2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) | 978-1-6654-9529-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ACCAI53970.2022.9752651

An Artificial Intelligence enabled Smart Industrial Automation System based on Internet of Things Assistance

Nirmala P[1], S. Ramesh[2], M. Tamilselvi[3], G. Ramkumar[4] and Anitha G[5]

[1,4,5]*Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai 602 105, Tamil Nadu, India.*

[2]*Department of Electronics and Communication Engineering, St. Mother Theresa College of Engineering, Vagaikulam-628102, Tamilnadu, India.*

[3]*Department of Mechatronics Engineering, T.S. Srinivasan Centre For Polytechnic College and Advanced Training, Chennai, Tamil Nadu, India*

E-mail : pgrvlsi@gmail.com, anipsg09@gmail.com, nirmalajai@gmail.com, ramembengineer@gmail.com, tamilselvivlsi@gmail.com

***Abstract*- Several applications adapt the smart technologies to the existing versions to make the application more comfortable to its consumers, in which the technologies such as Internet of Things (IoT), Artificial Intelligence and so on. The adaptation of such technologies provides a huge support to the organizations and individuals to attain the commercial and non-commercial needs in good manner. The logic of Internet of Things provides a great support to automate the organizations, industries and even a residential buildings in proper way using such powerful technology advancements as well as it provides a way to the users to operate and monitor the respective place in global perception without any range restrictions. In this paper, the logic of Internet of Things is applied to the industrial automation needs and attain the benefits from that in correct manner. This is done with the abilities of Artificial Intelligence as well and the proposed logic is named as Artificial Intelligence Assisted Network Paradigm (AIANP). The proposed AIANP provides a huge support to automation industry to control and monitor the industrial environment without any security lackings and delay by means of associating the AI logic in its approach. This is achieved by means of associating the internet enabled services to the industry to operate the machineries accordingly. In literature lots of IoT based automation approaches are available but all are strucked up with certain limitations and lackings, so that a new approach is required to resolve the issues over conventional automation technologies. This paper provides a robust industrial automation abilities to the users to control and monitor the industry in proper way using proposed Artificial Intelligence Assisted Network Paradigm. And the resulting section provides the proper proof for the proposed approach efficiency and security effectiveness in graphical manner.**

Index Terms*—Artificial Intelligence, AI, Machinery Control, Internet of Things, IoT, Industrial Automation, Remote Monitoring, Security

I. INTRODUCTION

Industrial Automation based on the Internet of Things is pushing the linking of millions of previously unconnected items into a massive network for usage in a wide variety of applications, ranging from automated cars to industrial management technologies, to building intelligent devices. These paradigms are predicated on the deployment of Cyber-Physical-Systems in conjunction with Artificial Intelligence assisted Internet of Things (IoT) technology. Because these types of methods are capable of collecting, analyzing and transferring enormous amounts of information, it is critical to maintain data security and integrity from malicious alterations and assaults in order to ensure a secure and dependable functioning. While data theft and cyber assaults in general pose a substantial risk, cyber security threats on IoT devices can be particularly dangerous owing to their closeness to humans, hence increasing the chance of physical injury. This paper demonstrates the important nature of safeguarding these technologies and seeking a safer operation while keeping in mind the number of security vulnerabilities discovered in embedded applications.

This paper describes potential security risks and vulnerabilities in two case studies from distinct IoT sectors, namely architectural automation and industry automation systems, with the goal of identifying ways to enhance the security of these systems. The internet of things (IoT) has been considered and implemented in a variety of business areas, including smart cities, energy management systems, hospital, water and food management, transportation industry and aviation. This system not only offers a systematic mechanism for uploading

and displaying a certain set of conditions, but also adapts to modifications in the specifications over the internet. In this endeavor, we are evaluating different characteristics relevant to the sector, namely temperature, humidity, gas detection and fire detection using a variety of sensors. The Internet of Things (IOT) is a technology with set of systematic and flexible system comprised of sensing devices and smart devices whose intention is to connect all objects, such as everyday as well as industrial entities, in such a way that they become smart, configurable and more capable of communicating with people [1]. All the Internet of Things applications, industrial, residential or other, are regulated and controlled by a number of criteria that the user implements and executes. As a result, their proper implementation varies depending on the collection of operational characteristics supplied or desired by the client.

A. IoT Assisted Industrial Automation

The adoption of an Industry-based Automation System connects businesses' assets to the Internet in order to collect a massive quantity of data that enables the development of applications and services that increase businesses' efficiency and effectiveness. These paradigms are predicated on the deployment of Cyber-Physical-Systems, which are supplemented by Internet of Things and artificial intelligence technology. While Cyber Physical Systems (CPS) manages the control of systems by integrating both hardware and software components in a networked collaborative environment, the Internet of Things (IoT) focuses on digitalizing products and resources through the placement of small sensors connected to the Internet throughout the system. A significant quantity of communication occurs between remote organizations exchanging massive amounts of acquired data, implying the critical necessity to rely on protection criteria [1]. According to a McKinsey research [2], as the IoT expands, the probability of attacks increases as well, and cyber-risks that previously affected just information technology increasingly threaten manufacturing processes and goods, prompting corporations to expend up to 500 U.S.D million in cyber security. Cisco's 2018 Annual Cyber security Report, however, indicates that this is insufficient, since 83% of IoT devices remain susceptible and 53 percentage of all Cyberattacks culminated in losses of 500,000 U.S Dollars or more [3]. Not just private corporations are particularly worried about cyber security; for example, the European-Commission promoting the research and innovation of cyber security work programme, which currently has five auditions in information security themes [4], the United Kingdom and German authorities have published information security regulations [5].

When discussing security, it is unavoidable to discuss the CIA trinity of secrecy, integrity, and availability [6]. This trio serves as a blueprint for designing an organization's security. It is vital to restrict access to information, prevent its alteration or deletion, and assure its timely availability. These three requirements serve as the foundation for security and are applicable to a wide variety of application areas, including manufacturing, logistics, building automation, and smart electrical grids. While the influence of IoT is significant in certain fields, security considerations are not typically a primary concern when adopting such solutions. The purpose of this research is to investigate security flaws in several IoT applications and to demonstrate how these flaws may be mitigated by applying widely disseminated security procedures. To accomplish this, the paper examines two examples from distinct domains, one from implementing this technology and another one from industrial automation, recognizing some many security problems and integrating some straightforward measure to avoid attacks that enhance the security of the network by attempting to prevent them from falling victim to the most known threats. The accompanying picture, Fig-1, depicts the suggested Artificial Intelligence-based Industrial Automation model in a clear and precise manner.

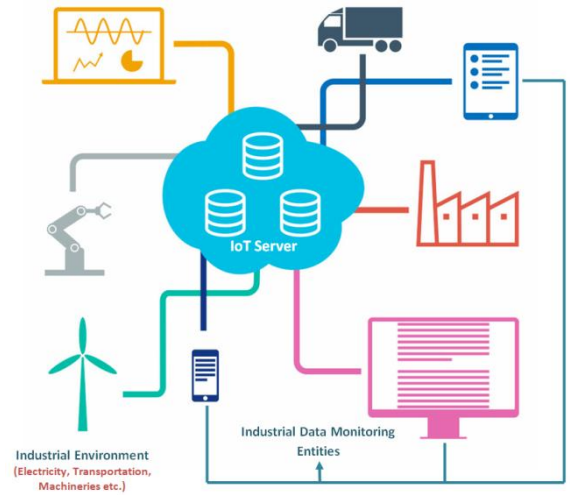


Fig.1 Industrial Automation Model using AIANP

B. Overview of the System

In this current era of advanced technology and powerful computing, combining Concept of internet of things and AI offers potential options for industrial automation systems. To get a better understanding of the industrialization of IoT, this research evaluates present development on IoT, important associated technology and significant industrial Internet of things based applications and highlights trends in the field as well as difficulties. In this approach different types of sensors such as temperature, humidity, gas detection and fire detection sensors are used to detect changes in the external environment and the state of objects. Researchers have identified different critical and vital factors for an industry as well as these include temperature and humidity readings, inventory counts and the identification of gases in the surrounding environment. A cost efficient industry is developed with the use of sensors that we employed in our research and then the characteristics that are simulated in real - time basis are analyzed and eventually transmitted to a remote server in which these parameters are presented together with their growth or reduction in significance.

II. Related Study

The Internet of Things is a today's technology society transformation that is rapidly that are used in commercial, manufacturing, medical, the finance and other sectors. Machine learning is assisting the Internet of Things, notably transportation, industrial automation and control systems, in a broad variety of daily deployments with predominant commercial processes. Internet of Things is a network of networked physical things that enables them to collect and exchange data through the use of programming, monitoring units and internet connectivity. In industries, the Internet of Things sparked a new transformation and the phrase "Industry-4.0" has been used in the field of Internet of Things to describe a state in which industrial equipment and materials are linked and come together to make choices using Artificial Intelligence. This paper concentrates on the global convergence of the Internet of Things with machine learning, including current and prospective applications for benefit to society [7].

Industry-4.0 and the Industrial-IoT are going to promote the connectivity of millions of previously unconnected devices into a massive network capable of being used in a wide variety of applications, ranging from automated vehicles to equipment and intelligent buildings. These paradigms are predicated on the adoption of Cyber Physical Systems, which are supplemented by Internet of Things and artificial intelligence technology. Because these types of systems are responsible for gathering, processing, and transferring massive amounts of data, it is critical to maintain data integrity and security from malicious alterations and assaults in order to ensure a secure and dependable functioning. While data theft and cyber assaults in general pose a substantial risk, cyber attacks on Industrial Internet of Things devices can be particularly dangerous owing to their closeness to humans, hence increasing the chance of physical injury. This article emphasizes the critical nature of safeguarding these systems and seeking a safer operation while keeping in mind the number of security vulnerabilities discovered in embedded devices. This paper examines potential security risks and vulnerabilities in two case studies from distinct IoT areas, namely building automation and industrial automation, with the goal of identifying methods to enhance the security of these systems [8].

Since many years, the Internet of Things has been utilized for home technology and control driving automatic toll collecting systems. As Industry-4.0 takes hold, the Internet of Things is being utilized in industry for industrial automation, preventative maintenance, micro grids and data analysis. With the Internet of Things boom, IoT devices will generate massive amounts of data that will be stored in the cloud. The primary impediment to factory automation via Connectivity is security and privacy. Researchers explored the limitations of the Internet of Things, its architecture, implementation of knowledge for the Internet of Things, the Industrial IoT and security concerns as well as several ways for protecting Internet of Things-assisted networks in this study [9].

The Internet of Things is frequently utilized in intelligent energy management, industrial automation, and a number of other applications. Internet of Things devices are installed at various phases of the SmartGrid to monitor and regulate grid statistics to ensure stable and efficient electricity distribution. While integrating the Internet of Things into the SmartGrid domain has several benefits, the problems associated with IoT-SmartGrid integration must be overcome in order for the grid to operate

efficiently. The purpose of this article is to offer an outline of SmartGrid and Internet of Things-based SmartGrid systems. This article discusses a power monitoring system based on the Internet of Things that is capable of measuring and analyzing electrical characteristics such as voltage, current, active power, and load energy usage. The software programme "Thing-Speak," which is based on the Internet of Things, is used to collect real-time electrical data from users. Consumers and power transmission firms in the SmartGrid model may use this data to better regulate their use and lower their billing expenses [10, 11].

III. METHODOLOGY

This paper introduced a new smart automation methodology called Artificial Intelligence Assisted Network Paradigm (AIANP), in which it is used to control and monitor the industrial environment without any range restrictions or other security related issues. The following figure, Fig-2 illustrates the perception of proposed block diagram in clear manner with proper specification.

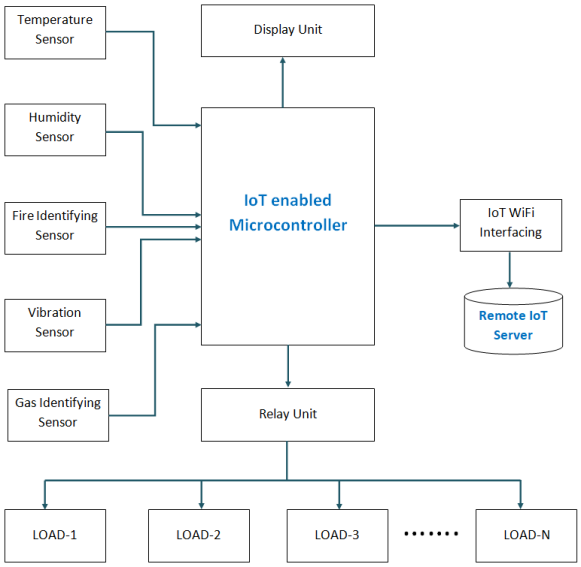


Fig.2 Proposed Block Diagram

The ESP 8266 based WiFi controller is a systematic controlling system on a chip with an inbuilt communication protocol stack that enables controller to connect to a WiFi network. The ESP8266 module may host an application or delegate all WiFi networking functionality to another central processing unit. The Wifi module is pre-programmed with AT instruction set software, which means you can just connect it to your Arduino platform and receive roughly as much WiFi functionality as a WiFi Protective layer, plus the WiFi module is an incredibly effective and cheaper device with a large and expanding network. The following figure, Fig-3 illustrates the perception of ESP8266 module in clear manner.

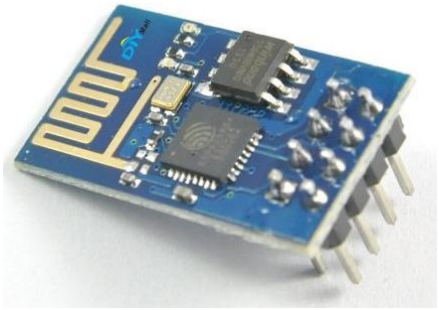


Fig.3 ESP8266 Module

The DHT11 is a temperature and humidity sensor and it is a cost efficient digital sensor in its purest terms. It measures the ambient air using a sensitive humidity sensor and a thermostat and outputs a signal pin. It's quite straightforward to use, but data collection needs some finesse. Each sensor in this design is temperature adjusted and calibrated in a precise calibration chamber, and the calibration coefficient is kept in the form of a programming inside the OTP storage. When the sensor detects, it will get the measurement coefficients from RAM. DHT11's small size, low power consumption and extended transmission distance make it suitable for a wide variety of demanding application scenarios. Single-row packaging with four pins simplifies connecting. The following figure, Fig-4 illustrates the perception of DHT11 sensor module in clear manner.

Fig.4 DHT11 Sensor

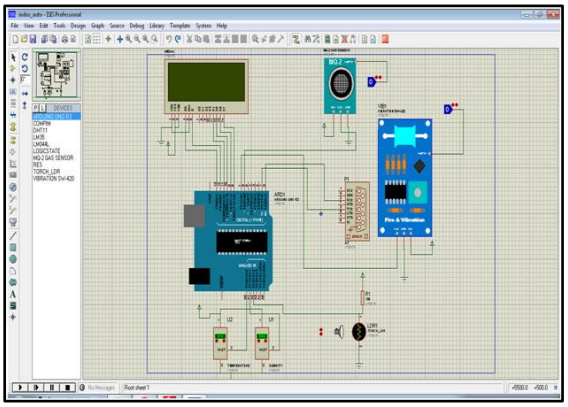
The MQ2 Module sensor is used to sense gases in the local environment. In fresh air, it has a reduced permeability. Whenever the target flammable gas is present, the conductivity of the sensor increases. Convert the change in conductivity to a gas

concentration output signal. The MQ2 gas sensor is extremely sensitive to ammonia, Sulphur dioxide and phenol vapor, as well as smoky and some other hazardous gases. It is inexpensive and useful for a variety of applications, including hazardous gas/smoke identification. The following figure, Fig-5 illustrates the perception of MQ2 gas sensor module in clear manner.

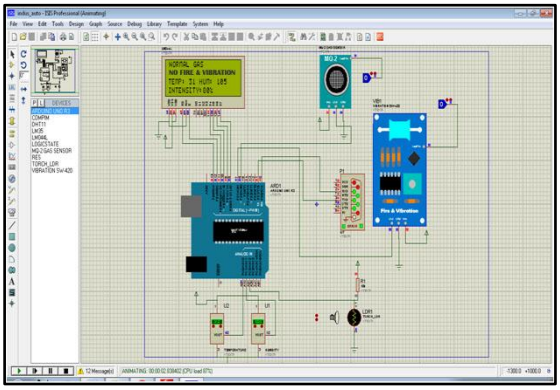
Fig.5 MQ2 Gas Sensor

IV. Results and Discussions

The proposed approach is developed with respect to the adaptation of Artificial Intelligence (AI) and the model is simulated by using the Proteus simulation toolkit. As well as the hardware unit is assembled based on the simulation model using the respective sensors mentioned into the methodology section figures, Fig-3, Fig-4 and Fig-5. The following figure, Fig-6 (a) illustrates the perception of exact schematic design of the proposed industrial automation model and the following figure, Fig-6 (b) illustrates the perception of outcome attained from the simulation model using Proteus simulation environment.



(a)



(b)

Fig.6 (a) Schematic Design and (b) Simulation Outcome

The following figure, Fig-7 illustrates the proposed approach efficiency in clear manner with the cross-validation of conventional industrial automation process without AI. In which the efficiency is cross-validated with respect to the number of loads associated into the relay unit.

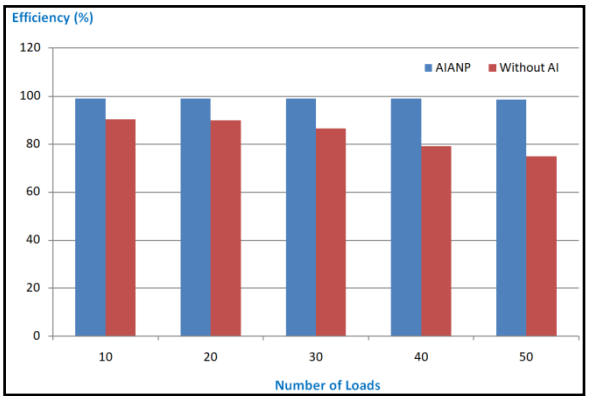


Fig.7 Efficiency Analysis

The following figure, Fig-8 illustrates the proposed approach security effectiveness in clear manner with the cross-validation of conventional industrial automation process without Artificial Intelligence. The lack of security points are caused by noise ratio over the trigger raised from the serve entities due to heavy load machines connected with the relay unit.

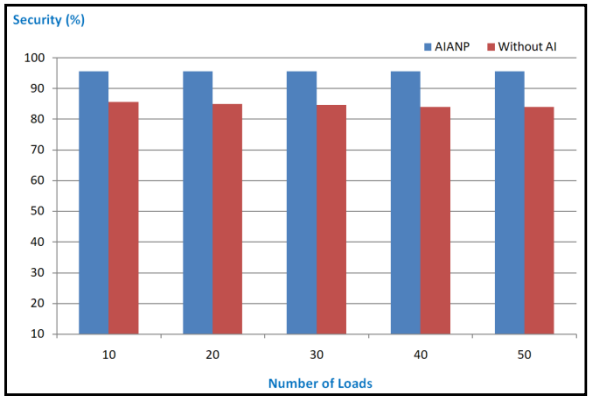


Fig.8 Enriched Security of AIANP

V. Conclusion and Future Scope

This document discusses all of the key features for industrial experts who want to comfortably and effectively operate and monitor the complete industry. The suggested Artificial Intelligence Assisted Network Paradigm (AIANP) enables the definition of all industrial automation requirements. There is no component that can be altered in terms of industrial safety. This paper would assist an individual in being informed of all required steps that he should be conscious of and would not do them any damage in the industrial environment or to the made items. The examination of the detailed test systems revealed potential security dangers to which the systems are exposed. Threats in both scenarios are primarily connected to gaining access to information transferred, whether it is data sent for remote system monitoring or data exchanged between agents. After identifying the security flaws in both systems, simple fixes were deployed to avoid or even eliminate possible security risks through the use of widely disseminated security mechanisms.

In future the work will focus on developing more complicated assault scenarios and on more advanced defense measures, such as the use of Machine Learning algorithms to recognize patterns of method is defined and threat.

References

[1] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework", Computers in Industry, vol. 103, pp. 97–110, 2018.

[2] T. Poppensieker, W. Richter, R. Riemenschnitter, and G. Scherf, "A new posture for cyberrisk in a networked world", in Leading in a disruptive world. McKinsey&Company, 2018, ch. 3.

[3] Maniyath, S.R., Vijayakumar, K., Singh, L. et al. Learning-based approach to underwater image dehazing using CycleGAN. Arab J Geosci 14, 1908 (2021). https://doi.org/10.1007/s12517-021-07742-8.

[4] ECSO, https://ecs-org.eu/cppp, accessed: 2019-07-26.

[5] D. Emm and V. Chebyshev, "Kaspersky security bulletin 2018. top security stories", https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/, 2018.

[6] Nirmala. et al. (2021). "Artificial Intelligence to Analyze the Performance of the Ceramic-Coated Diesel Engine Using Digital Filter Optimization"Advances in Materials Science and Engineering vol. 2021, Article ID 7663348, 10 pages, 2021. https://doi.org/10.1155/2021/7663348.

[7] Sherif El-Gendy, "IoT Based AI and its Implementations in Industries", International Conference on Computer Engineering and Systems, 2021.

[8] Saravanakumar, C. and Senthilvel, P. and Thirupurasundari, D. and Periyasamy, P. and Vijayakumar, K. (2021) Plant syndrome recognition by Gigapixel Image using Convolutional Neural Network. In: ICASISET 2020, 16-17 May 2020, Chennai, India.

[9] Supriya Vishal Dicholkar and Deepthi Sekhar, "Review-IoT Security Research Opportunities", International Conference on Convergence to Digital World - Quo Vadis, 2021.

[10] Ramkumar, G. et al. (2021). "A Short-Term Solar Photovoltaic Power Optimized Prediction Interval Model Based on FOS-ELM Algorithm", International Journal of Photoenergy, Volume 2021, Article ID 3981456, 12 pages, https://doi.org/10.1155/2021/3981456.

[11] K. Vijayakumar, Vinod J Kadam, Sudhir Kumar Sharma, 2021, Breast cancer diagnosis using multiple activation deep neural network, Concurrent Engineering, Volume: 29 issue: 3, page(s): 275-284.