IOT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment

Temechu G. Zewdie
Computer Science & Information Technology Department
University of the District of Columbia
temechu.zewdie@udc.edu

Anteneh Girma , **PhD**
Computer Science & Information Technology Department
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 attracting area of interest for the research world, and economically attractive for the business world. It involves interconnection of multiple devices and connections of devices to humans. IoT requires cloud computing environment to handle its data exchange and processing; and at the same time, it requires artificial intelligence (AI) to analyze the data stored at cloud infrastructure and make very fast and reliable intelligent decisions. These interconnected IoT devices use their unique-identifiers and the embedded sensor with each device to communicate to each other and exchange information among them using the internet and cloud-based network infrastructure [1]. 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 bigger role in improving the traditional cybersecurity, both the cloud vulnerability and the networking of IoT devices are still major threats. Beside the security issues of cloud and IoT devices, AI is also 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***

1. INTRODUCTION

IoT is, by far, considered to be the next best bet in technology. Together with big data on the loud and artificial intelligence IoT covers the data communication system. **[2]**. According to **[3]**, 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. **[3]** 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.

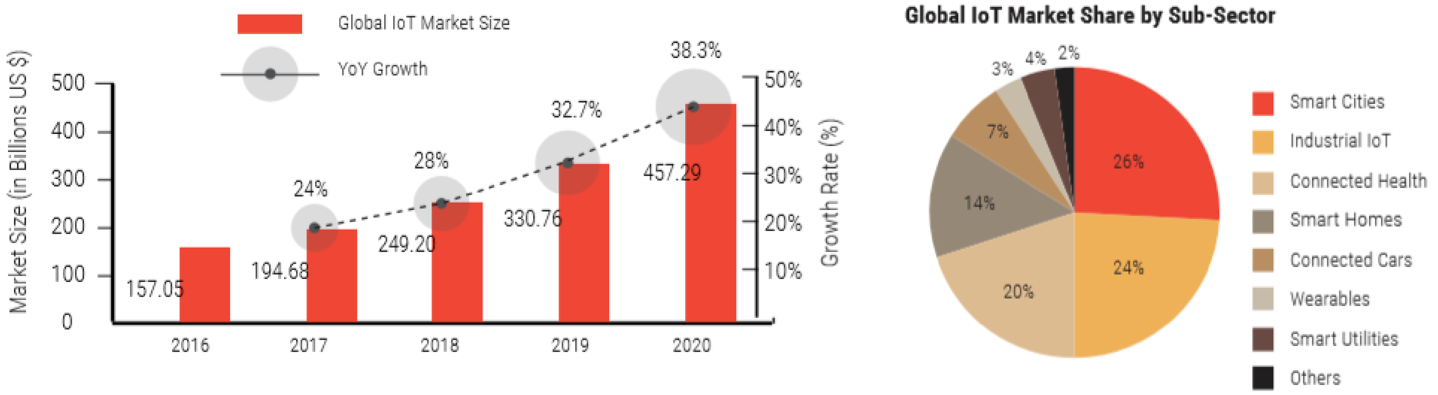

Figure 1 The Growth of IoT Market Size and its share by Submarket [4]

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. In order to meet this requirement, we are approaching these security issues using a hybrid proposed solution model applying AI/ML models including supervised learning, unsupervised learning, and reinforcement learning. The application of AL provides a more secured environment on the cloud and helps to ensure the possibility of realizing the full potential of Internet of things.

1.1. 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 highly affects the data and network vulnerabilities **[5]**.

IoT security in the interconnected network infrastructure, the security of the communication, and connectivity among IoT devices is a major threat and a 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. As Jason, ensuring the security of 4V's of big data volume, velocity, variety, and value will be a challenge. [6]

Besides, device identification (Object/Service Identifier) is another security challenge. This Identifier specific codes and identification codes for particular devices, like the IMEI number for your mobile phone. But that is not the case with all objects connected in the IoT network. Hence the present identification criteria will work for every device in the system.

Last but not least, Geo Location is another essential aspect of providing the right kind of security is when we know the exact physical location of the device. While we can extract such information from a mobile phone or smart TV, it is not the case with all devices connected to the network.

Finally, Leads Access to other devices which is Vulnerabilities in the devices could provide easy access for cybercriminals, and they could quickly gain access to other connected systems in the network is a significant challenge. For example, a simple compromise with a baby monitor connected to the IoT network would provide easy access for cybercriminals to other devices, including connected cars, connected homes, smart TVs, etc. To mitigate the aforementioned challenges IoT Security needs and artificial intelligence (AI) as a security tool.

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

According to Girma [1], the enormous and bulk presence of IoT devices has brought a new dimension and paradigm shift in the computing world. The scenario of interconnected devices at every household is very likely at an alarming rate, and the needs 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 major 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 at the highest level. [7]

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, 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 in order to have a reliable cyber defense posture to mitigate the risk aimed at their infrastructure.

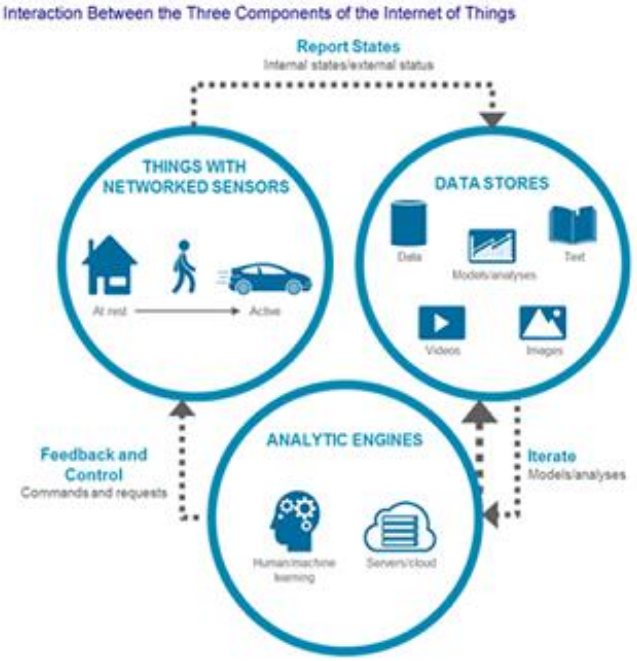

Figure 2 Interacting between IoT Components [8]

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 huge security control support in the continuing barrage of cyber-attacks. Given also all IoT data storage and computation take place on the cloud environment and cloud security is another paramount concern, even though AI is not bulletproof, its application as a part of cyber defense strategy is becoming a default norm and contributing tremendously at a high level. Among the major benefits that AI/ML deliver include but not limited to: Reporting existing vulnerabilities on real-time, Big IoT Data Analytics, Cyber Attack Detection, and Containment Delivering Threat Alert.

1.3. Threat and Drawbacks of AI/ML

Even though the advancement of AI/ML has promised and delivered a huge advantage to robotics science and cybersecurity, it has also displayed entirely opposite features and gave an opportunity for hackers to develop and deploy a fully sophisticated AI/ML for the purpose of cyber-attacks. They are working day and night to investigate and deliver a more sophisticated 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 own 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 will be the damage.

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 different sources. It requires accurate datasets to learn from at the required level because it lacks creativity and improvement even with experience.

Technology is getting spreading widely in a more sophisticated manner causing to have the potential for malicious insiders or external threats who are able to 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 it.

2. RELATED WORK

In the IOT Security area, many studies [9], [10] proposed various solutions for malware detection and prevention recently that include non-machine learning solution.

According to [11], they propose hybrid model for classification, and an enhanced History-based IP Filtering (eHIPF) scheme to make DDoS attack defender for the SDN-based cloud environment. In summary, this research focused on non-machine learning-based solution, and in this regard the research looks effective to evaluate in DDoS detection and prevention in SDN environment but the solution that provided by this researchers is not a best fit to address IoT Security issues to combat Emerging a cyber Threats in Cloud Computing Environment.

In [12], the authors proposed DQEAF framework that has been evaluated by other families of malicious software, which shows good robustness. 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 their ultimate solution is limited to their research problem.

In reference [13], the authors of flow-based malware detection using convolutional neural network research suggested an automated malware detection method using convolutional neural network (CNN) and other machine learning algorithms. For classification purpose, 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 needed to get a better precision result.

As referred from the aforementioned related works, we learned that malware detection from host side with non-machine algorithms have been worked with maximum of 85% precision. But our case is specifically focused the role of AI/ML for IoT Security to combat emerging Cyber threats (including malware) in 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.

3. PROPSED SOLUTION APPROACH

Security is neither particular nor unique to a computerized system or its configuration [14]. Protection always applies to a broader spectrum of computational technologies [15], 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. While hackers come up with new techniques every day, all attacks are 100% original, but 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 lot 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. In order 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 solve the problem. In fact, without the help of these advanced security systems, it would be quite impossible for security teams in large cloud datacenters 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 a right AI/ML application. [16]

3.1. Data Classification architecture

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

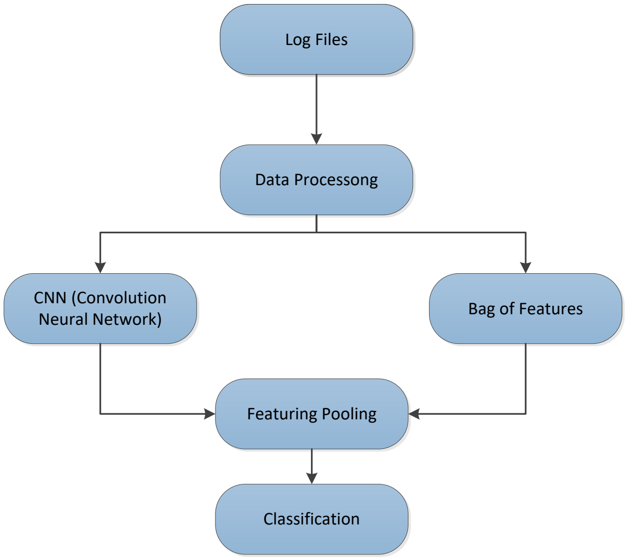

Figure 3 Data Classification Architecture

4. 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. [17]

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 is expressed in terms of exabytes. Once the data sets are defined and standardized, ML-based systems will become quite useful in combating of 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 research scope is only focused on a hybrid detection model to combat and mitigate IoT cyber threats on cloud computing environment both at the host-based and network-level, we additionally propose using different algorithms such as Apriori and Eclat for alerting purpose when detecting similar cyber attackers.

5. 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, 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.

6. REFERENCE

[1] A. Girma, "Analysis of Security Vulnerability and Analytics of Internet of Things (IOT) Platform," *Information Technology - New Generations*, vol. 738, pp. 101-104, 2018.

[2] Y. Chen, "IoT, cloud, big data and AI in interdisciplinary domains," *ScienceDirect*, 2020.

[3] J. S. a. C. T. Mark Patel, "McKinsey & Company," 13 01 2020. [Online]. Available: https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things. [Accessed 20 04 2020].

[4] GrowthEnablerIoT, "Market pulse report, Internet of things (IoT)," April 2017. [Online]. Available: https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf.

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

[6] J. Williamson, "Dummies," 2020. [Online]. Available: https://www.dummies.com/careers/find-a-job/the-4-vs-of-big-data/. [Accessed 26 04 2020].

[7] P. Efstathopoulos, "2019," 29 07 2019. [Online]. Available: https://www.nortonlifelock.com/blogs/research-group/cloud-security-overwhelming-ai-and-machine-learning-can-help. [Accessed 26 04 2020].

[8] "Dataflair Team," 15 09 2018. [Online]. Available: https://data-flair.training/blogs/how-iot-works/. [Accessed 20 04 2020].

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

[10] L. Wu, R. Ping, L. Ke and D. Hai-xin, "Behavior-based Malware Analysis and Detection," in *2011 First International Workshop on Complexity and Data Mining*, 2011.

[11] T. V. PHAN and M. PARK, "Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud," in *IEEE*, 2019.

[12] H. S. Anderson, A. Kharkar and B. Filar, "Evading Machine Learning Malware Detection," in *International Journal of Applied Engineering Research*, 2017.

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

[14] B. Chung, J. Kim and Y. Jeon, "On-demand security configuration for IoT devices," *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, no. IEEE, 2016.

[15] J. J. Cano, "ISACA JOURNAL," 01 September 2016. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/cyberattacksthe-instability-of-security-and-control-knowledge. [Accessed 04 04 2020].

[16] "Packt," 2020. [Online]. Available: https://hub.packtpub.com/25-datasets-deep-learning-iot/. [Accessed 04 05 2020].

[17] J. Ghanchi, 19 March 2019. [Online]. Available: https://thenewstack.io/the-possibilities-of-ai-and-machine-learning-for-cybersecurity/. [Accessed 30 03 2020].