Pervasive AI for Secure and Scalable IoT-Edge-Cloud Continuum: A Big Picture

Deepak Puthal*, Saraju P. Mohanty†, Chan Yeob Yeun*, Ernesto Damiani*‡, and Biswajeet Pradhan§
* Center for C2PS and Department of EECS, Khalifa University, Abu Dhabi, UAE
† Department of Computer Science and Engineering, University of North Texas, Denton, Texas, USA
‡ Department of Computer Science, Università degli Studi di Milano, Milan, Italy
§ Faculty of Engineering and IT, University of Technology, Sydney, Australia
Email: {deepak.puthal, chan.yeun, ernesto.damiani}@ku.ac.ae, saraju.mohanty@unt.edu and Biswajeet.Pradhan@uts.edu.au

***Abstract*—The proliferation of Internet of Things (IoT) devices has led to an explosion of data generated at the edge of the network. This has led to the development of the IoT-Edge-Cloud continuum, where data is processed and analyzed across multiple layers of the network. However, this also poses significant security and privacy challenges, as sensitive data is transmitted across the network. In this paper, we propose the use of Pervasive Artificial Intelligence (AI) to enhance the security and efficiency of the IoT-Edge-Cloud continuum. Pervasive AI can be used at each layer of the network to process and analyze data in real-time, reducing the amount of data that needs to be transmitted across the network. This can help to improve response times, reduce network traffic, and enhance security by keeping data localized. We also discuss the potential cybersecurity threats and future research directions for the use of Pervasive AI in the IoT-Edge-Cloud continuum. Our findings suggest that Pervasive AI has significant potential to enhance the security and efficiency of the IoT-Edge-Cloud continuum, and should be considered as a viable solution for future IoT deployments.**

***Index Terms*—Pervasive AI, Machine Learning, Edge-AI, TinyML, security, Privacy and Scalability.**

I. Introduction

In recent years, the rapid growth of the Internet of Things (IoT) and the widespread adoption of cloud computing have led to the emergence of new challenges and opportunities in the field of cybersecurity [1]. With billions of IoT devices and petabytes of data being generated every day, securing this massive amount of information is becoming increasingly challenging. Additionally, the use of cloud computing has led to a new paradigm of computing, where data is stored and processed remotely, presenting new security challenges such as data privacy, data confidentiality, and data integrity [2] [3].

Machine learning (ML) has emerged as a promising approach for cybersecurity due to its ability to automatically identify patterns and anomalies in data [4]. In recent years, ML has been extensively used in cloud computing for cybersecurity, but its application to edge computing and IoT layers is still in its infancy. This is partly due to the limited computational resources and memory available in edge devices and IoT sensors [5].

The field of cyber security is rapidly evolving to keep pace with the increasing sophistication of cyber threats. One promising area of research is the integration of AI and ML techniques into cyber security systems. In particular, the use of Artificial Intelligence (AI) and ML in cloud computing, edge computing, and IoT layers is gaining momentum due to the ever-increasing amount of data generated by connected devices [6]. Pervasive AI, which involves the deployment of AI algorithms across multiple layers of the computing stack, is a promising approach to achieve more effective cyber security [4] [7]. However, there are also significant challenges to be addressed, including ensuring the accuracy and reliability of AI models, protecting sensitive data, and addressing ethical considerations.

In this article, we present a comprehensive review of the current state of ML for cybersecurity in cloud computing, edge computing, and IoT layers. We discuss the challenges and opportunities of using ML in these environments and identify potential research directions to overcome the existing limitations. We also highlight the cybersecurity threats associated with the use of ML in these environments and propose possible solutions to address them. The paper also highlights future research directions in these areas, with a focus on developing more robust and secure AI and ML algorithms, and addressing the ethical and legal implications of their deployment in cyber security systems.

The rest of this article is organized as follows: Section 2 offers a concise overview of Pervasive AI. Section 3 explores the role of Pervasive AI within the IoT-Edge-Cloud continuum and its contributions across individual layers. In Section 4, we emphasize how Pervasive AI contributes to addressing security challenges within each layer of the IoT-Edge-Cloud continuum. Section 5 delves into the security threats associated with Pervasive AI in the IoT-Edge-Cloud continuum. In Section 6, we provide learning-based cybersecurity solutions of to the distinct layers of the IoT-Edge-Cloud continuum. Section 7 outlines future prospects for Pervasive AI within the IoT-Edge-Cloud continuum, categorized by taxonomy. Finally, we conclude the article in Section 7.

II. Pervasive AI

Pervasive AI refers to the integration of AI technologies into everyday devices and environments to enhance their functionality and automate tasks. It involves creating intelligent systems that can perceive their environment, reason about it, and take actions to achieve specific goals. Some examples

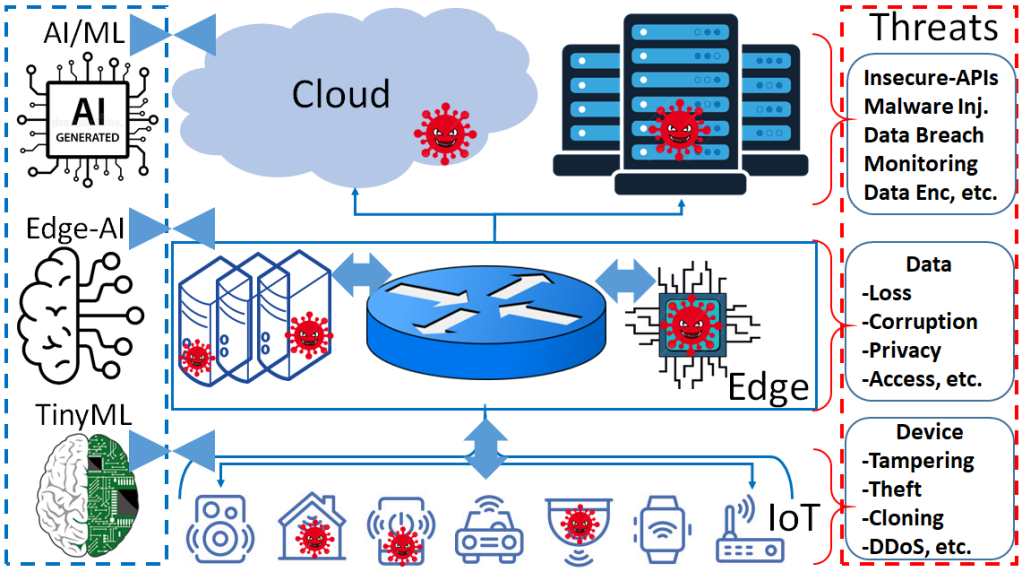

Fig. 1. System architecture of Pervasive AI in IoT-Edge-Cloud continuum

of pervasive AI include voice-activated personal assistants, smart home devices, intelligent transportation systems, and autonomous robots [8].

The goal of pervasive AI is to create seamless and intuitive interactions between humans and technology by leveraging the power of AI. It has the potential to transform various industries, such as healthcare, finance, and transportation, by improving efficiency, reducing costs, and enhancing the overall user experience. However, it also raises concerns about privacy, security, and ethical implications of AI [7]. Therefore, it is important to develop responsible AI systems that prioritize the safety and well-being of users while delivering the desired outcomes.

III. Pervasive AI in IoT-Edge-Cloud continuum

Pervasive AI in the IoT-Edge-Cloud continuum works by integrating AI algorithms and models at various layers of the architecture to enable efficient and intelligent decision-making. The complete architecture is shown in Figure 1 with layer classifications. The IoT-Edge-Cloud continuum consists of three layers: the IoT layer, the Edge layer, and the Cloud layer [9].

In the IoT layer, Pervasive AI (i.e. Tiny-ML(Tiny Machine Learning)) can be used to improve the efficiency of the data collection process, as well as to analyze this data in real-time to provide insights that can be used to improve the overall system [7]. In addition, Pervasive AI can be used to enhance the security of IoT devices by identifying and mitigating potential vulnerabilities and threats.

Moving on to the Edge layer, Pervasive AI (i.e. Edge-AI) can be used to optimize the processing of data that is collected from IoT devices. By analyzing this data in real-time, the Edge layer can make quick decisions and actions that can improve the overall performance of the system. In addition, Pervasive AI can be used to help manage the Edge infrastructure by identifying and fixing issues in real-time, as well as to predict potential failures and take preventative action.

In the Cloud layer, Pervasive AI (ML) can be used to manage the vast amounts of data that are collected from IoT devices and processed in the Edge layer. By analyzing this data, Pervasive AI can provide insights that can be used to optimize the overall system performance, as well as to identify potential issues and take corrective action [8]. In addition, Pervasive AI can be used to enhance the security of the Cloud infrastructure by identifying and mitigating potential threats and vulnerabilities.

Overall, Pervasive AI can help optimize the performance of the IoT-Edge-Cloud continuum by providing real-time analysis of data and making quick decisions and actions. It can also help enhance the security of the system by identifying and mitigating potential threats and vulnerabilities. As more and more devices are added to the IoT-Edge-Cloud continuum, Pervasive AI will become even more important in ensuring the efficiency and security of this architecture.

A. Role in IoT Layer

The IoT layer is the foundation of the IoT-Edge-Cloud continuum, which serves as the interface between the physical world and the digital world [10]. At this layer, Pervasive AI can be used to process data generated by IoT devices in real-time. By deploying AI algorithms at the IoT layer, data can be processed and analyzed on the device itself, reducing the amount of data that needs to be sent to the Edge or Cloud layers for processing [1] [9].

One of the primary advantages of using Tiny-ML at the IoT layer is the reduction of network traffic and latency [11]. With Edge AI, only relevant data is sent to the Edge or Cloud layers for further processing, which can significantly reduce network traffic and improve response times. This can be

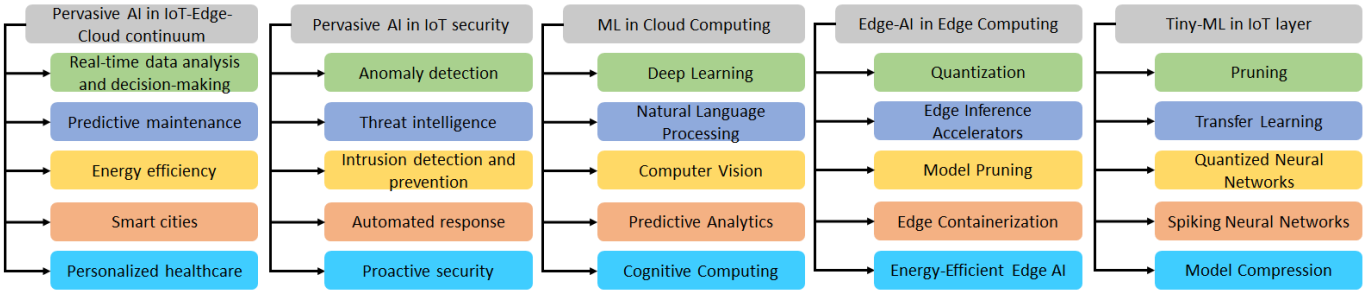

Fig. 2. Layer classifications of Pervasive AI in IoT-Edge-Cloud continuum

especially beneficial in scenarios where network connectivity is limited or unreliable, such as in remote locations or in mobile applications.

Another advantage of using Pervasive AI at the IoT layer is enhanced security and privacy. By processing and analyzing data on the device itself, sensitive data can be kept localized and not transmitted over the network, reducing the risk of data breaches or unauthorized access. This can be critical in scenarios where data privacy and security are of utmost importance, such as in healthcare or financial applications.

Pervasive AI at the IoT layer can also enable real-time decision-making capabilities, allowing IoT devices to autonomously respond to changing environments or conditions. For example, a smart thermostat equipped with AI algorithms can learn from user preferences and automatically adjust the temperature settings to provide optimal comfort and energy efficiency. Tiny-ML, extends AI into low-power IoT devices, enabling on-device data processing and analysis [12] [8]. By deploying machine learning at the IoT layer, it reduces data transmission to Edge or Cloud layers, improving network efficiency, reducing latency, and enhancing data security and privacy. Tiny-ML addresses resource limitations by optimizing algorithms for IoT devices with low computational power and memory as shown in figure 2. This approach revolutionizes IoT by bringing AI capabilities to resource-constrained devices, transforming how data is processed and utilized.

B. Role in Edge Layer

The Edge layer in the IoT-Edge-Cloud continuum is responsible for processing and analyzing data generated by IoT devices before sending it to the Cloud layer **??**. Pervasive AI can be used at the Edge layer to enable intelligent decision-making close to the source of data. This is achieved by deploying AI models (Edge-AI) on edge devices such as gateways or servers.

The deployment of AI models at the Edge layer enables real-time processing and analysis of data generated by IoT devices [8]. This reduces the amount of data that needs to be sent to the Cloud layer for further processing and analysis. In turn, this reduces network traffic, improves response times and enhances overall system performance.

One of the significant advantages of deploying Pervasive AI at the Edge layer is the reduction in latency. Latency is the time taken for data to be sent from the IoT device to the Cloud layer, processed, analyzed and a response sent back to the device. With Pervasive AI deployed at the Edge layer, decision-making can be made closer to the source of data, reducing the need to send data to the Cloud layer. This reduces the latency associated with sending data to the Cloud layer, improving response times significantly [13].

Moreover, deploying Edge-AI at the Edge layer improves the overall security and privacy of the system. Data is processed and analyzed on edge devices, reducing the need to send data to the Cloud layer. This keeps data localized and reduces the risk of data breaches or unauthorized access to sensitive information. By keeping data localized, Pervasive AI at the Edge layer enhances the security and privacy of the system.

Edge-AI combines AI with Edge Computing, it enables real-time data analysis, enhancing system responsiveness and minimizing data transfer. This approach empowers intelligent decision-making at data sources, improving system agility and data security. By keeping data on edge devices, Edge-AI reduces the risk of data breaches and can identify and mitigate potential threats, bolstering overall system security as shown in figure 2.

C. Role in Cloud Layer

In the Cloud layer of the IoT-Edge-Cloud continuum, Pervasive AI plays a critical role in managing the vast amounts of data that are collected from IoT devices and processed in the Edge layer [10]. With the help of AI algorithms, the Cloud layer can process and analyze large volumes of data quickly and efficiently, providing insights that can be used to optimize the overall system performance.

Pervasive AI (ML) enables Cloud infrastructure to identify potential issues and take corrective action to prevent system downtime. The Cloud layer can also utilize AI to identify and mitigate potential threats and vulnerabilities, enhancing the overall security of the system [14]. By analyzing data generated by IoT devices, Pervasive AI can help detect abnormal behavior patterns and potential security breaches, allowing for prompt and effective responses.

Furthermore, ML can be used in the Cloud layer to perform predictive maintenance on IoT devices [8]. By analyzing data collected from IoT devices, Pervasive AI can identify potential

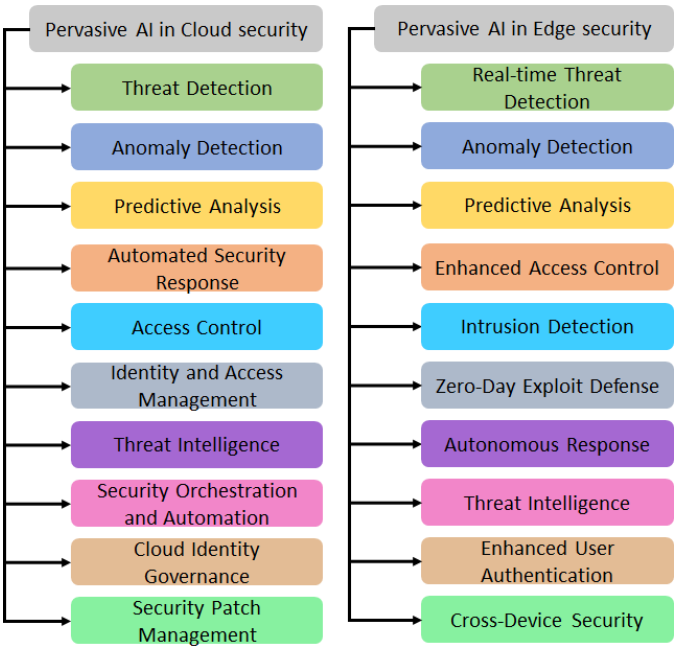

Fig. 3. Pervasive AI role in Security of IoT-Edge-Cloud continuum

equipment failures before they occur, allowing for proactive maintenance to be performed. This can help reduce downtime and improve system availability, ultimately leading to a better end-user experience.

ML is integral to cloud computing, enhancing predictive model accuracy by utilizing vast data and advanced algorithms. This synergy offers precise predictions in areas like personalized advertising, fraud detection, and predictive maintenance. Beyond prediction, ML powers applications like image recognition and natural language processing, demanding substantial computational resources available in the cloud [13]. Yet, challenges such as data privacy and algorithm bias must be addressed as shown in figure 2. Cloud providers adopt federated learning, differential privacy, and explainable AI to safeguard data, ensure fairness, and enhance transparency, especially in sensitive domains like healthcare and finance, making ML in cloud computing secure and equitable.

IV. Pervasive AI for Security in the IoT-Edge-Cloud Continuum

A. Pervasive AI in IoT security

With the rapid proliferation of IoT devices, securing these devices has become a critical concern. Pervasive AI has the potential to improve IoT security by enabling smart, adaptive and self-learning systems that can detect, prevent and respond to security threats. By leveraging AI algorithms, IoT devices can be programmed to learn and recognize normal patterns of behavior, detect anomalies, and take necessary actions to mitigate security risks [15].

One of the key benefits of pervasive AI in IoT security is the ability to perform real-time monitoring and analysis of large volumes of data. IoT devices generate a massive amount of data that can be analyzed by AI algorithms to detect potential security threats in real-time. These algorithms can be trained to recognize patterns of behavior that are indicative of malicious activities and can trigger alerts or automatically block suspicious traffic.

Pervasive AI can also be used to enhance the security of IoT devices by improving authentication and access control mechanisms [16]. For example, AI-based biometric authentication can be used to provide an additional layer of security for user authentication, while AI-powered access control systems can be used to automatically grant or deny access to devices and data based on user profiles and behavior patterns.

Another area where pervasive AI can be beneficial is in IoT device management. Managing a large number of IoT devices can be challenging, and this can increase the risk of security breaches. By using AI algorithms, IoT device management systems can be designed to automatically identify and address security vulnerabilities, optimize network performance, and manage device updates and patches.

B. Pervasive AI in Edge security

Pervasive AI can play a crucial role in ensuring security at the Edge layer of the IoT-Edge-Cloud continuum. Edge devices are often located in remote or harsh environments, and are thus more vulnerable to physical tampering or cyber-attacks. In addition, these devices typically have limited resources and processing capabilities, making them more susceptible to security breaches [16].

Pervasive AI can help address these challenges by enabling real-time monitoring and threat detection at the Edge layer. AI algorithms can be deployed on edge devices to detect anomalies and potential security threats in real-time. For example, AI models can analyze data streams generated by sensors and other IoT devices to identify patterns or deviations from normal behavior, which could indicate a security breach [15].

Pervasive AI can also be used to enable secure communication between edge devices and other components of the IoT-Edge-Cloud continuum. For instance, AI models can be used to encrypt data transmissions, authenticate users and devices, and establish secure communication channels. This can help prevent unauthorized access and protect sensitive information.

Moreover, Pervasive AI can enable Edge devices to be self-defending, by automatically identifying and responding to security threats without human intervention. AI models can be trained to recognize specific types of attacks or malicious behavior, and to take appropriate action to prevent or mitigate the impact of such attacks [17]. For instance, an AI model may be programmed to block or quarantine a device that is exhibiting suspicious behavior, or to shut down a communication channel that is being used for malicious purposes.

C. Pervasive AI in Cloud security

Pervasive AI can be used to enhance the security of the Cloud infrastructure by identifying and mitigating potential threats and vulnerabilities. With the increasing amount of

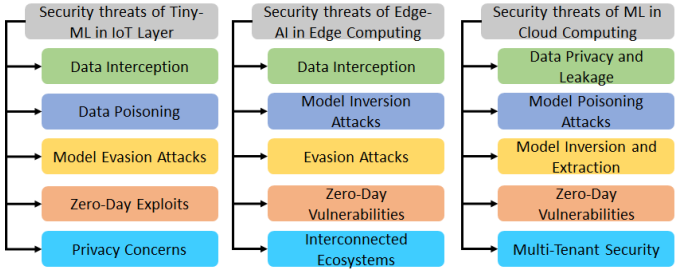

Fig. 4. Security Threats for the IoT-Edge-Cloud Layers

data being stored in the Cloud, security has become a major concern for organizations. Pervasive AI can help address this concern by providing advanced security features such as intrusion detection and prevention, threat intelligence, and anomaly detection [15].

One of the key benefits of Pervasive AI in Cloud security is its ability to identify potential threats and vulnerabilities in real-time. By analyzing large amounts of data generated by Cloud applications, Pervasive AI can detect unusual patterns and behaviors that may indicate an attack or security breach [16]. This allows organizations to take quick action to mitigate the threat and prevent any damage or loss of data.

In addition to detecting potential threats, Pervasive AI can also be used to prevent them from occurring in the first place. AI algorithms can be used to monitor and analyze network traffic in real-time, identifying and blocking any suspicious or malicious activity. This can help prevent unauthorized access to Cloud applications and data, as well as mitigate the risk of insider threats.

Another area where Pervasive AI can be used in Cloud security is in threat intelligence [17]. By continuously monitoring the threat landscape and analyzing data from multiple sources, Pervasive AI can provide real-time insights into emerging threats and vulnerabilities. This can help organizations stay ahead of potential attacks and take proactive measures to prevent them.

V. Security Threats for the IoT-Edge-Cloud Continuum Learning Models

A. Cyber security threats of Tiny-ML in IoT Layer

Tiny-ML is a rapidly growing field that focuses on developing low-power and resource-constrained machine learning models for IoT devices. However, this innovation also comes with potential cyber security threats [14].

One of the main cyber security threats of Tiny-ML in the IoT layer is the possibility of device hijacking. As Tiny-ML models run on the device itself, they can be vulnerable to tampering, and attackers may try to take control of the device by modifying the model parameters. This can lead to serious consequences, such as data theft, unauthorized access, and device malfunction [18].

Another cyber security threat associated with Tiny-ML in the IoT layer is data privacy. As Tiny-ML models are trained on user data, attackers may attempt to intercept the data transmission and obtain sensitive information. This can compromise the privacy of users and expose them to various forms of cyber attacks such as identity theft.

Furthermore, Tiny-ML in the IoT layer can be subject to adversarial attacks, where attackers manipulate input data to deceive the model and cause it to make incorrect predictions [18]. Adversarial attacks can be particularly harmful in scenarios such as autonomous driving, where a single wrong prediction can lead to serious accidents.

Lastly, the deployment of Tiny-ML in the IoT layer may introduce new vulnerabilities that were not previously considered. For example, the limited computational and memory resources available on IoT devices may make it difficult to implement standard security measures, leaving the device vulnerable to attacks. The threat classification is shown in Figure 4.

B. Cyber security threats of Edge-AI in Edge Computing

Edge-AI in edge computing is an emerging technology that is designed to bring AI capabilities to the edge of the network, allowing for real-time decision-making and analysis of data. While this technology has many benefits, there are also a number of cyber security threats associated with it that must be taken into consideration [14].

One of the biggest threats of Edge-AI in edge computing is the potential for data breaches. Because edge devices are often connected to the internet, they are vulnerable to attacks from hackers who may try to gain access to sensitive data [19]. This can be especially problematic in the case of medical or financial data, where the stakes are high.

Another threat is the potential for cyber attacks on the Edge-AI system itself. If a hacker gains access to an edge device, they may be able to tamper with the AI models or the data being processed, leading to inaccurate results or even malicious actions [19]. This can be especially problematic in critical systems such as autonomous vehicles or industrial control systems.

Finally, there is the potential for Edge-AI systems to be used in denial-of-service attacks. By overwhelming the system with data requests or other types of traffic, attackers can effectively shut down the system, causing disruptions and potentially significant damage. The threat classification is shown in Figure 4.

To mitigate these threats, it is important to implement robust security measures for Edge-AI systems. This may include using encryption to protect data in transit and at rest, implementing firewalls and intrusion detection systems to monitor for and prevent attacks, and implementing strict access control measures to limit who has access to the system. Additionally, it is important to stay up-to-date with the latest security patches and software updates to ensure that any vulnerabilities are quickly addressed.

C. Cyber security threats of ML in Cloud Computing

Machine learning (ML) in cloud computing has brought about significant advancements in various applications, but it

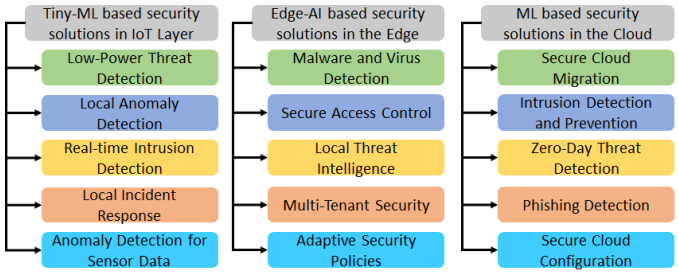

Fig. 5. Learning-based Security Solutions for the IoT-Edge-Cloud Layers

has also brought new security concerns. With the widespread adoption of ML in the cloud, cybercriminals are also looking for ways to exploit its vulnerabilities. There are several cyber security threats of ML in cloud computing [14].

One significant threat is data breaches. ML models rely heavily on data, and the storage and processing of this data in the cloud create new attack surfaces for cybercriminals. The data can be stolen or tampered with during storage or transit, leading to loss of confidentiality, integrity, and availability. Adversarial attacks are another major threat to ML in cloud computing. Adversarial attacks aim to deceive ML models by introducing malicious inputs or perturbations to the data to cause errors or misclassification [17].

Another threat is model poisoning. This involves modifying the training data used to train the ML model to introduce a backdoor, which can be exploited later to execute attacks. Model inversion attacks involve using the outputs of the ML model to extract sensitive information about the data it was trained on [4]. Finally, data privacy is a major concern when it comes to ML in cloud computing. As data is stored and processed in the cloud, the potential for data breaches and leaks increases, putting the privacy of sensitive data at risk. The threat classification is shown in Figure 4.

To mitigate these threats, ML models need to be trained on data that is representative of the actual data that the model will be processing to minimize the risk of adversarial attacks. Model validation techniques can also be employed to detect and prevent model poisoning attacks. Finally, data privacy can be ensured by implementing privacy-enhancing technologies such as differential privacy, homomorphic encryption, and secure multi-party computation.

VI. Security Solutions for the IoT-Edge-Cloud Continuum

A. Tiny-ML for Cyber security solutions in IoT Layer

Tiny-ML can also be used as a tool for enhancing cybersecurity solutions in the IoT layer. With the growing number of connected devices and the increasing amounts of sensitive data that are being processed at the edge, the need for effective cybersecurity solutions has become more critical than ever before. Tiny-ML can help address some of the challenges associated with securing the IoT layer by enabling intelligent decision-making capabilities to be embedded directly into edge devices [11].

One potential application of Tiny-ML in cybersecurity is anomaly detection. By training machine learning models on data generated by IoT devices, it is possible to identify patterns and behaviors that deviate from the norm, indicating the presence of potential cybersecurity threats. For example, an IoT device that suddenly starts sending large amounts of data to an unknown IP address could be indicative of a malware infection or a data breach [12]. Tiny-ML models can be trained to identify these types of anomalies and trigger alerts or take corrective actions [20].

Another application of Tiny-ML in cybersecurity is in the area of intrusion detection and prevention. Machine learning models can be trained on historical data to identify known attack patterns, and then applied in real-time to detect and prevent similar attacks from occurring. For example, a Tiny-ML model could be trained to detect brute-force attacks on IoT devices or identify patterns of suspicious network traffic.

Finally, Tiny-ML can also be used for securing communication channels between IoT devices and the Cloud. By embedding machine learning models into edge devices, it is possible to detect and prevent data exfiltration or unauthorized access to cloud-based resources. This can help enhance the overall security of the IoT ecosystem and protect sensitive data from being compromised. The Tiny-ML based security solution and layerwise classification is shown in Figure 5.

B. Edge-AI for Cyber security solutions in Edge Computing

Edge-AI can play a crucial role in improving the cybersecurity posture of Edge Computing systems. By enabling real-time processing and analysis of data generated by IoT devices and other sources, Edge-AI can help detect and respond to security threats in a timely and efficient manner [19]. Additionally, by performing data analysis and decision-making at the edge, Edge-AI can reduce the amount of sensitive data that needs to be transmitted to the cloud for processing, thereby reducing the attack surface and enhancing data privacy [21].

Edge-AI can be used for a variety of cybersecurity applications in Edge Computing, such as intrusion detection, threat intelligence, and anomaly detection. For example, Edge-AI algorithms can be trained to detect patterns and anomalies in network traffic or device behavior, which can indicate the presence of a cyber attack [21]. Similarly, Edge-AI can be used to analyze log data and identify potential security issues in real-time, allowing for quick response and remediation.

One of the key advantages of Edge-AI in cybersecurity is its ability to adapt and learn from new threats and attack vectors. By continuously analyzing data and learning from new threats, Edge-AI can become more effective over time in detecting and mitigating cybersecurity threats. Additionally, Edge-AI can be used to automate routine cybersecurity tasks, freeing up human analysts to focus on more complex threats and issues [22].

However, there are also potential cybersecurity risks associated with Edge-AI. For example, if Edge-AI algorithms are compromised or manipulated by an attacker, they could be used to propagate or amplify cyber attacks [21]. Additionally, as Edge-AI becomes more prevalent in Edge Computing

systems, it may become a target for attackers seeking to exploit vulnerabilities in these systems. To mitigate these risks, it is important to ensure that Edge-AI algorithms are secure, properly configured, and continuously monitored for potential security issues. The Edge-AI based security solution and layerwise classification is shown in Figure 5.

C. ML for Cyber security solutions in Cloud Computing

ML has emerged as a promising approach for cyber security solutions in Cloud Computing due to its ability to analyze and identify patterns in large datasets in real-time [13]. ML can be used to identify and prevent cyber attacks by detecting anomalies in network traffic, identifying malicious files or activity, and predicting potential threats based on historical data.

One key use case of ML for cyber security solutions in Cloud Computing is intrusion detection. By analyzing network traffic and monitoring system logs, ML algorithms can identify anomalous activity that may indicate an intrusion attempt. These algorithms can learn from historical data to improve their accuracy over time, allowing them to detect new and emerging threats.

Another use case of ML for cyber security solutions in Cloud Computing is threat hunting. This involves actively searching for potential threats within a system by analyzing data from various sources, such as network traffic, logs, and system events. ML algorithms can be used to identify patterns that may indicate a potential threat, enabling security teams to investigate and respond to the threat before it causes damage [22].

ML can also be used for anomaly detection and predicting potential threats. By analyzing historical data and identifying patterns of behavior, ML algorithms can predict potential threats and alert security teams to take action before the threat occurs [5]. This proactive approach to cyber security can help organizations prevent attacks before they cause damage.

However, ML for cyber security solutions in Cloud Computing is not without its challenges. One major challenge is the potential for false positives and false negatives. ML algorithms may incorrectly identify benign activity as malicious, or fail to detect actual threats. This requires ongoing monitoring and fine-tuning of the ML algorithms to ensure their accuracy [7].

Another challenge is the potential for adversarial attacks. Adversaries may attempt to bypass ML algorithms by manipulating data or exploiting weaknesses in the algorithm itself. This requires ongoing research and development to improve the robustness and resilience of ML algorithms to adversarial attacks. The learning-based security solution and layerwise classification is shown in Figure 5.

VII. Future Scope

A. Future of Tiny-ML for Cyber security in IoT Layer

Tiny-ML has shown great promise in providing advanced analytics capabilities for IoT devices with limited resources. As the number of connected devices continues to grow, so does the need for robust security measures. While Tiny-ML has the potential to revolutionize IoT security, there are still significant challenges that must be addressed.

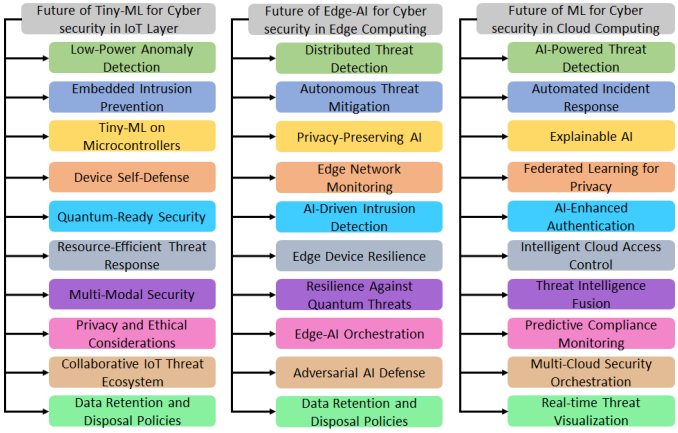

Fig. 6. Future of Pervasive AI in the Security of IoT-Edge-Cloud continuum

One area of future research for Tiny-ML in IoT security is the development of more advanced and efficient algorithms for anomaly detection. Anomaly detection is an essential component of IoT security, as it enables the detection of unusual behavior or events that may indicate a security breach. However, existing anomaly detection algorithms may not be suitable for deployment on resource-constrained IoT devices due to their computational complexity.

Another area of future research is the development of more efficient and accurate methods for intrusion detection and prevention. As IoT devices become more prevalent, they become increasingly attractive targets for cyber attacks. Effective intrusion detection and prevention are critical to maintaining the security and integrity of IoT systems.

Furthermore, future research should focus on the development of more efficient and effective techniques for secure data storage and communication in Tiny-ML-based IoT systems. As the amount of data generated by IoT devices continues to grow, it is essential to ensure that this data is stored and transmitted securely to prevent unauthorized access and manipulation.

B. Future of Edge-AI for Cyber security in Edge Computing

As Edge Computing continues to evolve and become more ubiquitous, there is an increasing need for effective security solutions to address the potential cyber security threats. Edge-AI has emerged as a promising approach to tackle the challenges of security in Edge Computing.

One potential future research direction is the development of more advanced and efficient Edge-AI algorithms for security applications. This includes the development of algorithms that can efficiently detect and respond to cyber attacks in real-time, as well as those that can learn from previous attacks to enhance future detection and response capabilities.

Another research direction is the exploration of more sophisticated data processing and storage techniques at the Edge layer. This includes the development of Edge-AI systems that can handle large volumes of data generated by IoT devices

in real-time, as well as those that can effectively manage and store sensitive data to prevent unauthorized access.

Additionally, the integration of Edge-AI with other emerging technologies such as blockchain and 5G networks could provide additional security benefits. For example, blockchain can be used to secure data sharing and transfer in the Edge layer, while 5G networks can provide higher bandwidth and lower latency for faster and more efficient data transfer.

C. Future of ML for Cyber security in Cloud Computing

ML has already made significant contributions to the field of cybersecurity, and its potential continues to grow. In the context of cloud computing, ML algorithms are being developed to address a variety of cybersecurity challenges, from identifying and responding to threats in real-time to detecting anomalies and protecting sensitive data as shown in Figure 6.

One of the most promising areas for ML in cloud security is in the field of intrusion detection. ML algorithms can be trained to recognize patterns in network traffic and identify potential attacks, helping to improve the speed and accuracy of threat detection. Additionally, ML can be used to analyze logs and other data generated by cloud systems to identify anomalies that may indicate a breach or other security incident.

Another area of potential for ML in cloud security is in the realm of data protection. ML algorithms can be used to monitor user behavior and identify potentially malicious activity, such as unauthorized attempts to access sensitive data. In addition, ML can be used to identify vulnerabilities in cloud systems and applications, allowing organizations to proactively address security risks before they can be exploited.

As ML algorithms continue to improve and become more sophisticated, their potential for use in cloud security will only continue to grow. In the future, we can expect to see ML used to develop more advanced and effective intrusion detection systems, as well as more powerful data protection and vulnerability management solutions. As organizations continue to move their operations to the cloud, ML will be an essential tool for ensuring the security and integrity of their data and systems, as shown in Figure 6.

VIII. Conclusion

The emergence of Pervasive AI has enabled a more distributed and intelligent approach to processing and analyzing data across the IoT-Edge-Cloud continuum. At the IoT layer, Pervasive AI can reduce network traffic and enhance security by enabling on-device data processing and analysis. At the Edge layer, Pervasive AI can enable intelligent decision-making close to the source of data, improving response times and reducing network traffic. In the Cloud layer, Pervasive AI can provide insights to optimize system performance and enhance security.

While the integration of AI in these layers offers great potential for improving the efficiency and security of the IoT-Edge-Cloud continuum, it also introduces new cyber security threats. Threats such as data breaches, system attacks, and adversarial attacks need to be addressed with appropriate cyber security measures.

References

[1] S. Madakam, V. Lake, V. Lake, V. Lake *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[2] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[3] T. Dillon, C. Wu, and E. Chang, "Cloud computing: issues and challenges," in *2010 24th IEEE international conference on advanced information networking and applications*. Ieee, 2010, pp. 27–33.

[4] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," *IEEE access*, vol. 6, pp. 12 103–12 117, 2018.

[5] M. S. Ansari, S. H. Alsamhi, Y. Qiao, Y. Ye, and B. Lee, "Security of distributed intelligence in edge computing: Threats and countermeasures," *The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing*, pp. 95–122, 2020.

[6] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "Ai4safe-iot: An ai-powered secure architecture for edge layer of internet of things," *Neural Computing and Applications*, vol. 32, pp. 16 119–16 133, 2020.

[7] E. Baccour, N. Mhaisen, A. A. Abdellatif, A. Erbad, A. Mohamed, M. Hamdi, and M. Guizani, "Pervasive ai for iot applications: A survey on resource-efficient distributed artificial intelligence," *IEEE Communications Surveys & Tutorials*, 2022.

[8] E. Baccour, N. Mhaisen, A. Awad Abdellatif, A. Erbad, A. Mohamed, M. Hamdi, and M. Guizani, "Pervasive ai for iot applications: Resource-efficient distributed artificial intelligence," *arXiv e-prints*, pp. arXiv–2105, 2021.

[9] M. Guo, L. Li, and Q. Guan, "Energy-efficient and delay-guaranteed workload allocation in iot-edge-cloud computing systems," *IEEE Access*, vol. 7, pp. 78 685–78 697, 2019.

[10] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, and C.-T. Lin, "Edge of things: The big picture on the integration of edge, iot and the cloud in a distributed computing environment," *ieee access*, vol. 6, pp. 1706–1717, 2017.

[11] R. Sanchez-Iborra and A. F. Skarmeta, "Tinyml-enabled frugal smart objects: Challenges and opportunities," *IEEE Circuits and Systems Magazine*, vol. 20, no. 3, pp. 4–18, 2020.

[12] L. Dutta and S. Bharali, "Tinyml meets iot: A comprehensive survey," *Internet of Things*, vol. 16, p. 100461, 2021.

[13] D. Rosendo, A. Costan, P. Valduriez, and G. Antoniu, "Distributed intelligence on the edge-to-cloud continuum: A systematic literature review," *Journal of Parallel and Distributed Computing*, vol. 166, pp. 71–94, 2022.

[14] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

[15] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey," *Ieee Access*, vol. 9, pp. 94 668–94 690, 2021.

[16] L. Mauri and E. Damiani, "Modeling threats to ai-ml systems using stride," *Sensors*, vol. 22, no. 17, p. 6662, 2022.

[17] D. Puthal and S. P. Mohanty, "Cybersecurity issues in ai," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 33–35, 2021.

[18] Y. Hu, W. Kuang, Z. Qin, K. Li, J. Zhang, Y. Gao, W. Li, and K. Li, "Artificial intelligence security: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, pp. 1–36, 2021.

[19] M. Shafique, A. Marchisio, R. V. W. Putra, and M. A. Hanif, "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)*. IEEE, 2021, pp. 1–9.

[20] D. Puthal, C. Y. Yeun, E. Damiani, A. K. Mishra, K. Yelamarthi, and B. Pradhan, "Blockchain data structures and integrated adaptive learning: Features and futures," *IEEE Consumer Electronics Magazine*, 2023.

[21] P. Porambage, T. Kumar, M. Liyanage, J. Partala, L. Lovén, M. Yliant-tila, and T. Seppänen, "Sec-edgeai: Ai for edge security vs security for edge ai," *The 1st 6G Wireless Summit,(Levi, Finland)*, 2019.

[22] E. Bertino and et al., "Ai for security and security for ai," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 2021, pp. 333–334.