The Great Debate: The Future of Security Risk Management (SRM)

Hainadine Chamane

University of Essex

UNIT 6 SEMINAR: THE GREAT DEBATE – THE FUTURE OF SRM

Edge computing is poised to be the major trend influencing the next five years.

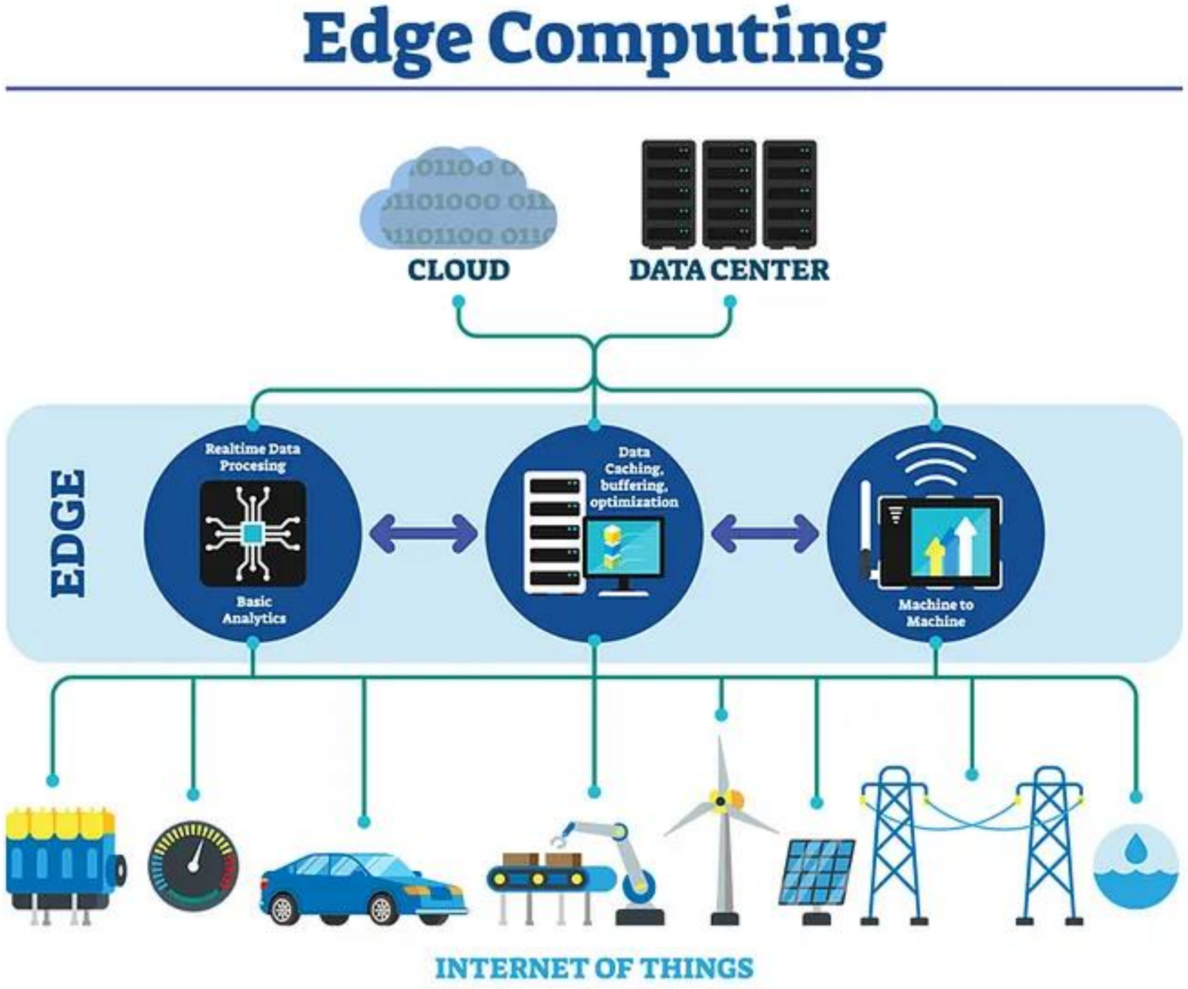
- In the next five years, edge computing, a rapidly expanding market, is anticipated to influence the technology sector significantly. Transport, logistics, manufacturing, healthcare, IT, and telecom elements drive growth in this industry, providing a wide range of goods and services, with hardware and software accounting for most sales. According to The Industry Outlook Report (2024), it is anticipated to reach multimillion-figure levels by 2030, exhibiting an unanticipated compound annual growth rate.

- Edge computing performs better in speed, dependability, and energy use than cloud-based computing. According to Shi et al. (2016), data processing at the network's edge lowers reaction times, energy consumption, and bandwidth utilisation.

- Security for edge computing is still in its infancy. Not enough research has been done on algorithms for anomaly detection, privacy protection, authentication, and trust assessment. Even though IoT devices create enormous amounts of data, protecting edge computing nodes is difficult due to their complexity and susceptibility (Zeyu et al. 2020).

WHY IS EDGE COMPUTING IMPORTANT?

- Edge computing is crucial when IoT devices have poor connectivity.
- It reduces latency by processing data closer to the source, which is particularly important in the manufacturing or financial services industries.
- With the buildout of 5G networks, edge computing is becoming even more critical.
- It provides direct access to the gateway into the telecom provider’s network, which connects to a public IaaS cloud provider.
- Data is compiled and sent as daily reports to the cloud for long-term storage, reducing the amount of data that needs to traverse over a network.
- Edge computing is a game-changer in the world of technology.



(Dey, 2020)

WHAT SECURITY DOES EDGE COMPUTING OFFER?

- Edge computing security offers extra security to edge devices placed outside the data centre. It entails protecting edge devices' physical and UI access and establishing edge network, application, and data security procedures as close to data centre standards as possible (Nolle, 2021).

- Enterprise security that guards users and apps beyond the protective perimeter of a centralised data centre, where sensitive data is particularly exposed to attacks, is known as edge security (AppViewX, N.D.).

- Through edge cybersecurity, secure computing operations are ensured at the furthest boundaries of an enterprise's network. These spaces are the most vulnerable to security breaches since the organisation's perimeter does not entirely enclose them. Self-driving cars, IoT gadgets, and sensors are a few instances of edge computing in action (Jones, 2022).

WHICH PARTICULAR SECTORS ARE THE BIGGEST WINNERS FROM EDGE COMPUTING TECHNOLOGY?

At or close to the network edge, edge computing is used to gather, filter, process, and analyse data (Bigelow, 2021). It comes in handy when there are technological, financial, or compliance-related reasons why data cannot be transferred to a single place. Among the many uses for edge computing are:

- Improving manufacturing quality.
- Improving network efficiency.
- Keeping an eye on worker safety.
- Enhancing medical treatment.
- Operating self-driving cars.
- Examining data from retail.

Which risks come with putting edge computing into practice, and how may they be reduced?

Data storage and protection, weak passwords and authentication, and data sprawl are among the security vulnerabilities associated with edge computing (Rauch, 2024). If data is transferred without processing, these risks can jeopardise important information, endanger numerous devices, and increase delay.

Rauch (2024) highlights that businesses should implement the "5 Ps" policy: People, Policies and Procedures, Processes, Products, and Proof to reduce edge security concerns. Cybersecurity training should be provided to the public, edge security should be routinely governed, procedures should be itemised, businesses should comprehend the elements of a cybersecurity solution, and vulnerability detection and remediation should be done regularly.

WHAT ARE THE MOST ESSENTIAL GUIDELINES THAT ORGANISATIONS SHOULD FOLLOW TO ENSURE SECURE EDGE COMPUTING OPERATIONS?

Moving from traditional data centre architecture to edge computing technology can significantly increase a company's cyber-attack exposure (Violino, 2020). To mitigate these risks, it is crucial to follow these five best practices:

1. Integrate edge computing into your security strategy without fail.
2. Implement a zero-trust policy and clearly understand what constitutes normal behaviour.
3. Prioritize security without any compromise when purchasing edge computing products.
4. Ensure that any vulnerabilities are addressed by prioritising patching.

An effective edge security strategy should include five elements: people, policy and procedures, process, product, and proof.

Furthermore, to ensure maximum security and protection for your organisation, Frank L. (2023) has highlighted the following best practices for edge computing:

1. Use automated and intelligent monitoring systems to detect security risks without fail.
2. Authenticate users with multi-factor authentication to ensure foolproof security.
3. Enforce security standards and integrate them into your network architecture without any exceptions.
4. Purchase hardware and software from companies prioritising security without compromise.

WHAT ARE THE MOST ESSENTIAL GUIDELINES THAT ORGANISATIONS SHOULD FOLLOW TO ENSURE SECURE EDGE COMPUTING OPERATIONS?

Moving from traditional data centre architecture to edge computing technology can significantly increase a company's cyber-attack exposure (Violino, 2020). To mitigate these risks, it is crucial to follow these five best practices:

1. Integrate edge computing into your security strategy without fail.
2. Implement a zero-trust policy and clearly understand what constitutes normal behaviour.
3. Prioritize security without any compromise when purchasing edge computing products.
4. Ensure that any vulnerabilities are addressed by prioritising patching.

An effective edge security strategy should include five elements: people, policy and procedures, process, product, and proof.

Furthermore, to ensure maximum security and protection for your organisation, Frank L. (2023) has highlighted the following best practices for edge computing:

1. Use automated and intelligent monitoring systems to detect security risks without fail.
2. Authenticate users with multi-factor authentication to ensure foolproof security.
3. Enforce security standards and integrate them into your network architecture without any exceptions.
4. Purchase hardware and software from companies prioritising security without compromise.

In Security Risk Management (SRM), detecting and assessing potential security threats that exploit weaknesses in edge computing components is critical. Once identified, security specifications and controls must be established to increase system security. Affia et al. (2023) provide a trade-off analysis process and security measure to rank threats according to their potential impact and available resources. To secure the system, prioritise controls and implement them.

REFERENCES

- Industry Outlook Report (2024). *Edge Computing Market Challenges (2023-2030)*. [online] Available at: https://www.linkedin.com/pulse/edge-computing-market-challenges-2023-2030/ [Accessed 4 Mar. 2024].

- Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5), pp.637–646. doi:https://doi.org/10.1109/jiot.2016.2579198.

- Zeyu, H., Geming, X., Zhaohang, W. and Sen, Y. (2020). *Survey on Edge Computing Security*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICBAIE49996.2020.00027.

- Dey, A. (2020). *A Primer on Edge Computing*. [online] DataSeries. Available at: https://medium.com/dataseries/a-primer-on-edge-computing-3ef550c3d84e.

- Nolle, T. (2021). *Edge computing security risks and how to overcome them*. [online] IoT Agenda. Available at: https://www.techtarget.com/iotagenda/tip/Edge-computing-security-risks-and-how-to-overcome-them.

- AppViewX. (N.D.). *Edge Security* | *Components of Edge Security* | *Edge computing*. [online] Available at: https://appviewx.com/education-center/edge-security/ [Accessed 5 Mar. 2024].

- Jones, C. (2022). *What Exactly Does 'Edge Security' Mean in Cybersecurity?* [online] Red River | Technology Decisions Aren't Black and White. Think Red. Available at: https://redriver.com/security/edge-security.

- Bigelow, S.J. (2021). *What Is Edge Computing? Everything You Need to Know*. [online] Techtarget. Available at: https://www.techtarget.com/searchdatacenter/definition/edge-computing.

- Rauch, S. (2024). *Edge Computing Security Risk And Challenges in 2021*. [online] Available at: https://www.simplilearn.com/edge-computing-security-risk-and-challenges-article.

- Violino, B. (2020). *5 best practices for securing the edge*. [online] Available at: https://www.csoonline.com/article/569757/5-best-practices-for-securing-the-edge.html [Accessed 5 Mar. 2024].

- Frank L. (2023). *Edge Computing Security: Risks, Considerations, and Best Practices*. [online] Available at: https://getstream.io/blog/edge-computing-security/.

- Affia, A.-A.O., Nolte, A. & Matulevičius, R. (2023). IoT Security Risk Management: A Framework and Teaching Approach. *Informatics in education*. doi:https://doi.org/10.15388/infedu.2023.30.

University
of Essex