Threats and Difficulties During Training and Inference in Machine Learning-Based Systems

Dr. Anumaan

[1]Senior IEEE Member
[1],Atlanta, USA
[1] anumaan134@gmail.com*
* corresponding author

ARTICLE INFO

Article History:
Received January 1, 2018
Revised March 31, 2019
Accepted July 12, 2019

Keywords:
IoT , ML, temperature ,smart building

Correspondence:
E-mail: anumaan134@gmail.com

ABSTRACT

The exponential rise in the interdependence of the cyber and physical worlds generates a massive volume of data that must be efficiently handled and stored. As a result, computing paradigms are shifting toward machine learning (ML)-based systems due to their capacity to analyse massive amounts of data rapidly and reliably. Although ML-based solutions solve the efficient computing needs of big data, they introduce security risks into the systems that traditional monitoring-based security measures cannot address. As a result, this article begins with a brief introduction of major security concerns in machine learning, as well as their corresponding threat models.

References

[1] Albarran AB (2002) Media Economics: Understanding Markets, Industries and Concepts, 2nd ed. Iowa: Iowa State Press.

[2] Albarran AB (2010) The Media Economy. New York: Routledge.

[3] Pawan Whig and S. N. Ahmad, Performance analysis and frequency Compensation Technique for Low Power Water Quality Monitoring Device Using ISFET Sensor. International Journal of Mobile and Adhoc Network (IJM AN) (May 2011) ISSN (ONLINE): 2231-6825 ,ISSN(PRINT):2249-202X,Volume 1, pp:80-85.

[4] Pawan Whig and S. N. Ahmad, On the Performance of ISFET-based Device for Water Quality Monitoring. Int'l J. of Communications, Network and System Sciences (IJCNS) (Nov 2011) ISSN (ONLINE): 1913-3715, ISSN (PRINT):1913-3723, Vol 4 pp: 709-719.

[5] Pawan Whig and S. N. Ahmad, DVCC based Readout Circuitry for Water Quality Monitoring System, International Journal of Computer Applications (IJCA) ISBN : 973-93-80869-71-6,Volume 49 pp: 1-7.

[6] Pawan Whig and S. N. Ahmad, A CMOS Integrated CC-ISFET Device for Water Quality Monitoring, International Journal of Computer Science Issues ,Volume 9, Issue 4, July 2012, ISSN (online): 1694-0814 pp: 365-371.

[7] Pawan Whig and S. N. Ahmad, Performance Analysis of Various Readout Circuits for Monitoring Quality of Water Using Analog Integrated Circuits, International Journal of Intelligent Systems and Applications (IJISA) ISSN: 2074-904X (Print), ISSN: 2074-9058 (Online) Volume 4, No.11, October 2012 pp:91-98.

[8] Pawan Whig and S. N. Ahmad, A Novel Pseudo PMOS Integrated CC-ISFET device for water quality monitoring, Journal of integrated circuit and system published 2013

Volume 8, No.2, October 2013 pp:1-6. ISSN, 1807-1953 (Scopus).

[9] Pawan Whig and S. N. Ahmad, "Simulation of Linear Dynamic Macro Model of Photo Catalytic Sensor in SPICE" Compel, the international journal of computation and mathematics in electrical and electronic engineering, Vol. 33 No. 1/2, 2014. ISSN: 0332-1649 (SCI, ISI index)

[10] Vaibhav Bhatia and Pawan Whig" A secured dual tune multi frequency based smart elevator control system," International journal of research in engineering and advanced technology",Vol. 4 Issue 1 , 2013. ISSN (Online): 2319-1163

[11] Pawan Whig and S. N. Ahmad, A Novel Pseudo NMOS Integrated ISFET device for water quality monitoring, Active and Passive Components Hindawi article i.d 258970. Vol. 1 Issue 1, 2013(Scopus). ISSN 0882-7516

[12] Arrese A and Albarran AB (2003) Time and media markets: Summary and research agenda. In: Albarran AB and Arrese A (eds) Time and Media Markets. London: Lawrence Erlbaum Associates Publishers, pp. 161–171.

[13] Becker G (1965) A theory of the allocation of time. Economic Journal 75(3): 493–517.

[14] Vaibhav Bhatia and Pawan Whig, "Modeling and Simulation of Electrical Load Control System Using RF Technology, International Journal of multidisplinary science and engineering",2013,Vol. 4 No.2, pp 44-47 ISSN 2045-7057.

[15] Pawan Whig and S. N. Ahmad, Development of Economical ASIC For PCS For Water Quality Monitoring ,Journal of Circuit System and Computers, Vol. 23, No. 6 , 2014, pp: 1-13. ISSN: 0218-1266 (SCI, ISI index)

[16] Pawan Whig and S. N Ahmad, "CMOS Integrated VDBA-ISFET Device for Water Quality Monitoring, International journal of intelligent engineering and systems, accepted for publication 2014,Vol.7, No.1,2014. (Scopus) ISSN: 2185-3118

[17] Pawan Whig and Vaibhav Bhatia," Performance Analysis of Multi-Functional Bot System Design Using Microcontroller" International Journal of Intelligent Systems and Applications,2014 ,02 pp 69-75.ISSN No: 2074-9058

[18] Pawan Whig and S. N. Ahmad, "Development of Low Power Dynamic Threshold PCS System", Journal of Electrical and Electronic Systems,2014, Vol. 3, Issue3, pp. 1-6. ISSN No:2332-0796

[19] Pawan Whig and S. N. Ahmad, "Novel FGMOS Based PCS Device for Low Power Applications ",Photonic Sensor(Springer), 2015,Vol.5,Issue 2, pp 1-5.(SCI, ISI Index) ISSN No: 1674-9251