BRIEFING NOTES

#BN-43-The role of AI-Feb2021

FUTURE OF PRIVACY AND SECURITY ISSUES OF AI SYSTEMS UNDER THE BRANCH OF FOG 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

SUMMARY

- Fog computing is the enabler of cloud and edge computing (a term sometimes used interchangeably for fog computing). It is the distributed processing capability that is provided by local data centers close to the edge device, that will form the next generation of distributed cloud computational services.
- Transparency, ethics, and fairness of AI systems issues with regards to the Internet-of-Things (IoT) are actually entangled with thousands of cloud servers that are operated by big companies such as Google and Amazon. Therefore, with the prevalence of edge-cloud computing the number of cloud servers will be significantly increased many folds.
- Our goal is to investigate how these issues would translate into the new era of computational technologies and what are the associated social and policy implications of these advances and developments.

CONTEXT

- Ethics, privacy, security, and fairness are said to be the characteristics of Ethical design of AI systems [1]. It leads to an AI system that is transparent, secure, and self-explanatory, such that it can aid with legal problems as well as ethical problems that result from a decision that is made by an AI system.
- Where cloud servers and IoT expand and become further distributed, the potential capabilities for developing a more powerful AI system increase. In other words, with capabilities that are offered by the fog computing, training capacities, speed, and processing capabilities of the AI systems also do get enhanced.
- However, that begs the question as to how can one monitor and promote ethical and transparent AI in light of new challenges such as fog computing? Our focus here will be on a specific issue related to the facial recognition systems but it will subsequently be expanded to other AI systems.
- A recent demonstration of integration of 5G and Edge Cloud has shown how machine learning models on autonomous drones, can be used to recognize humans. This strives towards a future where machines and humans can work safely together.
- Integration of 5G and Edge Cloud can also be valuable in situations where a stakeholder must make immediate decisions based on the data that are being processed [2].
- In [2], a solution to respond to health crisis of the COVID-19 pandemic is provided. This study provides a framework based on AI systems and integration of 5G and edge-cloud computing that enables mass surveillance to monitor social distancing, control mask-wearing, and reading body temperatures of people.
- The above referenced AI system will analyze features such as facial expressions, mask detection, and body temperature [2].
- Such experimentations can cause a problem in terms of ethics, invasion of privacy, and also can be used by adversaries to target individuals for their malicious purposes. How

can one then become proactive to manage and tackle both privacy and security issues and challenges?

CONSIDERATIONS

- The integration of AI and edge-cloud processing will massively contribute to enhancing facial recognition technology and may be able to increase the public health security [2]. It may also result in an increased invasion of individual privacy concerns by these systems.
- These technologies will enhance deep learning in such a manner that it will provide access to faster and more broad set of data for training purposes. Therefore, the resulting AI systems become more capable and enhanced.
- Nevertheless, the problems and challenges with explainability of the AI systems still are prevalent [3].
- Challenges with adversaries where attackers may be able to access the wireless communication links between fog node and the edge device are considered quote serious. For example, an adversary accessing an edge-based facial recognition system would represent a great threat to the privacy and security of the citizens [4,5].

NEXT STEPS

- There should be regulations that would limit and monitor authorization for the utilization of AI technologies by various companies and stakeholders.
- For example, integrating edge clouds and surveillance systems may be able to provide the capability for a company to constantly monitor people in a neighborhood. Therefore, purposes and justifications for access of the AI systems to fog nodes should be made specific and very clear.
- Access to edge-based servers with certain AI systems must be limited to trusted companies and stakeholders that go through an evaluation and review process. Otherwise, with installation of some security cameras and a facial recognition system, any company may be able to establish its own surveillance system.
- An evaluation process should consist of security checks, purpose identification, relevancy, security, robustness, and necessity. If it is not a necessary requirement for a company's or a stakeholder's AI system to access edge-cloud servers then the security risk might overtake the usefulness of granting these accesses.
- Collaborating companies and stakeholders that are involved with a client that utilize an AI system such as edge-cloud based facial recognition system should also be transparent and identifiable. This will provide the capability of holding them accountable to their decisions.

REFERENCES

[1] D. Doran, S. Schulz, and T. R. Besold, “What does explainable ai really mean? a new conceptualization of perspectives,” arXiv preprint arXiv:1710.00794, 2017.

[2] Hossain, M.S., Muhammad, G. and Guizani, N., 2020. Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-I9 Like Pandemics. *IEEE Network*, *34*(4), pp.126-132.

[3] A. Adadi and M. Berrada, “Peeking inside the black-box: A survey on explainable artificial intelligence (xai),” IEEE Access, vol. 6, pp. 52 138–52 160, 2018.

[4] Hossain, M.S. and Muhammad, G., 2019. Emotion recognition using secure edge and cloud computing. *Information Sciences*, *504*, pp.589-601.

[5] Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y. and Yao, X., 2017. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal*, *4*(5), pp.1143-1155.