Security Implications of Edge Computing

Contents

Overview of Edge Computing

What is Edge Computing?

Edge computing is a way of processing data closer to its source rather than transmitting it to a central location for analysis and storage, such as a remote data center or the cloud. Moving computing resources, such as local servers, sensors, and Internet of Things devices, to the network's "edge" improves processing speed, latency, and efficiency (Bigelow, 2021).

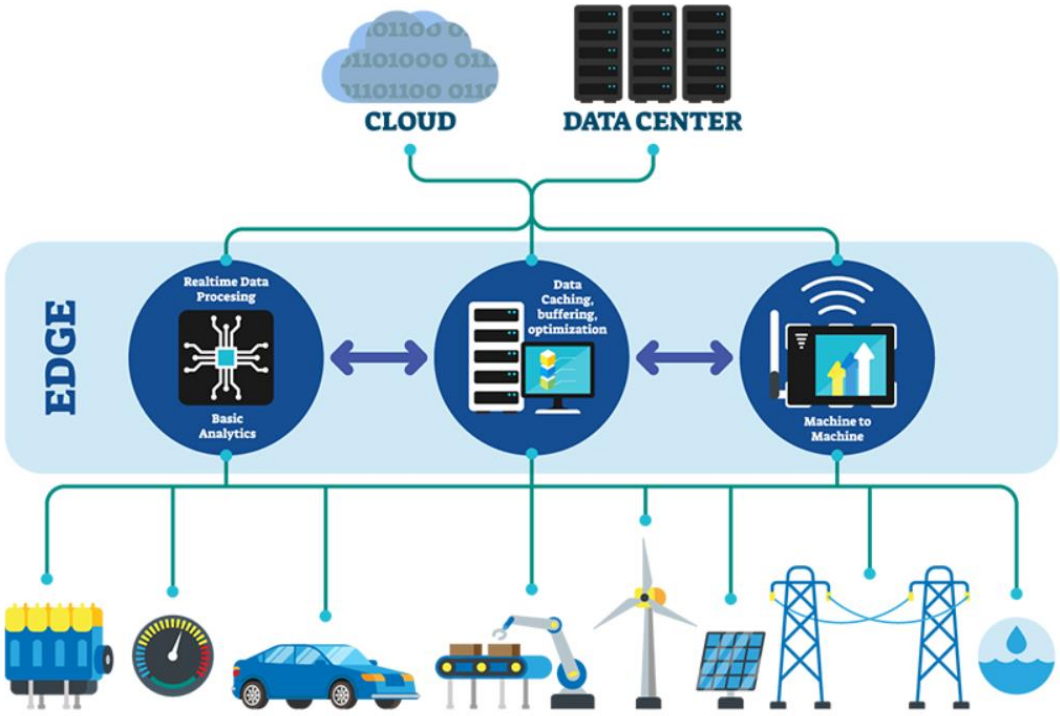

Figure 1: Edge Computing Overview (Ebyte, 2024)

For Example, we may compare edge computing to a popular pizza restaurant. It expands the number of little branches in the neighborhood, ensuring that everyone has access to hot, fresh pizza. A pizza baked in the main site would go cold on its route to a distant consumer. Still, a pizza made at a nearby neighborhood location would result in not just hot and fresh pizza, but also speedier delivery and a satisfied customer. Where the pizza restaurant is the Cloud, and its branches are the edge notes or edge locations in edge computing.

Key principles and technologies related to Edge Computing

- **Closeness to Data Source:** By bringing the processing and storage of data closer to the point of origin or consumption, edge computing minimizes latency and the distance that data must travel. Key technologies like edge devices (IOT sensors, gateways) and edge computing software (Operating systems, middleware).
- **Low Latency:** Edge computing improves reaction times and real-time processing by bringing data closer to the source, reducing the amount of time data needs to transfer between devices and centralized servers.
- **Flexibility:** Edge computing technology can function independently even if cloud connectivity is lost, ensuring reliability and ongoing operation in challenging network conditions.
- **Bandwidth Effectiveness:** Edge computing lowers the need to transport huge amounts of raw data to centralized computers across the network, reducing bandwidth use and network congestion.
- **Scalability:** Because edge computing designs are naturally scalable, organizations may handle increasing workloads and data volumes without overburdening the centralized infrastructure by adding additional edge devices to the network as required.
- **Security:** Edge computing increases data security by decreasing the need for sensitive data sent across networks. Local data processing and analysis reduces the chance of interception or unauthorized access while in transit.

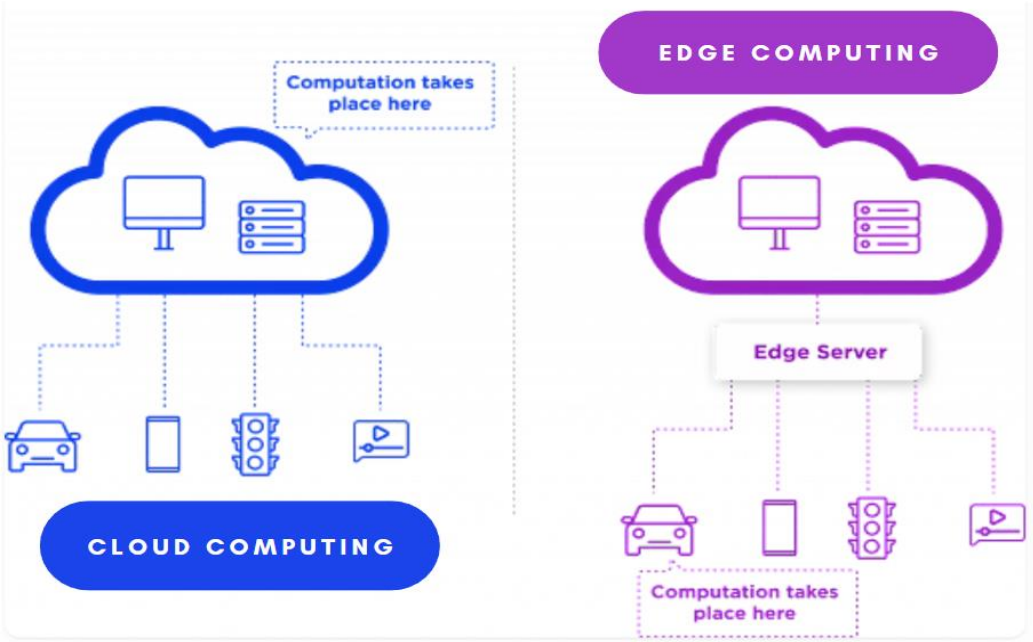

Figure 2: Cloud Computing vs Edge Computing

Edge Computing Vs Traditional Cloud Computing

Edge Computing	Cloud Computing
Computing Resources are placed closer to the data source.	Computing Resources are placed in centralized data centers.
Data is processed locally resulting in low latency.	Data travels to and from far data centers resulting in high latency.
The use of bandwidth is reduced by local data processing.	The use of bandwidth is high as the data needs to be transferred from centralized servers.
Even with irregular connectivity, it can operate independently.	Network connection is crucial for accessing centralized resources and transmitting data.

Risks Related to Edge Computing

Edge computing is not free from the risks involved with technology. Despite its numerous benefits, edge computing has issues that enterprises must solve in order to successfully implement it.

- Edge devices may have fewer security measures than centralized servers, making them vulnerable to hacker attacks and unauthorized access.
- Processing sensitive data at the edge raises concerns about data privacy and conformity to regulations such as HIPAA and GDPR.
- Compatibility challenges may develop when merging many edge systems and devices from different providers, limiting device-to-device communication and data exchange.
- Data redundancy and fragmentation can result from dispersed data processing at the edge, making it challenging to manage and synchronize data across several devices and locations.
- Edge devices often have fewer processing, memory, and storage capacities than centralized servers, which might limit the functionality of edge apps and affect performance.
- Businesses that rely on outside-edge vendors for infrastructure and services face the risk of vendor lock-in, service disruptions, and changes to service terms or pricing.

Security Risk and Vulnerabilities

Security Risks in Edge Computing

1. Data Security

- Data stored at the edge does not have the same level of physical security measures as data centers. It is conceivable that someone could easily take an entire database by taking out the disk from the edge computing device or by using a USB stick to duplicate the data. Due to the restricted local storage capabilities of edge computing facilities, it could be challenging or unfeasible to create backups of essential files. Consequently, if an issue arises, there may not be a backup available to recover the database.
- The operability of data encrypted by traditional encryption algorithms is low, which creates significant barriers to subsequent data processing. Traditional encryption algorithms include symmetric encryption algorithms (such as DES, 3DES, ADES, etc.) and asymmetric encryption algorithms (such as RSA, Diffe-Hellman, ECC, etc.).
- Integrity audit schemes cannot be performed by either the data storage server or the data owner, as they are both unsuitable for this purpose. Frequently, they are developed using a third-party auditing platform (TPA). In this instance, security risks like data leakage and tampering are highly likely when the TPA is semi-trusted or untrusted, and data privacy cannot be guaranteed (Kimachia, 2022).

2. Access controls

- Access control presents a very difficult challenge to edge computing security. Many low-power IoT devices will be directly connected to edge nodes. Deploying security solutions in a traditional cloud computing environment is challenging due to the extremely limited resources, heterogeneous hardware, diverse communication protocols, and difficulty installing patches on time in these Internet of Things devices. As a result, creating an access control mechanism for Internet of Things devices in an edge computing environment will be difficult and crucial.
- The distribution of processing and data storage in edge computing brings them closer to the data source, resulting in an increased number of access points within the network.

However, this decentralized structure poses difficulties in implementing uniform and strong access controls across all edge devices and nodes.

- Communication between edge devices, gateways, and central servers takes place over wireless or public networks that may not be fully secured. Without proper encryption and authentication methods, attackers can intercept or manipulate these communication channels, resulting in unauthorized access or data breaches.
- Because many edge devices have limited processing power, putting strong access control mechanisms in place can be difficult. Due to resource limitations, security measures may have to be compromised, making edge devices vulnerable to attack.

3. Privacy protection

- Edge computing systems often work closely with data-generating sources such as IoT devices, sensors, or mobile devices. This proximity means that sensitive data, including personal information, health data, or location data, is processed and stored close to where it was collected. As a result, the risk of unauthorized access or disclosure of sensitive data increases if adequate privacy protection measures are not implemented.
- Edge computing frequently requires the consolidation of data from various origins to extract valuable insights or facilitate prompt decision-making. Nevertheless, the amalgamation of data from different sources may heighten the likelihood of privacy violations, potentially resulting in the inadvertent exposure of confidential details or the deduction of personally identifiable information (PII) via data correlation and examination.

4. Identity Authentication

- Edge computing environments frequently comprise a variety of devices with different capabilities and security profiles, such as gateways, edge servers, IoT sensors, and central cloud services. It can be difficult to manage identity authentication in this heterogeneous environment because different devices might employ various protocols or authentication mechanisms.
- Centralized authentication methods, and identity providers in a decentralized computing environment represent a single point of failure. If these key components are disrupted or

unavailable, services may be disrupted or unauthorized access to resources may occur throughout the infrastructure.

- Identity verification methods may require sharing sensitive details like user credentials, biometric information, or cryptographic keys. Failure to adequately safeguard this data could result in privacy breaches or unauthorized entry to personal information, creating potential threats to user privacy and regulatory adherence.

5. Network security

- Edge devices, especially those connected to the internet, might run software that is out-of-date or vulnerable and has few security features. By taking advantage of flaws in edge devices, attackers can gain illegal access to the network and use it to launch attacks or steal confidential information from the edge infrastructure.
- Edge devices and gateways within edge computing environments are interconnected through wired and wireless communication channels, forming a complex network topology. Attackers can exploit vulnerabilities in interconnected devices to gain unauthorized access to sensitive data, launch denial-of-service (DoS) attacks, or pivot within the network to compromise other devices or services.

6. Physical security

- Edge computing devices are vulnerable to theft, especially those deployed outdoors or in unsecured environments. Device theft can result in lost revenue, data loss or organizational disruption. This is especially true if the stolen device contains confidential or proprietary information.
- Extreme temperatures, high humidity, dust, or water intrusion are some of the environmental risks that edge computing devices may be subjected to. These risks can harm hardware components and impair the infrastructure's dependability and efficiency. Service disruptions, data loss, and equipment failures may arise from edge devices' failure to protect themselves from environmental threats.
- The proper functioning of edge computing devices heavily relies on a stable and uninterrupted power source. Any power outages or interruptions, be it caused by natural

disasters, accidents, or deliberate actions, can significantly disrupt edge computing services and result in the loss of valuable data or system downtime. To counteract these potential issues, it is crucial to implement backup power solutions such as uninterruptible power supplies (UPS) or alternative energy sources. These measures can effectively mitigate the impact of power disruptions on edge infrastructure.

7. Edge to cloud communication

- Edge-to-cloud communications often occur over network connections, which can be vulnerable to various vulnerabilities and threats. Features such as unsecured wireless networks, weak encryption protocols, or unreliable APIs can expose communication channels to risks such as eavesdropping, man-in-the-middle attacks, or unauthorized access.
- The transmission of data from edge devices to the cloud is often hindered by limited bandwidth, particularly in cases where there is a high volume of data being generated or real-time processing is necessary. These bandwidth restrictions can cause congestion, delays, or bottlenecks in communication between the edge and the cloud, impacting the efficiency and responsiveness of edge computing applications.
- Because cloud servers are located far away from edge devices, latency is introduced during edge-to-cloud communication. Autonomous vehicles or industrial automation are two examples of real-time applications or services that can suffer from latency. In edge computing environments, latency minimization is critical to timely data processing and decision-making.

Vulnerabilities in Edge Computing

1. Device Vulnerabilities

- A possible danger is gaining physical access to the machine. Edge nodes are positioned near where data is generated or needs processing. As a result, they are not under the physical control of the vendor or service provider. An adversary could use physical access to the device to execute various malicious activities.

- Devices used in real-world deployments might be created by several vendors and are extremely diverse. This is a debatable fact, particularly in light of the Internet of Things. These devices are frequently discovered to be running firmware or code that is vulnerable and has not undergone adequate security analysis. Adversaries may take advantage of common vulnerabilities on some devices, like out-of-bounds writing. For example, a heap-based buffer overflow in the Philips Hue Bridge (model 2.X) permits remote code execution.
- Network nodes such as NAT (Network Address Translation) have their vulnerabilities. NAT "hides" the IP addresses of internal network devices from the external network. All internal devices share one public IP address (IPspecialist, 2023).

2. Vulnerabilities in edge services

- Edge services frequently depend on interconnected elements for their operation, including the exchange of information between edge devices, gateways, and centralized servers. Attackers can exploit weaknesses in these communication channels to intercept, manipulate, or disrupt the flow of data.
- APIs (Application Programming Interfaces) are typically exposed by edge services to facilitate data exchange and communication. These APIs' inadequate authorization, authentication, or input validation can result in security flaws like data exposure, injection attacks, and broken authentication.
- Edge services often rely on third-party libraries, frameworks, or components for their functionality. Vulnerabilities in these dependencies, such as outdated software versions or unpatched security flaws, can leave secondary services vulnerable to attackers.

3. Protocol Vulnerabilities

- The Edge network commonly employs efficient communication protocols like LTE, Wi-Fi, Bluetooth, MQTT, CoAP, AMQP, LoRa, and Zigbee. The attack surface expands to include the protocol itself. An attacker may be able to initiate an attack by taking advantage of weak points in the communication protocols.
- Message Telemetry Transport (MQTT) is a widely used application layer communication protocol for edge-to-edge communication in the IoT. The MQTT protocol supports

encrypted communications but is optional. This configuration allows a man-in-the-middle to spoof messages at the same time, which can result in serious privacy violations. For example, data generated by wearable devices can include highly sensitive health data, personal information, and even human movements.

4. Cloud Vulnerabilities

- A misconfiguration allowed public access to a cloud server hosting data without authorized access rights. For example, a misconfiguration of Amazon Web Services S3 resulted in the exposure of highly sensitive user data provided by the cloud provider.
- Inadequate access control, injection, and excessive data exposure are among the most serious problems with API security. Attackers were able to send unauthorized HTTP requests to any Exchange server by taking advantage of a vulnerability in Microsoft Exchange Server. Adversaries were able to take advantage of security flaws and broken user authentication to use the server's back-end API to escalate privileges and preserve persistence.

5. Network vulnerabilities

- Inadequate separation of edge networks from other components of the infrastructure may lead to a larger attack surface and the spread of security vulnerabilities. Unauthorized access to other areas of the network or the spread of malware can occur from compromised edge devices or services.
- Communication lacking encryption between edge devices, gateways, and central systems exposes data to interception and eavesdropping by malicious actors. Protocols like Telnet or FTP, which do not utilize encryption, transmit data in plain text, putting sensitive information at risk of compromise.
- Many edge devices in Internet of Things (IoT) installations have security vulnerabilities due to limited resources, lack of security updates, and security vulnerabilities. Attackers can use compromised IoT devices to launch attacks against edge networks or centralized systems.

Edge Computing exposes businesses to new threat vector

Because of its decentralized architecture and dependence on networked devices, edge computing presents new security risks for organizations. Edge computing can expose businesses to these risks in the following ways:

1. Expanded Attack Surface: By dispersing computing resources closer to the data source, edge computing creates more entry points for attackers to exploit. The proliferation of edge devices and services increases the complexity of securing the entire ecosystem, making it harder for organizations to defend against potential threats.

2. Distributed Environment: Edge computing operates across multiple locations with interconnected devices and services, allowing attackers to exploit vulnerabilities in one area to compromise others. This makes it challenging for organizations to detect and mitigate threats across the entire edge infrastructure.

3. Data Exposure and Leakage: Storing sensitive data closer to the source increases the risk of exposure and leakage if proper security measures are not in place. Attackers may target edge devices or communication channels to access, manipulate, or steal sensitive information, leading to privacy breaches or compliance violations.

4. Security Management Complexity: Security management in edge computing environments is more complex than in centralized architectures due to the diversity of hardware and services. Organizations must manage different security features, software versions, and configurations across different domains, making it difficult to implement policies and controls.

5. Dynamic nature of edge computing environments: It is characterized by the dynamic joining and leaving of devices from the network. Because of its dynamic nature, the edge infrastructure presents difficulties in maintaining uniform security configurations, policies, and controls, which raises the possibility of security lapses or misconfigurations that an attacker could exploit.

6. Emerging Risks and Vulnerabilities: As edge computing develops further, new risks and weaknesses could appear. As a result, businesses will need to modify their security plans and defenses. To effectively identify and counter new threats, attackers must constantly adapt their

strategies, methods, and procedures to take advantage of vulnerabilities in edge computing environments. Proactive security measures and ongoing monitoring are therefore essential.

Real World examples of security incidents in Edge computing

A few real-world examples of security incidents in edge computing are given below:

1. **CSRF** and **SSRF** primarily target traditional Internet infrastructures. In 2016, it was discovered that edge systems are also vulnerable to these two attacks. CSRF is an attack where the end user (ie in this case the edge server) is forced to perform unwanted actions via web applications. SSRF is an attack in which edge servers are abused to read or modify internal resources. The coarse-grained design of the verification mechanism, which uses an easily broken identity verification method, is the primary cause of both attacks. An attacker can pose as a "legitimate" edge server and use coarse-grained verification to send commands to other edge servers covertly, leaving those other edge servers vulnerable to CSRF and SSRF attacks.

2. In the first 20 hours following its release, the attackers of the infamous **Mirai botnet** managed to seize control of over 60,000 Internet of Things devices. Then, a DDoS attack was launched against well-known edge service providers like Krebs, OVH, and Dyn using these rogue IoT devices. Several variation botnets, including Hajime and BrickerBot, were discovered soon after the Mirai outbreak. DDoS is the most widely used and straightforward attack in real-world scenarios. Because of this, it seriously jeopardizes real-world edge computing services.

Mitigation Strategies

Mitigation strategies to address security challenges posed by Edge Computing

1. Data security:

- Use robust encryption for all data in use, in transit, and at rest. This scrambles the data as a result, making it unreadable without a decryption key.
- The important data should be given priority for storage and unnecessary data should be dumped because less data means less attack surface for the attackers.
- Data should be stored centrally with multiple layers of security making it harder to breach.

2. Device security:

- Ensure the regular update of software and firmware on edge devices to address vulnerabilities and patch them before it is too late. Also, set up security measures for newly configured devices.
- Implementation of strong access control mechanisms which restrict unauthorized access to devices and data. This can include the use of multi-factor authentication and the implementation of a strong password policy.

3. Self-defending network security:

- Organizations should develop their own network and device security mechanisms so that they can monitor themselves. This leads to the response to threats through automation by identifying potential threats and reduction of potential human errors.
- A network that is self-defended helps organizations to make their edge security less complex and reduce the cost for management. The self-defending network is integrated with the installed firewalls and does not require any third-party security software and systems to be installed in the endpoint devices (WALKER, 2023).

4. Additional Strategies

- Implementation of a zero-trust security model is essential where all users and devices must be continuously authenticated and authorized before accessing resources.
- Physical security measures must be implemented for the protection of edge devices from unauthorized access, tampering, or theft. This can include locking cabinets or restricted access areas.

- Training of the personnel involved in managing edge deployments on the best security practices of the industry is essential.

Managing Edge devices

The best practices for managing edge devices must ensure the security, efficiency, and performance delivery of the system. Some of the best practices prevalent in the industry are mentioned below:

1. **Prioritize the security of edge devices:**

   Edge devices are managed locally, and data is also processed and stored locally, as a result, there are high security risks of these devices being compromised. The devices can be used as entry points into the network. Therefore, it is essential to prioritize the security of these devices and every other component equally as other critical infrastructure such as central data centers. The most common security practices in Edge are data encryption during transmission and storage, multi-factor authentication, endpoint protection, and end-user training (Fernandez, 2022).

2. **Automate the updates and management:**

   Edge computing has many different devices under operation. It is not feasible to manage and maintain these devices manually. Hence, the updates of software, system deployments, and configuration of changes should be managed through automation. This reduces risks and the occurrence of errors.

3. **Resource optimization:**

   The processing power, storage, and capacity of devices in Edge computing are limited. It is essential for maximum utilization of the available resources. This can be achieved by dynamic resource allocation, lightweight design of applications and systems, deployment of distributed architecture to balance workloads and offloading tasks are some of the prevalent options (IBM, 2023).

Best practices for data encryption

Generally, there are two popular practices for data encryption for edge computing.

- **Data at transit encryption**

  Data that is to be transferred between edge devices, gateways, and servers should be encrypted for protection against attacks such as interception. Secure communication protocols such as SSL and TSL can be used.

- **Data at rest encryption**

  In the case of edge devices and servers where data is to be stored, the data should be encrypted using robust encryption algorithms for the prevention of data theft and data loss (IBM, 2023)

Important reasons for security-aware application development

Increased attack surface

- Edge computing has a lot of different devices, and the list of devices increases with time and the operational needs of the organization. So, each additional device can be a new point of target for attackers which they can breach easily.
- Edge devices are often located beyond the bounds of traditional security perimeter usually in remote locations. It is difficult to implement robust security mechanisms as in centralized systems.
- Attackers are aware of these vulnerability factors, and this leads edge devices to become more attractive targets for attackers. They might target applications running on the devices, and communication channels or might exploit the vulnerabilities of the device itself.

Limited resources

- Edge devices generally have limited memory and processing power, due to which there is limited capacity for implementing security measures.
- The cost of security also is a significant factor in implementing security measures in edge computing.

Data Sensitivity

- Attackers can gain access to the sensitive data through compromised devices it processes or stores. These can cause significant damage to the edge ecosystem.
- These sensitive data can be protected by the implementation of mechanisms such as Encryption, secure storage practices, and access controls. These measures also help to minimize the chances of data breaches and their potential impact.

Conclusion

At last, our review of edge computing has brought out its distinct technologies and guiding principles, outlining its decentralization in comparison to traditional cloud computing. Although edge computing provides benefits such as lower latency, it also poses security risks such as network attacks and data leaks.

Key points:

- Edge computing differs from traditional cloud computing since it brings computer resources closer to data-generating areas.
- While there are benefits, such as reducing latency, there are also security threats, such as network attacks and data breaches.
- Strong device management, encryption, and the development of security-aware applications are all examples of effective mitigation approaches.

To address these concerns, organizations must implement strong security measures and integrate security into the edge application development process. This allows them to make use of the promise of edge computing while also protecting themselves against security weaknesses and threats.

References

Bigelow, S. J. (2021, 12 08). *What Is Edge Computing? Everything You Need to Know*. Retrieved from TechTarget: https://www.techtarget.com/searchdatacenter/definition/edge-computing

Ebyte. (2024, 03 26). *Edge Computing Overview*. Retrieved from Chengdu Ebyte Electronic Technology Co., Ltd.: https://www.cdebyte.com/news/531

Fernandez, R. (2022, 09 12). *Top 4 best practices for edge computing*. Retrieved from TechRepublic: https://www.techrepublic.com/article/best-practices-edge-computing/

IBM. (2023, 08 21). *Best Practices for developing edge services*. Retrieved from IBM: https://www.ibm.com/docs/en/cloud-private/3.2.0?topic=developing-best-practices

IPspecialist. (2023, 10 10). *Edge Computing Security Risk And Challenges In 2023*. Retrieved from IPSpecialist: https://ipspecialist.net/edge-computing-security-risk-and-challenges/

Kimachia, K. (2022, 09 09). *The risks of edge computing*. Retrieved from TechRepublic: https://www.techrepublic.com/article/edge-computing-risks/

WALKER, G. (2023, 11 20). *The Importance of Security for Edge Computing*. Retrieved from Allied Telesis: https://www.alliedtelesis.com/ca/en/blog/importance-security-edge-computing