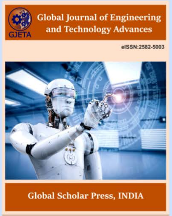
Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/


Global Journal of Engineering and Technology Advances
GJETA
eISSN:2582-5003
Global Scholar Press, INDIA

(Review Article)

Check for updates

Artificial Intelligence vulnerability prevention for closed-loop control system

Whyte Asukwo Akpan [1, *], Chikodili Martha Orazulume [2], Godwin Daniel Essien [3], Ifeoma Ugochi Ohaeri [4], Nsikakabasi Nsedu Inyang [5] and Peter Okechukwu Chikelu [6]

[1] *Department of Mechanical Engineering, School of Engineering and Engineering Technology, Federal University of Technology, Ikot Abasi,Akwa Ibom State, Nigeria.*
[2] *Department of Electrical and Electronics Engineering, Faculty of Engineering, TopFaith University Mkpatak, Akwa Ibom State, Nigeria.*
[3] *Department of Computer Engineering, Faculty of Engineering, TopFaith University Mkpatak, Akwa Ibom State, Nigeria.*
[4] *Department of Computing, Faculty of Compuing and Applied Sciences,TopFaith University Mkpatak, Akwa Ibom State, Nigeria.*
[5] *Department of Electrical and Electronics Engineering, School of Engineering and Engineering, Technology, Ikot Abasi, Akwa Ibom State, Nigeria.*
[6] *Department of Mechanical Engineering, Faculty of Engineering,Nnamdi Azikiwe University, Awka,Anambra State,Nigeria.*

Global Journal of Engineering and Technology Advances, 2025, 23(02), 025-030

Publication history: Received on 19 March 2025; revised on 01 May 2025; accepted on 03 May 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.23.2.0121

Abstract

Artificial intelligence has created much impact in so many scientific and engineering fields because of its ease, versatility and capability to be adopted to suit different applications. Concerns have arisen for online applications which can be exposed to cyber threats. The various benefits expected to be derived from online application of Artificial intelligence are so huge that these threats cannot be allowed to form a stumbling block to its utilization. Just like many technologies that may usually be faced with some initial challenges in its development and applications, priority should be on how to identify such possible cyber threats and then build up necessary cyber security measures to prevent these threats. It is in this wisdom that this research is focused to offer solutions that will accelerate its safe applications on closed-loop control systems environment. Prevention to AI based control loop vulnerability can be achieved by building strong security controls and zero trust procedures to prevent hackers, intruders, cyber-criminals and blind-cyber wanderers from penetrating into the system either internally or externally. With such protocols which is possible and achievable the objective of application of AI in online closed -loop control system is practicable and will improve the efficiency of the overall system.

Keywords: Closed-Loop; Control System; Vulnerability; Cyber-Attack; Security; AI

1. Introduction

Artificial Intelligence (AI) is a science concerned with the design of intelligent computer systems, exhibiting the characteristics associated with intelligence in human behavior [1]. AI is to understand model and implement theories of intelligence in this functions to design intelligent systems. Artificial intelligence involves developing PC's solution, using computing techniques to make decisions [2].

There are other main categories into which artificial intelligence care categorized. These are: expert system, robotics, fuzzy-logic, neural networks: supervised learning, unsupervised learning, reinforced learning and Hebbian learning, machine learning, among others.

[*] Corresponding author: Whyte Asukwo Akpan

Expert System is a computer-based programme created to simulate human judgment. It is a computer programme that applies artificial intelligence methods to resolve problems in a particular field that calls for human knowledge [3]. Figure 1 shows the components of expert system.

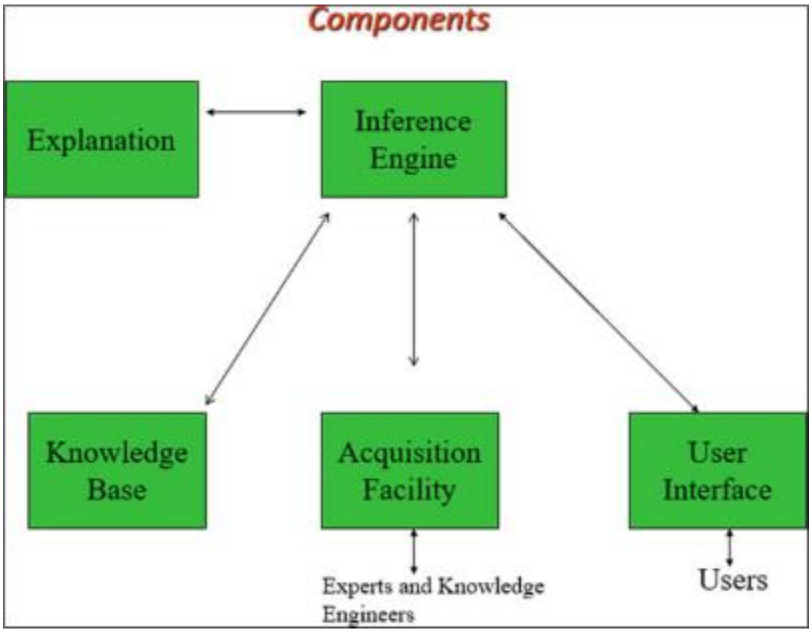


Figure 1 Components of an Expert system [3]

Robotics is an area that allows repetitive work that should be done by human being to be over taken be robots [3], [4], [5].

Fuzzy Logic is applied to problems that are partly true, in this case the truth takes a probabilistic outlook, between the maximum values for it being true and false [6]. Figure 2 is the representation of Boolean and Fuzzy logic.

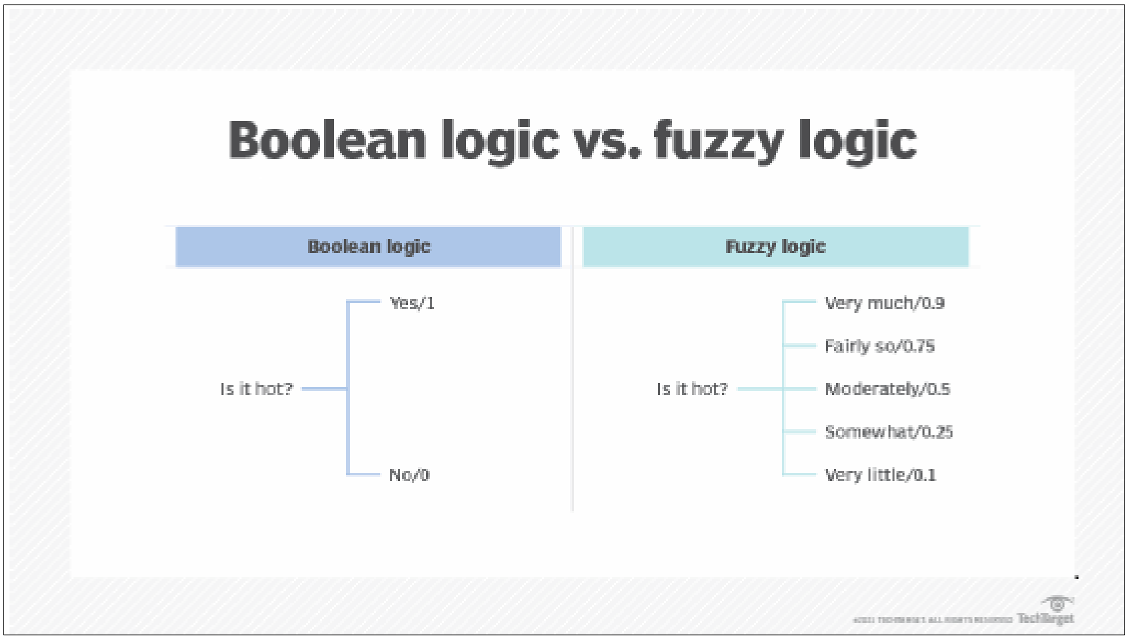


Figure 2 Figure showing the difference between Boolean logic and Fuzzy logic [6]]

Neural Networks is synonymous with network of neurons that learns and performs tasks independently through the use of deep learning. It can be-supervised, unsupervised, reinforced, and Hebbian learning.

In supervised learning case every input that is used to train the network is associated with an output pattern, which is the desired output [7]. However, in unsupervised Learning, the target output is not presented to the network. No teacher is available to present the expected pattern [7].

In reinforced learning, the teacher though present, does not present the expected answer but only indicates if the computed output is correct or incorrect. In Hebbian learning, the learnin is inspired by biology, relying on correlative weight adjustment.

The neural network may be single layer feed forward, multilayer feed forward or recurrent networks.

Machine Learning allows a computer or machine to process, analyze, and interpret data in order to use that data to solve problems in the real world.

Artificial intelligence and machine learning are revolutionizing signal processing in control systems. The integration of AI algorithms enhances the ability of control systems to process and interpret complex signals more efficiently, leading to smarter automation and predictive maintenance capabilities and applications of signal processing in control systems [8]. [9].

AI functions through the learning process, where named-information are properly analyzed to learn and extract the features in the information, so as to make projections into the future.

In a world like ours with emerging technologies like AI and the need to introduce Artificial intelligence into manufacturing and industrial processes, there is a need to develop and implement specific procedures for data shared by the control system and the Artificial intelligence. It is crucial to identify the possible attacks that may be prevalent and also build necessary structures to prevent their incursions into the overall system loop.

The following are the possible vulnerability attacks: cyber-attacks, adversarial attacks, data manipulation and data poisoning, model thefts, model supply chain attack and surveillance and privacy. There should be proprietary system to handle sophisticated, targeted and attacks that are difficult to detect. This should be able to discover vulnerabilities, and prevent phishing campaigns that mimics human behavior capable of bypassing traditional security systems. The system should be capable to scale adversarial attacks, which are targeted at AI models. They do this by manipulating data to impede the system into making wrong decisions and producing harmful outputs. They navigate model's algorithm by inputting parameters, strings and figures that will produce undesired results. This can adversely affect the control system module. They can manipulate and poison the training data used for the model by inserting false or misleading information into the dataset, leading to flawed outcomes. This type of attack targets the foundation of AI systems-their learning data, corrupting their decision-making capabilities. This is reported to have serious impact on users of AI models in high-impact fields like healthcare, finance, and automotive [10].

Model theft occurs where attackers are concerned to replicate and steal proprietary AI models. This allows them to understand and exploit the model's weaknesses, as well as disable security apparatus and endangering the system. Extracting an AI model requires obtaining the software or source code via unintended exposure, organizational leakage, or by penetrating and harvesting information from protected computer systems [10].

Attacks can evolve as 'model supply chain attacks' that targets the components involved in the development and deployment of AI models. By doing this, they compromise the integrity of AI systems by injecting malicious code or data into third-party libraries, training datasets, or during the model transfer process [10]. This can open ways for security breaches, including unauthorized access to sensitive information or manipulation of model behavior. The system should be able to prevent surveillance and privacy concerns relating to the potential misuse of AI technology to monitor individuals or processes without their approval. AI systems, particularly those involving facial recognition and data analytics, are prone to such attacks be raising ethical and legal issues. The problem is compounded by the risk that data collected by AI may fall into the hands of cybercriminals or hostile state actors or destroyers capable of sabotaging a given system, organization or process [10].

To ensure AI robust security measures for closed-loop control system, the following measures are suggested:

- Ensuring data integrity and implementing stringent measures to authenticate the source and quality of data before using it to train AI models. In this case the data authentication should be from the closed-loop system and not floating or any other source. This includes conducting thorough checks for data source.

- Adopting rigorous validation techniques to help identify and address inaccuracies in datasets, protecting against data poisoning attacks that poise to skew AI decisions. Data handling practices should also prioritize privacy and compliance with regulatory standards, requiring encryption of sensitive information and adherence to data minimization principles [10].
- Limiting application permissions- This ensures that AI systems have only the necessary access rights to perform their functions. It minimizes the risk of unauthorized actions and reduces the damage from compromised AI applications or software. Least privilege technique should limit data used by AI to control element alone.
- Frequent audits of permission settings should be embedded to help identify and address unauthorized data penetration. Organizations need to establish a process for continuously monitoring and adjusting permissions in line with changing requirements.

Various training data is important for developing AI systems that are fair and effective across varied scenarios and populations. Different dataset reduces the risk of bias and errors in AI decisions, leading to fairness, and also reduces the risk of data poisoning and dataset manipulation. This requires collecting data from a wide range of sources and ensuring that it represents the right configuration of the system [10].

By putting to focus diversity in training data, organizations can promote the performance of AI models while reducing the risks associated with biased outcomes. Continuous evaluation of training data for diversity assists to identify gaps or biases that may emanates as AI systems evolve.

Continuous monitoring demands the constant surveillance of AI applications and infrastructure to uncover anomalies and potential issues in real time. By tracking key performance indicators, data distribution shifts, and model performance fluctuations, irregularities can easily be quickly identified that may indicate a security breach or malfunction of the system.

Incident response supports continuous monitoring by providing a structured way to tackle security incidents. This includes outlined procedures for isolating affected systems, analyzing the breach’s scope, and implementing remediation strategies and measures. A quick and coordinated incident response minimizes the impact of attacks, ensuring business continuity and protecting data integrity [10].

Practical Implication

AI inspired closed-loop control system has many benefits to harvest from if appropriate procedures and measures are put in place by scientists, engineers and other stakeholders in developing and applying suitable technologies to its implementation. The technology is not without challenges, that if not well applied can produce unprofitable results. Such challenges include cyber-attacks by intruders that can manipulate AI data and intrude and impede the information in the control system architecture. The manipulation has the potential of altering the set point or reference value with potential risk on the performance of the system. Pressure or temperature can increase beyond the fixed value or design limits, outputs of industrial processes will be affected and safety of both human and equipment not left out. The potentials and benefits of adopting and application of AI to closed-loop control systems are huge. Looking at the current and future benefits, there is need to develop robust security system to enhance its full-scale applications that will improve performance, increase productivity and efficiency of the system. These opportunities need to be explored progreesively to obtain its full potentials.

2. Background to the Problem

The operation of the internet system has been met with various challenges, among which include internet security. This is growing day by day. The attacks on the internet have multiple reasons and some may not be easily defined. Technologies are emerging on regular basis and control of the cyberspace is difficult. Technology is like air, which occupies empty space, even with tight regulations, the cyberspace is seriously under attacks. Most technologies in recent times are built on the internet, and others in future are expected to be so because of the ease and friendly atmosphere provided by the internet. One of such technologies is the Artificial intelligence which is revolutionizing the world today. Its application has been proposed for closed-loop control systems, to optimize the overall functions of the system. The concern now is the vulnerability to attacks by intruders that can affect industrial or manufacturing processes. Imagine an intruder manipulating the control configuration of a nuclear plant or furnace. Failure of such plants can lead to explosion leading to loss of life and property. There is a need to address such possible attacks and come out with measures that will enable a robust system to be built for AI inspired closed-loop control system.

3. AI-Based Closed-Loop System

[12] have proposed an AI Based closed-loop system model. According to [12] AI is introduced into at the output from the plant or process terminal and, data are taken to be processed and recorded. It is a link that is used to create and train the model on AI desired objective- the input value. After which, it is compared with the desired value and signal and sent to the control element to verify if there is a deviation from the desired value. If there exist any deviation, the information is used for actuation proportional to the error signal. In doing so, AI assist the controller in performing complementary function.

4. AI-Based Closed-Loop Signal Processing Path

According to [12], the signal should be conditioned in the transmission path before it is allowed entry into AI loop. It is a necessary and sufficient condition to enable the AI to act effectively. This condition will prevent other unnecessary activities like modulation, demodulation, filtering and complex mathematical transformations like Fourier series or Laplace transformation, which otherwise will make the entire process complex and increase the processing time[13].

5. Signal Path Vulnerability

The coupling of the AI unit to the control system has been proposed by [12]. With the huge advantage expected with this technology with closed-loop control system, it is essential to navigate the loop and identify possible routes where these attacks can emanate. From Figure 3, three points of linkage are identified (one from the controlled output, and each from error signal and control element point respectively). Protocols should be built to prevent only one way signal transmission from the AI unit to these three points. Cyber-security attacks on the control system unit can be easily be done through the AI unit, since it is linked to the internet. It is through such attacks that intruders can alter AI model, harm and distort the whole system. Once the intruders get access to the AI unit, they can thus penetrate and distort damage and cause failure of the control system and may alter the set point. Protocols should be built to disconnect the AI unit in such an attack to keep the integrity of the process intact. Such protocols may need an alarm and degree of severity. Depending on the criticality of the process, the degree of severity can be categorized as low, medium and high and help the engineer in decisions making.

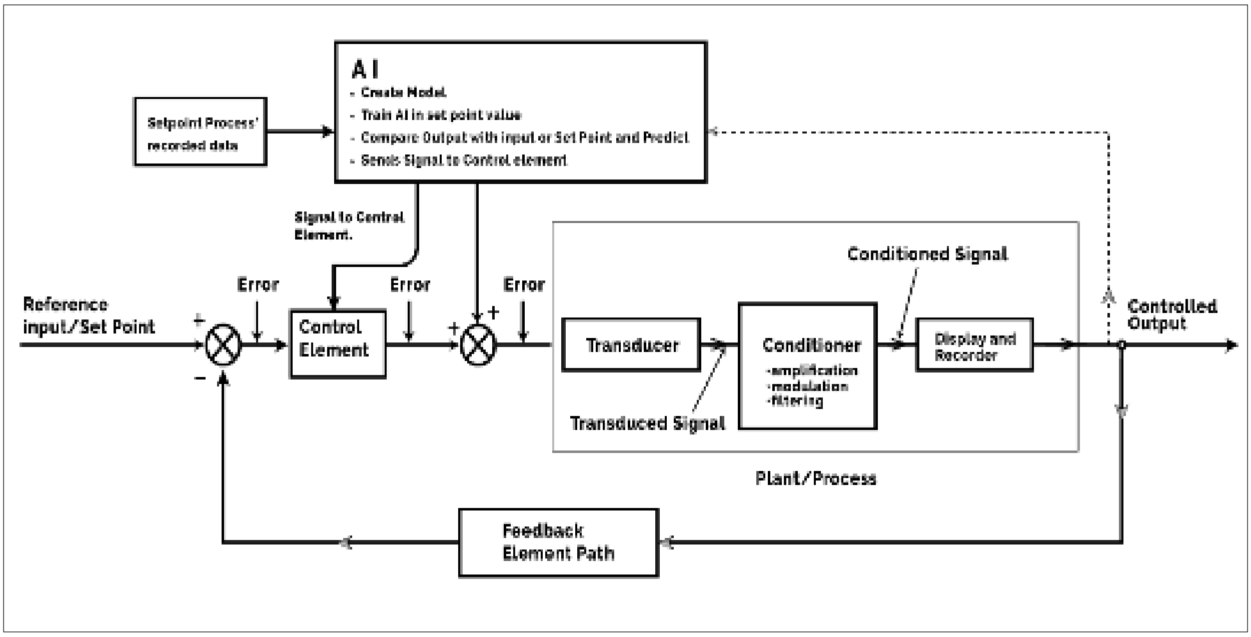


Figure 3 Proposed AI-Based Closed-Loop Signal Processing Path [12]

6. Conclusion

Cyber-attack is a serious concern to closed-Loop control system application. However, the expected benefits from AI based control system are so huge that cyber threats should not discourage reaping these huge benefits. Prevention to AI based control loop vulnerability can be achieved by building strong security controls and zero trust procedures to prevent hackers, intruders, cyber-criminals and blind-cyber wanderers from penetrating into the system either internally or externally. With such protocols which is possible and achievable the objective of application of AI in online closed-loop control system is practicable and will improve the efficiency of the overall system.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Barr. and E. Feigenbaum (Eds,) 1981Handbook of Artificial Intelligence, Vol.1, II, Los Altos, CA, Williams Laufmann.

[2] W. A. Akpan, N.T. Effeng and C.M. Orazulume and E.J. Awaka-Ama ‘ Artificial Intelligence Based Quality Assurance of Surface Finish of Parts in Assembly Line’ Engineering and Technology Journal Vol.8 Issue 9 September, pp 2685-2709, 2023

[3] Barbara, A., Schreiber, H. & Moravec, S. A. (2022). Robotics technology. Encyclopedia ritannica German national library. International classification system of German national Library (GND).

[4] W.A.Akpan, C.M.Orazulume, G.D. Essien Kinematics of Human Hand for Robotics Applications International Journal of Science and Research Archive 12(3) 883-891 12 02 1697-1715

[5] W. A. Akpan, E.J. Awaka-Ama and C.M. Orazulume ‘Robotic Arm Application for Pick and Drop Operations’ International Journal of Applied Science (IJASR) Vol. 6 issue 4 July- August pp 22-36 ,2023

[6] Novak V., Perfilieva, I. & Mockor, J. (1999). Mathematical principles of fuzzy logic. Dordrecht. Kluwer Academic. ISBN 978-0-79238595-0.

[7] Rajasekaran, S. and Vijayalakshmi P. ‘Neural Networks, Fuzzy Logic and Genetic Algorithms syntheses and Applications (2012) PHI learning, New Delhi 110001

[8] Schoning, J.;Riechmann, A.; Pfisterer, H. AI for closed-loop Control Systems-New opportunities for Modeling, Designing and Tuning Control and Tuning Control Systems

[9] [Online Available]; arXiv: 220106961lvl [eess.SY] 18 Jan 2022. (2 March, 2025).

[10] Tal Z. ‘The rise of Generative AI and the impact on security’Avaiable Online, Accessed 18th March, 2025

[11] W.A.Akpan; C.M. Orazulume, I.U.Ohari, G.D.Essien,N.N.Inyang and I.U.Ibanag Artificial Intelligence Based Closed-Loop Control System Design World Journal of Advanced Engineering Technology and Sciences (WJAETS) Vol. 14 issue 03 pp 2025

[12] W. A. Akpan, C.M. Orazulume, I.U.Oharei, N.N. Nsedu, U,O,Ibanga Artificial Intelligence Based Closed-Loop Control System Design World Journal of Advanced Engineering Technology and Sciences (WJAETS) Vol. 14 03 pp 505-511, 2025

[13] W. A. Akpan, I.U.Oharei, G.D. Essien, C.M. OrazulumeN.N. Nsedu, B.O. Daniel. Data Capture, Transmission and Signal Processing in AI Based Closed-Loop Control System Design Global Journal of Engineering and Technology Advances (GJETA) Vol. pp 20 27,2025