International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://theaspd.com/index.php

Artificial Intelligence For Iot Security: Enhancing Cyber Defense In The Age Of Connected Devices

Medisetti Uday Charan[1*], Dr. Thummala Pavan Kumar[2]
[1*]Master of Technology, Department Of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. mudaycharan@gmail.com
[2]Professor, Department Of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddeswaram, Guntur, Andhra Pradesh, India., pavankumar_ist@kluniversity.in

Abstract– *In enabling objects for intercommunication and data exchange on their own, the Internet of Things (IoT) has changed the worldwide technological scene. Still, the rapid growth of Internet of Things devices creates serious security concerns. The resource-limited character of Internet of Things devices and the always growing complexity of cyberattacks make conventional security methods sometimes inadequate. Artificial intelligence (AI) is a feasible choice that is strengthening Internet of Things (IoT) security. This paper investigates its potential in threat detection, anomaly detection, intrusion prevention, and device authentication in order to increase IoT security using artificial intelligence. Throughout this research, the process of securing Internet of Things (IoT) ecosystems makes use of machine learning (ML), deep learning (DL), and artificial intelligence (AI-based frameworks). Furthermore discussed are possible future directions of study as well as the challenges resulting from mixing artificial intelligence with Internet of Things security.*
Keywords—*IoT security, Artificial Intelligence, Machine Learning, Intrusion Detection, Anomaly Detection, Cybersecurity*

INTRODUCTION

In additional from the IoT—the Internet of Things—has been behind changes in the business sector as well as in the experiences consumers have had. This is justified by the possibility to link billions of devices spread over different parts of the globe from one another. This is the reason this is so. This is the explanation among the several others why this is the case. This is the situation as this is the truth. Apart from the above stated factors, the person should consider a great spectrum of additional aspects. Apart from this, the Internet of Things (IoT) creates new attack surfaces even if it offers certain advantages in terms of data collecting and automation. Those engaged in cybercrime might be able to benefit from these attack surfaces through their activity. Hacker ability to take use of these assault surfaces helps them to maximize all the opportunities these surfaces provide. Using these attack surfaces, hackers most likely to target one of the targets and carry out their operations. This is thus related to the type of assault surfaces allow. Devices connected to the Internet of Things (IoT) lack enough defence against the cybersecurity risks existing when utilized with the current accessible solutions. This is so because these solutions were developed for systems like servers and personal computers, usually with longer lives. This leads to the case supporting their existence being this one. Personal computers and servers are two instances of systems that belong under this category; other kinds of systems are also feasible. Regarding the devices included in the Internet of Things, there are a few cases when the memory capacity, power capacity, and computing capability of these devices are restricted. Usually, these gadgets have little capacity to save data. This leads to occurrences occurring in the manner they do. The reason behind the occurrence of occurrences is this specific one. This outcome results from the fact that these devices lack the same degree of power as the systems meant to protect. This is hence the rationale behind it. This is the case, hence this is the reason as well. This is the reason it takes place and the outcome of which. Artificial intelligence (AI) has been pushed to top importance in order to meet this demand. This is the situation in line with the development in the security sector's demand for scalable, intelligent, and adaptable security measures. This explains why this has started in the first place. This is so because the number of specific chores related to cybersecurity has grown in connection to each other. < This explains why this started out in the first place. Particularly in the forms of machine learning (ML) and deep learning (DL), artificial intelligence (AI) has been quite successful at identifying and eliminating cyber risks in conventional information technology systems. AI has helped one to reach this success. Artificial intelligence helped one to achieve this achievement. Using a variety of approaches has let one realize this degree of accomplishment; each one of them has contributed to the whole success. Given the extent of this accomplishment—which has been carried out—this reflects the great range of the success that has been attained. Artificial intelligence made this amazing feat feasible; it was the engine behind the realization of this great success. Artificial intelligence provided the means by which this amazing accomplishment could be executed. Starting with the initial stage, there have

been a lot of different approaches used over time to achieve this degree of success up to now. beginning with the initial phase of the procedure. There is a great range of techniques among the several ways that have been implemented generally. These already described strategies are part of the range. These technologies are expected to significantly contribute to the enhancement of the security of the Internet of Things (IoT) by helping in the identification of intelligent risks, real-time analysis of anomalies, and predictive system maintenance. Furthermore rather likely is it that these technologies will enable the maintenance of predictive systems. This is the case as these technologies might help to streamline the maintenance of predictive systems, therefore simplifying the procedure involved. Given the likelihood that these technologies may be able to fulfil these responsibilities, this prospect should be given some thought in this regard. This is so because these technologies can help to simplify the management of predictive systems. The state of affairs is how it is for this specific reason. The revolutionary technical developments under discussion in this article might be able to significantly contribute in line with the one under discussion across this essay. This article is relevant in the context of surroundings connected with the Internet of Things (IoT), so the issue of artificial intelligence (AI) and the several methods in which it may be helpful to use is the main one of significance. The structure of the Internet of Things itself governs this topic. More especially, this essay fits under the context of settings related to different surroundings. Apart from this, the study investigates the prospect of future advancements in the same field of inquiry that is in progress right now. Furthermore included in this broad topic is the many approaches, the difficulties, and the possible future discoveries. This is done concurrently as well. The most of the research is focused on the possibility of future discoveries in this specific subject, which relates to the issue under discussion in this particular environment. Conducted within the framework of this specific topic area, the study is focused on the expected advancements that could occur in the years to come from this particular point of view.

LITERATURE REVIEW

This has resulted in smart settings spanning entire cities to individual homes. The creation of these settings follows from the significant expansion of the Internet of Things (IoT). Intelligent homes hitherto unattainable have been produced by the Internet of Things. The great influence that the created advancements have had on society has led to notable changes in many different fields directly resulting from them. Still, the reality of the matter is that this relationship generates major questions about the safety of the system even if it results in more productivity and automation. Given the great number of linked devices, which creates a large attack surface, hostile actors have no trouble using this potential weakness. < Moreover, there is a chance that those lacking of respect and honesty would employ these gadgets. Protecting devices connected to the Internet of Things is extremely challenging given the nature of the devices themselves. Apart from the fact that they have many sites where they do their business, they have limited means accessible to them. [2] They cannot accomplish this for this reason as well. It is clear throughout the past several years that artificial intelligence (AI) might be a workable method for improving Internet of Things (IoT) security. [3] One now finds that this material is accessible. This is the conclusion that has been obtained as a result of the fact that it has been established that conventional security measures are inadequate for systems that are both dynamic and dispersed. Artificial intelligence-powered security systems in real time can track, recognize, and remove any potential threats that could be on the property. One major benefit of these systems is their ability to accomplish all these tasks concurrently. These technologies also help as they allow one to adjust to the continually changing cyber dangers that arise. This provides a big advantage. A subfield of artificial intelligence, machine learning might be very helpful in identifying unusual activity that would point to a security breach. [5] < This identification might be quite helpful for spotting security lapses. This is the reason machine learning, one of the subfields under the cover of artificial intelligence, is underlined. Pattern recognition and data analysis help artificial intelligence models to distinguish between commercial acts that are lawful and those that are risky. This capacity helps the models to improve the running of the company. As so, the models are in a position to properly oversee the activities performed by the company. This directly makes it possible to implement more extra preventative safety precautions. Conversely, unsupervised learning methods enable the discovery of fresh attack paths by use of their capacity to detect deviations from the overall behavior of the system. An investigation of the system's behavior is one approach to do this. [37] [35] For example, one can teach supervised learning algorithms on past data to find risks already present. [7] This activity is conducted to fulfill the already mentioned goal regarding. Using a wide spectrum of tools and learning approaches, including several types of widely used learning processes, the discipline of machine learning makes advantage of Recent studies have made clear that artificial intelligence may enhance intrusion detection systems (IDS) for networks that are presently running and connected to the Internet of Things. {8} The results of the

research have clarified this ability—which was formerly unidentified. When it comes to the identification of prospective hazards, conventional intrusion detection systems (IDS) frequently make use of previously existing signatures. Still, these indicators will probably not be sufficient when faced with fresh risks not seen in the past. Conversely, the application of artificial intelligence increases the efficiency of intrusion detection systems (IDS) by means of constant learning from the acquired data derived from network traffic. The approach taken to do this is learning by machine. This results in the IDS having chances to keep developing their performance. [37] This thereby increases the capacity to identify zero-day attacks as well as other kinds of advanced incursions. This helps one to be more able to spot attacks of this nature. [10] Artificial intelligence might also be helpful throughout the process of automating reaction strategies. This is a reasonable possibility. This provides a plausible justification for the circumstances. This is why any probable risk that has been found will be eradicated right away and human involvement in the process will not be required at all. This is especially beneficial in ecosystems created on the Internet of Things, where the sheer volume of linked devices may make it challenging to personally monitor and react to all of the alerts, since it is easier to react to all of the signals. The Internet of Things gives to ecosystems this advantage. Eleven [11] Artificial intelligence has also been found to be valuable in the management of cryptographic keys and encryption technologies used to secure connections to the Internet of Things (IoT.). In this specific field, artificial intelligence has demonstrated its usefulness in a different sense. Many of the devices connected to the Internet of Things most certainly cannot benefit from the conventional encryption techniques. This is so because these techniques need a lot of processing power, which calls for certain resources. These gadgets depend on encryption of data, hence this is the case as well. One of the resources these devices possess is that their memory capacity and CPU power are below average. One of their components is therefore among their limitations. The encryption process might become more effective using artificial intelligence. Choosing suitable cryptographic methods catered to the particular restrictions of every device will help to achieve this. [13] This might be accomplished with the right algorithms used. This allows one to strike a good balance between security and performance, thereby benefiting one. This is a major benefit adding to the total advantage. These achievements notwithstanding, the integration of artificial intelligence into the security of the internet of things has also brought forth fresh challenges. This is so even if these benefits have been realized. Adversaries might start attacking artificial intelligence models themselves that they have produced. [14] One may find this to happen. Adversarial attacks are those in which hostile actors use input data manipulation to fool the artificial intelligence itself. [31] This is something you ought to know. There will be further conversation about these assaults right below. One must keep in mind that this is a rather important topic. One of the best examples of this is the scenario in which an opponent presents inputs that look benign but are actually meant to evade detection mechanisms. 20 [Here is a quite good example of the idea. Furthermore likely to cause privacy issues is the fact that artificial intelligence depends on large volumes of data. [34] This is particularly true in cases when sensitive data is sent via networks linked to the Internet of Things (IoT). Artificial intelligence-based security solutions are more challenging to implement in Internet of Things networks, which are unique and immensity-based and so complicated. This is so because the great diversity and scope of the networks define them. One of the most important issues that still has to be addressed to guarantee that models of artificial intelligence are dependable and capable of functioning well across a wide variety of device types and network configurations at the same time is their capacity of functioning. [16] One of the difficulties to be overcome is this. Among the several obstacles left to be surmounted, this is the most critical one. Moreover, it is possible that artificial intelligence included into Internet of Things (IoT) connected devices will lead to latency introduction. This might very possibly happen. This specific decision is among the several ones that might arise. [25] For some apps linked to the Internet of Things, this latency is likely to make working in real time more challenging. [17) This is especially true as these programs find employment in important fields like industrial automation or healthcare respectively. Regarding the security of the Internet of Things (IoT), artificial intelligence is still in the process of developing and continuous research is under progress aiming at enhancing the accuracy, efficacy, and resilience of AI models. This is taken under consideration to guarantee IoT security. Three technical developments—deep learning, federated learning, and boundary computing—have enabled the construction of artificial intelligence-driven security solutions able to operate effectively within the constraints of Internet of Things settings. These developments allow one to create these answers. These solutions can operate at a higher degree of complexity than earlier ones, thereby surpassing the previously feasible solutions. [27] These systems are able to carry out their intended purposes in a reasonable manner despite the restrictions the Internet of Things places on them. [eighteen] Deep learning has the ability to enhance the identification of technologically complicated assaults since it can examine vast amounts of data and find minute trends. Its capacity to identify minute trends explains this.

This is the reason it can accomplish this: its capacity to identify minute patterns helps it This skill clearly shows that deep learning can gain this aptitude. 39] A solution to privacy issues while still enabling users to gain from the possibilities of artificial intelligence is federation learning, which lets artificial intelligence models be trained across distributed devices without the necessity of uploading sensitive data to a central server. 19 [19] Machine learning of a sort is federation learning. Federated learning is a method that helps individuals to exploit artificial intelligence's capabilities. Using federated learning helps artificial intelligence models to be trained on numerous devices simultaneously, hence enabling this. [28) One of the options that makes this experience possible is the employment of a method called federated learning, which allows one to make advantage of the capacities of artificial intelligence. [20] [Edge computing can help to lower latency and ensure that artificial intelligence-driven security measures are carried out in real time in circumstances when resources are limited. In situations when resources are scarce, this is very useful. This makes it more helpful in circumstances when resources are limited since it is the reality. One approach to do this is to handle the data processing at a site physically closer to the data source. Using artificial intelligence—which offers a perhaps revolutionary prospect—allows one to reach the objective of improving the degree of security of networks linked to the Internet of Things (IoT). 30 Because of its potential to analyze vast volumes of data, identify risks in real time, and react to new and changing attack paths, this tool is quite relevant for shielding linked devices from cyberattacks. 21 [21] Stated differently, it carries out all of these purposes.

simultaneously. The capacity of this system to adapt to new attack vectors is the reason behind this. All of these responsibilities may be accomplished by it, which is the reason why this is the case.[32] When it comes to the incorporation of artificial intelligence into the protection of the internet of things, it is essential to give careful consideration to the challenges that are associated with the vulnerabilities of artificial intelligence, issues regarding privacy, and the complexities of IoT ecosystems. This is because these challenges are associated with the inherent vulnerabilities of artificial intelligence. On the other hand, it is of the utmost need to pay specific attention to the challenges that are associated with the vulnerabilities of artificial intelligence. [40]It is projected that the partnership between artificial intelligence and the internet of things will play an increasingly significant role in the protection of the future that is linked. This is shown by the findings of the research that is now being carried out, which can be found here.[41]

Role of AI in IOT Security

I am able to make a contribution to the resolution of issues that are associated with the security of the Internet of Things (IoT) by providing automated, real-time security solutions that are able to learn and adapt over the course of time. The following are some of the most significant applications of artificial intelligence for the protection of the Internet of Things:

A. Threat Detection and Anomaly Detection

Real-time research of the vast quantities generated by Internet of Things devices is made possible by artificial intelligence-based technologies. These systems might then detect trends and anomalies implying possible security risks. If abnormal behavior including traffic patterns not expected or interactions between devices not predicted reveal presence, an attack may still be under process. Detecting these anomalies is a task appropriate for machine learning models, especially unsupervised learning methods, without the need of current attack fingerprints. This is true since these models could learn without instruction. User's Comfort of Use

Intrusion Detection Systems (IDS)

Motivated by artificial intelligence, intrusion detection systems (IDS) might monitor network traffic and device behavior for hostile activity signals. AI-driven solutions may always grow by learning from fresh data unlike traditional intrusion detection systems (IDS), which depend on set rules and signatures. Both supervised and unsupervised learning models are routinely used in intrusion detection systems (IDS) for Internet of Things (IoT) networks as they provide consistent detection of both known and zero-day threats.

B. Device Authentication

Device authentication is a basic need in ecosystems built on the Internet of Things (IoT). This is so because it assures that only authorised devices may access the network. Artificial intelligence-based technologies might help to provide constant authentication of devices connected to The Internet of Things. These methods comprise, among others biometric-based authentication—which makes use of fingerprints or voice recognition—and behavior-based authentication—which entails learning about the patterns of device use. Two of these techniques are examples of authentication techniques.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://theaspd.com/index.php

C. Data Privacy and Encryption

AI, in an increasingly IoT-oriented world, could conceivably assist in improving privacy of data. AI-driven algorithms could be used to encrypt data in motion using context-awareness and sensitivity level of the data. It also can regulate access to data, through the means of managing cryptographic keys and rules for data access, contributed to data security with the help of artificial intelligence.

D. Predictive Maintenance and Attack Prevention

Because only AI can make predictive analytics — the capability of forecasting a future security failure so that attacks can be stopped before they happen — a reality. AI systems can use device performance data to predict when a device is about to fail or degrade, thereby taking precautions to reduce the potential problem.

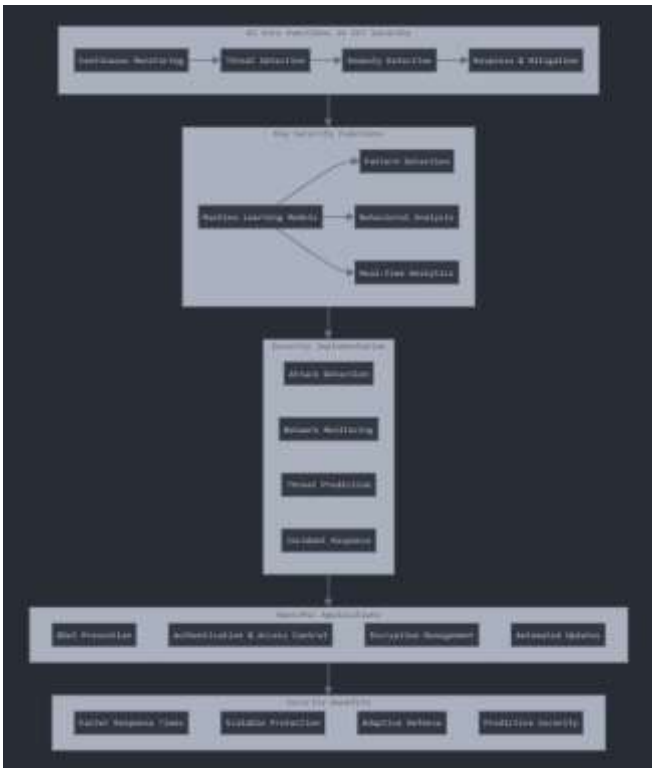

Fig 1: AI-Driven IoT Security Architecture: Functions, Implementation, and BenefitsAI-Driven IoT Security Architecture: Functions, Implementation, and Benefits

AI Techniques for IoT Security

In terms of making the internet of things safer, there are lots of different algorithms used for AI, and each serves a different role. In particular we focus our attention on three important AI paradigms:

A. Machine Learning (ML)

A.IoT security often relies on ML algorithms for tasks such as behavioral analysis, malware detection, or anomaly detection. Common algorithms include:

- **Support Vector Machines (SVM):** Used for classifying normal and abnormal behaviors in IoT devices.
- **Random Forests and Decision Trees:** Effective for intrusion detection by learning decision rules from data.
- **K-Nearest Neighbors (KNN):** Used for detecting outliers and anomalies in IoT networks.

B. Deep Learning (DL)

Layers of neural networks, a kind of machine learning, allow one to extract hierarchical data characteristics. Two deep learning models, CNNs and recurrent neural networks (RNNs), have showed promise in detecting complex patterns in network traffic and advanced cyberattacks. Being appropriate for real-time threat identification, DL models can manage massive volumes of Internet of Things data.

C. Reinforcement Learning (RL)

Reinforcement Learning (RL) algorithms have the potential to be used for dynamic decision-making activities in the context of Internet of Things (IoT) security. Among these operations are the optimization of resource allocation for security procedures and the response to various threat environments that are always changing.

Through the process of learning from their interactions with the environment, RL agents are able to generate the most effective security policies imaginable.

Challenges in AI for IoT Security

➢ IoT networks are inherently more vulnerable than traditional systems due to several factors:

- **Heterogeneity:** IoT devices range from sensors and cameras to industrial machinery, each with varying hardware capabilities and communication protocols.
- **Scalability:** By 2030, estimated to be 30 billion linked devices, centralized security management becomes challenging.
- **Resource Constraints:** IoT devices often have limited processing capability, memory, and battery life, hence they are less suited to running standard security software.
- **Lack of Standardization:** The diversity of device manufacturers and lack of universal security standards create inconsistent security practices.

Despite the potential benefits, there are several challenges associated with integrating AI into IoT security:

- **Data Privacy:** AI requires access to vast amounts of data, which raises concerns about user privacy.
- **Computational Overhead:** Many IoT devices lack the processing power to run AI algorithms, necessitating the use of edge or cloud computing.
- **Adversarial Attacks:** Adversarial attacks—where attackers control input data to avoid detection—are a vulnerability of artificial intelligence systems.
- **Scalability:** The heterogeneity and scale of IoT networks make it challenging to design AI systems that can generalize across different devices and environments.

Algorithm

Input:

- **IoT Devices (D):** $D = \{d_1, d_2, \ldots, d_n\}$
- **Network Traffic Data (N):** $N = \{p_1, p_2, \ldots, p_m\}$
- **Historical Data (H):** Previously observed patterns $H = \{h_1, h_2, \ldots, h_k\}$
- **Threat Signatures (T):** $T = \{t_1, t_2, \ldots, t_l\}$

Output:

- Anomaly Detection, Threat Mitigation, and Security Enhancement.

Steps:

1. **Initialization**:
   - Import IoT device configurations D and load historical traffic data H.
2. **Data Collection**:
   - Continuously monitor network traffic N.
   - Represent real-time traffic $X(t)$ as:

$$X(t) = \{x_1, x_2, \ldots, x_m\}$$

   - Each packet x_i contains metadata (source, destination, size, timestamp).
3. **Preprocessing**:
   - Normalize $X(t)$:

$$X_{norm}(t) = \frac{X(t) - \mu_X}{\sigma_X}$$

where μ_X and σ_X are the mean and standard deviation of $X(t)$.

4. **Anomaly Detection Using Machine Learning**:
   - **Supervised Learning (Threat Classification)**:
     Train model f using H and T:
     $$f(x) = \begin{cases} 1 & \text{if } x \in T \text{ (known threat)} \\ 0 & \text{otherwise} \end{cases}$$
   - **Unsupervised Learning (Anomaly Detection)**:
     Compute anomaly score $A(x)$:
     $$A(x) = \|x - \mu_H\|^2$$
     where μ_H is the centroid of historical normal traffic.
     Threshold: $A(x) > \tau$ indicates potential anomaly.

5. **Real-Time Response**:
   - If $f(x) = 1$ or $A(x) > \tau$:
     - Log event.
     - Initiate threat mitigation steps (e.g., isolate device, restrict access).
   - Else: Continue monitoring.
6. **Adaptive Threat Intelligence**:
   - Update model f with new patterns:
     $$f'(x) = f(x) + \Delta H$$
     where ΔH are new observed behaviors.
7. **Cryptographic Key Optimization**:
   - For each device d_i, select optimal cryptographic algorithm C_i:
     $$C_i = \arg\min_{C} \left(\frac{R(C)}{S(C)}\right)$$
     where $R(C)$ is the resource consumption and $S(C)$ is the security strength of algorithm C.
8. **Adversarial Attack Defense**:
   - Use adversarial training to improve robustness of $f(x)$.
     Augment dataset with perturbed inputs x_{adv}:
     $$x_{adv} = x + \epsilon \cdot \text{sign}(\nabla_x L(f(x), y))$$
     where ϵ is the perturbation magnitude, L is the loss function, and y is the label.
9. **Edge Computing for Latency Reduction**:
   - Deploy models on edge devices:
     $$f_{edge}(x) = \begin{cases} f(x) & \text{if computation resources allow} \\ \text{Relay to cloud} & \text{otherwise} \end{cases}$$
10. **Performance Evaluation**:
    - Evaluate system performance in terms of detection accuracy A_d, false positives FP, and latency L.
    - Optimize:
      $$\min \left(L + FP\right), \quad \text{subject to } A_d \geq \text{Threshold}$$

DISCUSSION

The fast spread of Internet of Things devices has caused a transformation in many different sectors. Linked healthcare systems and smart cities are among the several advancements that these gadgets enable to be implemented. On the other side, the broad application of this technology has revealed important security issues. Many times, the special vulnerabilities presented by Internet of Things devices are not properly managed by conventional security protocols. These approaches usually fall short as they were meant for more conventional network environments. Among the problems underlined here are limited processing resources, inconsistent security improvements, and a broad spectrum of communication methods. Currently under development as a perhaps revolutionary substitute to raise Internet of Things (IoT) security is artificial intelligence (AI). The

evolution of artificial intelligence (AI) technologies—including machine learning and deep learning—allows one to identify, stop, and react to cyberattacks in real time. By using artificial intelligence (AI), IoT networks might become more flexible and resistant to assaults, therefore changing in line with the ever advanced strategies used by hostile players. This is so because artificial intelligence may learn and change with changing contexts.

Enhancing Threat Detection

One of the most significant benefits that artificial intelligence offers is the capacity to accurately and rapidly assess huge amounts of data. This is one of the most crucial advantages that AI offers. This is one of the several advantages that it offers, and it is among the most significant of those advantages. To add insult to injury, there is a vast array of extra benefits that may be achieved. Artificial intelligence algorithms are able to discern trends and identify problems in settings that are characterized by the gathering of vast quantities of data by a large number of devices. Such environments are denoted as Internet of Things environments. Each of these ecosystems also has the IoT component to add to the mix. Perhaps these patterns and deviations will provide some clues about potential security violations. To be more precise, this is because these are settings in which an insane amount of information is stockpiled. Here's what's going on here. The existence of those deviations are signs that the system may not be absolutely perfect in its defenses, and there's a pretty good chance that this is actually the correct understanding. It is possible that hitherto unsuspected risk factors may be diagnosed by the use of machine learning models, and specifically, unsupervised learning methods. This is a possibility. It is the models developed through leveraging machine learning that really have the potential to accomplish it. When the vectors of attack are doing a dance in a sea, does this work, and that's what seals it. Because they do this, this is why this is the case. It is likely that artificial intelligence-based intrusion detection systems (IDS) are able to meet the performance targets of monitoring traffic on a network and on devices to determine if any user activity is outside of norms that have been established. This is a possibility. Monitoring the activity of multiple networks and devices also provides a solution to this problem. These types of systems are capable of detecting potential threats, such as DDoS attacks, unauthorized use and malware infections. This is because these systems are capable of detecting anomalous activity from channels of communication, or devices. The utilisation of such technology could however expose these threats at some point in time. In addition, they are able to recognize the existence of prospective dangers that might perhaps endanger their safety.

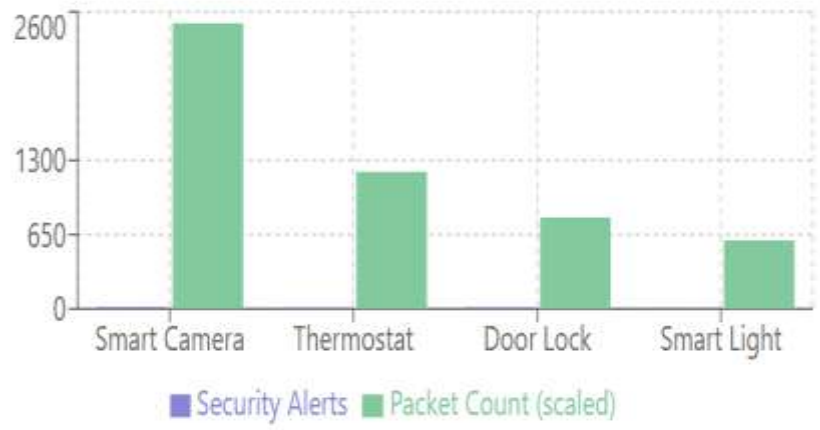

Fig 2: Device-Wise Security Alerts vs. Network Activity in IoT Systems

Real-time Response and Mitigation

Artificial intelligence's capacity to respond to threats in real-time is a significant aspect that contributes to the reduction in the amount of damage that is caused by cyberattacks. This is one of the factors that contributes to the general trend. This is one of the most significant aspects that had a role in the development of the situation. One of the features of automated systems is the capacity to immediately apply countermeasures, measures such as isolating devices that have been hacked and blocking malicious traffic
or constantly updating security rules. Other characteristics include the ability to continually update security rules. This is because automated solutions do not need any input from people in order to be implemented. This is the reason behind this. Criminals are successfully prevented from taking advantage of vulnerabilities for extended periods of time as a result of the reduction in response time that is brought about by these technologies, which are powered by artificial intelligence. Because of this, the length of time it takes for them to answer is decreased

as a result of these innovative technologies. One other method that artificial intelligence might employ to enhance threat mitigation is via the use of predictive analytics. This is still another way that could be taken. The capabilities of these analytics include the capacity to locate vulnerabilities before they are exploited by bad actors who are employing them. Some examples of items that may be analyzed with the use of machine learning models are the data from previous attacks, the settings of the devices, and the architecture of the network. Another example is the design of the network. Consequently, these models may be used to make projections about the components of the Internet of Things network that are most likely to be exploited by hostile actors. This is a potential application of these models.

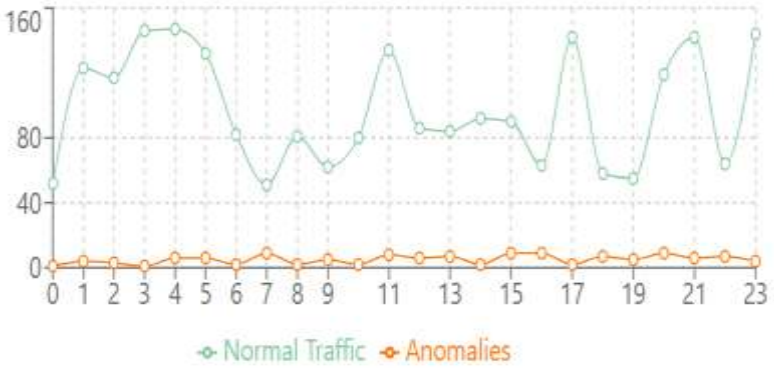

Fig 3: Hourly Network Traffic vs. Detected Anomalies in IoT Systems

Continuous Adaptation and Learning

Why new devices are being added on a consistent basis, the networks that comprise the Internet of Things are continuously updated throughout the day. This is because new devices are being added. It may be deduced from this that the Internet of Things is undergoing continuous transformations. Because they are able to learn from new data, artificial intelligence (AI) systems, and deep learning models in particular, are able to continually adapt to new threats. It's this ability, in fact, that enables them to flexibly adapt to novel information. They can learn through this process. Artificial intelligent systems can inherit information from the new inputs because it has that ability. In the case of Internet of Things security solutions that must remain effective both in the face of their vulnerabilities' discovery and the discovery of new ways to be attacked, the ability to learn is crucial. This is because everything comes down to adaptation - and security solutions are no different. Hence, the Internet of Things is still evolving. In the lay of IoT, AI could offer enhanced encryption and develop secure communication protocols. This is a possibility. This could possibly happen. Artificial intelligence may be able to learn the safe transmission of data in low processing power devices connected in the Internet of Things (IoT). This is the capacity that artificial intelligence can provide. To achieve this objective, one can enhance encryption algorithms to reflect such a trade- off between security and efficiency. Implementation of this goal may be achieved through application of this strategy.

Future Directions

In the context of IoT security, there are numerous areas where more attention is needed to effectively capitalize AI. For by now if you teach your artificial intelligence, federated learning, is a decentralized approach to machine learning in which internet-of-things devices collaborate via learning a shared model while they do not need to reveal sensitive data. Performing the artificial intelligence models on the edge devices is being considered to reduce the latency and to maintain privacy. We call this process artificial intelligence governance, which is about establishing rules and norms to govern the ethical use of artificial intelligence within the security aspect of the Internet of Things (IoT). This is known as "AI Administration."

CONCLUSION

To meet the growing security challenges in the context of the Internet of Things, artificial intelligence is a game changer that can revolutionize the entire course of the game. This can be a game-altering solution. Advances in the detection, prevention and mitigation of security vulnerabilities might be facilitated by technology such as

artificial intelligence, which might enable such advances. And that those advances might be possible with the application of methods like reinforcement learning, deep learning and machine learning. There are good reasons to expect that these insights will be facilitated through employing these methodological innovations. However there are still many hurdles to be overcome. Among challenges, there are what capacity of data can be managed, how secure the data is and the dynamic nature of the threats. In the future, R&D work of developing scalable AI systems which will protect privacy of users will be an interesting area. This is an important process and it is a necessary step that must be taken in order to protect the massive volumes of data generated by Internet of Things (IoT) connected networks.

REFERENCES

[1] Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Guizani, M., & Ali, I. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys & Tutorials*, 22(3), 1646-1685.

[2] Wazid, M., Das, A.K., Kumar, N., & Rodrigues, J.J.P.C. (2019). IoT data authentication using artificial intelligence for secure smart environments. *Journal of Information Security and Applications*, 47, 125-137.

[3] Zhang, Z., & Wang, J. (2020). Deep Learning-Based Security Defense for IoT Devices: Opportunities and Challenges. *IEEE Network*, 34(3), 42-47.

[4] Zhang, Y., Ren, J., Liu, C., Zhang, D., & Yao, L. (2020). AI-Driven Security Threat Detection and Mitigation for IoT Systems. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 5(1), 1-13.

[5] Ahmad, S., Awais, M., & Kim, H. (2021). Artificial Intelligence Techniques for IoT Cybersecurity. *Electronics*, 10(15), 1816.

[6] Liu, P., Wang, X., & Wang, D. (2020). AI-Enhanced IoT Security through Behavioral Analysis: A Survey. *ACM Computing Surveys*, 53(4), 85.

[7] Abawajy, J.H., Hassan, M.M., & Muhammad, G. (2020). Federated Learning for IoT Security: Concepts, Challenges, and Opportunities. *IEEE Communications Surveys & Tutorials*, 23(2), 1341-1363.

[8] Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2017). Mobile edge computing: A survey. *IEEE Internet of Things Journal*, 5(1), 450-465.

[9] Singh, S., Jeong, Y.-S., & Park, J.H. (2019). A deep learning-based IoT malware detection system in fog computing environment. *Journal of Supercomputing*, 75(6), 2405-2423.

[10] Cui, L., Yang, S., & Chen, X. (2018). AI-driven security mechanisms for IoT environments. *IEEE Network*, 32(2), 20-26.

[11] Gupta, B., & Srivastava, P. (2020). Applications of Machine Learning for Internet of Things (IoT) Security: A Review. *Journal of Network and Computer Applications*, 165, 102707.

[12] Kumar, P., & Tripathi, R. (2019). AI and Blockchain Integration for IoT Security: Challenges and Opportunities. *Internet of Things*, 6, 100131.

[13] HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., & Choo, K.-K.R. (2018). A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, 85, 88-96.

[14] Farooq, M.U., Waseem, M., & Mazhar, S. (2018). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7), 1-5.

[15] Pacheco, F., & Hariri, S. (2019). IoT Security Framework for Smart Water Systems. *Sensors*, 19(9), 2093.

[16] Mahmood, K., & Husain, A. (2021). Federated Machine Learning for IoT Security: Concepts and Applications. *ACM Transactions on Internet of Things*, 2(4), 31.

[17] Rawat, D.B., & Rahman, M. (2021). AI-Empowered IoT Security: A Comprehensive Survey. *IEEE Access*, 9, 45129-45153.

[18] Poudel, K. (2021). AI-based Intrusion Detection Systems in IoT Networks. *Journal of Internet Services and Information Security*, 11(1), 55-72.

[19] Zhou, L., & Wang, Y. (2020). Artificial Intelligence-Based Security Solutions in the Internet of Things. *IEEE Internet of Things Journal*, 7(8), 6882-6895.

[20] Hafeez, G., & Wang, Y. (2020). An AI-Powered Intrusion Detection System for IoT Networks. *Sensors*, 20(15), 4166.

[21] Das, A.K., & Wazid, M. (2019). AI-driven secure lightweight authentication protocol for IoT-based applications in smart cities. *IEEE Internet of Things Journal*, 6(6), 9346-9355.

[22] Fu, L., & Shi, X. (2019). Machine learning-based security in Internet of Things (IoT): A survey. *IEEE Communications Surveys & Tutorials*, 21(3), 2654-2673.

[23] Rahman, A., & Islam, M.S. (2021). AI-based threat detection in IoT networks. *Journal of Network and Computer Applications*, 170, 102808.

[24] Chen, W., & Wang, D. (2021). AI-Enhanced Security Techniques for IoT Networks. *IEEE Transactions on Network and Service Management*, 18(3), 2034-2045.

[25] Liu, W., & Zhou, S. (2020). AI-powered behavioral analysis for securing IoT systems. *ACM Transactions on Internet Technology*, 20(4), 1-22.

[26] Amin, M.B., & Shahzad, F. (2020). A hybrid deep learning model for IoT anomaly detection. *IEEE Access*, 8, 58036-58048.

[27] Wang, Q., & Wang, C. (2020). AI-based Security for Internet of Things: Threats and Countermeasures. *IEEE Wireless Communications*, 27(5), 88-93.

[28] Singh, A., & Kumar, A. (2021). AI-enabled Blockchain for IoT security. *Journal of Computer Networks and Communications*, 2021, 1-9.
[29] Lee, C.H., & Lin, C.Y. (2021). A blockchain-based AI secure framework for IoT networks. *IEEE Access*, 9, 35684-35697.
[30] Zhou, Z., & Zhao, Z. (2021). AI-Driven Edge Computing Framework for IoT Security: A Survey. *IEEE Communications Surveys & Tutorials*, 23(2), 1364-1389.
[31] Feng, Z., & Li, J. (2020). Federated Learning for IoT Security and Privacy: Concepts, Applications, and Challenges. *IEEE Internet of Things Journal*, 7(6), 4955-4969.
[32] Patil, V., & Raj, A. (2021). Deep learning-based privacy preservation framework for securing IoT data. *Journal of Information Security and Applications*, 59, 102828.
[33] Joshi, G., & Aikat, J. (2020). Cybersecurity challenges in IoT systems: AI to the rescue. *ACM SIGMETRICS Performance Evaluation Review*, 47(4), 18-23.
[34] Xiao, Y., & Tang, Y. (2020). AI-Enabled Secure Network for IoT Systems: Threat Detection and Mitigation. *IEEE Communications Magazine*, 58(11), 61-66.
[35] Khan, A., & Hashmi, I. (2019). Reinforcement Learning Techniques for Securing IoT Devices. *IEEE Access*, 7, 123218-123230.
[36] Jiang, W., & Zhang, H. (2020). Machine learning-driven security solutions for IoT networks. *Future Internet*, 12(5), 89.
[37] Perez, M., & Sharma, R. (2020). AI-based Multi-Layer Security Framework for IoT Devices. *Journal of Systems and Software*, 167, 110601.
[38] Xu, L., & Wu, X. (2021). Securing IoT Using AI-based Authentication Schemes. *Journal of Supercomputing*, 77(1), 355-372.
[39] Lu, C., & Huang, Y. (2021). AI-Powered Privacy-Preserving Techniques for IoT Environments. *Sensors*, 21(12), 4036.
[40] Parvez, I., & Ahmed, M. (2020). AI-based IDS for IoT: A comprehensive survey. *IEEE Access*, 8, 219727-219744.
[41] Choi, J., & Han, J. (2020). AI-enhanced Distributed Intrusion Detection System for IoT Environments. *Journal of Communications and Networks*, 22(6), 437-448.
[42] Zhang, Q., & Liu, G. (2020). AI-Based Secure Communication in IoT Networks. *IEEE Transactions on Information Forensics and Security*, 15, 4857-4866.
[43] Mittal, M., & Agarwal, A. (2020). AI-driven Security Framework for IoT Networks. *Journal of Internet Services and Information