Cyber-Edge Computing Applications and Challenges: A Review

Muhammad Ali Paracha[1], Syed Noman Jamil[2], Abdul Rasheed[3], Nadia Jamil[4]

[1]Transurban, Melbourne, Australia
[2]IU International University of Applied Sciences, Berlin, Germany
[3]NTT, Auckland, New Zealand
[4]Immigration and Passport, Islamabad, Pakistan

parachamuhammadali@yahoo.com.au, nomanjamilsyed@gmail.com, rasyeed_sf@yahoo.com, nadiajamilshah@gmail.com

Abstract

This research paper investigates the realm of Cyber-Edge computing, further reviewing its fundamental concepts, challenges, and applications. In a rapidly evolving landscape of interconnected devices and data-driven paradigms, the convergence of edge computing and cybersecurity takes centre stage. The paper commences by explaining the core components of Cyber-Edge architecture, encompassing policies, management, and protocols. Furthermore, it explores the Cyber-Edge applications, showcasing its transfor- mative potential in domains such as smart agriculture, smart homes, and enhanced healthcare systems. In navigating the landscape of Cyber-Edge, inherent challenges surface, ranging from cyber threats to privacy concerns, thereby prompting an analysis of future directions. Additionally, the paper formulates pivotal research questions that pave the way for further exploration in this dynamic field. The manuscript is structured on Cyber-Edge fundamentals, examines challenges, highlights practical IoT applications within the Edge paradigm and finally, presents research questions, followed by comprehensive conclusions. As the digital landscape continues to evolve, the interdependent relationship between Cyber-Edge computing and security emerges as a cornerstone in shaping the landscape of the Internet of Things (IoT) and edge networking.

Keywords: Cyber-Edge, IoT, Edge Computing, Edge networking, Security, Privacy, Machine learning, Blockchain, Protocols

Article Number: IOARP-JCN04-001
IOARP Journal of Communication and Networks
Volume 4, Issue 1, June 2024
Appeared on Digital Library: 15 July 2024

1. Introduction

1.1. Background

In the context of Cyber-Edge, the edge [1] is the outermost part of the network, where devices such as computers, phones, and sensors connect to the network and communicate with the rest of the internet. Edge computing is a set of technologies and architectures that enable these devices to communicate quickly, safely, and securely with each other and the rest of the internet.

However, edge computing also introduces several security and privacy concerns [2]. Internet of Things (IoT) devices often found at the edge of the network, have limited computing and storage capabilities and may not have the same level of security as more powerful devices. They also generate and transmit large amounts of data, which may contain sensitive information about the device, the user, or the environment. Edge networks also consist of a large number of devices that are connected to the internet, which can make them more vulnerable to network-based attacks. In addition, edge networks may raise privacy concerns as shown in Figure 1, as they often involve collecting and processing personal data.

To address these concerns, it is important to implement appropriate security measures [3] such as encryption, authentication, access control, continuous security assessment and following best data protection and privacy practices. Regulations such as the General Data Protection Regulation (GDPR) [4] also provide guidelines for protecting personal data in edge networks. Ensuring the security and privacy of edge networks is essential for the smooth and safe operation of IoT systems, edge computing, and other applications that rely on edge networking.

1.2. Edge Computing

Edge computing is a paradigm shift in data processing where data is processed at the source or ”edge” of the network, rather than being sent to a centralized location for processing. This approach allows for faster processing, reduced latency, and increased security, as well as the ability to support a wide range of IoT devices and applications that require low-latency and high-bandwidth connectivity.

1.3. IoT

IoT [5] denotes the interconnection of ordinary objects that are equipped with sensors and internet capability. This enables these objects to gather and share data. The range of such devices encompasses various items, spanning from intelligent household gadgets like thermostats and security cameras to industrial machinery and transportation networks.

1.4. Cyber Security

Articles Cybersecurity protects systems, networks, and data from digital attacks, unauthorized access, or other malicious activities. It is a rapidly growing field that encompasses a wide range of technologies, processes, and practices designed to detect and prevent cyber threats [6].

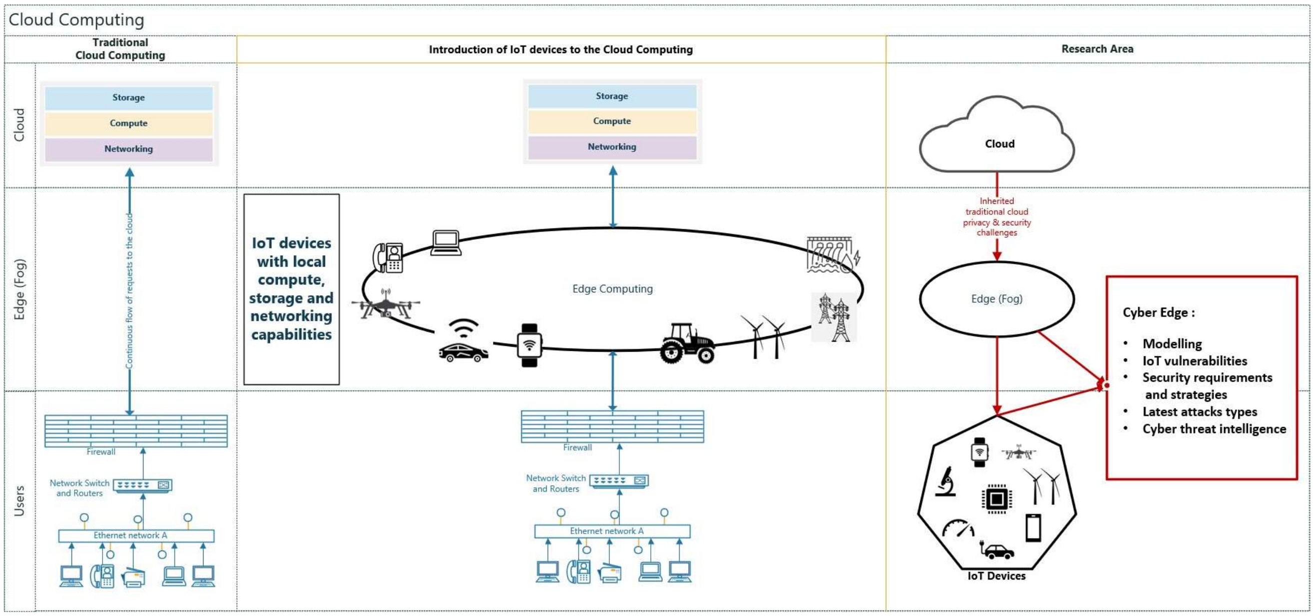

Fig. 1: Cyber-Edge Security and Privacy layered approach.

The key motivation of this research paper is to elaborate on Cyber-Edge computing, its funda- mentals, challenges and applications. In this paper, we present:

i. Cyber-Edge fundamentals by explaining the architecture, policies, management and protocols.

ii. Elaborated Cyber-Edge applications by explaining smart agriculture, smart homes and smart health.

iii. Cyber-Edge challenges are presented to review Cyber-Edge problems, existing solutions and future directions.

iv. Outlined related Cyber-Edge research questions to formulate our research problem.

The rest of the paper is organized as follows: Section II presents the cyber security edge fundamentals. Section IV, outlines the cyber edge challenges. Section III, outlines the practical application and usage of IoT devices in the Edge paradigm. Finally the section V outlines the research questions followed by the conclusions.

2. Cyber-Edge Fundamentals

The Cyber-Edge fundamentals are based on architecture, policies, management and protocols.

2.1. Architecture

The design and implementation of technologies and protocols that enable devices at the edge of the network to communicate with each other and with the rest of the internet in a fast, reliable, and secure manner. This includes measures such as network infrastructure, communication protocols, and security measures such as encryption and authentication.

2.2. Policies

The policies involve making decisions about the types of security measures to implement, the level of security required, and the roles and responsibilities of different stakeholders in maintaining and enforcing the security of the network. It also involves establishing processes for reviewing and updating the security measures in response to changing threats and vulnerabilities.

2.3. Management

Management refers to the process of protecting devices, data, and networks at the edge of the network against cyber threats and guaranteeing the confidentiality, integrity, and availability of these assets. This includes implementing and maintaining appropriate security measures, i.e., access control encryption, intrusion detection/prevention and firewalls, as well as establishing policies, procedures, and guidelines for security management.

2.4. Protocols

To Protocols are used in edge computing to protect the devices, data, and networks from unauthorized access or tampering. Transport Layer Security (TLS): It serves as a cryptographic protocol utilized to establish secure communication between devices via the Internet. It ensures the privacy, integrity, and authenticity of the data exchanged between these devices and is commonly used to secure web traffic, email, and other types of internet communication. Secure Shell (SSH): a cryptographic network protocol that is used to securely connect to and remotely manage devices over the internet. It provides strong authentication and encryption and is commonly used to re- motely access servers and other types of networking equipment. Internet Protocol Security (IPSec): constitutes a collection of protocols utilized to enhance the security of Internet communication at the network layer. It assures the authenticity, integrity and confidentiality of data as it travels between devices and is commonly used to secure virtual private networks (VPNs) and other types of internet communication. Secure Sockets Layer (SSL): represents a cryptographic protocol employed to ensure the security of communication between devices across the internet. Its role encompasses safeguarding the confidentiality, integrity, and authenticity of data as it's transmitted between these devices and is commonly used to secure web traffic, email, and other types of internet communication. Internet Key Exchange (IKE): a protocol utilized for the establishment and maintenance of secure communication between devices via the Internet. It is commonly used in conjunction with IPSec to establish and maintain VPN connections.

3. Cyber-Edge Applications

3.1. Cyber-Edge Smart Agriculture

In the smart agriculture sector, edge computing can be used to enable the real-time analysis and processing of data collected from connected devices, such as sensors and drones, to improve efficiency, productivity, and food safety. For example, edge computing can be used to enable the real-time monitoring of crop health, soil moisture, and weather conditions, and to trigger auto- mated responses based on this data. For example, edge computing can be used to automatically adjust soil moisture level-based irrigation systems, or to alert farmers to potential pests or diseases based on data collected from sensors. Edge computing can also be used to improve the efficiency of farming operations by enabling the real-time analysis of data collected from connected equipment, such as tractors and combine harvesters. For example, edge computing can be used to optimize routes and schedules, reduce fuel consumption and downtime, and improve the accuracy of yield estimates.

Overall, the use of edge computing in the agriculture sector can help to improve the efficiency, productivity, and sustainability of farming operations, and to reduce the risk of food safety incidents. Nonetheless, it's crucial to guarantee the presence of suitable security precautions to shield against cyber threats and to ensure the integrity and availability of sensitive data and critical systems.

Existing works	Cyber Edge	IoT	Cyber Threat Intelligence	Security	Privacy	Cyber Management	Edge Applications
[7]	✓	✓	x	✓	✓	x	x
[8]	✓	✓	✓	✓	✓	x	✓
[9]	✓	✓	x	✓	✓	✓	✓
[10]	✓	✓	✓	✓	✓	✓	x
[11]	✓	✓	✓	✓	✓	x	x
This Work	✓	✓	✓	✓	✓	✓	✓

Table 1: Cyber-Edge related work

3.2. Cyber-Edge in Smart Homes

In the smart homes sector, edge computing can be used to enable the real-time monitoring and control of energy use, lighting, and security in the home. It can be used to optimize the performance of smart appliances, such as refrigerators, washing machines, and water heaters, and to enable the automation of tasks such as scheduling, temperature control, and security. Edge computing can also be used to improve the convenience of smart home systems by enabling the real-time analysis and integration of data collected from multiple devices and systems. For example, edge computing can be used to enable voice assistants to respond to complex commands and queries, or to enable the integration of smart home devices with other IoT devices, such as smartwatches and fitness trackers. Overall, the use of edge computing in smart homes can help to improve the efficiency, convenience, and safety of the home, and to enable the integration of mul- tiple devices and systems. However, it's vital to make sure that adequate security measures have been implemented to safeguard against cyber threats and to ensure the integrity and availability of sensitive data and critical systems.

3.3. Cyber-Edge in Smart Health

In the context of human health and aging, edge computing can be used to enable the real-time processing and analysis of data collected from connected IoE devices, such as wearable sensors and smart home systems, to improve the health, safety, and independence of older adults. For example, edge computing can be used to enable the real-time monitoring of vital signs, such as heart rate and blood pressure, and to trigger alerts if abnormal values are detected. It can also be used to enable the real-time monitoring of activities of daily living (ADLs), such as bathing, dressing, and eating, and to trigger alerts if unusual patterns are detected. Edge computing can also be used to improve the safety and independence of older adults by enabling the real-time analysis and integration of data collected from multiple devices and systems. For example, edge computing can be used to enable the integration of wearable sensors with smart home systems, such as smart thermostats, smart lights, and security cameras, to enable the automation of tasks such as lighting and temperature control. Overall, the use of edge computing in the human aging sector can help to improve the health, safety, and independence of older adults, and to enable the integration of multiple devices and systems. However, it's imperative to verify the existence of proper security measures to defend against cyber threats and to ensure the integrity and availability of sensitive data and critical systems.

3.4. Smart Cyber-Edge Common Risks

Some examples of edge computing security risks that may be relevant in the smart sector include:

Device Compromise: Connected devices, such as smart thermostats, smart lights, and security cameras, may be vulnerable to compromise if they are not properly secured or if they are not configured with strong passwords and other security measures. This could result in the unauthorized access or tampering of devices, which could disrupt critical systems and potentially lead to safety risks.

Network Attacks: The network infrastructure, including the communication channels between devices and the internet, may be vulnerable to attacks such as denial of service (DoS) attacks or man-in-the-middle (MitM) attacks. This could result in the disruption of critical systems, as well as the potential for unauthorized access or tampering of devices and data."

Malware: Malware: Authors such as viruses and worms, may be introduced onto the network through infected devices or software and could spread to other devices, leading to the compromise of critical systems.To address these risks, it is important to implement appropriate security measures to protect against cyber threats and to ensure the integrity and availability of sensitive data and critical systems in the smart agriculture, smart home and smart health sectors.

4. Cyber-Edge Challenges, Solutions, and Future Directions

There are several key problems in Cyber-Edge computing security and privacy. Table I presents the review of existing work.

4.1. Security Issues in Cyber-Edge computing

Device Security: Many IoT devices, which are often found at the edge of the network, have limited computing and storage capabilities, and may not have the same level of security as more powerful devices. This makes them more vulnerable to attacks such as malware, denial of service (DoS), and unauthorized access.

Data Security: IoT devices often generate and transmit large amounts of data, and this data may contain sensitive information about the device, the user, or the environment. Ensuring the secure transmission and storage of this data is crucial in order to prevent unauthorized access or manipulation.

Network Security: Edge networks often consist of a large number of devices that are connected to each other and to the internet, and this can make them more vulnerable to network-based attacks such as man-in-the-middle (MitM) attacks, eavesdropping, and denial of service (DoS) attacks.

Privacy: Privacy concerns can also be associated with edge networks, given their involvement in gathering and processing personal data. It remains vital to safeguard users' privacy and restrict data collection and utilization strictly to authorized intentions.

Scalability: Edge networks often consist of a large number of devices that are geographically distributed, and this can make it challenging to manage and maintain the network. It is important to ensure that the network is scalable and can handle the increasing demands of IoT and other applications.

Interoperability: Edge networks often consist of a wide variety of devices and technologies, and it is important to ensure that these devices and technologies can work together seamlessly. This requires standards and protocols that enable interoperability between different devices and systems.

4.2. Privacy Issues in the Cyber-Edge Computing

Privacy has been one of the major consumer concerns and grey areas when using IoT devices in Cyber-Edge computing. Following is the high-level summary of some of the key privacy concerns that will need further investigations.

Data Collection: Edge devices may collect and store sensitive personal data, which could be vulnerable to breaches or misuse if not properly secured.

Data Sharing: Edge devices may transmit data to centralized locations or third parties, which could lead to data being shared or sold without the user's consent.

Lack of Transparency: Edge devices might lack transparency in terms of the data they gather, the manner of its utilization, and the parties it's shared with.

Limited Control: Users might possess restricted influence over the data amassed and processed by edge devices and may not be able to easily delete or opt out of data collection.

Limited Regulation: There may be limited regulation and oversight of edge devices and the data they collect, which could lead to data misuse or abuse. To address these issues, it is important to implement strong security measures to protect data, provide clear information and transparency to users about data collection and use, and ensure that users have control over their data. Additionally, the development of regulations and industry standards that specifically address the privacy concerns of edge computing can be beneficial.

4.3. Existing Solutions in the Cyber-Edge Computing

There are several solutions to the problems in Cyber-Edge computing security and privacy:

Device Security: One solution is to use secure boot and firmware update mechanisms to ensure that only trusted software is running on the device. Other solutions include using strong pass- words, enabling two-factor authentication, and implementing network segmentation to limit the spread of any compromise.

Data Security: One solution is to use encryption to secure data in transit and at rest. Other solutions include using secure protocols for data transport, such as HTTPS, and implementing access control measures to ensure that only authorized users have access to sensitive data.

Network Security: One of the approaches involves employing firewalls and intrusion detection/prevention systems to shield the network against external threats. Other solutions include using network segmentation to isolate different parts of the network and using virtual private networks (VPNs) to secure communication between devices.

Privacy: One solution is to follow best practices for data protection and privacy, such as those outlined in regulations such as GDPR. Other additional remedies encompass introducing access control mechanisms to confirm that solely authorized users can access personal data and employing encryption to safeguard data during transmission and storage.

Scalability: One of the solutions is to use distributed architectures and protocols that enable devices to communicate directly with each other, rather than relying on a central server. Other solutions include using load balancing and content delivery networks (CDNs) to distribute traf- fic across the network, and implementing mechanisms for self-organization and self-healing to maintain the integrity of the network.

Interoperability: One of the approaches involves utilising open standards and protocols that facilitate communication between various devices and systems. Other solutions include using middleware and gateways to translate between different protocols and implementing abstractions and APIs to hide the complexity of the underlying systems.

4.4. Cyber-Edge Future Directions

Here are a few potential new ideas to address the problems in edge network security and privacy:

Machine Learning: Employ machine learning algorithms to assess network traffic, identifying anomalies or threats promptly as they arise. This could help to identify and mitigate attacks more quickly and effectively.

Blockchain: Implement blockchain-based solutions to secure data and ensure its integrity. For example, data could be stored on a decentralized ledger that is managed by multiple parties, making it more difficult to tamper with.

Artificial Intelligence: The Future of AI in Cyber-Edge computing security and privacy lies in creating AI systems that are not only intelligent but also adaptable, transparent, and privacy- conscious. These systems should seamlessly integrate with human expertise to provide holistic cybersecurity solutions that stay ahead of emerging threats. Moreover, AI and machine learning become more integral to cybersecurity and the development of adaptive and explainable AI models could significantly improve the effectiveness and trustworthiness of security measures at the edge.

Secure Modules: Develop secure hardware modules that can be used to protect devices at the edge of the network. These modules could provide hardware-level security measures such as secure boot, secure storage, and hardware-based encryption.

Virtualisation: Use virtualisation technologies to create secure and isolated environments for devices at the edge of the network. This could help to prevent the spread of any compromise and allow for easier management and maintenance of the network.

Protocols Mechanisms: Implement protocols and mechanisms for self-sovereign identity, enabling devices at the edge of the network to have their own unique and verifiable identities that the users themselves control. This could help to protect privacy and give users more control over their data.

State-of-the-Art Algorithms: Develop new algorithms and protocols for efficient and secure data transport and delivery at the network's edge. This could include technologies for compression, error correction, and routing optimization, as well as mechanisms for securing the data itself.

Cyber Threat Intelligence model: The field of cyber threat intelligence is evolving in response to the ever-changing threat landscape. As technologies like AI, machine learning, and automation continue to mature, the role of cyber threat intelligence will become more crucial in defending against sophisticated cyber adversaries.

Security of Cyber-Edge Algorithms: Cyber-Edge computing continues to evolve, ensuring the security of algorithms becomes paramount. Therefore, Developing and adopting cryptographic algorithms that are resistant to attacks from emerging quantum computers. As quantum comput- ing threatens to break traditional encryption methods, investing in quantum-resistant algorithms will safeguard data against future threats.

5. Research Questions

1) What are the key architectural components, policies, and protocols that form the foundation of Cyber-Edge computing?
2) What are the main challenges and vulnerabilities faced by IoT devices at the edge, and how can these challenges be mitigated?
3) What are the unique security requirements and strategies for implementing Cyber-Edge solutions in domains such as smart agriculture, smart homes, and healthcare?
4) What are the most common types of latest network-based attacks targeting edge networks, and how can Cyber-Edge architecture be designed to thwart these attacks?
5) How can cyber threat intelligence be integrated into edge networks to prevent and detect emerging cyber threats in real time?
6) How Cyber-Edge computing continue to evolve, ensuring the security of algorithms from quantum computing?

6. Conclusion

In the rapidly evolving landscape of technology and interconnected devices, the convergence of edge computing, IoT and cybersecurity emerges as a pivotal force shaping the digital realm. This research paper presented a review of Cyber-Edge computing, addressing its fundamental aspects, challenges, applications, and implications. By highlighting the architectural components of Cyber-Edge systems, including policies, management, and protocols, this paper underscores the importance of designing robust and secure frameworks for IoT devices at the network's edge. The integration of encryption, authentication, and access control mechanisms emerges as a critical strategy to fortify these networks against evolving cyber threats. The transformative potential of Cyber-Edge computing is vividly illustrated through its applications in diverse domains. From revolutionizing agricultural practices to enhancing the efficiency of healthcare systems and en- abling smarter homes, Cyber-Edge solutions exemplify the fusion of innovation and security.

The dynamic landscape of Cyber-Edge computing needs further exploration. The dependable relationship between edge computing, IoT, and cybersecurity necessitates a multidisciplinary approach to innovation, security, and regulation. As this field continues to evolve, it is imperative to introduce the balance between innovation and safeguarding, ensuring that the promises of a connected world are realized without compromising security and privacy.

References

[1] S. U. Jamil, M. A. Khan *et al.*, "Edge computing enabled technologies for secure 6G smart environment-an overview," in *International Conference on Soft Computing and Pattern Recognition*. Springer, 2021, pp. 934–945.

[2] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A survey of security in cloud, edge, and fog computing," *Sensors*, vol. 22, no. 3, p. 927, 2022.

[3] J. L. Hernandez-Ramos, J. A. Martinez, V. Savarino, M. Angelini, V. Napolitano, A. F. Skarmeta, and G. Baldini, "Security and privacy in Internet of Things-enabled smart cities: Challenges and future directions," *IEEE Security & Privacy*, vol. 19, no. 1, pp. 12–23, 2020.

[4] M. Goddard, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact," *International Journal of Market Research*, vol. 59, no. 6, pp. 703–705, 2017.

[5] "Emerging iot applications in sustainable smart cities for covid-19: Network security and data preservation challenges with future directions," *Sustainable Cities and Society*, vol. 75, p. 103311, 2021.

[6] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: a comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[7] S. Hamdan, S. Almajali, M. Ayyash, H. B. Salameh, and Y. Jararweh, "An intelligent edge-enabled distributed multi-task learning architecture for large-scale IoT-based cyber-physical systems," *Simulation Modelling Practice and Theory*, vol. 122, p. 102685, 2023.

[8] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. Ramana, and R. Mohanty, "Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method," *ACM Transactions on Sensor Networks*, 2023.

[9] K. Baranitharan, V. Dineshbabu, R. Concepcio´n-La´zaro, R. Balamanigandan, K. Selvakumarasamy, R. Mahaveerakannan, and M. W. Bhatt, "A collaborative and adaptive cyber de´fense strategic assessment for healthcare networks using edge computing," *Healthcare Analytics*, vol. 3, p. 100184, 2023.

[10] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Communications*

Surveys & Tutorials, 2023.

[11] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, “Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection,” *Journal of Network and Systems Management*, vol. 31, no. 1, p. 3, 2023.