https://doi.org/10.48009/4_iis_2020_253-263

Issues in Information Systems
Volume 21, Issue 4, pp. 253-263, 2020

IOT SECURITY AND THE ROLE OF AI/ML TO COMBAT EMERGING CYBER THREATS IN CLOUD COMPUTING ENVIRONMENT

Temechu G. Zewdie, University of the District of Columbia, temechu.zewdie@udc.edu
Anteneh Girma, University of the District of Columbia, anteneh.girma@udc.edu

ABSTRACT

Internet of Things (IoT) has become one of the cutting-edge technologies and an attractive area of interest for the research world, and economically attractive for the business world. It involves the interconnection of multiple devices and connections of devices to humans. IoT requires a cloud computing environment to handle its data exchange and processing. At the same time, it requires artificial intelligence (AI) to analyze the data stored at cloud infrastructure and make fast and reliable intelligent decisions. These interconnected IoT devices use their unique-identifiers and the embedded sensor with each device to communicate with each other, and exchange information among them using an Internet and cloud-based network infrastructure (Girma, 2018). *We are living in the era of big data where the necessity of applying AI/ML has been very critical to the process and analyze the collected cloud-based big data fast and accurately. However, even though AI is currently playing a vital role in improving the traditional cybersecurity, both the cloud vulnerability and the networking of IoT devices are still major threats. Besides the security issues of cloud computing, IoT devices, and AI is being used by hackers and continues to be a threat to the world of cybersecurity. Moreover, most of wirelessly accessed IoT devices deployed on a public network are also under constant cyber threats. This research paper will propose a hybrid detection model as a solution approach using artificial intelligence and machine learning (AI/ML) to combat and mitigate IoT cyber threats on cloud computing environments both at the host-based and network level.*

KEYWORDS- IoT security; cyber threats, Cloud Computing, artificial intelligence, machine learning

INTRODUCTION

IoT is, by far, considered to be the next best bet in technology. Together with big data on the cloud and artificial intelligence Internet of Things covers the data communication system. (Chen, 2020). According to (Mark Patel, 2020), approximately 127 new devices connected to the internet every second, and it is anticipated that the worldwide number of connected devices will increase by more than 27 billion by 2025, which is almost a threefold increase from 2018. (Mark Patel, 2020) The higher the deployment of IoT devices, the higher has been the trend in IoT Market size growth. Moreover, the higher the number of IoT devices, the higher has been the amount of cloud-based big data and the importance of data and network security. But even though the growth and gain of IoT devices deployment brought a high ROI (Return on Investment) value, the security of IoT devices and the constant cyber threat on the cloud network infrastructure has been one of the critical security issues.

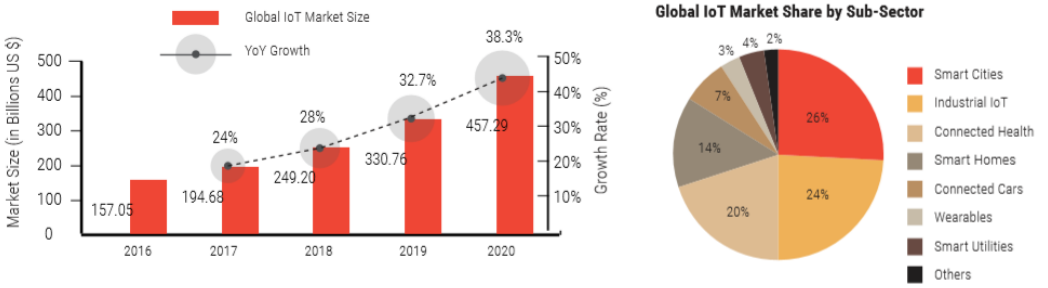

Figure 1 The Growth of IoT Market Size and its share by Submarket **(GrowthEnablerIoT, 2017)**

Given The Internet of things (IoT), which is the network of variety of interconnected devices, provide intelligent based services using the Internet, the users' privacy and different cyber-attacks while data is in use, on transit, or at rest requires the highest level of protection. To meet this requirement, we are approaching these security issues using a hybrid proposed solution model applying AI/ML models that include supervised learning, unsupervised learning, and reinforcement learning. The application of AL provides a more secure environment on the cloud and helps to ensure the possibility of realizing the full potential of the Internet of things.

IoT Security Challenge

Proper protection helps keep data private, restricts access to devices and cloud resources, offers secure ways to connect to the cloud, and audits device usage. An IoT security strategy reduces vulnerabilities using policies like device identity management, encryption, and access control. Yadav, Pooja, and Ankur explained how IoT becomes a worth, but massive amounts of data increased its complexity in detection, communications, controller, and in producing awareness. They also described how the growth of its data size on a real-time significantly affects the data and network vulnerabilities (Yadav, Mittal, & Yadav, IoT: Challenges and Issues in Indian Perspective, 2018).

IoT security in the interconnected network infrastructure, the security of IoT communication, and connectivity among IoT devices are the main threat and vital concern. From the Data Security point of view, the major problem with IoT devices is that the design of most of them is incompetent to handle cyberattacks and privacy threats. Thus, it leaves the whole IoT network exposed to vulnerabilities. Security experts state that most of the IoT devices come with a lack of safeguards and, therefore, become an easy target for attackers. Even though it is not the case with all objects connected in the IoT network, identifier specific codes and identification codes for particular devices, like the IMEI number for mobile phones is another security challenge. Finally, access to vulnerable devices could provide easy access for cybercriminals, and they could quickly gain access to other connected systems in the network. To mitigate these challenges, IoT Security needs artificial intelligence played a significant role as a security tool.

IoT Security Needs and Artificial Intelligence (AI) as a Security Tool

The enormous and bulk presence of IoT devices has brought a new dimension and paradigm shift in the computing world (Girma, 2018). The scenario of interconnected devices at every household is very likely at an alarming rate. The need for having a more reliable cybersecurity infrastructure to handle and mitigate the risk against the data at rest, data in use, and data in motion, has been one of the critical security needs. Moreover, a high level of security requirements for IoT data collection, its information exchanging route, and the cloud platform where the data storage and analytics taking place, reach the highest level. (Efstathopoulos, 2019)

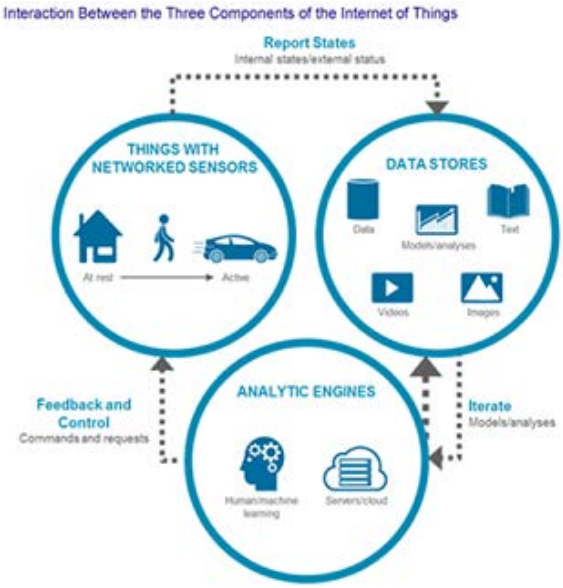

Figure 2 Interacting between IoT Components **(Dataflair Team, 2018)**

Given its highly scalable cyber-physical system nature and having as many as interconnected devices where its data movement and analytics happen in a very complex Wide Area Network(WAN), the application of different AI mechanisms has been very critical and exploited more to deliver a more viable Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) capabilities. Many organizations have deployed Artificial Intelligence (AI) as a part of their threat intelligence mechanism to have a reliable cyber defense posture to mitigate the risk aimed at their infrastructure.

The shortcoming of traditional security techniques, which are very much rule-based, has led mainly to see AI serving as the main workhorse of cyber defense. Currently, AI is delivering organizations to have security control support in the continuing barrage of cyber-attacks. Given all IoT data storage and computation take place on the cloud environment and cloud security is another paramount concern, AI applications as a part of cyber defense strategy is becoming a default norm and contributing tremendously at a high level. Among the main benefits that AI/ML delivers include but not limited to: Reporting existing vulnerabilities on real-time, Big IoT Data Analytics, Cyber Attack Detection, and Containment Delivering Threat Alert.

Threat and Drawbacks of AI/ML

Even though the advancement of AI/ML has promised and delivered an advantage to robotics science and cybersecurity, it has also displayed contrary features and allowed hackers to develop and deploy sophisticated AI/ML for cyber-attacks. They are working day and night to investigate and deliver a more advanced AI/M that adapts to new attack vectors and uses it to stimulate the same type of attacks. Moreover, hackers could apply AI /MI to test their malware and learn and enhance its effectiveness to be able to penetrate and breach their adversary's infrastructure equipped with another AI/ML. The more the AI/ML tested and trained, the most catastrophic damage will be inevitable.

Other drawbacks associated with AI include its high cost, limitation of originality, being incapacitated to replicate human beings, unemployment, still needs human inputs to improve, and responding effectively to different cyber-attacks. Its effectiveness is almost dependent on the accuracy and availability of its training dataset coming from various sources. It requires accurate datasets to learn from the required level because it lacks creativity and improvement even with experience. Technology is getting spread widely in a sophisticated manner. It caused to have the potential for malicious insiders or external threats who can precisely exploit and poison the training

data to develop algorithms that have catastrophic effects and dangerous flaws that are very difficult to detect and almost impossible to trace.

IoT and Cloud Computing

Cloud Computing is needed to address the dynamic, exponentially growing demands for real-time, reliable data processing of IoT, and both Cloud computing and the IoT have a complementary relationship. (ESDS, 2018) The IoT generates massive amounts of data whereas, cloud computing ads in offering a pathway for that data to travel to its destination, thus helping to increase efficiency in our work.

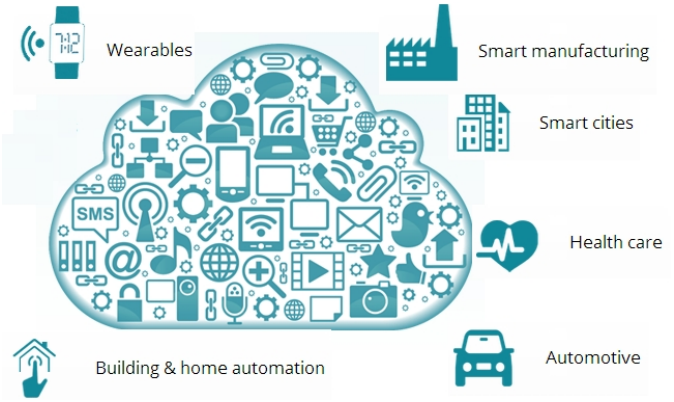

Figure 3 Cloud computing and IoT security Issue **(Javed, 2017)**

When some clouds are compromised, a hybrid detection technique is useful to detect malicious code. To mitigate such malicious code, they advised on their research to using combined with signature-based detection technique and behavior-based detection technique highly advisable (Stojmenovic & Wen, 2014).

From the Data Protection perspective, Messages generated from IoT devices sent to the nearest cloud. When distributed and processed data have merged, the integrity of the data should be guaranteed in a cloud environment. Because of limited resources, it is difficult to encrypt or decrypt data on the IoT device, so light-weight encryption algorithms or masking techniques are required. (Stojmenovic & Wen, 2014)

The Challenges to AI Adoption in Cloud Computing

AI is not a bulletproof tool to use for all business problems, and its adoption is not an easy process. Its deployment could bring several technical challenges as there are not enough AI skills on board at most of the business organizations to tackle them promptly. Data issues such as having a lack of structure and relevance are another significant factor not to adopt AI on the cloud. Even though its expansion and deployment in the cloud with big data is increasing, moving AI workloads to the cloud has been the biggest challenge. Dealing with sparse and unstructured data, data access, and managing AI workload in the cloud are big challenges for AI adoption on the cloud. Ethical issues are another main factor that proves the controversial nature of AI applications. These challenges have based on how we apply the AI tools and how it ends up causing a lot of harm. Organizations planning or initiating plans to adopt AI should have (or be prepared if they don't) to build a culture particularly among the technical people who deploy AI technologies and exposed to observe the potential risks earlier to alarm the senior management.

RELATED WORK

IoT Security studies (Yadav, Mittal, & Yadav, IoT: Challenges and Issues in Indian Perspective, 2018), (Wu, Ping, Ke, & Hai-xin, 2011) proposed various solutions for malware detection and prevention recently that include non-machine learning solution.

Researchers propose a hybrid model for classification, and an enhanced History-based IP Filtering scheme to mitigate a DDoS attack on the SDN-based cloud environment (PHAN & PARK, 2019). This research focused on the non-machine learning-based solution. Moreover, it looks effective to evaluate DDoS detection and prevention on a software-defined network (SDN) environment. But a solution provided by the researcher was not the best fit to address IoT Security issues to combat emerging cyber Threats in a cloud computing environment.

The researchers proposed the DQEAF framework that has been evaluated by other families of malicious software, which shows good robustness (Anderson, Kharkar, & Filar, 2017). The training process depends on the characteristics of the raw binary stream features of samples. The experiments show that the proposed method has a success rate of 75%. But their solution still needs further work to maximize the detection efficiency, and their ultimate solution is limited to their research problem.

In flow-based malware detection using convolutional neural network research, the researchers suggested an automated malware detection method using CNN, and other machine learning algorithms (Yeo, et al., Flow-based Malware Detection Using Convolutional Neural Network, 2018). For classification purposes, they applied CNN, multi-layer perceptron (MLP), support vector machine (SVM), and random forest (RF), and their research showed >85% accuracy, precision, and recall for all classes using CNN and RF. From this result, we learned the result depicted that further methodology will be needed to get a better precision result.

As referred from the aforementioned related works, we learned that malware detection from the host side with non-machine algorithms take with a maximum of 85% precision. But our case will be focused on the role of AI/ML for IoT Security to combat emerging Cyber threats (including malware) in the Cloud Computing environment. By considering the work-related AI/ML algorithms, this research will follow the following solution approach to combat and mitigate IoT cyber threats on cloud computing environments both at the host-based and network level.

PROPOSED SOLUTION APPROACH

Security is neither particular nor unique to a computerized system or its configuration (Chung, Kim, & Jeon, 2016). Protection always applies to a broader spectrum of computational technologies (Cano, 2016), Cybercriminals and hackers are still coming with new-age techniques and strategies to discover vulnerabilities in our systems. Hence, a more dynamic and responsive system is required to provide a solid defense against these threats. Security experts consider AI and ML to provide a water-tight security mechanism as these solutions collect and analyze information from previous attacks and provide a solution based on this data. These systems continuously monitor the network and keep investigating previous attacks and even identify attacks that could similarly occur in the future. Hence, AI/ML solutions do not wait for an attack to happen but work on predicting an attack based on history and suggest solutions to fight the threat. All attacks are 100% original, and they come up with new techniques every day. Instead of a slightly modified version of the older methods, this research approaches to resolve the IoT devices' security issues by learning and analyzing the previously detecting cyber-attacks. So that our AI/ML solutions will equip with the history of attacks and their patterns, and it can easily detect future attacks and walled security against zero-day attacks.

Moreover, artificial intelligence and machine learning work without human intervention, and hence the need for physical resources to monitor the network is not required 24x7. It even saves a significant amount of money for enterprises in hiring cybersecurity experts in large numbers. Machine learning (ML) is quite active when it has a vast database to work. To implement the algorithm in practice, our research use and apply mandatory datasets user data and endpoint log files for host base detection and network data for network-level detection. While the number of security warnings and alerts can be a lot to handle for humans, the application of advanced security systems using AI/ML solves the problem. In fact, without the help of these advanced security systems, it would be quite impossible for security teams in cloud data centers to maintain security. This research approaches the security issues at cloud network infrastructure by developing predictive analysis to

prevent future attacks. Therefore, this paper will use a suitable dataset taken from CIADA and Packt to build the right AI/ML application (Packt, 2020).

Data Classification Architecture

IoT security is a crucial component to provide reactive and preventive security policies so that controls can in place to physical platform and software layers. The following architecture depicts the uses of deep learning that can help in identifying or classifying the attacks.

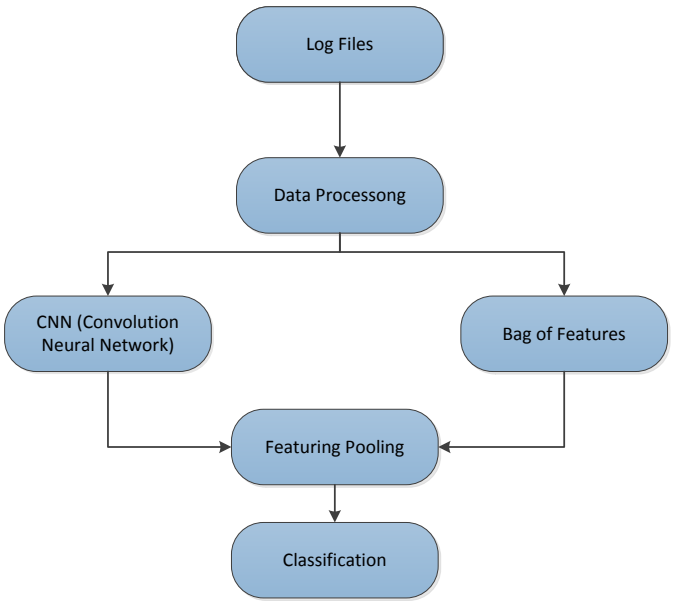

Figure 4 Data Classification Architecture **(Sakhavi, Guan, & Yan, 2015)**

Deep learning artifacts consist of different layers operating in parallel. These layers include, primarily an input layer, multiple hidden layers, and an output layer. They are interconnected through neurons with each layer using the output of the previous layer as its input. The hidden layers are the keystone of Deep Learning. Each of these layers focuses on one specific feature with the output of the other layers to better learn and improve its inference.

Proposes Methodology

Machine learning helps in identifying attacks in IoT security by using extraction and classification processes. **CNN** can be used to perform the Extraction of features from the raw data by using backpropagation while training the data and SVM can be used to classify the attacks based on the features obtained. Convolutional neural networks (CNNs) work well on large datasets. But a considerable amount of datasets are not always available. Therefore, in this research, Bayesian CNN will play a vital role, which offers better robustness to over-fitting on small data than traditional approaches (Gal & Ghahramani, 2016).

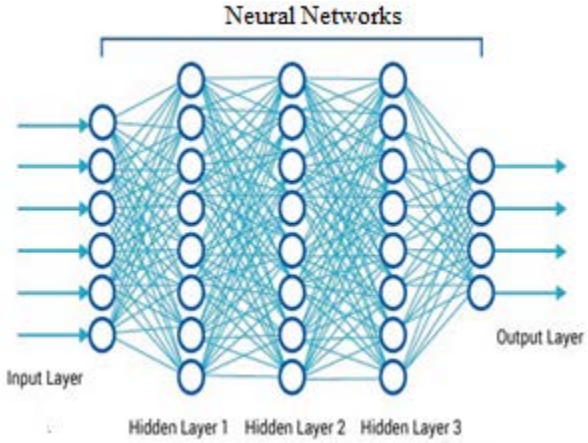

Figure 5 the Neural Network Architecture **(Ekababisong, 2020)**

Extraction

Bag of features generated in parallel to CNN can also be incorporated with the features extracted from CNN by feature pooling (Parisi, 2019) (Islamia, 2006). In our proposed Data Classification Architecture shows a feature pooling combines the features generated from both the pipeline. See Figure 4.

Classification algorithm

In this research, Convolutional neural network (CNN) and three other machine learning algorithms, such as multi-layer perceptron (MLP), support vector machine (SVM), and random forest (RF), classified six-class flow data with five-fold cross-validation (Yeo, et al., Flow-based Malware Detection Using Convolutional, 2018). SVM supervised learning that requires big data and helps in predicting the threats after the models have trained. With a significant amount of data, we can avoid both under-fitting and overfitting cases (Parisi, 2019). Moreover, Linear SVM uses a discriminant Hyperplane that maximizes a margin. That is the distance from the nearest training point (Hasan, 2017).

Given a set of data x_i (i=1, 2... M), where *M* is the number of given data set. These sets have two classes that are positive class and negative class. We denote $\mathbf{y}_i = 1$ for the positive class and $\mathbf{y}_i = -1$ for the negative class, respectively. It is possible to find a hyperplane $f(\mathbf{x}) = 0$ that classifies the given dataset

$$f(\boldsymbol{x}) = \boldsymbol{w}^{\mathrm{T}}\boldsymbol{x} + b = \sum_{j=1}^{M} w_j x_j + b = 0$$

(Lei, 2017)

Where **w** is an *M*-dimensional vector, and *b* is a scalar, and they are used to define the hyperplane.

To implement the CNN model, we use Colab, which is a Jupyter notebook environment that runs entirely in the cloud. In this environment, Keras packages and other machine learning algorithms will implement include using Scikit-learn package, and python3 programming language that can use to build our models

We also calculate the cost, error, or loss C of a given batch N of the dataset.

$$C(W) = \frac{1}{2}\sum_{i=1}^{N} \|y_i - \hat{y}_i\|^2$$

(Cover & Thomas, 2005)

Where C (**W)** is a *Cost of Error* and *N* is a given dataset, 'i' is the number of data points in the given dataset.

Pattern Matching

As referred (Quan & Hong-Yi, 2009)**,** an entropy-based approach is suitable to detect modern malware based on anomalous patterns in a network. This network anomaly detection method can use for the detection of malicious patterns and indicators in our given datasets (Parisi, 2019).
As we are dealing with determining pattern or anomaly detection using a statistical approach, We use the idea of entropy to calculate the randomness of the incoming internet packets X1, X2, X3,… , X4 associated with random variable (vector) X, where
X= (X1, X2, X3,…,Xn) and each incoming packets have p number of features. The entropy of a multivariate random variable is:

$$H(X) = -\sum_{xi \in X} p(xi) * log(p(xi)) \qquad \text{(Cover \& Thomas, 2005)}$$

Where p(xi) is the frequency/probability of letter x, i.e. called the (Shannon) entropy.

ANALYSIS AND DISCUSSIONS

A successful cybersecurity solution is one that could detect threats and attacks promptly before they create havoc in the system. Most cybersecurity professionals think tactically about security, but effective security decisions always originate with a prudent policy. (Nash, 2009) Timely detection is the key, and that is where traditional security solutions fail. Most of these solutions can be termed mainly as responsive solutions as they react only after an attack. Hence, we can rightly call the next-gen solutions AI/ML as they not only combat attacks but also come up with predictive analysis to prevent attacks in the future. Solutions developed using AI and ML can primarily help to detect the similarities among numerous attacks that happened in the past and provide an instant warning when it detects another with the same pattern. The best thing about AI/ML is that it can continuously decipher user behavior, changing use patterns, and all types of irregularities. However, there are a few pre-requisites like data availability and restrictions to an efficient AI/ML solution. For Machine learning solutions, it is essential to have access to an appropriate level of datasets. Limited data access would largely handicap ML security solutions to evaluate security risks or study past behavior and patterns.

FUTURE WORK AND RECOMMENDATION

Artificial Intelligence and Machine Learning play a massive role in enhancing cybersecurity. In the same manner, they also improve the quality of our daily lives through IoT devices, smarter homes, smart cars, etc. Any advanced security solution cannot be a complete solution unless it contains some parts of AI and ML features in it. Solutions developed using AI and ML can primarily help to detect the similarities among numerous attacks that happened in the past and provide an instant warning when it detects another with the same pattern. The best thing about AI/ML is that it can continuously decipher user behavior, changing use patterns, and all types of irregularities. (Ghanchi, 2019)

One of our research recommendations that security experts agreed upon is to standardize the data sets available to make things easy for ML-based solutions to decipher the data and analyze it quickly. The volume of our research dataset will express in terms of exabytes. Once the data sets are defined and standardized, ML-based systems will become quite useful in combating cyber threats.

Based on our proposed research solution, we recommend drawing a fine line between finalizing on whether to go for an unsupervised solution or a supervised one based on features extracting from our data set. While AI and ML systems can work independently without the supervision of humans, it is still prudent that a small intervention by humans will make the system more balanced and effective.

Even though our proposed hybrid detection model focused on combat emerging cyber threats on both host and network level, we additionally proposed using different algorithms such as Apriori and Eclat for alerting purposes while detecting similar cyberattacks.

Finally, we do apply different performance indicators such as Accuracy, Specificity, and Sensitivity to evaluate the performance of our research methodology. Accuracy is the proximity of measurement results to the true value. Whereas, precision is the degree to which repeated measurements under unchanged conditions show the same results. Whereas, Specificity is the true negative rate or the proportion of negatives that are correctly identified [23].

Accuracy = (TP + TN) / (TP + TN + FP + FN)	(Nash, 2009)
Specificity = TN / (TN + FP)	(Nash, 2009)
Sensitivity = TP (TP + FN)	(Nash, 2009)
Precision = TP (TO + FP)	(Nash, 2009)

Where, TP, TN, FP, and FN indicate true positive, true negative, false positive, and false negative, respectively.

CONCLUSION

We are living an era where most of the advanced security solution contains some form of AI/ML to be a complete solution. Artificial Intelligence and Machine Learning play not only a massive role in enhancing traditional cybersecurity but also improve the quality of our daily lives through IoT devices like smarter homes, smart cars, etc. Security experts also recommend that organizations need to draw a fine line between finalizing on whether to go for an unsupervised solution or a supervised one. While AI and ML systems can work independently without the supervision of humans, it is still prudent that a small intervention by humans will make the system more balanced and effective. One of the most fundamental recommendations that security experts make is to standardize the data sets available to make things easy for ML-based solutions to decipher the data and analyze it quickly. Once the data sets are defined and standardized, our ML-based systems will become quite useful in combating any kind of cyber threats. We are going to present our preliminary result and discuss the data analysis report with our next research paper.

REFERENCES

Allwin . (2019). *Allwin* . Retrieved 04 05, 2020, from https://www.allwyncorp.com/5-ways-to-fight-cyber-attacks-using-ai/

Anderson, H. S., Kharkar, A., & Filar, B. (2017). Evading Machine Learning Malware Detection. *International Journal of Applied Engineering Research*, *12*.

Cano, J. J. (2016, September 01). *ISACA JOURNAL*. Retrieved 04 04, 2020, from https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/cyberattacksthe-instability-of-security-and-control-knowledge

Capgemine reseach inistitute. (2019). Retrieved 03 26, 2020, from https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

Chen, Y. (2020). IoT, cloud, big data and AI in interdisciplinary domains. *ScienceDirect*. doi:https://doi.org/10.1016/j.simpat.2020.102070

Chung, B., Kim, J., & Jeon, Y. (2016). On-demand security configuration for IoT devices. *2016 International Conference on Information and Communication Technology Convergence (ICTC)*(IEEE). Retrieved from On-demand security configuration for IoT devices

Cover, h. M., & Thomas, J. A. (2005). Elements of Information Theory. A John Wiley and Sons.

Dataflair Team. (2018, 09 15). Retrieved 04 20, 2020, from https://data-flair.training/blogs/how-iot-works/

Efstathopoulos, P. (2019, 07 29). *2019*. Retrieved 04 26, 2020, from https://www.nortonlifelock.com/blogs/research-group/cloud-security-overwhelming-ai-and-machine-learning-can-help

Ekababisong. (2020). *Deep Learning*. Retrieved from https://ekababisong.org/ieee-ompi-workshop/deep_learning/

ESDS. (2018, 07 07). *Cloud Computing & IOT*. Retrieved 04 26, 2020, from https://www.esds.co.in/blog/cloud-computing-iot/#sthash.KxMbmjwy.dpbs

Gal, Y., & Ghahramani, Z. (2016). , offering better robustness to over-fitting on small data than traditional approaches.

Ghanchi, J. (2019, March 19). Retrieved 03 30, 2020, from https://thenewstack.io/the-possibilities-of-ai-and-machine-learning-for-cybersecurity/

Girma, A. (2018). Analysis of Security Vulnerability and Analytics of Internet of Things (IOT) Platform. *Information Technology - New Generations, 738*, 101-104. Retrieved 04 04, 2020, from https://link.springer.com/chapter/10.1007/978-3-319-77028-4_16

GrowthEnablerIoT. (2017, April). *Market pulse report, Internet of things (IoT)*. Retrieved from https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

Hasan, M. S. (2017). An Application of pre-Trained CNN for ImageClassification. *2017 20th International Conference of Computer and Information Technology (ICCIT).* Dhaka.

Islamia, J. M. (2006). A neuro-fuzzy approach for prediction of human work efficiency in noisy environment. *Applied Soft Computing, 6*(3), 283-294.

Jaleesa, B. (2020). *Smart Home Statistics.* Retrieved 03 2020, from https://ipropertymanagement.com/research/iot-statistics

Javed, A. (2017, 01 09). *IoT, and the emerging era of Cloud Computing*. Retrieved 04 02, 2020, from IoT, and the emerging era of Cloud Computing

Khan, M. (2016, January). *ISACA Journal.* Retrieved 03 26, 2020, from https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/managing-data-protection-and-cybersecurityaudits-role

Lea, P. (2018). *Internet of Things for Architects.* Mumbai: Packt Publishing Ltd.

Lei, Y. (2017). *Linear Support Vector Machine*. (Individual intelligent method-based fault diagnosis) Retrieved from https://www.sciencedirect.com/topics/engineering/linear-support-vector-machine

Mark Patel, J. S. (2020, 01 13). *McKinsey & Company*. Retrieved 04 20, 2020, from https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things

Nash, J. (2009, 05). Retrieved 04 04, 2020, from https://www.cio.com/article/2427814/enterprise-data-security--definition-and-solutions.html

Nash, J. (2009). *Enterprise Data Security: Definition and Solutions.* Retrieved from https://www.cio.com/article/2427814/enterprise-data-security--definition-and-solutions.html

Packt. (2020). Retrieved 05 04, 2020, from https://hub.packtpub.com/25-datasets-deep-learning-iot/

Parisi, A. (2019). *Hands-on Artificial Intelligence for Cybersecurity.* Birmingham: Packt.

PHAN, T. V., & PARK, M. (2019). Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud. *IEEE.*

Quan, Q., & Hong-Yi, C. (2009). Entropy Based Method for Network Anomaly Detection. *15th IEEE Pacific Rim International Symposium on Dependable Computing.* Shanghai.
risks, C.-c. a. (2018, 07 07). *itbusiness.ca*. Retrieved 04 10, 2020, from https://www.itbusiness.ca/news/cloud-computing-and-the-seven-deadly-data-risks/11810

Sakhavi, S., Guan, C., & Yan, S. (2015). Parallel Convolutional linear neural network for motor Imagery classification. *European Signal Processing Conference (EUSIPCO).*

Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *Federated Conference on, 2*.

Tano-Consultants. (2020). Retrieved from http://tano-consultants.com/home/
Wikipedia. (2017). *https://en.wikipedia.org/wiki/Sensitivity_and_specificity.* Retrieved 04 26, 2020, from https://en.wikipedia.org/wiki/Sensitivity_and_specificity

Williamson, J. (2020). *Dummies.* Retrieved 04 26, 2020, from https://www.dummies.com/careers/find-a-job/the-4-vs-of-big-data/

Wu, L., Ping, R., Ke, L., & Hai-xin, D. (2011). Behavior-based Malware Analysis and Detection . *2011 First International Workshop on Complexity and Data Mining.*

Yadav, E. P., Mittal, E. A., & Yadav, D. H. (2018). IoT: Challenges and Issues in Indian Perspective. *3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU).* Bhimtal, India.

Yadav, E. P., Mittal, E. A., & Yadav, H. (2018). IoT: Challenges and Issues in Indian Perspective. *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU).* Bhimtal, India.

Yeo, M., Koo, Y., Yoon, Y., Hwang, T., Ryu, J., & Song, J. (2018). Flow-based Malware Detection Using Convolutional Neural Network. *2018 International Conference on Information Networking (ICOIN).* Chiang Mai.

Yeo, M., Koo, Y., Yoon, Y., Hwang, T., Ryu, J., Song, J., & Park, C. (2018). Flow-based Malware Detection Using Convolutional. *2018 International Conference on Information Networking (ICOIN).*