10. CONCLUSION AND FUTURE RESEARCH WORK

Although there is a tremendous research effort to achieve a green technology, green IoT technology is still in its early stage and there are many obstacles and challenges that needs to be addressed before it is fully adopted. However, applications should be green to minimize their effects on the environment and efficient energy efficient mechanism for IoT such as wind, solar, vibration, thermal should be considered to make IoT promising. Furthermore, both devices and protocols used in IoT communication should be energy efficient with less power consumption.
A possible research direction in this report would be exploring the applicability and impact of machine learning classifiers in the field of intrusion detection for an effective and improved detection accuracy. Secondly, evaluating these classifiers with a new and a more recent dataset to determine their performance against evolving attacks. Indeed, machine learning is a technology searching for challenges and as we keep our eye on such technology, more research should be encouraged on Machine Learning Techniques for Intrusion detection in IoT scenarios.

REFERENCES

[1] Mohiuddin, I., & Almogren, A. (2019). Workload aware VM consolidation method in edge/cloud computing for IoT applications. *Journal of Parallel and Distributed Computing*, *123*, 204-214. https://doi.org/10.1016/j.jpdc.2018.09.011 , [accessed on Sept. 2020]

[2] Arshad, R., Zahoor, S., Shah, M. A., Wahid, A., & Yu, H. (2017). Green IoT: An investigation on energy saving practices for 2020 and beyond. *IEEE Access*, *5*, 15667-15681.

[3] Aazam, M., & Huh, E. N. (2014, August). Fog computing and smart gateway-based communication for cloud of things. In *2014 International Conference on Future Internet of Things and Cloud* (pp. 464-470). https://doi.org/10.1109/ficloud.2014.83 , [accessed on Sept. 2020]

[4] X. Jia, O. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in internet of things (IoT)," in Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Yichang, China, Apr. 21–23, 2012, pp. 1282–1285 https://doi.org/10.1109/cecnet.2012.6201508 , [accessed on Sept. 2020]

[5] S. Li, L. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 2177–2186, Nov. 2013. https://doi.org/10.1109/tii.2012.2189222 , [accessed on Sept. 2020]

[6] W. He and L. Xu, "Integration of distributed enterprise applications: A survey," IEEE Trans. Ind. Informat., vol. 10, no. 1,pp. 35–42, Feb. 2014. https://doi.org/10.1109/tii.2012.2189221 , [accessed on Sept. 2020]

[7] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015. https://doi.org/10.1007/s10796-014-9492-7 , [accessed on Sept. 2020]

[8] Z. Pang, Q. Chen, W.Han,andL. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," Inf. Syst. Front., vol. 17, no. 2, pp. 289–319, 2015 https://doi.org/10.1007/s10796-012-9374-9., [accessed on Sept. 2020]

[9] Zanella, N.Bui, Castellani, L.Vangelista, and M.Zorzi,"Intern et of Things for Smart Cities,"IEEEInternetThingsJ.,vol.1,no. 1, pp. 22–32, 2014.

[10] https://doi.org/10.1109/jiot.2014.2306328. , [accessed on Sept. 2020]

[11] E. Gelenbe and Y.Caseau,“ The impact of information technology on energy consumption and carbon emissions,” Ubiquity, vol. 2015, no. June, pp. 1–15, 2015. https://doi.org/10.1145/2755977 , [accessed on Sept. 2020]

[12] F. K. Shaikh, S. Zeadally, and E. Exposito, “Enabling Technologies for Green Internet of Things,” IEEE Syst. J., no. 99, pp. 1–12, 2015. https://ieeexplore.ieee.org/document/7088546 , [accessed on Sept. 2020]

[13] Huang, Y. Meng, X. Gong, Y. Liu and Q. Duan, "A Novel Deployment Scheme for Green Internet of Things," in *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 196-205, April 2014, https://ieeexplore.ieee.org/document/6718032 , [accessed on Sept. 2020]

[14] Y. Amin, “Printable green RFID antennas for embedded sensors,” Ph.D. dissertation, KTH School Inf. Commun. Technol., Kista, Sweden, 2013.

[15] M. Dayarathna, Y. Wen and R. Fan, "Data Center Energy Consumption Modelling: A Survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 732-794, First quarter 2016, doi: 10.1109/COMST.2015.2481183, https://ieeexplore.ieee.org/document/7279063 , [accessed on Sept. 2020]

[16] T. Li, S. S. Wu, S. Chen and M. C. K. Yang, "Generalized Energy-Efficient Algorithms for the RFID Estimation Problem," in IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp.1978-1990, Dec. 2012,doi: 10.1109/TNET.2012.2192448, https://ieeexplore.ieee.org/document/6188523 , [accessed on Sept. 2020]

[17] X. Xu, L. Gu, J. Wang, G. Xing and S. Cheung, "Read More with Less: An Adaptive Approach to Energy-Efficient RFID Systems," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1684-1697, September 2011, doi:10.1109/JSAC.2011.110917, https://www.infona.pl/resource/bwmeta1.element.ieee-art-000005992837 , [accessed on Sept. 2020]

[18] D. K. Klair, K. Chin and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," in IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 400-421, Third Quarter 2010, doi: 10.1109/SURV.2010.031810.00037, https://ieeexplore.ieee.org/document/5455790 , [accessed on Sept. 2020]

[19] C. Lee, D. Kim and J. Kim, "An Energy Efficient Active RFID Protocol to Avoid Overhearing Problem," in IEEE Sensors Journal, vol. 14, no. 1, pp. 15-24, Jan. 2014, doi: 10.1109/JSEN.2013.2279391., https://ieeexplore.ieee.org/document/6584733, [accessed on Sept. 2020]

[20] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, ‘‘Energy conservation in wireless sensor networks: A survey,’’ *Ad Hoc Netw.*, vol. 7, no. 3, pp. 537–568, May 2009. https://doi.org/10.1016/j.adhoc.2008.06.003 , [accessed on Sept. 2020]

[21] T. Rault, A. Bouabdallah, and Y. Challal, ‘‘Energy efficiency in wireless sensor networks: A top-down survey,’’ *Comput. Netw.*, vol. 67, pp. 104–122, Jul. 2014. https://doi.org/10.1016/j.comnet.2014.03.027, [accessed on Sept. 2020]

[22] C. Peoples, G. Parr, S. McClean, B. Scotney, and P. Morrow, “Performance evaluation of green data centre management supporting sustainable growth of the Internet of Things," Simul. Model. Pract. Theory.

[23] Z. Wang, Y. Liu, Y. Sun, Y. Li, D. Zhang, and H. Yang, “An energy efficient heterogeneous dual-core processor for Internet of Things," in Proc. IEEE Int. Symp. Circuits Syst., Jul. 2015, pp. 2301_2304.

[24] C.McKerracher and J. Torriti, “Energy consumption feedback in perspective: Integrating Australian data to meta-analyses on in-home displays, "Energy Efficiency, vol. 6, no. 2, pp. 387_405, 2013

[25] C. Occhiuzzi, S. Caizzone, and G. Marrocco, “Passive UHF RFID antennas for sensing applications: Principles, methods, and classifications "IEEE Antennas Propag. Mag., vol. 55

[26] A. Fensel,V.Kumar, and S. D. K. Tomic, “End-user interfaces for energy efficient semantically enabled smart homes," Energy Efficiency, vol. 7, no. 4, pp. 655_675, 2014.

[27] M. Aazam, I. Khan, A. A. Alsaffar and E. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," Proceedings of 2014

11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014, Islamabad, 2014, pp. 414-419, doi: 10.1109/IBCAST.2014.6778179., https://ieeexplore.ieee.org/document/6778179 , [accessed on July 2020]

[28] M. M. E. Mahmoud et al., "Enabling Technologies on Cloud of Things for Smart Healthcare," in IEEE Access, vol. 6, pp. 31950-31967, 2018, doi: 10.1109/ACCESS.2018.2845399. https://ieeexplore.ieee.org/document/8375951 , [accessed on 18 July 2017].

[29] Mingay, S. Green IT: The New Industry Shock Wave. 2007. Available online:http://www.ictliteracy.info/rf.pdf/Gartner_on_Green_IT.pdf (accessed on 18 July 2017).

[30] Kliazovich, D., Bouvry, P. & Khan, S.U. GreenCloud: a packet-level simulator of energy-aware cloud computing data centers. *J Supercomput*62, 1263–1283 (2012). https://doi.org/10.1007/s11227-010-0504-1 , [accessed on July 2020]

[31] M. V. Moreno-Cano, M. A. Zamora-Izquierdo, J. Santa, and A. F. Skarmeta, "An indoor localization system based on artificial neural networks and particle filters applied to intelligent buildings", Neurocomputing, vol 122, pp.116-125, Dec 2013.

[32] H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, "A first look at traffic on smartphones," in Proc. 10th Annu. Conf. Internet Meas. (IMC), 2010, p. 281.

[33] Ferdous, M. S., Hussein, R., Alassafi, M., Alharthi, A., Walters, R., & Wills, G. (2016). Threat taxonomy for cloud of things. *Internet Things Big Data Anal Recent Trends Challenges*, *1*, 149-191.

[34] B. Alohali, Security in Cloud of Things (CoT), in: Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, 1188–1212, 2019.DOI: 10.4018/978-1-5225-8176-5.ch061 , [accessed on July 2020]

[35] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018, [accessed on July 2020

[36] Ari, A.A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroui, A.M., Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges, Applied Computing and Informatics (2019), doi: https://doi.org/10.1016/j.aci.2019.11.005, [accessed on July 2020]

[37] CSA, The Treacherous 12 - Cloud Computing Top Threats in 2016, Tech. Rep., Cloud Security Alliance, https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf, [Accessed on 10-Feb-2018], 2016.

[38] CSA, Top Threats to Cloud Computing, Tech. Rep. V1.0, Cloud Security Alliance, URL https://cloudsecurityalliance.org/topthreats/csathreats.v1.0., [Accessed on 10-Feb-2018], 2010