Scopus

## Documents

Sheikh, A.M., Islam, M.R., Habaebi, M.H., Zabidi, S.A., Najeeb, A.R.B., Basahel, A.

**Machine Learning (ML) assisted Edge security framework on FPGAs**
(2023) *Proceedings of the 9th International Conference on Computer and Communication Engineering, ICCCE 2023*, pp. 155-160.

**DOI:** 10.1109/ICCCE58854.2023.10246095

International Islamic University Malaysia, Department of Electrical and Computer Engineering, Kuala Lumpur, Malaysia

**Abstract**
Edge computing (EC) is an act of bringing computational and storage capability near data sources. It helps to reduce response times and bandwidth requirements. However, the rapid proliferation of edge devices has expanded the attack surface and opportunity for adversaries to penetrate corporate networks. The limited computational abilities of edge devices and the heterogeneous nature of communication protocols further increase the security challenges of EC. Also, the trustworthiness of hardware devices is challenged due to security and privacy threats like trojan insertion, IP cloning, and hardware counterfeits. The application of Machine Language (ML) models in the edge computing paradigm creates a distributed intelligence architecture. Also, Field Programmable Gate Arrays (FPGAs) can exploit Physical Unclonable Functions (PUFs) characteristics to generate and store authentication keys. The PUF structure deployed with ML models in the edge layer can learn its complex input-output mapping from the Challenge and Response pairs (CRPs) to identify the suspicious and unknown responses. This article discusses the security and privacy issues in various layers of the EC architecture and proposes intrusion detection systems through the integration of FPGA-based edge sever and ML models. A PUF-assisted ML framework of the intrusion detection system is proposed to authenticate and detect potential attacks on the network. © 2023 IEEE.

**Author Keywords**
CRPs; Edge computing; FPGAs; Machine Language; PUFs

**Index Keywords**
Authentication, Chromium compounds, Computer architecture, Cryptography, Edge computing, Field programmable gate arrays (FPGA), Intrusion detection, Machine learning, Malware, Network architecture, Network security; Challenge and response, Challenge and response pair, Edge computing, Field programmable gate array, Field programmables, Intrusion Detection Systems, Machine languages, Machine learning models, Machine-learning, Programmable gate array; Hardware security

**References**

- Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., Rana, O.
  **Fog computing for the internet of things: A survey**
  (2019) *Acm Transactions on Internet Technology (TOIT)*, 19 (2), pp. 1-41.
- Khan, W.Z., Ahmed, E., Hakak, S., Yaqoob, I., Ahmed, A.
  **Edge computing: A survey**
  (2019) *Future Generation Computer Systems*, 97, pp. 219-235.
- Roman, R., Lopez, J., Mambo, M.
  **Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges**
  (2018) *Future Generation Computer Systems*, 78, pp. 680-698.
- Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., Yang, X.
  **A survey on the edge computing for the internet of things**
  (2017) *Ieee Access*, 6, pp. 6900-6919.
- Howarth, J.
  (2023) *80+ Amazing Iot Statistics (2023-2030)*,
  May, 17 2023
- Ni, J., Lin, X., Shen, X.S.
  **Toward edge-assisted internet of things: From security and efficiency perspectives**

(2019) *Ieee Network*, 33 (2), pp. 50-57.

- Kalnoskas, A.
(2022) *Edge Computing Security: Challenges and Techniques*,
May, 11 2023

- Kimachia, K.
(2022) *The Risks of Edge Computing*,
May, 13 2023

- Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., Materne, S.
**Cyber risk and cybersecurity: A systematic review of data availability**
(2022) *The Geneva Papers on Risk and Insurance-Issues and Practice*, 47 (3), pp. 698-736.

- Sheehan, B., Murphy, F., Kia, A.N., Kiely, R.
**A quantitative bowtie cyber risk classification and assessment framework**
(2021) *Journal of Risk Research*, 24 (12), pp. 1619-1638.

- (2023) *Edge Computing Security Risks and Solutions*,
element14, May, 14 2023

- Hassan, M.M., Hassan, M.R., De Albuquerque, V.H.C., Pedrycz, W.
(2022) *Soft Computing for Intelligent Edge Computing*,

- Sittón-Candanedo, I., Alonso, R.S., Corchado, J.M., Rodríguez-González, S., Casado-Vara, R.
**A review of edge computing reference architectures and a new global edge proposal**
(2019) *Future Generation Computer Systems*, 99, pp. 278-294.

- Consortium, E.C.
*Edge Computing Reference Architecture 2.0. 2017*,

- Zhang, J., Chen, B., Zhao, Y., Cheng, X., Hu, F.
**Data security and privacy-preserving in edge computing paradigm: Survey and open issues**
(2018) *Ieee Access*, 6, pp. 18209-18237.

- Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J., Hamdi, M.
**A survey on security and privacy issues in edge-computingassisted internet of things**
(2020) *Ieee Internet of Things Journal*, 8 (6), pp. 4004-4022.

- Gao, L., Luan, T.H., Gu, B., Qu, Y., Xiang, Y.
**Privacy issues in edge computing**
(2021) *Privacy-Preserving in Edge Computing*, pp. 15-34.
Springer

- Yahuza, M., Idris, M.Y.I.B., Wahab, A.W.B.A., Ho, A.T., Khan, S., Musa, S.N.B., Taha, A.Z.B.
**Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities**
(2020) *Ieee Access*, 8, pp. 76541-76567.

- Cao, K., Liu, Y., Meng, G., Sun, Q.
**An overview on edge computing research**
(2020) *Ieee Access*, 8, pp. 85714-85728.

- Yahuza, M., Idris, M.Y.I.B., Wahab, A.W.B.A., Ho, A.T.S., Khan, S., Musa, S.N.B., Taha, A.Z.B.
**Systematic review on security and privacy requirements in edge computing: State**

**of the art and future research opportunities**
(2020) *Ieee Access*, 8, pp. 76541-76567.

- Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A.
**Internet of things: Security and solutions survey**
(2022) *Sensors*, 22 (19), p. 7433.

- Walters, J.P., Liang, Z., Shi, W., Chaudhary, V.
**Wireless sensor network security: A survey**
(2007) *Security in Distributed, Grid, Mobile, and Pervasive Computing*, pp. 367-409.
Auerbach Publications

- Carracedo, J.M., Milliken, M., Chouhan, P.K., Scotney, B., Lin, Z., Sajjad, A., Shackleton, M.
**Cryptography for security in iot**
(2018) *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pp. 23-30.

- Misra, S.
(2015) *Rethinking Security of the Ultimate Panopticon: The Internet of Things*,
McGill University Canada

- (2023) *Battling Cyber Threats: How to Overcome the Challenges in Edge Computing*,
E. team, May 22 2023

- Shamsoshoara, A., Korenda, A., Afghah, F., Zeadally, S.
**A survey on physical unclonable function (puf)-based security solutions for internet of things**
(2020) *Computer Networks*, 183, p. 107593.

- Gassend, B., Clarke, D., Van Dijk, M., Devadas, S.
**Silicon physical random functions**
(2002) *Proceedings of the 9th Acm Conference on Computer and Communications Security*, pp. 148-160.

- Cui, A., Chang, C.-H., Zhou, W., Zheng, Y.
**A new puf based lock and key solution for secure in-field testing of cryptographic chips**
(2021) *Ieee Transactions on Emerging Topics in Computing*, 9 (2), pp. 1095-1105.

- Goutsos, K.
(2019) *Puf-based Authority Device Scheme*,
Newcastle University

- Michael, J.B.
**Security and privacy for edge artificial intelligence**
(2021) *Ieee Security & Privacy*, 19 (4), pp. 4-7.

- Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., Zomaya, A.Y.
**Edge intelligence: The confluence of edge computing and artificial intelligence**
(2020) *Ieee Internet of Things Journal*, 7 (8), pp. 7457-7469.

- El Mrabet, M.A., El Makkaoui, K., Faize, A.
**Supervised machine learning: A survey**
(2021) *2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1-10.

- Manan, A.
**Implementation of image processing algorithm on fpga**
(2006) *Akgec Journal of Technology*, 2 (1), pp. 25-28.

- Ahmad, J., Jervis, M., Venkata, R.
*IntelR Fpgas and Socs with IntelR Fpga Ai Suite and Openvino Toolkit Drive Embedded/edge Ai/machine Learning Applications*,

- Malishev, D.
(2020) *Machine Learning Becomes Easier and Faster with Openvino*,
May 27, 2023

- Drake, K.
(2022) *Ai Inference with IntelR Fpga Ai Suite*,
May 28, 2023


**Correspondence Address**
Islam M.R.; International Islamic University Malaysia, Malaysia; email: rafiq@iium.edu.my

**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Conference name:** 9th International Conference on Computer and Communication Engineering, ICCCE 2023
**Conference date:** 15 August 2023 through 16 August 2023
**Conference code:** 192690

**ISBN:** 9798350325218
**Language of Original Document:** English
**Abbreviated Source Title:** Proc. Int. Conf. Comput. Commun. Eng., ICCCE
2-s2.0-85173721244
**Document Type:** Conference Paper
**Publication Stage:** Final
**Source:** Scopus