Embedding AI Logic and Cyber Security into Field and Cloud Edge Gateways

Sumanth Tatineni

Abstract: ***Artificial intelligence application in cloud edge gateways through real-world devices is called Edge AI. The process entails using AI computations close to the networks' edge rather than the conventional centralized locations such as the cloud service or infrastructure that makes up the data center. Today, multiple innovations have proven to make AI more efficient and effective with sufficient capacity to be applied to the emerging Internet of Things (IoT). The rise of edge computing presents great potential for implementing AI logic to address various cybersecurity issues prevalent in cyberspace today. This article shows how AI logic can be embedded in cloud edge gateways, its capabilities, paradigms, and transitioning towards the new approach to guarantee a more robust security approach for cloud edge gateways. Furthermore, the paper will also delve into the various AI algorithms and models that can be utilized on edge devices,especially when dealing with devices at the edge of various networks.***

Keywords: Cloud Computing, Cybersecurity, Edge Computing, Cloud Edge Gateways, Artificial Intelligence, AI Logic

1. Introduction

Over the past few decades, technology has been consistently developing, and to date, multiple technologies have been coming up. Among the prominent innovations in the technological space, today is Cloud Computing which has turned out to be a novel computing infrastructure for most internet-based infrastructures. It is the most preferred approach when going for highly resourced data centers. Adopting cloud computing has further led to a major surge in global cloud IP traffic. As a result, it has presented multiple advantages to the cloud computing space, where it continues to enjoy unlimited computing infrastructure and storage capacity, accompanied by a major decrease in capital expenditure. All these benefits have proven beneficial in minimizing the global carbon footprint.

Unfortunately, despite the various challenges and benefits that seem to accrue from the technology, there are multiple concerns around slow connections and speed of services. However, the major concern today is security which has proven to be a major bottleneck undermining the effectiveness of cloud computing services. The more the cloud computing network grows, the more major challenges become prevalent, especially with the heavy proliferation of mobile and fixed internet-connected devices. It is vital to re-imagine and re-invent the approaches that should be embraced to guarantee better security and focus on a distinct "edge" separate from the paramount core (Cao et al., 2020).

Some of the key considerations that should be considered when addressing some of the prevailing challenges is recognizing that today, there is more reliance on mega-data centers that host all cloud computing services. Other challenges include narrow bandwidths and high latency, all of which have reduced users' Quality of Experience (QoE). Edge computing presents a major opportunity where the highly distributed cloud is now focused on connected devices and mobile users (Deng et al., 2020). The emergence of mobile vendors and the increased demands for IoT devices also present a broader avenue to look into guaranteeing control and a sense of personal privacy.

2. Overview of Edge AI

The major innovation in the Artificial Intelligence space has presented great efficiency and effectiveness. The heavy adoption of IoT devices has also presented a great opportunity for the immense potential of edge AI. Therefore, the new approach has presented a major opportunity for developing edge AI applications. For instance, medical practitioners are more capable of diagnosing diseases effectively, and automated vehicles on the highway and even in the agricultural sector. Conversations around adopting edge computing continue gaining traction across all sectors (Qiu et al., 2020). With the emergence of delivering content to customers, edge servers have proven ideal, unlocking the full potential that could be achieved with edge computing. Edge applications portray a major potential and are likely to significantly impact the everyday lives of workplaces, homes, and classrooms, among others.

AI at the edge essentially uses AI in some of the existing real-world devices. Edge AI focuses on doing AI computations close to the network's edge rather than focusing on centralized cloud services or cloud data centers (Zhou et al., 2019). Currently, the internet has penetrated worldwide, implying that each region may as well be considered to be a periphery. Some common examples may include mobile phones, driverless equipment, and traffic signals. The goal has always been to achieve the greatest efficiency, security, and productivity. Computer programs play a vital role in ensuring they are likely to spot patterns through learning from historical data allowing them to carry out multiple actions repeatedly and reliably.

However, the main challenges are that the world continues to become chaotic, and everyday activities render it almost impossible to outline the ideal algorithms and rules to govern these systems' operations. But with the advent of Edge AI, the approach is becoming more advanced, allowing the adoption of gadgets and robots which operate with the 'intelligence' imitating human cognition. Intelligent IoT applicationsthatAI drives have a proven capability to adapt and adjust to new situations while also allowing them to learn to trigger certain tasks and effectively execute them to suit the intended needs (Huh& Seo, 2019).

With some of the major advances that have been made, it is now possible to deploy AI models that operate at the edge. The major foundations that pavedthe way for generalized machine learning have been triggered by the major improvements made in neural networks, among other domains in AI. AI models are subjected to intense training, making it possible to deploy at the edge, a perspective that multiple organizations are adopting. It is an initiative that also calls for robust computing capacity. The same approach has presented an opportunity to adopt parallel GPUs (Hammoud et al., 2020). It is also important to realize that the heavy adoption of IoT prevalent today has contributed immensely to the massive growth in data volume. It has even reached a point where devices are required to implement AI models at the edge. This initiative can be achieved by embracing the approach in all aspects of the industry, for instance, robotics, sensors, cameras, and other data-gathering tools.

3. Background Information

The main proposition being propagated by edge computing is to move all capabilities associated with data processing further from the consolidated data centers. The alternative approach is instead focusing only on resources that are physically but not exclusively located closer to the end user. It is one of the strategies intended to guarantee high QoE applications for heterogenous devices on the users' side. The approach also applies to fixed internet-connected streaming devices through wireless networks. Some paradigms that emerged over the past two decades include mobile edge computing, fog computing, cloudlets, and adoptingmicro data centers (Sodhro et al., 2019). All these options still stand as the ideal options that could be utilized instead of edge computing.

Unfortunately, some of the studies that have been done in the past have highlighted how some of the options that could be used in place of edge computing presented a mutual occupation and overlap of the various conceptual approaches. Even though previous surveys have been heavily focused on some of the existing edge computing paradigms, an in-depth review of the various architecture and definitions all focus on some of the major concepts and technologies today, such as IoT and 5G. As a result, there are chances that edge computing can be defined differently depending on how businesses and technologies have adopted the technology.

For instance, fog computing focuses on simplifying how IoT devices reduce the time required to execute time-critical processing. Big data analytics and mobile edge computing only focus on the applications created to handle the needs of many mobile devices and micro data centers (Laroui et al., 2021). For businesses operating in the small-enterprise scenarios, it is possible to expand them to reach publicly funded arrangements where they can easily access some of the open-source software with limited or no requirements for access.

However, it is vital to note that mobile edge computing was changed to Multi-Access edge computing. The idea was to ensure that there is an explicit recognition of the most significant IoT components which would eventually help harmonize all edge computing applications even when working with highly heterogenous networks. Essentially, it is quite evident that AI efficiency is among the major realizations embraced by the rise of edge computing. It further indicates a greater potential that can be leveraged to ensure that edge AI has a greater future.

4. Edge Computing Threats and Challenges

Despite the various advantages that have accrued from the adoption of edge computing, there are myriad challenges, and topping the list are those targeting the privacy and security posture of the technology. Edge computing has an increased attack surface instigated by hardware constraints and software heterogeneities (Wu et al., 2020). The hardware constraints are recorded from how most physical edge computing devices are characterized by limited storage capacity and minimal computational power. This setback differs from cloud or cloud servers, rendering them less ideal for ensuring they can effectively prevent an attack on its systems. The hardware cannot support additional mitigation measures, such as firewalls, rendering them more vulnerable to attacks. Regarding software heterogeneities, most of the devices found on the edge layer rely on a myriad of protocols with little or no standardization. This attributemakes setting up a unified mode of protection a challenge.

Most of the threats in edge computing revolve around device misconfigurations, implementation bugs, and even multiple design flaws. The absence of a robust and full-fledged interface amongst most of the devices operating at the edge renders it a challenge to establish whether there is an attack going on or not. Some common attacks targeting edge computing resources include side-channel attacks, malware injection, DDoS attacks, and authorization and authentication attacks.

4.1 DDoS Attacks

For this type of attack, adversaries often strive to engage all the resources available, including the target's bandwidth, to limit the target's ability to utilize the affected system effectively. The attack is also executed by sending an unusually massive number of packets to the target, a strategy geared towards exhausting the available resources (Xiao et al., 2019). As a result, genuine requests cannot be handled. The attacks are often successful, considering they assume greater priority in the affected systems, more so if they are less powerful with limited resources than cloud servers. As a result, they may be unable to hold or run strong defense systems. DDoS attacks can therefore be classified as ICMP flooding, ping of death (POD), UDP flooding attacks, HTTP flooding, and SYN flooding attacks (Arshi et al., 2020).

Mitigating DDoS attacks would require a detect-and-filter technique. Malicious traffic can be detected by assessing each packet so that it undergoes inspection then those found to be suspicious can be discarded. The alternative approach that can also be implemented is the employment of packet entropy, among other machine learning techniques. Mitigating zero-day attacks on edge computing is mostly ineffective or inapplicable due to the unavailability of the primary source codes for the various programs installed on the device. Also, in most cases, most of the devices are usually released with firmware that cannot easily be altered or even inspected.

4.2 Side-Channel Attacks

Side channel attacks are commonly employed by adversaries and are deployed by first capturing publicly available information. The information is usually non-privacy sensitive but is later utilized by the attacker to infer sensitive information that the targets may use to access various platforms that require authentication. Usually, adversaries leverage this technique by leveraging the non-privacy information to access login details or guess passwords that are likely to be used by the targeted victims. Some common attacks may include capturing communication signals, for instance, wave signals or packets. By capturing such information, adversaries can easily monitor power consumption by edge devices or even leak users' private data (Sayakkara et al., 2019). Once an attacker accesses such information, it can easily be utilized to establish usage patterns.

Mitigating side-channel attacks may be challenging due to their passive nature. However, some mechanisms that have since been employed to defend systems against such attacks include differential privacy and data perturbation. A common data perturbation algorithm is *k*-anonymity which applies by modifying any form of identifier information of the data before any sensitive attributes or details are published.

4.3 Malware Injection Attacks

The resources used to make edge devices are usually unable to handle the utilization of fully-fledged firewalls, rendering them the most vulnerable to malware injection attacks. Such a loophole allows adversaries to install malicious programs on the target systems. Through malware injection, edge servers or devices can easily be executed (Prabhavathy & Umamaheswari, 2022). On the other hand, server-side injection attacks can also be leveraged by adversaries. Some server-side injections include XML signature wrapping, cross-site scripting (XSS), SQL injection, and Server-Site Request Forgery (SSRF) (Devi & Kumar, 2020). End devices are easily attacked by Device-Side injection attacks, which usually target their firmware.

The main focus of SQL injection attacks is usually to destroy backend databases. This attack is usually executed with the help of SQL queries containing malicious executable codes. XSS attacks inject malignant HTML/ JavaScript codes into the data content. CSRF attacks are a common technique used to attack edge servers, with their operation focused on tricking the target system. SSRF attack, on the other hand, is executed through a compromised edge server or device,then making alterations to the internal services of data. Finally, XML signature wrapping employs a strategy that intercepts and makes modifications to an XML message and re-transmitting the modified version to a target machine (Mokbal et al., 2019). Server-side injection attacks can be mitigated through detection and filtering techniques. Even though the approach may not be as effective, the most precise and effective defense mechanism against injection attacks relies on static analysis to detect malicious code.

4.4 Authentication and Authorization Attacks

Authentication and authorization attacks can be classified into four categories; those targeting authentication mechanisms, those exploiting vulnerabilities in authorization protocols, over-privileged attacks, and dictionary attacks. Attacks targeting authentication mechanisms exploit gaps prevalent in common security protocols such as WPA/WPA2. The attacks taking advantage of authorization protocols explore any form of gaps prevalent in the design architecture, a common challenge prevalent in edge computing systems. Over-privileged attacks often utilize a technique where the target or the victim system is tricked into assigning higher authorization rights to a service or a device to use the credentials to perform malicious activities.

Some common defenses and countermeasures against authentication and authorization mechanisms include adding more layers to the authentication process. This countermeasure is quite effective in mitigating dictionary attacks. Additionally, to mitigate all attacks targeting authentication protocols, the common techniques that could be used include implementing robust cryptographic measures and enhancing communication protocols. The most recommended approach is deploying the OAuth 2.0 protocol, which is the most effective for countering most authorization attacks (Xiao et al., 2019). Over-privileged attacks can only be mitigated by reinforcing the existing permission models, especially when addressing the needs of on-edge devices.

5. Use of AI Logic in Edge Computing

Application of AI Logic in Edge Computing; two major advantages accompany Edge AI. First, Edge AI creates room for faster inference. This is an attribute that can easily be utilized by the use of a machine learning model that has already been trained. It ensures that the data processing steps are significantly reduced to guarantee faster results. The steps are reduced significantly through less data transfer time between the edge device and cloud servers. Second, Edge AI foster data locality. This perspective results from the attribute,allowing data processing and inference at the edge layer. Essentially, no data leaves the edge layer (Fraga-Lamas et al., 2021). The data locality feature is an additional advantage since it focuses on increasing user privacy more so when dealing with applications such as indoor localization and health monitoring.Additionally, maintaining the approach of keeping data close to the source rather than transferring it to the cloud negates the various legal issues surroundingthe handling and management of data. Even though there are advantages, such as faster inference when data is kept near the edge device, the main challenge is the edge layer's resource constraints. This sophistication calls for more advanced and sophisticated techniques to ensure that the edge device is adequately trained to perform comprehensive inference using AI.

5.1 Lightweight Models for Edge AI

This first scenario entails where edge computing nodes are only deployed for inference, achieved with the help of pre-trained models. Such scenarios call for only dwelling on lightweight models that would be robust enough to operate in resource-constrained environments (Ren et al., 2020). The approach is only effective due toimplementing the Convolutional Neural Networks (CNN), which facilitates features such as classification tasks, and image recognition, among other computational requirements. AlexNet emerged as the first CNN variant and utilized the Group Convolution technique to reduce the number of model parameters (Ismail Fawaz et al., 2020). On the other hand, GoogleNetcould also reduce the parameter while maintaining a great deal of accuracy size to 27 MB. However, the most significant breakthrough is evident from MobileNet, which would only require approximately 8-9 times less computation than the standard CNN. The model size was 16 MB. MobileNet V2 later provided major improvements, reducing the model size to 14 MB. SqueezeNet is the most efficient and capable, with its level comparable to AlexNet, which provides only 5 MB. The smallest size, 5MB, is a relatively small-sized model and can be effectively used when handling low-complexity embedded hardware like Raspberry Pi (Alafif et al., 2020).

5.2 Data and Model Parallelism

Data parallelism and model parallelism are also effective and most appropriate for training. Data parallelism, the process of training datasets, starts with dividing into overlapping partitions. The second step then goes to feeding all the participating nodes. All the nodes are subjected to a training process with the help of a subset of data. The most significant benefit is that it allows the training of multiple nodes concurrently. With the presence of other algorithms, such as Asynchronous Stochastic Gradient Descent (Async-SGD) and Synchronous Stochastic Gradient Descent (Sync-SGD), have all been developed to guarantee a more effective and timelier update (Jia et al., 2019).

Model parallelism the machine learning model is first subdivided into multiple partitions where each node maintains a single partition. Developing the model partitions is non-trivial and NP-complete for such an instance. It should be noted that the participating machines usually have different storages, networking abilities and computing capacities. Also, the division process when dealing with the datasets is not as clear since all the logical partitions must be settled on before deciding according to the partitions scheme outlined in the input layer (Jia et al., 2019). Model compression can be employed to reduce communication, especially when dealing with multiple numbers of parameters of all the participating devices. Studies have demonstrated that quantizing the bandwidth may not significantly impact the accuracy of architectures that leverage the CNN model.

5.3 Federated Learning

Privacy remains one of the most significant concerns, especially if data has to be relayed over the cloud. Excellent examples include health monitoring devices which are usually relayed over the cloud. Such instances call for the adoption of Federated Learning. Federated Learning creates room for the sharing of prediction models. The approach also ensures that all the training data is kept on the device. It is an effective technique that ensures the learning processes are decoupled,thus mitigating the need to store data centrally. It also goes beyond the use of pre-trained models for making predictions on mobile devices (Khan et al., 2021). The updating process then occurs based on the locally stored data before updates are directed to a central server subjected to Federated Averaging. Furthermore, no data is disseminated from the device, while the various individual updates are not stored in the cloud. This feature is among many features guaranteeing privacy and data security.

The approach allows for high-quality updates which contain additional information, including changes in gradients which are all subjected to computing and compressing processes. Once that step is done, the data is then relayed for processing. This technique guarantees a great deal of minimal communication by approximately 100 times. With the help of scheduling algorithms, it is possible to ensure that training will only occur when the edge devices are idle or charging. The functionality does not also allow the changes to happen during instances where the device has been connected to a free wireless connection. This feature ensures that the userexperience is not affected in any way. Today, most smartphones being introduced into the market have a dedicated AI chip (Khan et al., 2021). It is approximated that over two billion smartphones are underutilized. Federated learning is among the major approaches with immense capacity to utilize various available computing resources to guarantee significant improvements to some of the existing models. They can also be used to train new models a fresh.

Embedding distributed intelligence over the various end devices is among the strategies likely to improve how conventional IoT devices work. Unfortunately, there would still be various challenges around security and privacy which would have to be addressed significantly (Ali& Choi, 2020).

6. Threats to Edge AI

Integrating intelligence into the edge layer presents various advantages, including how potential attacks could only be limited to the localized environment. However, the major setback would still be how the edge devices remain resource-constrained, implying that there would still be chances those attacks can still be executed (Groumpos, 2022). The ignorant nature further reinforces the major challenge amongst users configuring and maintaining edge devices. The other challenge also comes in during the need to install new updates or run re-configurations due to the presence of devices which would still allow for a myriad of challenges in handling the already constrained hardware resources. Additionally, edge networks are heterogenous, and no uniform security policy can be employed. Also, most micro servers that run the edge devices do not have sufficient hardware capabilities to guarantee robust security mechanisms.

6.1 Threats to Edge AI for Inference

Currently, most of the devices that are currently in use utilize pre-trained models. This is the most effective approach that would work for edge devices considering the limited nature of the resources offered by the devices. Significant progress has been made in modeling compressions that would accommodate the needs of high-performance models even when running in resource-constrained environments (He et al., 2020). However, the challenge that would still be prevalent here is how devices operating in standalone environments can still be trained and fed with multiple adversarial examples. This perspective would mean the model will still output incorrect predictions.

6.2 Evasion Attacks

Evasion attacks are prevalent when adversarial samples imitate the actual machine learning models. They even look similar to the untampered samples, only that they are well documented. There have been cases where such attacks have been reported considering how some attackers can easily trick models by carefully crafting changes into texts (Apruzzese et al., 2020). The major vulnerability remains to be how models are devised to be used in low-resource environments of edge computing resources. That compressed variants can only be employed, presenting a major opportunity for adversaries to utilize still. Evasion attacks can be Hard Label based, Brute-force attacks, Gradient-based, Surrogate model-based or Gradient Based attacks.

6.3 Privacy Attacks

Privacy attacks are geared towards siphoning off valuable information and data the various models use. An excellent example may be when an attacker wants to know whether a certain person has been registered with a specific healthcare program. Other additional details adversaries often use include location information, credit card details, and energy consumption (Nguyen et al., 2021). Even though the process that may come with the exposure of such details may be straightforward, the attacker can still misuse the availability to make additional attacks on the victim.

6.4 Threats to Edge AI for Training

First, no guarantees have been made regarding federated learning algorithms, which are still yet to be established. Approximate convergence may be guaranteed but would still require two unreasonable assumptions. The first assumption is that the training data is distributed amongst devices operating independently and identically distributed. The second assumption is that all devices engaged in a communication process entailing regular updates for each round.

Second, adversaries can easily take control of various participating devices in the federated learning scenarios. It is a move that will easily allow them to inject unrecognized or scrupulous updates to manipulate the overall training process. The approach can also be referred to as model poisoning (Shafique et al., 2021). Intruders can also manipulate the training data to their wish, an approach that would compromise the training process entirely, a process that is referred to as data poisoning. Data poisoning can involve manipulating the inputting process of the labels making up the training data. Eavesdropping is another challenge that is likely to surface when centralized servers are utilized to communicate the intermediate models. Availability is a vital component that often undermines the effectiveness of a system. Availability can be compromised by injecting conspicuous data into training sets rendering the learning process ineffective. These forms of attacks are often employing the concepts of conventional DoS attacks. Another category of attacks targets the model's integrity and is the most sophisticated compared to availability attacks. Even though the classifier may be left to function similarly, backdoor inputs are left behind and will automatically contribute to the higher chances of backdoor inputs.

7. Countering Threats to Edge AI

7.1 Defenses Against Data Poisoning

Detecting data poisoning calls for the implementation or the use of outlier detection, which is also referred to as anomaly detection. The approach focuses on identifying and eliminating the outliers that may have been present before the training process. However, anomaly detection has not proven effective over the years considering how various attackers can develop poison samples that are identical to the pristine samples. Instead, micromodels can be employed since they effectively ascertain which training slices may have been corrupted. An additional defense technique that can also be leveraged is the analysis of a new sample's effect on the model's accuracy before it has been actively added to the sample making up the data set. Reject On Negative Impact (RONI) stands out the most and has effectively tackled dictionary attacks (Fang et al., 2020). Unfortunately, it may not be able to detect anomalies considering instances where some attacks may not lead to significant performance drops.

The perturbation approach is effective for anomaly detection and can be used to mitigate the chances of attacks. STRong Intentional Perturbation (STRIP) executes by perturbing all the incoming data, then subjecting multiple patterns on the sample images (Gao et al., 2021). The following step is characterized by observing how random the predicted classes are for the perturbed inputs. An additional method is TRIM which is the most effective for regression learning. The technique estimates the parameters iteratively while removing samples that translate to large residuals. The method utilizes a trimmed loss function.

7.2 Countering Adversarial Attacks

Mitigating evasion attacks can either integrate formal or empirical techniques. Formal methods encompass mathematical techniques applied to models compared with adversary samples generated within allowable limits. The approach may imply that a device or system may be impenetrable but is not applicable today, where most applications operate with machine learning and require a significantly huge number of computational resources.

Empirical defenses depend on experiments to ascertain how effective a defense mechanism is. Multiple defense strategies are employedto ensure that the models will eventually learn to ignore any distractions and only focus on outright evident features in the overall training set.

Some recently proposed techniques include Ensemble Adversarial Training (EAT), which relies on training data with perturbations from similar models, a feature that renders the approach likely effective (Bai et al., 2021). Cascade adversarial training sources knowledge from other models to enhance new models. Input modification can also be utilized against evasion attacks. The technique entails usingan input sample and passing the outcome through sanitizing. Some methods that can be leveraged include high-level denoising techniques, for instance, pixel deflection, JPEG compression, and denoisers.

7.3 Hardening Federated Learning Systems

It is vital to reinforce the training, aggregation and model updating process, especially since all these processes have been spread over the client. Privacy on the client side can be guaranteed by ensuring there are more perturbations. In any case,more sensitive attributes are prevalent in the update; they can be obscured through the various differential privacy techniques. The process that can be utilized to reinforce the server side is the Secure Multi-Party Computation (SMC) (Reich et al., 2019). It is focused on ensuring the server renders all updates unacceptable. The aggregation protocol can be made secure by deploying various cryptographic techniques. Other schemes that can also be utilized include anonymization and homomorphic encryption.

8. Future Directions

More research should be directed towards improving the learning performances since the approach will translate to enhanced learning accuracy and minimal communication with the centralized servers and edge devices. A major tradeoff exists between the convergence speed need and the desire to enhance privacy. Today, there are still major challenges around recognizing and preventing data and model poisoning, which calls for more attention (Gill et al., 2022). Also, there is a dire need to ensure that the aggregation process is robust by integrating additional mechanisms, such as identifying any form of malicious updates. Reward functions are also an avenue that can be pursued, especially during the infancy stage of the various participating nodes. Future considerations should focus on reinforcement learning, which can be leveraged to improve the already existing intelligence in edge devices.

9. Conclusion

Edge AI is one of the pertinent issues prevalent in edge computing today. Currently, there are major concerns around privacy and security. AI presents a major opportunity to retract how such challenges can be addressed, especially since most edge devices operate with constrained resources. Edge AI should be able to collaborate with the various edge nodes to ensure that all the models can operate effectively without external compromise from adversaries or even human support for them to function effectively. The paper has effectively outlined the various pertinent issues, the possible countermeasures and how they can all be used to address the merging need as the world adopts edge computing.

References

[1] Alafif, T., Qari, S., Albassam, A., & Alrefaei, A. (2020, November). Deep transfer learning for nucleus and micronucleus recognition. In *2020 First international conference of smart systems and emerging technologies (SMARTTECH)* (pp. 21-27). IEEE.

[2] Ali, S. S., & Choi, B. J. (2020). State-of-the-art artificial intelligence techniques for distributed smart grids: A review. *Electronics*, *9*(6), 1030.

[3] Apruzzese, G., Andreolini, M., Marchetti, M., Venturi, A., & Colajanni, M. (2020). Deep reinforcement adversarial learning against botnet evasion attacks. *IEEE Transactions on Network and Service Management*, *17*(4), 1975-1987.

[4] Arshi, M., Nasreen, M. D., & Madhavi, K. (2020). A survey of DDoS attacks using machine learning techniques. In *E3S Web of Conferences* (Vol. 184, p. 01052). EDP Sciences.

[5] Bai, T., Luo, J., Zhao, J., Wen, B., & Wang, Q. (2021). Recent advances in adversarial training for adversarial robustness. *arXiv preprint arXiv:2102.01356*.

[6] Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An overview on edge computing research. *IEEE access*, *8*, 85714-85728.

[7] Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., & Zomaya, A. Y. (2020). Edge intelligence: The confluence of edge computing and artificial intelligence. *IEEE Internet of Things Journal*, *7*(8), 7457-7469.

[8] Devi, R. S., & Kumar, M. M. (2020, June). Testing for security weakness of web applications using ethical hacking. In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* (pp. 354-361). IEEE.

[9] Fang, M., Cao, X., Jia, J., & Gong, N. (2020). Local model poisoning attacks to {Byzantine-Robust} federated learning. In *29th USENIX security symposium (USENIX Security 20)* (pp. 1605-1622).

[10] Fraga-Lamas, P., Lopes, S. I., & Fernández-Caramés, T. M. (2021). Green IoT and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: An industry 5.0 use case. *Sensors*, *21*(17), 5745.

[11] Gao, Y., Kim, Y., Doan, B. G., Zhang, Z., Zhang, G., Nepal, S., ... & Kim, H. (2021). Design and evaluation of a multi-domain trojan detection method on deep neural networks. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2349-2364.

[12] Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514.

[13] Groumpos, P. P. (2022). A Critical Historic Overview of Artificial Intelligence: Issues, Challenges,

Opportunities and Threats. In *Artificial Intelligence and Applications*.

[14] Hammoud, A., Sami, H., Mourad, A., Otrok, H., Mizouni, R., & Bentahar, J. (2020). AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. *IEEE Internet of Things Magazine*, *3*(2), 68-73.

[15] He, Z., Zhang, T., & Lee, R. B. (2020). Attacking and protecting data privacy in edge–cloud collaborative inference systems. *IEEE Internet of Things Journal*, *8*(12), 9706-9716.

[16] Huh, J. H., & Seo, Y. S. (2019). Understanding edge computing: Engineering evolution with artificial intelligence. *IEEE Access*, *7*, 164229-164245.

[17] Ismail Fawaz, H., Lucas, B., Forestier, G., Pelletier, C., Schmidt, D. F., Weber, J., ... & Petitjean, F. (2020). Inceptiontime: Finding alexnet for time series classification. *Data Mining and Knowledge Discovery*, *34*(6), 1936-1962.

[18] Jia, Z., Zaharia, M., & Aiken, A. (2019). Beyond Data and Model Parallelism for Deep Neural Networks. *Proceedings of Machine Learning and Systems*, *1*, 1-13.

[19] Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials*, *23*(3), 1759-1799.

[20] Laroui, M., Nour, B., Moungla, H., Cherif, M. A., Afifi, H., & Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications*, *180*, 210-231.

[21] Mokbal, F. M. M., Dan, W., Imran, A., Jiuchuan, L., Akhtar, F., & Xiaoxi, W. (2019). MLPXSS: an integrated XSS-based attack detection scheme in web applications using multilayer perceptron technique. *IEEE Access*, *7*, 100567-100580.

[22] Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, *8*(16), 12806-12825.

[23] Prabhavathy, M., & Umamaheswari, S. (2022). Prevention of Runtime Malware Injection Attack in Cloud Using Unsupervised Learning. *Intelligent Automation & Soft Computing*, *32*(1).

[24] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Communications Surveys & Tutorials*, *22*(4), 2462-2488.

[25] Reich, D., Todoki, A., Dowsley, R., & De Cock, M. (2019). Privacy-preserving classification of personal text messages with secure multi-party computation. *Advances in Neural Information Processing Systems*, *32*.

[26] Ren, L., Liu, Y., Wang, X., Lü, J., & Deen, M. J. (2020). Cloud–edge-based lightweight temporal convolutional networks for remaining useful life prediction in IIoT. *IEEE Internet of Things Journal*, *8*(16), 12578-12587.

[27] Sayakkara, A., Le-Khac, N. A., & Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, *29*, 43-54.

[28] Shafique, M., Marchisio, A., Putra, R. V. W., & Hanif, M. A. (2021, November). Towards energy-efficient and secure edge AI: A cross-layer framework ICCAD special session paper. In *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)* (pp. 1-9). IEEE.

[29] Sodhro, A. H., Pirbhulal, S., & De Albuquerque, V. H. C. (2019). Artificial intelligence-driven mechanism for edge computing-based industrial applications. *IEEE Transactions on Industrial Informatics*, *15*(7), 4235-4243.

[30] Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.

[31] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, *107*(8), 1608-1631.

[32] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE*, *107*(8), 1738-1762.