Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

#BN-39-The role of AI-Feb2021

PRIVACY, FAIRNESS, AND SECURITY: AI AND EDGE COMPUTING

Authors: Reza Bahrevar[1] and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

MINDS

MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy NET Nexus of Emerging Technologies

SUMMARY

- It is critical to investigate the topics of security, privacy, and fairness of AI systems with regard to edge computing. Edge computing that at times is referred to as fog computing, is regarded as a complement to the current cloud computing.
- The prevalence of distributed data centers implies that data computing will be closer to the end-user or the “edge”. Our goal is to investigate risks and challenges as they are related to this development and study their effects on considerations such as privacy and trust with regards to AI systems.
- It is important to compare advantages and disadvantages of edge computing with respect to centralized information processing.
- Edge computing or fog computing is an emerging technology for distributed computing (as opposed to a centralized processing center) through multiple near end-user data centers, which requires special attention to minimize the after-effects such as legal and security considerations.
- Some of the issues that are of significant importance to investigate as the following: What are the privacy, security, and transparency issues related to edge computing that would impact and affect clients and users that are utilizing the AI systems? What are the possible and desirable approaches that can help us overcome these issues?

CONTEXT

- Currently, a few companies such as Google and Amazon manage major data centers for today's information distribution, which implies that given the centralized nature of information distribution centers, data travels through many routers.
- With the exponential growth of AI systems, and push for prevalence of smart technologies such as autonomous transportation systems, these companies may not be able to efficiently fulfill their duties and responsibilities. Issues such as lag in information transfer may impede technologies that need high-speed delivery of information [1].
- Therefore, key industry and academic stakeholders are pushing toward edge cloud computing, which are distributed data centers that make the processing and computing closer to the smart devices and systems. Consequently, every smart technology that uses an AI-based system will also be affected by this change [1, 2].
- Advantages of AI systems are as follows: large distance data transmission jeopardizes the security of AI systems and IoT devices, therefore the usage of edge cloud computing will minimize the possibility of cyberattacks and compromization on data enroute [3].
- Disadvantage of AI systems are as follows: given that the edge cloud computing is combination of technologies such as NFV (Network Function Virtualization), SDN (Software Defined Networking), and IoT (Internet of Things), security issues for these technologies still exist for the edge cloud computing [1, 2].

- Due to more experience and a more reliable security system, a centralized cloud owned by Google or Amazon might not suffer from the same issues that a local edge computing node will suffer. Also, edge clouds are more prone to physical attacks [2].
- The issue of concern is that when one looks at the AI policies that are merged with IoT, most of the current work are considering centralized data centers, while a futuristic vision should consider a segment of a small corporation can be potentially in charge of distributed data centers [3].
- To address privacy, security, and accountability in edge computing, one should invest in policies that are suitable for the new era [4,7].
- Issues with trust [4] are as follows: In cloud computing, data centers are associated with the cloud service providers such as Google and Amazon. However, internet service providers may also be interested in providing local computational servers for end users. Therefore, what are the desired characteristics of companies that users could trust their private info with?
- Another aspect of edge computing is authentication-based performance [2]. For example, a user allows an AI system to process its information, what fog nodes this AI system chooses to process the users' information? Should the user be informed about this? To what extent? What is the security level associated with these fog nodes?
- In edge computing, a node may process a given information by itself, or it may use nearby nodes to perform a distributed processing of information for the assigned task [8].
- In a situation where a client uses multiple computational nodes, the location and the task handled by the client should not be traceable by unauthorized third parties [9]. This is referred to as traceable effects.
- What directions should our policies aim and be focused on so that one can negate the traceable effects?
- A client can enable a fog node to process its task. However, the client may not be aware of all the sub-nodes that cooperate with the given main node. Therefore, how can one act in the interest of clients [9].
- Client identity is also part of the traceable effects. Stored client information must be regulated in order to avoid identification of the user by adversaries [9, 10, 11].

CONSIDERATIONS

- Quebec AI established a steering committee through the University of Montreal in order to promote mathematical literacy and responsible AI among AI students and deliver specialized AI trainees to the industry [1]. However, a responsible AI has received less attention since the concept may seem more dubious.
- For resolving issues with trust, one possibility is reputation-based trust models [2, 6]. One needs to also consider the possibility of insider attacks [1, 2]. Issues with security, privacy, and fairness regarding the decision making of fog based autonomous vehicles [5].

- Note that neither fog nodes nor service providers should be fully trusted [5]. Finally, issues such as usage privacy, location privacy, and data privacy [2, 4] are of importance to policy makers.
- Further investigation on cooperation by industry and academia and utilization and implementation of existing technologies for tackling the security concerns such as cyber and cyber-physical attacks [17, 18] will be required.
- The utilization of identity obfuscation to respect the rights of clients by remaining anonymous while performing a task [14, 9].
- A client identity should be defined in a manner similar to how personal identity is defined [12].
- Identification of clients should be avoided by associating off-line dummy tasks to the edge nodes [9].

NEXT STEPS

- When a user is utilizing an AI system, she/he must be informed of what type of cloud servers are used for processing the information, and the level of security standards corresponding to the distributed data centers should be transparent to the public.
- For example, when an autonomous car company is utilizing an AI technology, it should be encouraged to obtain at least a grade-based security certification from trustable industry-standard providers, which ensures the customers that their utilized data servers are robust against attacks such as jamming attacks and the man in the middle attacks [2,5].
- By establishing relevant regulations, one should ensure that the server allocation of a company in terms of cost, security, and data gathering is properly determined with regards to different regions.
- Information that is stored by data servers on a user should be transparent to them. Users should have the right to be forgotten, since the location privacy and data privacy may become more prone to being compromised due to the edge cloud technology.
- Traceable effects imply when one is dealing with applications for systems such as UAVs and autonomous vehicles to examine the tasks that are performed by the clients, the adversaries may be able to identify information about their routes and tasks. Furthermore, the clients would be more prone to adversary attacks given their unique identity, attackers may gain more time to monitor them.
- Elevating the problem with traceable effect needs establishing practices such as identity protection in a manner that a user has the right to utilize the edge node through an alternative assigned random identity [9, 14].
- Due to utilization of wireless communications by the fog nodes, network security is an important aspect of operations, especially when one is concerned with dealing with small businesses [9]. Adversaries can introduce attacks such as a jamming attacks and man in the

middle attacks to disrupt, cause financial, mental, or physical damage to clients working with edge nodes.

- Use of intrusion detection systems must be mandated for improving security of the fog nodes. Methods for encountering DoS attacks, insider attacks, single targets, or distributed attacks must be encouraged to be implemented and practiced by companies [9, 15].
- A client should be able to request for its information what is shared by an authorized node to third parties as well as to sub-nodes.
- A client may not have adequate time to monitor all the shared data to third-party nodes that cooperate with a specific node. It is the policymaker's responsibility to mandate requirements and regulations that would supervise distributed computing of certified fog nodes with non-certified ones.
- Policymakers should specify a supervisory element that ensures the verifiable and trustable computing for distributed computing by authorized fog nodes, e.g. using computational verification methods by the main fog node [13, 16].
- Client's confidential information can be classified as direct or indirect [12], implying that they can either directly point at a client or through an AI search system can trace a client with processing a set of identifier information. Companies in charge of fog nodes should avoid storing sensitive data that would put the privacy and security of their clients at risk [9].

REFERENCES

[1] Pan, J. and McElhannon, J., 2017. Future edge cloud and edge computing for internet of things applications. *IEEE Internet of Things Journal*, *5*(1), pp.439-449.

[2] Yi, S., Qin, Z. and Li, Q., 2015, August. Security and privacy issues of fog computing: A survey. In *International conference on wireless algorithms, systems, and applications* (pp. 685-695). Springer, Cham.

[3] Stoica, I., Song, D., Popa, R.A., Patterson, D., Mahoney, M.W., Katz, R., Joseph, A.D., Jordan, M., Hellerstein, J.M., Gonzalez, J.E. and Goldberg, K., 2017. A berkeley view of systems challenges for ai. *arXiv preprint arXiv:1712.05855*.

[4] Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X., 2017. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), pp.34-42.

[5] Ni, J., Zhang, A., Lin, X. and Shen, X.S., 2017. Security, privacy, and fairness in fog-based vehicular crowdsensing. *IEEE Communications Magazine*, *55*(6), pp.146-152.

[6] Jøsang, A., Ismail, R. and Boyd, C., 2007. A survey of trust and reputation systems for online service provision. *Decision support systems*, *43*(2), pp.618-644.

[7] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V., 2017. Security and privacy in fog computing: Challenges. *IEEE Access*, *5*, pp.19293-19304.

[8] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V., 2017. Security and privacy in fog computing: Challenges. *IEEE Access*, *5*, pp.19293-19304.

[9] S. Yi, Z. Qin, and Q. Li, “Security and privacy issues of fog computing: A survey,” pp. 685–695, 2015. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” pp. 44–55,
2000.

[10] Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X., 2017. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), pp.34-42.

[11] Ni, J., Zhang, A., Lin, X. and Shen, X.S., 2017. Security, privacy, and fairness in fog-based vehicular crowdsensing. *IEEE Communications Magazine*, *55*(6), pp.146-152. P.

[12] Nguyen and L. Solomon, “Consumer data and the digital economy: Emerging issues in data collection, use and sharing,” 2018

[13] R. Gennaro, C. Gentry, and B. Parno, “Non-interactive verifiable computing: Outsourcing computation to untrusted workers,” pp. 465–482, 2010.

[14] F. Bonchi, A. Gionis, and T. Tassa, “Identity obfuscation in graphs through the information theoretic lens,” Information Sciences, vol. 275, pp. 232–256, 2014.

[15] S. S. G. G. CloudWatcher, “Network security monitoring using OpenFlow in dynamic cloud networks,” Proc.
NPSec12, 2012.

[16] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, “Talking to strangers: Authentication in ad-hoc wireless networks.” 2002.

[17] Loukas, G., 2015. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.

[18] Uma, M. and Padmavathi, G., 2013. A Survey on Various Cyber Attacks and their Classification. *IJ Network Security*, *15*(5), pp.390-396.