International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2022.8.4.9

Volume 8, Issue 4
April - 2022

Incorporating Environmental Protection Requirement in Industrial IoT Access Control Security Using Arduino Technology MQ2 and DHT11 Sensor Networks

Joseph Kalunga[1] Simon Tembo [2] and Jackson Phiri [3]

Ph.D Student [1] & Professor[2 3]

[1,2] Department of Electrical and Electronic Engineering, School of Engineering

[3]Computer Science Department, School of Natural Sciences,

University of Zambia Lusaka

Zambia

ABSTRACT

This paper presents the development of environmental monitoring mechanism based on Arduino Sensor Technology for Industrial Internet of Things (Industrial IoT) Critical Infrastructure (CI) Protection in an Access Control role. Access control of hazardous substances is one of the most vulnerable aspects of Industrial IoT CI. The idea behind this study is to harden environmental security through live ecological monitoring of Temperature, Humidity and emitted hazardous substances or gases due to Industrial activities and processes in Smart CI places such as Nuclear Processing Plant, Thermal Generation Power Industries, Fossil Processing Plant, Military Chemical warfare plant, food processing factory, Agriculture Chemical Manufacturing Plant and many other CI industries. Live monitoring is one of the most important security requirements for any cyber-Access Control Mechanism. The literature revealed that similar systems were developed and implemented in different organizations and with different System Requirements and specifications. However, most CI industries have not automated environmental monitoring requirements and integrated the requirement into a broad institution security continuum. The consequence of neglecting environmental security is climate change. Furthermore, Toxic gas pollution affects millions of people around the world and contributes to about 5.4 percent of deaths worldwide. Pollution kills more people than the combination of malaria, AIDS, and tuberculosis hence the development of security mechanisms to monitor pollutants in the atmosphere. The main objective of this study was to develop a computer-based application for monitoring environmental hazardous substances such as extreme temperature, humidity, carbon dioxide (CO2), carbon monoxide (CO), and Smoke in the atmosphere surrounding Industrial IoT CI Industries. The system development approach employed was the Arduino engineering process model. To achieve this objective, cheaper ecological sensor Networks that include MQ2 and DHT11 Arduino Sensors are connected to Arduino Uno Microcontroller through a solderless breadboard Arduino component. The backend database was MySQL Relational database management system. The developed prototype application produced a number of results including live monitoring of temperature, humidity, CO2, CO, Smoke, and many others. A system evaluation process was conducted and the result indicated 99.999% accuracy levels. The results, it evidence that the developed prototype application can improve environmental security in Industrial IoT CI institutions.

Key Words: Industrial IoT Security, Environmental Security, Critical Infrastructure Security, Arduino Technology, MQ2 Sensor, DHT1 Sensor.

1. INTRODUCTION

With an advancement of computer technologies especially in the field of Communications, Internet of things (IoT) and Industrial Control Systems (ICSs), Environmental security is a source of safety concerns especially to Industrial Internet of Things (Industrial IoT) Institutional critical Infrastructure (CI) Protection. Industrial IoT is not only plagued with authentication, and access control security issues at physical layer, but also does not work as it should be with fourth industrial revolution in terms of environmental security. Even though, the coming of Industrial IoT has reduced carbon emission into the atmosphere and boost production efficiency much more has to be done in terms of monitoring and controlling of pollution and extreme weather conditions. Access control of

things, object or substance is one of the most vulnerable aspects of Smart industry [1]. That being stated, it is evidence that modern industrial sector is being challenged by several ecological threats that requires resolution before achieving environmental sustainability.

Environmental sustainability deals with conservation of natural resources and protection of global ecosystems to support health and wellbeing of people and living organism, at present and in the future[1]. Environmental sustainability is dependent on monitoring of hazardous substance and things affecting industrial sector resulting from industrial activities and processes. Therefore, live monitoring is one of the most important security requirements for any Cyber- Physical Access Control Mechanism. That being highlighted, environmental Sustenance can be described as an umbrella terms for many greenhouse concepts and it is the subject of corporate, political, social and economic responsibility.

People all over the world need clean breathing air, fresh drinking water and live in places free of toxic substances and other hazards. This explains rationale that, well-being of human and essential living organism is closely related to the health of natural environment. Arising from that fact one of the greatest environmental problems facing the world today is monitoring and controlling of carbon emitted toxic gases and extreme weather condition that could result in global warming and extreme weather condition[2]. Carbon emitted substances are important constituent of environment security. However, Environmental security can only be improved through live monitoring and control of hazardous substances and observing extreme weather conditions within CI industrial area. Emitted carbon gases from various industrial activities sources are accumulated to pollute the environment in a specific geographic area like Nuclear Processing Plant, Thermal Generation Power Industries, Fossil Processing Plant, Military Chemical warfare plant, food processing factory, Cement Plant, Agriculture Chemical Manufacturing plant and many other CI industries.

According to World Health organization (WHO), climate change due to rapid industrialization, fast urbanization, rapid growth of population, increase in carbon emission is expected to cause approximately 250 000 additional deaths per year between 2030 and 2050[3]. Furthermore, toxic gas pollution has already affected millions of people around the world, and contributes about 5.4 percent deaths worldwide[4]. The implication is that, Pollution resulting from industrial activities and processes kills more people than the combination of malaria, AIDS and tuberculosis[4]. That being stated, air and water pollution has become global source of health concerns for human and other living organism especially from industrial process and activities. Poor air quality have caused many respiratory problems like asthma and bronchitis; intensify the risk of life-threatening conditions with substantial medical costs[2].

However, it is important to note that there is no clear cut solution to Environmental Sustainability and Climate Change problem. Industrial IoT CI ecological sustainability problem can effectively be addressed by multilayered security approach [5]. Nevertheless, the development of environmental live hazardous substance monitoring and controlling mechanism in access Control role based on Arduino technology can improve environmental security. That being stated, the main objective of this paper is to develop a computer application for monitoring live environmental hazardous substances (extreme temperature, humidity, CO2, CO and Smoke) in the atmosphere surrounding Industrial IoT CI by employing MQ-2 and DHT11 Sensor Networks. Live environmental hazardous substance monitoring and control may help in mitigating the effect of climate change and global warming. Furthermore, the developed environmental security mechanism provided means for live monitoring of dynamic weather changes specifically ecological unbearable Temperatures and humidity.

2. MOTIVATION

Providing security to CI industry is not only protecting information, Industrial Physical Perimeters or CI Computer Network assets but also lives of people and natural resources against emitted toxic gases and extreme weather conditions (temperature and precipitation). Continuous monitoring of these climate variables in access control role and the development of live environmental monitoring mechanism can play a greater role in addressing negative effects of climate change. An access control of hazardous emitted environmental substance and extreme weather condition may help in maintaining environmental sustainability. In this context, an Access Control is described as a Cyber- Physical Access Control Mechanism including Environmental Sustainability measures for Monitoring and Identification of hazardous substance or extreme Weather condition in specific Industrial IIoT geographical areas due to industrial activities and processes. An Access Control is therefore a fundamental requirement in Industrial IoT CI Security and can be categorized into Logical, Physical and Environmental security[5]. In recent years, IIoT technology has been massively enabled in CI Institution based four design principles of Interoperability, Information Transparency, and Technical Assistance and decentralized Decision Making [6]. Each of these Industrial IoT principles generates an attack surface that can be exploited by the malicious person, object or substance in absence of proper Safety and Security controls. Environmental and machine induced threats to IIoT Perimeters can only be mitigated with a proper Security and Safety Systems. That being stated, Security and Safety of IoT components have negatively affected the full scale implementation of IIoT concepts in modern Industrial IoT CI Industry[7]. Though, in recent studies

DOI: 10.31695/IJASRE.2022.8.4.9

approximately 4.8 billion Industrial IoT devices were activated globally in the last few years[8][9]. This development has resulted in high productivity and enhanced human living conditions [2]. Other benefit includes good performance; attain fast and efficient processes, continuous product improvement and monitoring, reliability, reduced operation costs and many other benefits mentioned in [10]. All these improvement are attributed to merging of Information Technology (IT) and Operation Technology (OT) in what is referred to as "Industry4.0" or Industrial IoT. Hence the key motivations of this paper include:

- To improve environmental security in Industrial IoT operation areas and surrounding through monitoring of hazardous substances and extreme weather conditions.
- To protect the health of people and other living organism from toxic hazardous gases and extreme temperature due to industrial activities and processes.
- To promote ecological sustainability through monitoring.
- To develop less expensive and efficient computer application for Industrial IoT CI environmental protection through observation and control.

This paper is organized as follows: In section 2, Contribution of the study, Section 3, related works are discussed. In section 4, Materials and Methods are presented. Section 5, Modelling and Analysis are highlighted. Sections 6, System Activities are stressed. In section 7, Architectural Design is detailed. Sections 8, Sensing Algorithms are highlighted. A section 9, Entity Relationship Diagram (ERD) is highlighted. Section 10, System Configurations is described. Section 11, conclusion and future works are provided.

3. CONTRIBUTION

The contribution of this paper includes:

- The literature on Industrial IoT security in access Control Role
- Proposes a suitable approach to visualize Industrial IoT threat Pattern.
- The Model to detect and Monitor live environmental hazardous substance due to Industrial Processes and activities.
- The Model to detect and Monitor live temperature and humidity in Industrial IoT CI Environment.
- Highlighted some areas of the research which require further works.

4. RELATED WORKS

In [11], The climate change was discussed through the United Nations (UN) Framework Convention on Climate Change (UNFCCC). The European Union (EU)'s commitment was to reduce the amount of CO2 and other hazardous gas emissions levels in the atmosphere. The prescribed model of fighting climate change was through Policy formulation. The interventions targeted car manufacture and were aimed at addressing climate change through reducing fuel intakes in passenger vehicles. Among the key action plan were sharing information between Member States and agreement with car manufacturing industries on modalities of reducing CO_2 emissions from vehicles, and introduction energy/CO2 taxes within EU member states. African countries also have embraced vehicle taxation Models citing introduction of carbon taxes on car owners in Zambia and other African Countries[12]. These interventions only targeted car manufacturing industries and car owners at a policy level and not any other CI manufacturing industries which are also known to be greater sources of emitted hazardous gases in the atmosphere[11].

In[13], Industrial IoT Technologies were employed as security mechanisms to promote environmental sustainability in Agriculture Sector being an example of CI industry. The IoT Technologies were engaged to spearhead the vision of Smart Agriculture in order to promote food and environmental security. The project scored same success in that it managed to improve crop yield, profitability and reduce environmental footprint especially from Greenhouse gas Emissions. Furthermore, it enabled the reduction of the inherent environmental impact by performing real-time detection of weeds or infestations, monitoring weather conditions and soil Condition etc. However, the developed security mechanism targeted only agriculture sector specifically to improve soil fertility and watering systems neglecting other source of climate change like industrialization processes and air pollution resulting from industrial smoke or wild fire. During industrial IoT processes, different gases such as CO_2,CO, CH2, N2O and CFC are released into the atmosphere [2].

DOI: 10.31695/IJASRE.2022.8.4.9

In[14] , Arduino based environmental air monitoring system was developed to detect atmosphere air quality in workplaces. The environmental air monitoring system was designed to provide an efficient, straight forward and robust solution to continuously monitor air quality in real time. Considering that, most people spend majority of their time in door. The proposed environmental monitoring system was able to give real-time measure of air parameter, measuring temperature, humidity and the concentration of CO2 in the atmosphere. However, the developed mechanism was employed in monitoring obligation rather in an access control role. Furthermore, the proposed system was designed to operate indoor and therefore, may contribute less to fight against climate change and global warming. On the other hand, the proposed system contributed favorably in fighting human respiratory problems like asthma; bronchitis and intensify the risk of life-threatening conditions with substantial medical costs.

In [15], a Cyber-Physical Access Control Mechanism was proposed based on fingerprint biometric optical sensor device and traditional national identity document to provide an access control for human unauthorized entry into Military CI industry like physical military base or installations. The proposed Access Control mechanism was based on role based Access Control (RBAC) Model[16]. In roles based access control model users are assigned different role[17]. Most of the traditional access control models are based on RBAC or Attribute Based Access Control Mechanism (ABAC). However, environmental contexts such as day and time night, summer or pollutions are considered under environmental roles[18]. But in this paper, environmental role was not considered but very important due to climate change and global warming problem[19].

In[20] , the Access Control Mechanism was proposed and developed for Military CI protection. The proposed mechanism was aimed at mitigating CI threats resulting from human intrusion to military CI Industry. Furthermore, other researchers have proposed logical and physical access control mechanism for Industrial IoT protection[21][22]. For example, a logical access control mechanism was proposed for Critical Information Infrastructure (CII) collaborative entities dedicated for power generation, transport, distribution and financial services to CI Industrial environment[5]. Additionally, physical access control mechanism of IoT devices and Human object was proposed for hardening physical security in Industrial IoT CI Security at perspective layer [4]. On the other hand, a physical Infrastructure protection Access Control Mechanism was proposed for CI strong room security[23].

However, In terms of Industrial IoT environmental protection and promoting health of people, living things and essential ecological organism from hazardous gases and extreme weather condition (Temperature and Humidity) resulting from industrial processes and activities in Access Control role at perspective layer, nothing of such nature has been proposed. Therefore, this study proposes the development of a computer application for monitoring live environmental hazardous substances in the atmosphere surrounding Industrial IoT CI using Arduino Technology MQ2 and DHT11 Sensor Networks. As stated earlier, live monitoring is one of the most important requirements in cyber-physical access control security mechanism[24].

5. METHODOLOGY

The Methodology Section is divided into Arduino Engineering Process Modelling and Material Aspects. Arduino Engineering Process Modelling paragraph highlights various software development techniques used in application development process of this research. While Materials section include tangible and intangible tools employed to achieve the mentioned study objective.

5.1 Arduino Engineering Process Modelling

As already stated, the system development methodology employed in this study was Arduino engineering process Model. Arduino engineering process model shows the framework employed to structure, plan and control the system development process. This model has been employed in many engineering project and applications starting from every day object to complex scientific instrument[25]. Arduino Engineering Process Model has seven important stages include requirement gathering, documentation, hardware/software gathering, configuration, sketch writing, compilation (debugging), uploading and prototype[26]. Figure 1 shows Arduino Engineering Process Model:

DOI: 10.31695/IJASRE.2022.8.4.9

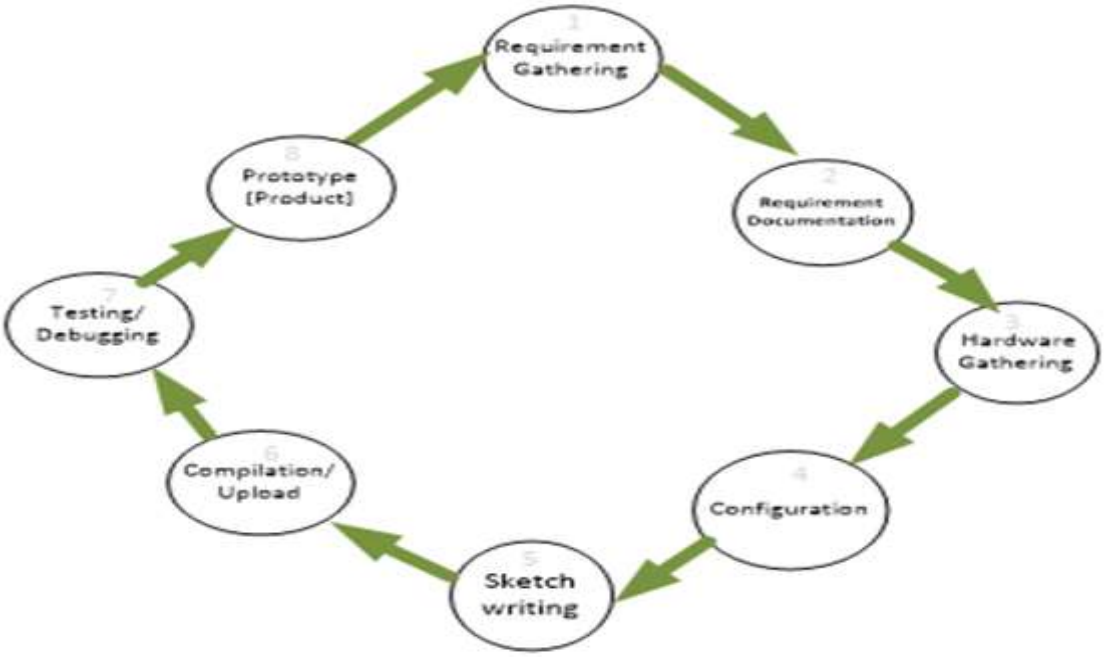


Figure 1: Arduino Engineering Process

5.1.1 Requirement Gathering

Requirement gathering is the first stage in Arduino engineering process application development approach. It starts with the entire process of identifying software needs and documenting deliverables. Normally, requirement elicitation process occurs during the project initiation phase. Proper requirement gathering can lead to successful project outcomes and avoid unnecessary cost resulting from poor requirement planning.

5.1.2 Requirement Documentation

After the requirement gathering process, the requirement documentation was conducted. Requirement documentation process is one of the key stages of Arduino engineering process. It involved requirements gathering, stakeholder's concerns definition and solution detailing. Requirement documentation is important in IoT application development process because it provides the basis for estimates, timelines, and, if used effectively can help in preventing failures. There are a lot of commercial requirement gathering and documentation tools include jama, modern, code beamer, etc [27]. But in study, we employed traditional xml requirement gathering and documentation agile nature of the developed application.

5.1.3 Hardware Gathering

Hardware gathering process involved procurement and acquisition of various Arduino components such as sensors, SDK and many other tools employed in access control application development process. This includes Arduino hardware components such as breadboard, DHT11, optical fingerprint, MQ2 sensors and many other tools mentioned in appendix C section.

5.1.4 Configuration

The configuration process involved setup of various IoT components of the research. That being stated, IoT device configuration is an arbitrary user-defined data type sent from Cloud Core to IoT device. The stated data can be structured or unstructured. It can also be of any format, such as arbitrary binary data, text, JSON, or serialized protocol buffers. Device configuration is persisted in database by Cloud IoT Core services.

5.1.5 Sketch writing, uploading debug

The sketches were written for each sensor to coordinate and operate with Arduino microcontroller and coordinate with the backend database. Sketch is the term refers to a computer program written in Arduino IDE using C language. A sketch could be the unit of code written to run on any Arduino board. A basic Arduino sketch must consists of two important functions include setup () and loop (). Once the sketch is written, compiled and errors are removed, it is uploaded on the Arduino microcontroller. The process of removing errors in the sketch is what is referred to as debugging.

5.1.6 Prototype production

In Arduino engineering development process, the final result is production of new product and makes an improvement to it while using it. This type of engineering logical process is what referred to as a prototype. A prototype is therefore an early sample, model, or released product built on to test the concepts or process. A prototype is generally used to evaluate a new design and enhancement of precision by system analysts or users.

DOI: 10.31695/IJASRE.2022.8.4.9

5.2 Material

The tools employed in this study were divided in to two categories Hardware and Software. Hardware tools refer to physical devices such as Personal Computer (PC), sensors, breadboard, Wifi board and Arduino Uno microcontroller. Software product refers to computer-generated apparatus employed to perform System documentation, design and programming requirements. These software products included Arduino IDE, operating system, python compiler, device drivers, drawing application and word processors. The design specification of both Hardware and Software are given in Table 1:

Table 1: Hardware and Software Requirement

Requirement	Specification
- Laptop	- Hard disk 80GB Minimum - Processor 3.2 MHz Minimum. Preferable core i3 and above - RAM 4.0 GB - Graphics frequency 3.30 MHz - 64-bit Operating System
Arduino Sensor	- Temperature Sensor (DH11) and Gas Sensors (MQ-2)
- Wamp Server	Version 2.2
- Arduino Uno	Microcontroller
- Microsoft Visio	Version 2003
- Python Programming Language	- Version 3.9 - 64 bits version

6. MODELLING AND ANALYSIS

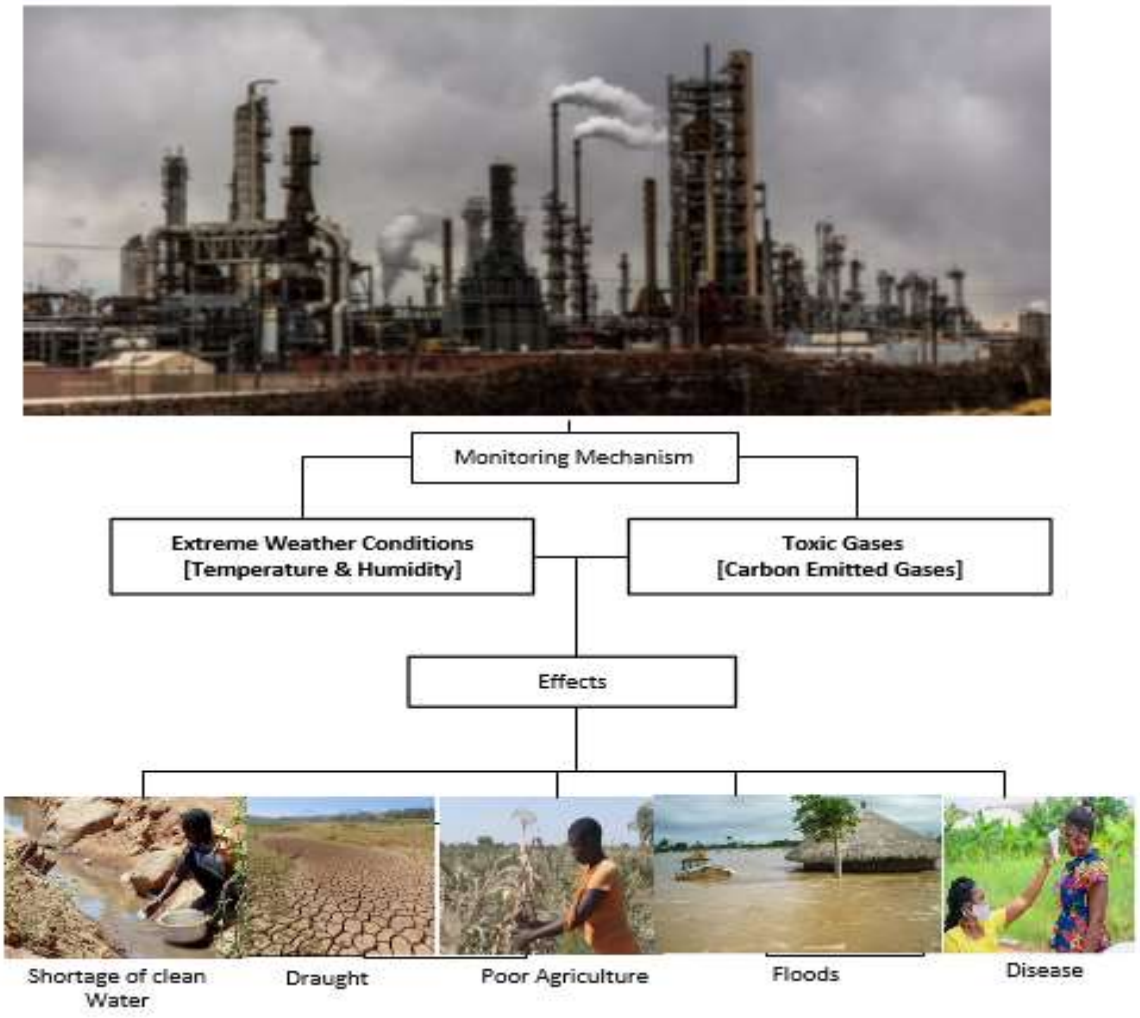
Requirement Modelling and analysis phase of the developed Environmental Monitoring System combines many other stage of Arduino Engineering Process model. It started with requirement gathering, documentation and basic integration of various software and hardware devices components as highlighted in paragraph 5.1. Having stated that, requirement Modelling and Analysis section include aspects of Problem domain definition, Approaches to Industrial IoT Threats, Cyber-Physical Security Strategies, and Use Case Models.

6.1 Problem Domain

In modern CI Industrial production process line, toxic gases can leak unintentionally due to lack of control of temperature and other emitted gases. Although, the installation of Industrial IoT technology in CI industry have partially helped the enterprises to achieve safe, smart and sustainable environmental security[28]. In some cases, toxic gases can intentionally be released into the atmosphere for safety reasons at the wellhead or to reduce pressure in equipment or pipelines. In other cases toxic gases substance are emitted as an end product of industrial processes. Emitted toxic gases maybe contaminated by toxic substance and could drastically affect environmental temperature and humidity that in turn contribute to climate change. Furthermore, toxic gases and extreme temperature are harmful to the lives of both human and Industrial IoT components. That being stated, It is important to realise that for industry 4.0 institution to become climate compatible, it must fulfil four condition include promote energy efficiency and achieve substantial energy gains, enable the circular economy and allow greater productivity and improved use of resources within closed loop supply chains which include re-use and recovery, achieve sustainable development through eco-innovation, and allow significant technology transfer to the least developed countries (LDCs) which must participate in industry 4.0[29]. That being stated, Industrial development has brought about not only rapid economic growth, but also serious environment pollution in many countries, which has led to serious health problems and heavy economic burden on heathy care. Climate change adaptation and mitigation, and industry 4.0 are two important challenges that world leaders are facing today and have already resulted in to catastrophic consequences considering world bush fire, heat waves, droughts and global warming [30], droughts and floods [31]. In view of the above, there is need to continuously monitor climatic variables such as

DOI: 10.31695/IJASRE.2022.8.4.9

temperature, humidity and poisonous substance at emission point in this case Industrial IoT CI environment. To amplify the gravity of Industrial IoT pollution problem, the rich picture was employed. Figure 2 shows the rich picture representing the effect of climate change to the environmental surrounding.



6.2 Functional Layered Approaches to Industrial IoT Threats

Before development process of environmental monitoring security mechanism, we need to visualise approaches to Industrial IoT CI threats. Threats to Industrial IoT CI can be evaluated using functional IoT layered security Approaches. Functional Layered security approach is one the approach that can be engaged to analyse and implement security requirements in IT and OT systems. Layered Security Approach consist horizontal layers with each lower layer providing an abstraction to upper stratum. Each layer in horizontal stratum addresses a specific organizational security vulnerabilities or threats and has a well-defined interface. Layered institutional security configurations have strict rules that the dependencies must only be in a top down approach. Additionally, a change or removal of an upper layer does not mandate any modification in the lower layers. This approach has been employed effectively in traditional IT environment [32]. However, in industrial 4.0 or Industrial IoT institutional frameworks, there is neither anniversary accepted IoT architecture nor predefined number of security layers in the structural design [33]. It is all dependent on applied industrial sector and context of the security problem. That being stated, we visualize Industrial 4.0 CI protection to have four security layers include application, middleware, network and perspective layers and further categorize them in to physical and logical security as opposed to other IoT functional architecture proposed in [34]. In this study, we concentrated on development of physical access control security access control security mechanism at perspective layer. Perspective layer in industry 4.0 is sometime referring to physical layer. Perspective layer is further dissected to come up with environmental layer which is one of the requirement included in developed Access Control Mechanism. The developed Access Control Mechanism is employed to harden physical security of Industrial IoT CI. Figure 3 highlights the layered functional Security approach to Industrial IoT CI.

DOI: 10.31695/IJASRE.2022.8.4.9

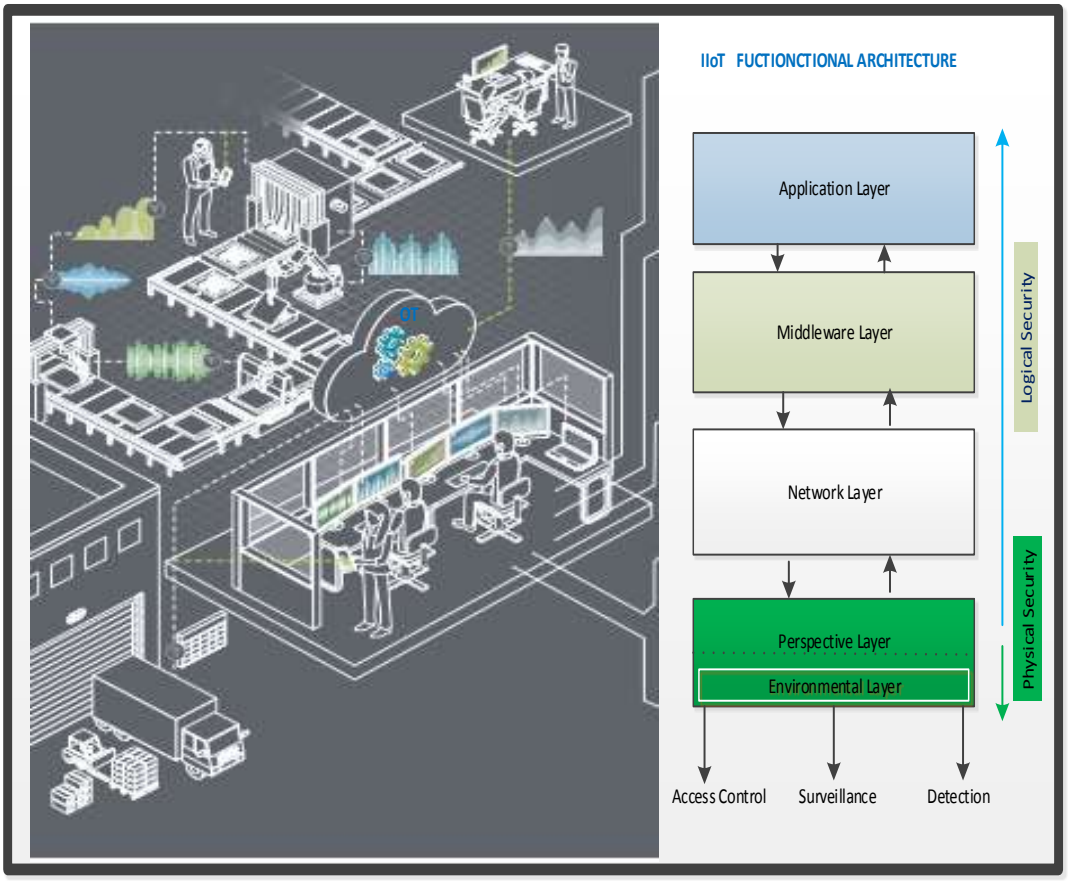


Figure 3: Layered Approaches to Industrial IoT Threats

As already indicated Industrial IoT security is a complex problem and cannot be mitigated by a single security layer or mechanism. That being stated, layered functional approach was adopted to illustrate Industrial IoT huge security demand. Each layer is designed to perform a specific role toward open connectivity of object in ICS, Industrial IoT or any other industrial systems. In similar way, each layer is associated with the specific security threats and present different set of vulnerabilities to Industrial IoT CI. Each vulnerability or threats indicates a piece of security requirement for a specific purpose and designed to promote and mitigate specific threats that compromises particular fundamental IT security need such as availability, integrity and confidentiality.

6.3 Cyber-Physical Security Strategies

Cyber-physical security strategies involve a set of practice intended to keep data and environmental secure from unauthorised access or exposure. Generally, cyber-physical security system design is complex and broad in scope. That being stated an efficient modern CI access control security is generally evaluated according to fundamental principles of confidentiality, integrity and availability. These security principles are also known as CIA triad [35]. While a wide variety of factors determine the security situation of industrial IoT CI infrastructure, information systems and networks, some security principles are more important that the other [36]. For example, in CI infrastructure industry like national utilities such as power grid and waste management systems, service availability and integrity are more important that confidentiality. But the introduction of IoT in CI industry has brought in confidentiality and other security service like authenticity, privacy and nonrepudiation into introspective. For this reason, it is imperative for any developed security mechanism to factor in these new security requirements according layered approach. Figure 4 shows Fundamental ICT Security Principles, while table 2 describe Industrial IoT functional layers and its attributes.

DOI: 10.31695/IJASRE.2022.8.4.9

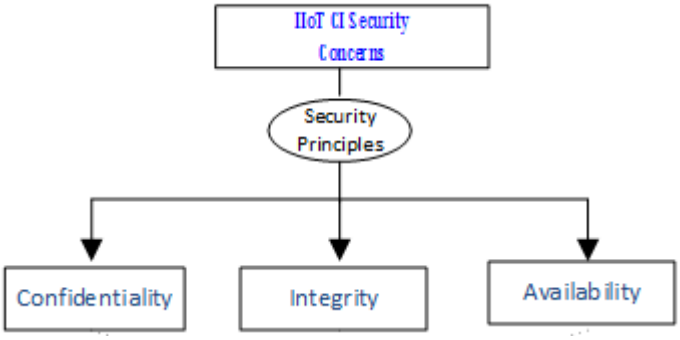


Figure 4: Fundamental Security Principles

Table 2: Layered Approaches to Industrial IoT Threats

Layer	Description	Possible Attacks	Security Principle	Operation Cost
Application	Defines all applications that use the IoT technology or in which IoT has been deployed [33].	Cross site scripting, melicoius code, big data handling issues, etc.	Availability & Integrity	Huge [logical]
Middleware	Middleware Layer resides on top of the operating system and connects different software components or applications. It provides interoperability and other services like the distribution of functionality, scalability, load balancing and fault tolerance [37].	DoS, DDoS injection, Malicious Insider Attack, man-in-middle attack, etc.	Confidentiality	Huge [logical]
Network	Network layer acts as bridge between perception layer and application layer. It carries and transmits the information collected from the physical objects through sensors.	DoS,Man-in-the-Midle, Storage attacks and Exploit attack,etc.	Availability & Integrity	Huge [logical]
Perspective	Gathering information from the surrounding IoT environment capture the users' information.	Intrusion, vandalism, fraud, sabotage, temperamental , terrorism, etc.	Availability, integrity & confidentiality	Low /Medium [logical/physical]
Environmental	Novel layer developed for monitoring and control of environmental hazardous in industrial environment. Includes hazardous substance to be detected or places to be observed. The objects to be detected vary from physical moving objects, such as humans, cars, to environmental factors such as, temperature, or humidity.	Extreme temperature, extreme humidity, flood, fire toxic gases, etc.	Availability, integrity & confidentiality	Low /Medium [logical/physical]

6.4 Use Case Modelling

Use case diagram was employed as the first step in system process modelling. System process Modelling is sometimes referred to as data diagramming. The Use Case diagram is an UML design tool and is used to visualize the behaviour of the proposed system. It includes the description of expected users and their system interaction levels that ultimately specify system requirements. In other words, the use case diagram demonstrates the different ways users interact with the system. It depicted high level system requirements overview of the relationships between sensors, System Development Kit (SDK), users and other actor. System requirements composed system users, activities, their associations, dependencies, roles, processes and goals. The developed application model consists of the following two modules: Humidity and Temperature Sensor monitoring module and environmental hazardous gases monitoring module. Figure 5 shows the use case diagram for the developed environmental monitoring system:

DOI: 10.31695/IJASRE.2022.8.4.9

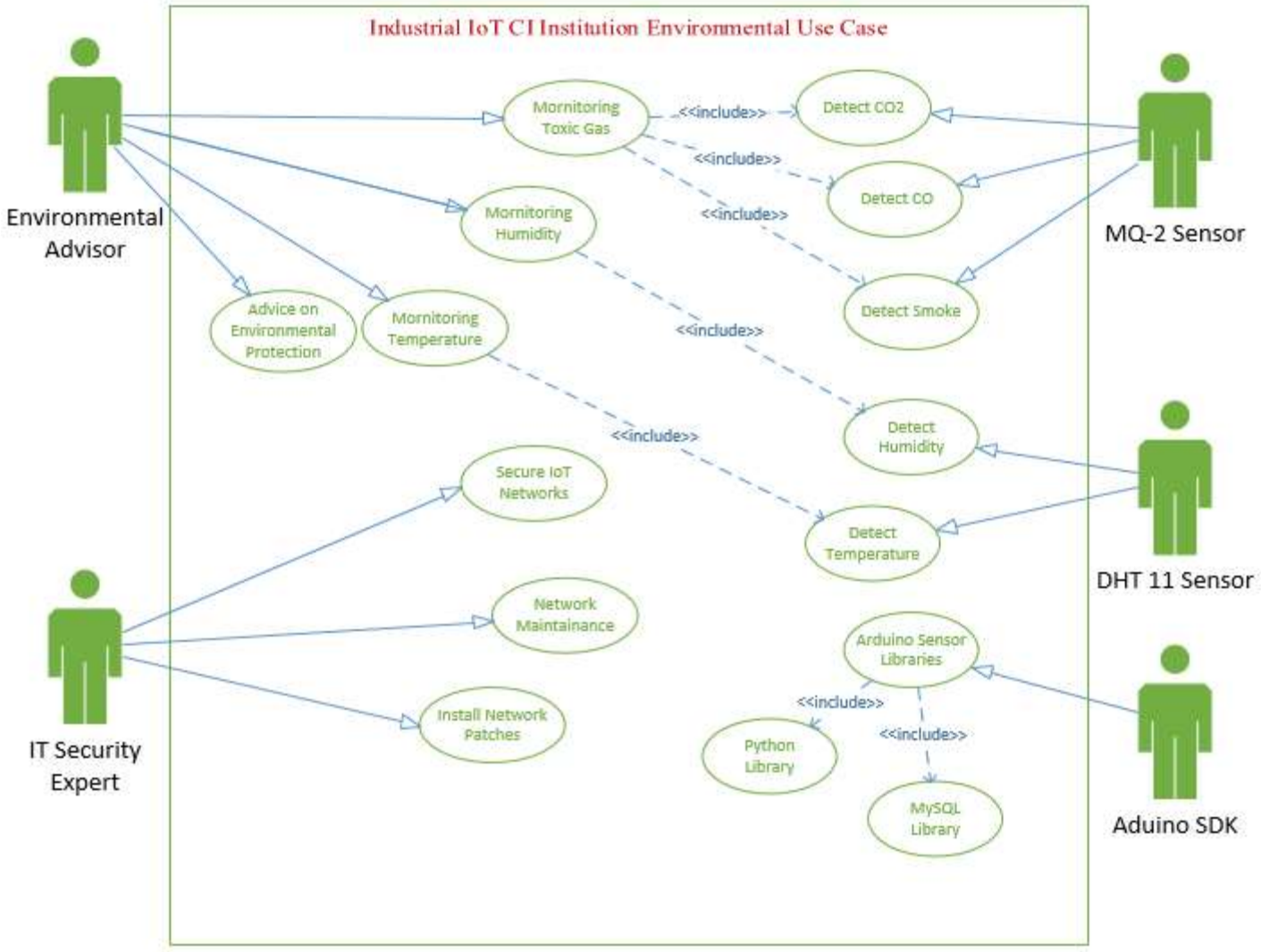


Figure 5: Use Case Diagram for Environment Monitoring System

7. SYSTEM ACTIVITIES

To model the entire systems behaviours, activity diagram was employed. An activity is any operation aspect of the system which focuses on condition of flow and the sequence in which various processes occur. An Activity diagram offer high level description of our environmental monitoring mechanism. Basically, it offered high and low level object or things interact with each other in the virtual environment, opening the way to wide variety of application, from monitoring , sensing, parameter storage, analysis and reporting aspect of the developed application. Additionally, within the process issues' concerning what triggered a particular event may also be detailed clearly [38] . Ultimately, each activity diagram portrays the activity flow of information from starting to finishing point, showing various decision paths that exist while certain activities are being executed. However, activity diagram does not model the system and user interaction which is another important aspect in modern software projects development. There are two important monitoring activities in this study. These Monitoring activities include temperature and humidity monitoring activity and toxic gases monitoring activities:

7.1 Temperature and Humidity Monitoring Activity

The developed Cyber-Physical Access Control Mechanism included activity to monitoring atmospheric air situation in terms of temperature and humidity. Industrial IoT environment internal atmospheric air condition may change dynamically due to the leakage hot gases from industrial process or natural climate. This has to be controlled to secure the heath of Industrial IoT components, human and other living organism. To perform this task capacitive humidity sensor and a thermistor are employed to monitor atmospheric air situation, and spits out a digital signal. Extreme low/high temperature has adverse consequences to environmental security. This may

DOI: 10.31695/IJASRE.2022.8.4.9

compromises key security principles of Industrial IoT CI security service of Availability and Integrity. Figure 6 shows Temperature and humidity activity diagram.

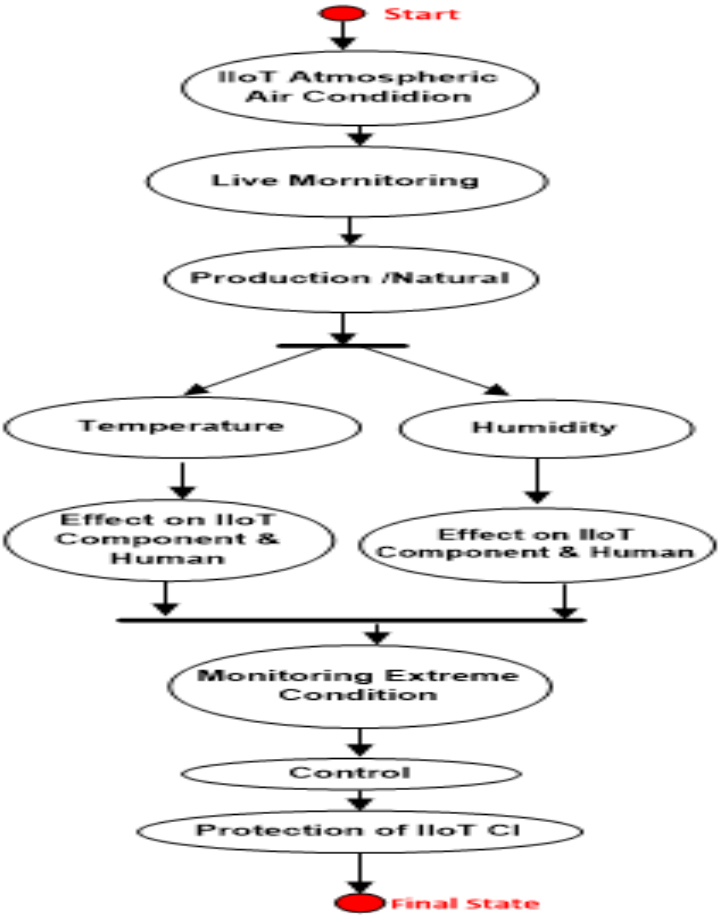


Figure 6: Temperature & Humidity Activity

7.2 Gas Sensor Activity

Continuous monitoring of toxic substance due to Industrial Processes is an important security requirement for sustainability of Industrial IoT CI surrounding environment. During industrial combustion, various toxic substances are emitted into the atmosphere. Other emission comes from industrial gas leakage that can be detected easily by MQ sensor series. In this prototype access control mechanism, MQ2 sensor was employed because of its ability to detect and monitor toxic gases. The sensitive material of MQ2 gas is Tin oxide Sno_2 which changes in conductivity by the interaction with the surrounding atmosphere. Sno2 based gas sensors have received extensive attention in the field of toxic gases detection due to their excellence performance with high sensitivity, fast response and long term stability [39]. Furthermore, Sno_2 species have already been used in CI security especially power generation transformers to boost the availability and integrity of service[40]. Detection and analysis of Tine oxide volumes' quantities and generation rate of fault gases mixed in the fluids allow for identification of power transformers fault type such as partial discharge corona, sparking, overheating and arcing. That being stated, MQ2 gas sensors have highly sensitive to LPG, Propane and Hydrogen also could be activated to detect Methane and other combustible steam like smoke as shown in figure 7.

DOI: 10.31695/IJASRE.2022.8.4.9

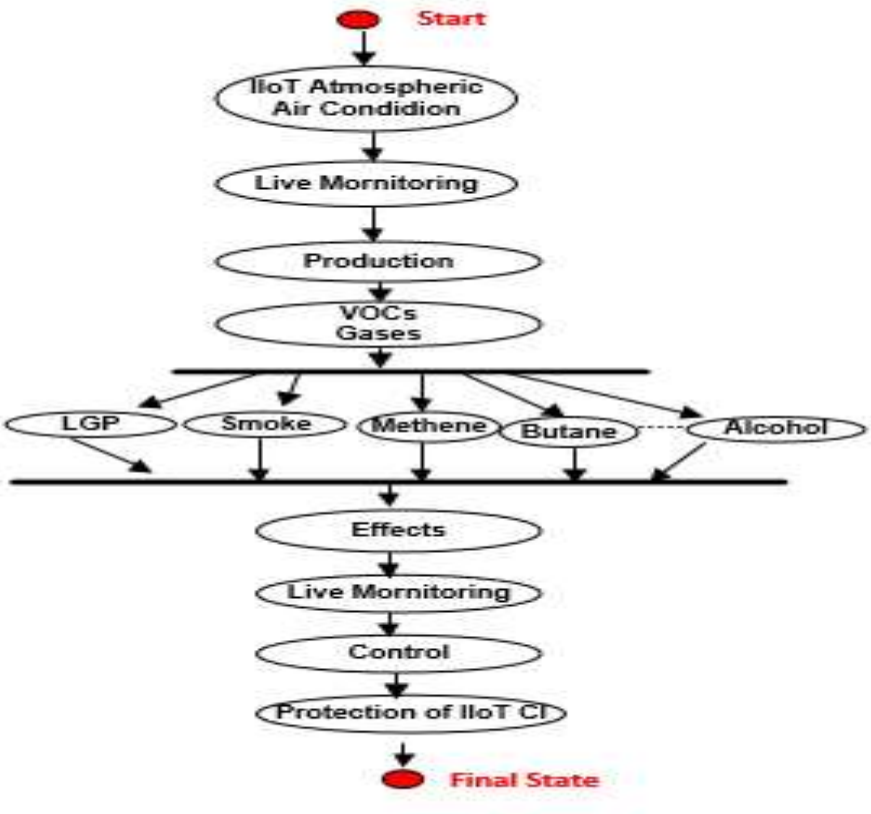


Figure 7:Gas Sensor Activity

8.0 ARCHITECTURAL DESIGN

The architectural design of the developed environmental Access Control Mechanism has five important components namely Central Processing Unit (CPU), Microcontroller, IoT Sensor, Business Logic and Relational database components. These components were broken down further into specialized sub-components such as hardware device driver, middleware and Arduino Libraries. Others are hardware components including Wifi (ESP8266) Module, Gas Sensor (MQ2) Module, Liquid Crystal Display (LCD) and Temperature Sensor (DHT11) Modules. Device drivers and Arduino libraries define operating parameters of various component connected to the Microcontroller. Each device is connected to the Computer and Microcontroller Systems has its own driver that administers its operations. Middleware application acted has an adapter between application and System Components. Figure 8 shows the developed application design Architecture:

DOI: 10.31695/IJASRE.2022.8.4.9

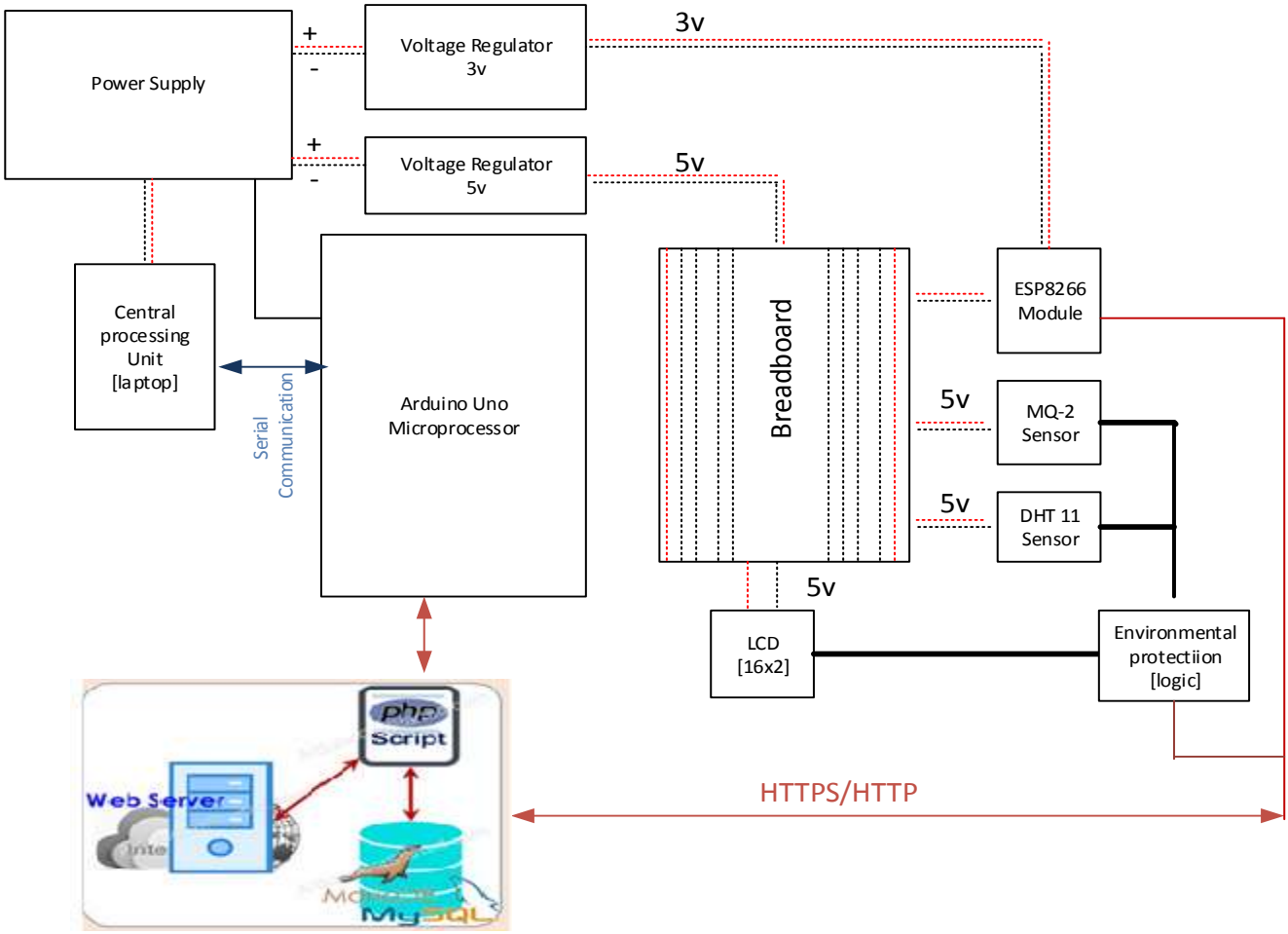


Figure 8: Application Design Architecture

8.1 Central Processing Unit (CPU)

CPU is described as the component of a computer that retrieves and executes instructions. The Arduino and its components are connected to the CPU. In this project, the CPU (laptop) provides power source and the visual display unit through serial port. CPU also provides means of host the MySql database management systems (DBMS). In physical architecture, CPU is described as the component of a computer that retrieves and executes instructions. However, in cloud based architecture, it is referred to as a physical server or data centre. Data centre is associated with computer system components that include physical and logical components for the provision of telecommunication and storage services.

8.2 Database

The database component is responsible for data storage. The database consists of relational which are physical structures responsible for data storage. A relation or table is broken further into attributes, constraints and relationships. The collection of tables attributes and relationship in relational database is referred to as database schema[41]. The table in the relation database is manipulated by script. A script is written in any script language. In this case Python programming language on pyCharm environment was employed. Arduino Microcontroller and sensors has registers responsible to store sketches that control the operations of each sensor. Arduino IDE is responsible for sketch generation, compilation and uploading operation.

8.3 Microcontroller

Our study employed Arduino Uno microcontroller. Arduino Uno is a microcontroller panel based on the ATmega328P [42]. It has 14 digital input/output pins, 6 analogy inputs and a 16 MHz quartz crystal. It contains many micro components required to support the microcontroller. Arduino was connected to the CPU (computer system) with a USB cable in order to power-up various sensor elements on the breadboard.

DOI: 10.31695/IJASRE.2022.8.4.9

8.4 Breadboard

A breadboard is a solderless panel for wiring various sensors on microcontroller board. Breadboards consists of operational areas called strips, and are often separated from the middle portion[43] . The breadboard has strips of metal underneath the board and connects the holes on the top of the board. Various sensors are connected to Arduino microcontroller employing breadboard panel.

8.5 Liquid Crystal Display (LCD)

The LCD is connected to Arduino microcontroller. LCD screen can be described as an electronic display module that uses liquid crystal to produce a visible image. There are many types of Arduino LCD screen. In this project 16×2 LCD display was employed. It translates and displays 16 characters per line in two lines. Each LCD character is displayed in a 5×7 pixel matrix.

8.6 ESP8266 Wi-Fi

The **ESP8266** is a very user friendly and low cost device to provide internet and Network connectivity to the IoT project [44]. The module has abilities to work as an Access point, station or both. It can also fetch data from internet using API's hence this project could access any information that is available on the internet, thus making it smarter. The module can also be programmed using the Arduino IDE which makes it a lot more user friendly. However, ESP8266 module has only 2 GPIO pins, hence limited in functionality as compared to ESP-12 or ESP-32 versions and many other WI-FI Modules.

8.7 Temperature Sensor (DHT11)

Extreme Temperature and humidity contribute extensively to global warming and consequently climate change. To monitor temperature and humidity parameters in Industrial IoT CI environment, DHT11 sensor was employed. DH11 sensor is a digital sensor that comes with dedicated NTC to measure temperature and an 8-bit microcontroller to output the values of temperature and humidity as serial data[44]. This type of sensor is factory calibrated and easy to interface with other microcontrollers. DHT11 sensor is capable of measuring temperature from 0°C to 50°C and humidity from 20% to 90% with an accuracy of ±1°C and ±1%.

8.8 Gas Sensor

Toxic emitted gases from industrial processes negatively affect healthy of environment and workers in industrial IoT CI environment and generally considered as a key security requirement in CI security provision. In this project, Arduino MQ2 sensor was employed to detect leakage of toxic gases due to industrial processes. It is based on Metal Oxide Semiconductor (MOS) or S_no_2 known as Chemiresistors [39] **.** It is called Chemiresistor, because the detection of gases is as the result of changing resistance of the sensing material when the Gas comes in contact with the LGP substances. By employing simple voltage divider network, concentrations of gas can be detected. MQ2 sensor senses the inflammable gases present in the sample, the oxidization of gases resulting in increased temperature and resistance of a sensor resistor will reduce. That means more current and voltage will flow through the load resistor. At normal environment conditions (no LPG in the air), the sensor resistor is normally very high around 850K and voltage drop across the load resistor to around zero reading. When the sensor is fully exposed to LPG, its resistance drops to around 800 ohms and the voltage drop across the load resistance to around 4.62 volts. MQ2 Gas sensor works on constrained environment take in input voltage of 5V DC and draws around 800mW. MQ2 sensor can detect LPG, Smoke, Alcohol, Propane, Hydrogen, Methane and Carbon Monoxide concentrations anywhere from 200 to 10000ppm [43].

9. SENSOR PROCESS ALGORITHMS

The process model for the developed environmental monitoring system in Access Control Role Requirements are divided into two process mechanics; the process that discern live atmosphere temperature and humidity and the process that sense live toxic gases emitted in to the atmosphere due to industrial processes and activities:

9.1 Temperature and humidity Sensing

The temperature sensor detects moisture by measuring the electrical resistance between two electrodes. The humidity sensing component is a moisture holding substrate with electrodes applied to the surface. When water vapour is absorbed by the substrate, ions are released by the substrate which increases the conductivity between the electrodes. The change in resistance between the two electrodes is proportional to the relative humidity. Higher relative humidity decreases the resistance between the electrodes, while lower relative humidity increases the resistance between the electrodes. Relative humidity can be calculated as shown in equation 1:

DOI: 10.31695/IJASRE.2022.8.4.9

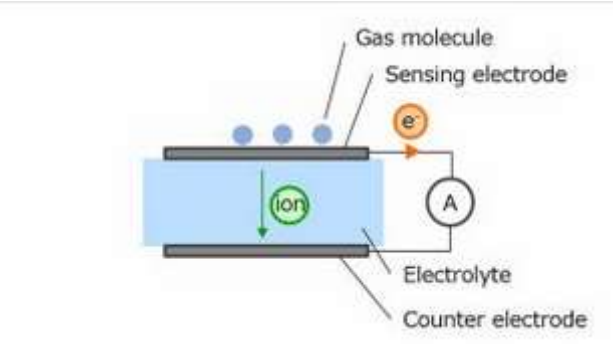
$$RH = \left(\frac{Pw}{p_s}\right) x\ 100\ \% \quad \text{..... (1)}$$

Where

RH: Relative Humidity, P_w density of water and P_s Density of water vapor of saturation

9.2 Gas Sensing

MQ2 sensor uses electrochemical typical gas method of detecting toxic gases. Electrochemical gas sensor uses oxidation and reduction reaction processes to measure gas concentration[45]. Generally, N-type metal oxide, such as Tin and Zinc oxide are used for the metal oxide where gas is observed. Toxic sensor is a surface controlled gas sensor and is based on the chemical reaction of Tin Oxide [43]. This chemical absorption process can therefore, be explained as indicated in figure 9 and equation 2 to 8. It is also described in step1 to step 4.



Source:[45]

Figure 9: Electrochemical gas of sensing mechanism

(I) **Step1**. When toxic gas sensor is exposed to air, oxygen molecules is absorbed on the surface of the Tin oxide nanostructures and capture electrons from the conduction band of N-type metal oxide to generate chemisorbed oxygen species as shown in chemical reactions of chemical equations 2, 3, 4 and 5.

$$O^2\ (gas) \leftrightarrow O^2\ (ads) \quad \text{.....,... (2)}$$

$$O^2\ (ads) + e^- \leftrightarrow O^{2-}(ads)\ (T < 150{\circ}C) \quad \text{..... (3)}$$

(II) **Step2.** When the sensor contacts with emitted toxic gas, its resistance changes according to the oxidation or reduction characteristics of the gas as shown in equations 4 and equation 5.

$$O^{2-}(ads) + e- \leftrightarrow 2O^-(ads)\ \ (150{\circ}C < T < 400{\circ}C) \text{.....(4)}$$

$$O^-(ads) + e^- \leftrightarrow O^{2-}(ads)\ (T > 400{\circ}C) \text{.....(5)}$$

(III) **Step 3**: If sensor material surface comes into contact with a reducing gas, the reducing gas will react with oxygen anions to produce carbon dioxide and water, and the resulting electrons will return to the conduction band of the semiconductor. This process model is as indicated in equations 6,7 and 8 :

$$C6H5CH3 + 18O- \rightarrow 7CO2 + 4H2O + 18e- \text{.....(6)}$$

$$HCHO + 2O- \rightarrow CO2 + H2O + 2e- \text{.....(7)}$$

$$C3H6O + 8O- \rightarrow 3CO2 + 3H2O + 8e- \text{.....(8)}$$

(IV) **Step 4**: Finally restored to the air environment, the sensor returns to its original state.

DOI: 10.31695/IJASRE.2022.8.4.9

10. ENTITY RELATIONSHIP (ER) DIAGRAM

An Entity–Relationship (ER) Model was used to define the data or information characteristics of a business domain or its process requirements. The ERD in abstract may lends to ultimate implementation in the relational database. The main components of ER models are entities (things), Attributes and their relationships. An entity is any person, place, thing, or event of interest to the CI organisation and about which data are captured, stored, or processed. ER diagrams also are often used in conjunction with data flow diagrams (DFDs), which map out the flow of information for processes or systems The ER diagram of the study consisted entities as shown in figure 10.

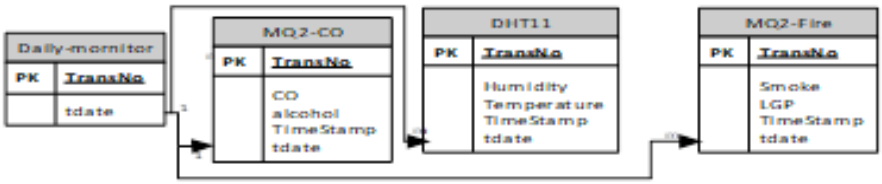


Figure 10: ERD Schema

11. CONFIGURATION

The configuration section of this study is divided into two aspects include relational database configuration and business logic configuration. In this methodology business logic configuration is also referred to sketch configuration. Database Configuration involves range of activities starting from database parameter settings, creating or change objects and attributes, and customizing the database itself. An object is a self-contained software entity that consists of both data and functions to manipulate data. Most applications are associated with two thing main object and related objects. When you use the Database Configuration application, you interact at the business object level. Inside, the application determines the actions to take on the database tables to support the needs of business objects. While Software Configuration is described as systematically manage, organize, and control the changes in the documents, codes, and other entities during the Software engineering Development process. The primary goal of application engineering configuration process is to increase productivity with minimal mistakes.

11.1 Relation Configuration

The database for the developed Environmental Monitoring Mechanism is based on the relational database concepts. The relational database is managed by the RDBMS. Any relational database consists of one or more data relations linked together through keys and relationships. The tables, keys, and relationships are the three core components of a relational database. Tables are made up of rows and columns and are used to store data. Rows represent individual entities in a table where columns represent their attributes and data types. As already stated, MySQL database is an open source application and runs on XAMP sever. The developed database schema consist various database entities, attributes, relationships. The development environment adopted to create access control database for Industrial IoT CI physical security hardening mechanism is XAMPP. **XAMPP** is one of the most famous web development platforms. The major advantage of XAMPP over the other web environments is that, it helps developers to configure a local server which is fully equipped with all necessary tools. Furthermore, XAMPP is a totally free and very simple to install on any operating system. Figure 11 shows control panel for the XAMPP web development Platform.

DOI: 10.31695/IJASRE.2022.8.4.9

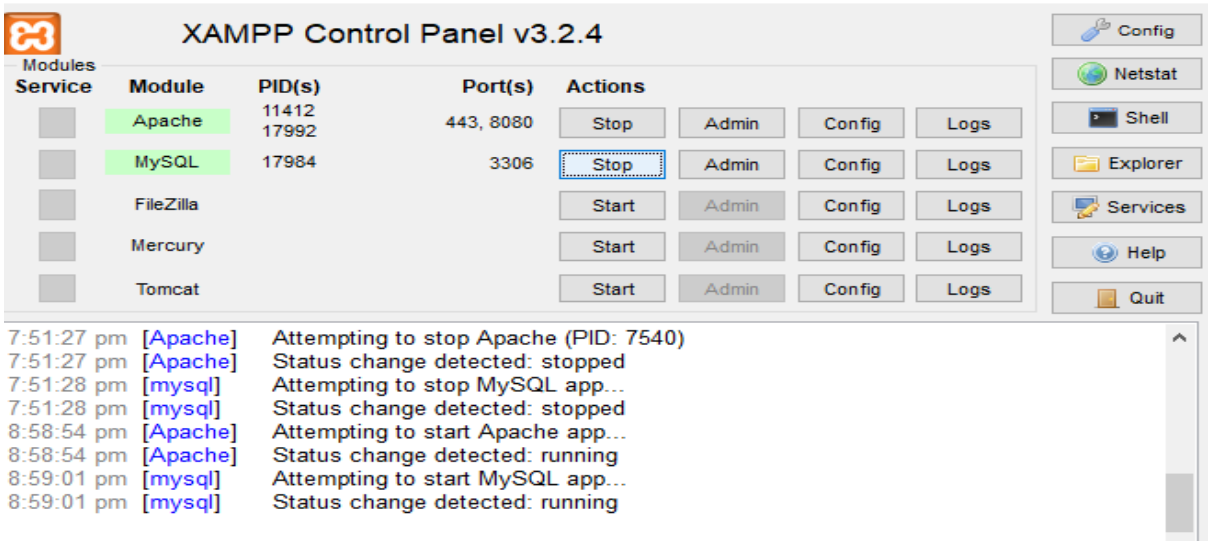


Figure 11: Figure XAMP Control Panel

11.2 Business Logic Configuration

In this project, there are two important programming language Environmental Configuration setup namely Arduino IDE and Python IDE programming Environment. Python is a powerful general-purpose programming language. It is used in many applications such as web development, data science, creating software prototypes, and so on[46]. It has simple syntax. Programs written using Arduino Software (IDE) are called **sketches**. Arduino Sketches are the practical guide to microcontroller programming. These sketches are written in the text editor and are saved with the file extension dot ino (.ino). While Python program are saved with the file extension dot py (.py). The editor has configurable features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right hand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor. The Arduino development board comes with an embedded processor and sockets that allow you to quickly attach peripherals without tools or solders. It's easy to build, easy to program, and requires no specialized hardware[47]. There are many sketches and programs in this project. But the most important ones includes (I) Sketch for Temperature and Humidity Sensing, (II) program to Insert Temperature and Humidity in the Database Relation, (III) Sketch for smoke and CO_2 Sensing and finally (IV) program to insert Smoke and CO_2 into MySQL database relation.

(I) **Sketch for Temperature and Humidity Sensing:** DHT11 sensor was connected to Arduino Uno microcontroller to read temperature from Industrial IoT CI environment. Live temperature and humidity is displayed on LCD screen and consequently inserted into the relational database using python script as highlighted below:

```
#include <dht.h>
#include <LiquidCrystal.h>
#define outPin 8
const int rs = 12, en = 11, d4 = 5, d5 = 4, d6 = 3, d7 = 2;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);
dht DHT
void setup() {
Serial.begin(9600),
lcd.begin(16, 2);
}
void loop() {
int readData = DHT.read11(outPin);
float t = DHT.temperature;
float h = DHT.humidity;
lcd.setCursor(0,0);
lcd.print("Temperature =");
```


DOI: 10.31695/IJASRE.2022.8.4.9

```
lcd.print(t);
lcd.setCursor(0,1);
lcd.print("Humidity = ") ;
Serial.print(h);
lcd.print(h);
Serial.print(" ");
Serial.print(t);
Serial.println("\t ");
lcd.println("% ");
lcd.println("") ;
delay(2000); // wait two seconds
}.
```

(II) **Program to insert Smoke and CO2 into MySQL database relation:** Once data is capture on LCD. Serial port is read and data encoded in the specific format and then inserted into php my phpmyadmin table. The Python code to perform that action is as highlighted below:

```
import serial
import MySQLdb
import time
dbConn=MySQLdb.connect("localhost", "root","","critical")or die(" Could not connect to database")
cursor = dbConn.cursor()
device = 'COM7'
try:
print("Trying..."),device
arduino = serial.Serial(device,9600)
except:
print ("Failed to connect on"),device
try:
time.sleep(1)
data=arduino.readline().decode("utf-8")
print (data)
pieces = data.split( )
try:
cursor.execute("INSERT INTO dht11 (humidity,temperature )VALUES(%s,%s)",(pieces[0],pieces[1]))
dbConn.commit()
cursor.close()
except MySQLdb.IntegrityError:
print ("failed to insert data")
finally:
```

(III) **Sketch for smoke and CO_2 Sensing**. MQ2 gas sensor detects the concentration of gases in the air such as Smoke and CO_2.

```
#include<MQ2.h>
#include <LiquidCrystal.h>
#define outPin 8
const int rs = 12, en = 11, d4 = 5, d5 = 4, d6 = 3, d7 = 2;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);
int gs= A0;
int smoke;
MQ2 mq2(gs);
void setup()
{
Serial.begin(9600);
mq2.begin();
lcd.begin(16, 2);
```


DOI: 10.31695/IJASRE.2022.8.4.9

```
}
void loop()
{
smoke = mq2.readSmoke();
if ( smoke > 1)
{
Serial.print(" There is Smoke");
Serial.print("SMOKE: ");
Serial.println(smoke);
lcd.print("SMOKE: ");
lcd.println(smoke);
}
Serial.print("SMOKE: ");
Serial.println(smoke);
lcd.print("SMOKE: ");
lcd.println(smoke);
delay(1000);
}
```

(IV) **Insert CO2 into MySQL database relation**: Detected sensor data is inserted into MySQL database using python script shown below.

```
import serial
import MySQLdb
import time
dbConn=MySQLdb.connect("localhost", "root","","critical")or die(" Could not connect to database")
cursor = dbConn.cursor()
device = 'COM7'
try:
print("Trying..."),device
arduino = serial.Serial(device,9600)
except:
print ("Failed to connect on"),device
try:
time.sleep(1)
data=arduino.readline().decode("utf-8")
print (data)
try:
cursor.execute("INSERT INTO smoke(smoke1)VALUES(%s)",(smoke1))
dbConn.commit()
cursor.close()
except MySQLdb.IntegrityError:
print ("failed to insert data")
finally:
cursor.close()
except:
print ("Failed to get data from Arduino!")
```

12. RESULTS

In the result, the first screenshot show the general configuration of the project aimed at monitoring environmental hazardous substances. As stated already, the result of the study included created database for storing environmental monitored dataset. The dataset included the relations for storing live readings from DHT11 and MQ2 Sensors. But before that, the project configuration was modelled that powered the system with practical capabilities of five common and inseparable components for IoT functionality and deliverables. These include[48].

DOI: 10.31695/IJASRE.2022.8.4.9

(I) **Sensors and Actuator:** connecting the physical object to different computer systems;
(II) **Connectivity**: the network is essential to connect the object to the Internet (Wifi, wired, 4G or soon 5G...);
(III) **Data:** The main purpose of IoT is to collect and transmit data;
(IV) **Information:** Translating data into information is essential to be able to read and then exploit the data;
(V) **Operating applications**: allowing you to control IoTs but also to read the information you receive.

The idea is to create a big data for hazardous environmental conditions for analysis and scientific projection. The screenshot 1 to 8 shows environmental protection module start from the results of physical environmental Monitoring Architecture configuration and the results of environmental protection module. Figure 12 show the architecture of environmental protection module:

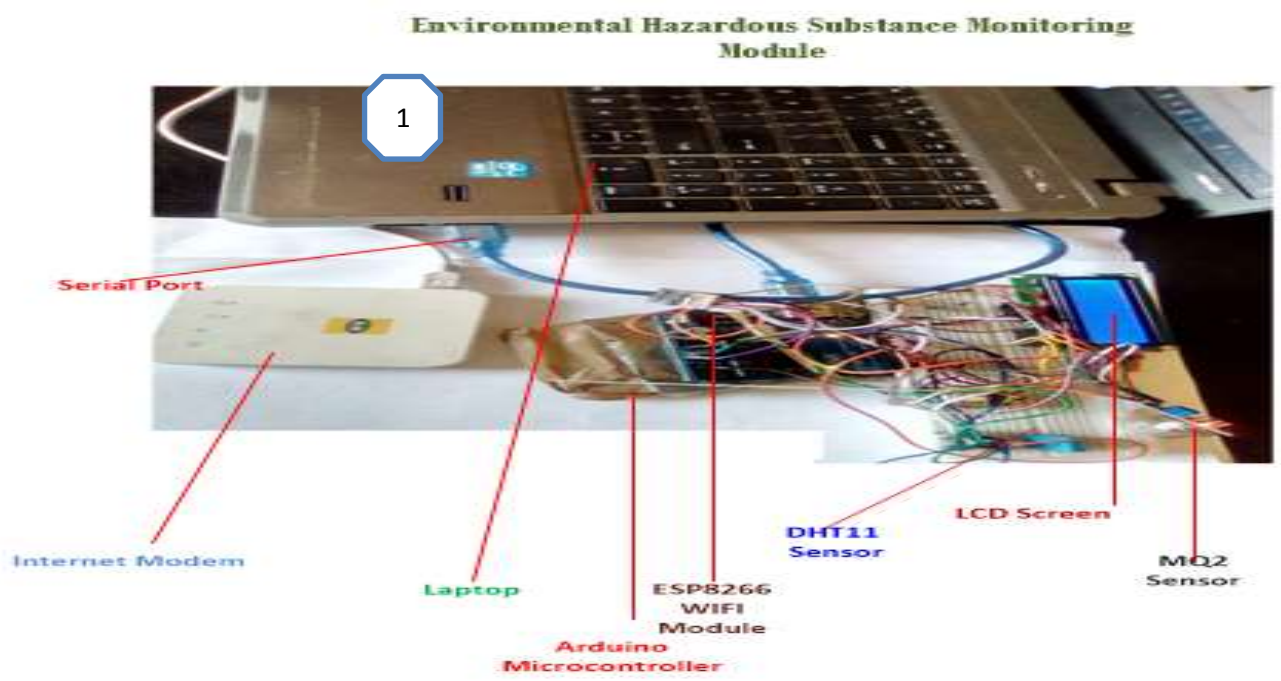


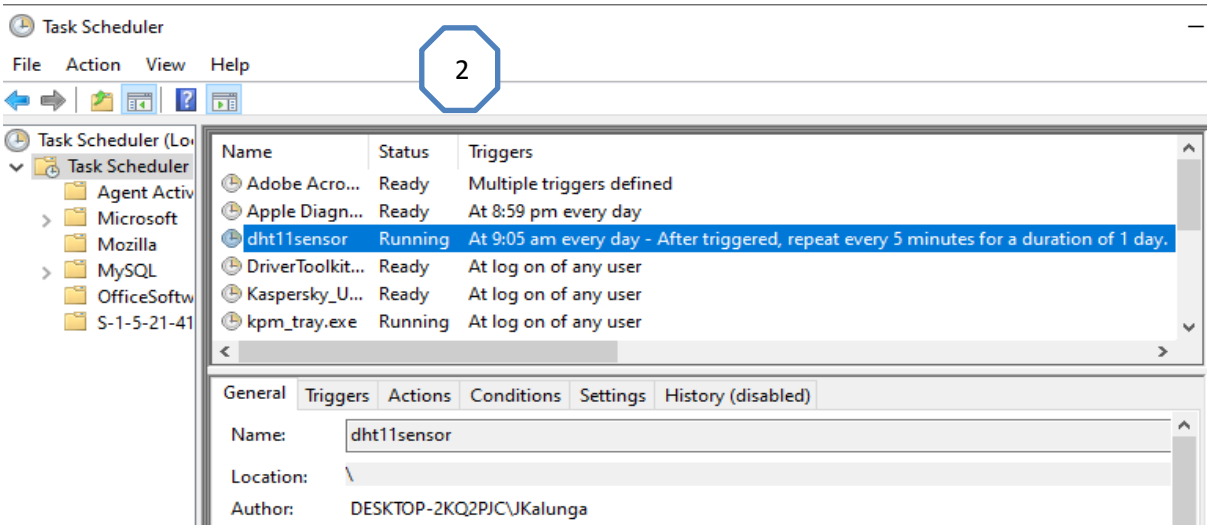
Figure 12: Environmental Monitoring Architectural Configuration

Environmental protection physical architecture included the following IoT components:

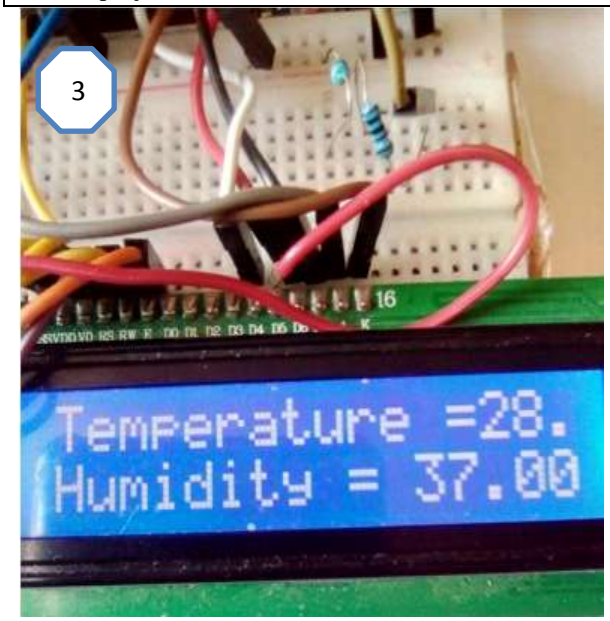
(I) **Laptop:** Provide 5 volts to power on Microcontroller and connected sensor network. .
(II) **Arduino Uno:** The Microcontroller of this module. It coordinates various sensor Networks processes.
(III) **Internet Modem:** Provided internet connectivity to the module. The module as a gateway for email security alert messages.
(IV) **ESP8266 Module:** Wifi module provides IoT connectivity Capabilities.
(V) **DHT11:** Digital temperature sensor
(VI) **LCD Screen:** Visual display screen for module. Other display module is serial monitor
(VII) **MQ-2:** Toxic Gas Sensor.

DOI: 10.31695/IJASRE.2022.8.4.9

TASK SCHEDULER



Sensors data collection was automated and inserted continuously into MySQL data table after five minutes. If hazardous condition are detected the email is scrabbled automatically and alert the security team. To achieve this deliverable windows OS task schedule was employed. Task schedule was creation result is shown in screenshot 3.



Temperature & Humidity Display on LCD Screen

Scheduler Automatically capture Data from sensors DHT11 Sensors

DOI: 10.31695/IJASRE.2022.8.4.9

id ▲ 1	humidity	temperature	date
67	38	28	2021-10-24 08:52:16
68	37	28	2021-10-24 09:10:43
69	36	27	2021-10-24 09:13:36
70	37	28	2021-10-24 09:15:41
71	37	28	2021-10-24 09:20:41
72	37	28	2021-10-24 09:25:41
73	37	28	2021-10-24 09:30:41
74	38	29	2021-10-24 09:35:41
75	38	28	2021-10-24 09:40:44
76	37	28	2021-10-24 09:45:41
77	37	29	2021-10-24 09:50:41
78	36	29	2021-10-24 09:55:41
79	36	29	2021-10-24 10:00:41
80	35	28	2021-10-24 10:05:41

5

Snapshot of dataset of Temperature & Humidity in relational table

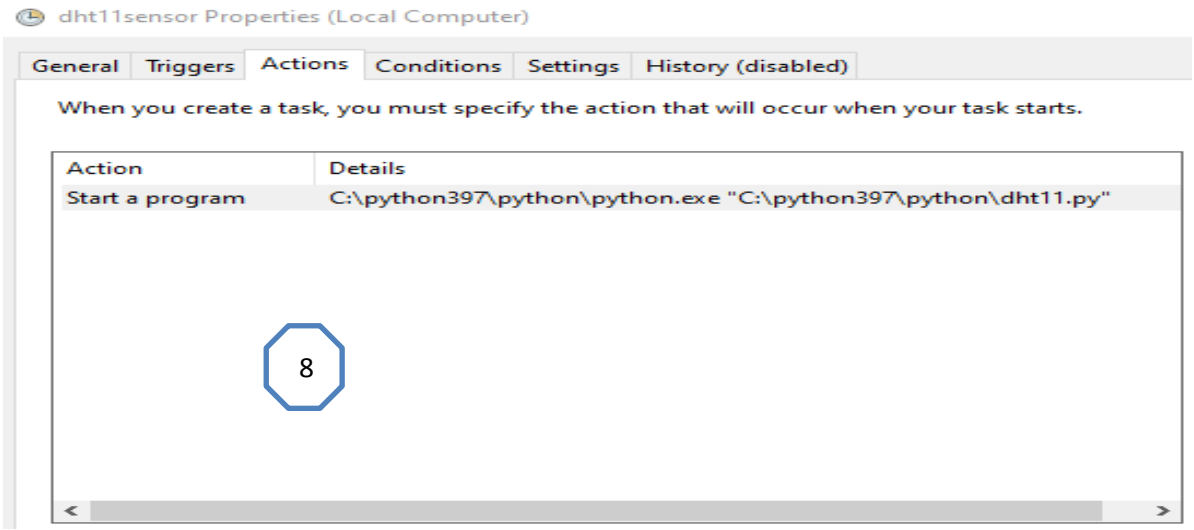
Smoke & Fire

```
Sensor Value: 121.00
Sensor Value: 121.00
Gas sensor initialisation Process!
Sensor Value: 118.00
Sensor Value: 121.00
Sensor Value: 128.00
Sensor Value: 200.00
Sensor Value: 578.00 | Smoke detected! | Security threat alarm initiated

Sensor Value: 552.00 | Smoke detected! | Security threat alarm initiated

Sensor Value: 380.00 | Smoke detected! | Security threat alarm initiated
```

7

Smoke detected using serial monitor

DOI: 10.31695/IJASRE.2022.8.4.9



DHT11 Sensor created Task in task schedule to automate sensing process

Screenshot of detected LPG, CO and smoke

13. CONCLUSIONS

The paper presented the development of environmental monitoring system. The developed application operated at environmental layer of physical security. This system was designed and developed to harden environmental security in Industrial IoT CI Institution. Cheaper Ecological Sensor Networks were employed on Arduino Technology. Comparative studies on the related application were conducted especially in Industrial IoT CI institution. During the study, it was discovered that similar systems were developed and implementation in different organisation and different System Requirements, specification and deliverables. However, environmental security in access control role has not yet been integrated into broad Industrial IoT CI institution security needs. Many manufacturing CI industries neglect environmental security requirement out of their security needs and concentrate on implementing Cyber (logical) and physical security requirements[49]. However, the catastrophic consequences of neglecting environmental security have disastrous concerns citing climate Change and its negative effects to humanity and other living things. Considering that toxic pollution affects millions of people around the world, and contributes about 5.4 percent deaths worldwide. The implication is that, Pollution resulting from industrial activities and processes kills more people than malaria, AIDS and tuberculosis combined. The developed system if implement in CI industries like smart manufacturing, power generating plant, nuclear plant, cement processing plant, military industry and many other can improve environmental security in Industrial IoT installation and surrounding areas.

DOI: 10.31695/IJASRE.2022.8.4.9

.

14. FUTURE WORKS

The developed mechanism detects only emission of CO2, CO and Smoke. Even though, gases like CO_2 support living organisms, it is also a pollutant, generated mostly by human activities such as deforestation and the fossil fuel combustion due to industrial processes. Additionally, there are many dangerous gases which pollute the environment like methane, nitrous oxide, nitrogen, Sulphur oxide etc. While these gases are not the only ones contributing to air pollution, they represent the dominant sources of this world-wide climate problem. The prototype can be extended to detect other gases that cause damage to the environment. This extension includes those gases not mentioned in this paragraph but produced due to industrial processes. The other areas that urgently need research attention include:

(I) Conduct the research on modalities of regulating the amount CO_2 that is released in the atmosphere only for plant consumption. CO2 support living organisms such as plants in growing.
(II) Formulation legislation to mitigate Climate Change.
(III) Framework of integrating environmental security in Access Control
(IV) Ascertaining the correct quantities of hazardous gases to be produced in the atmosphere without causing climate change.

REFERENCES

[1] Sphera, 'What Is Environmental Sustainability?', *May 19, 2020*, 2020. [Online]. Available: https://sphera.com/glossary/what-is-environmental-sustainability/. [Accessed: 09-Feb-2022].

[2] D. M. N. Rajkumar, S. M. S, and D. V. V. Kumar, 'IOT Based Smart System for Controlling Co2 Emission', *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 2, pp. 284–288, 2017, doi: 10.13140/RG.2.2.26703.33444.

[3] WHO, 'Climate change and health', *30 October 2021*, 2021. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/climate-change-and-health. [Accessed: 09-Feb-2022].

[4] M. Sherrard, 'Gases That Cause Air Pollution', *April 30, 2018*, 2018. [Online]. Available: https://sciencing.com/gases-cause-air-pollution-7445467.html. [Accessed: 01-Mar-2022].

[5] J. Kalunga, S. Tembo, and J. Phiri, 'Development of Access Control Mechanism Based on Fingerprint Biometrics and Mobile Phone Identity for Industrial Internet of Things Critical Infrastructure Protection', vol. 6, no. 12, pp. 15–34, 2020, doi: 10.31695/IJASRE.2020.33940.

[6] T. P. Raptis, A. Passarella, and M. Conti, 'State of the Art and Open Challenges', *IEEE Access*, vol. PP, p. 1, 2019, doi: 10.1109/ACCESS.2019.2929296.

[7] J. Kalunga, S. Tembo, and J. Phiri, 'Industrial Internet of Things Common Concepts , Prospects and Software Requirements', vol. 9, no. 1, pp. 1–11, 2020, doi: 10.5923/j.ijit.20200901.01.

[8] C. Petrov, '49 Stunning Internet of Things Statistics 2021 [The Rise Of IoT]', *Techjury.net*, 2021. [Online]. Available: https://techjury.net/blog/internet-of-things-statistics/#gref. [Accessed: 03-Feb-2022].

[9] S. G. Abbas, F. Hashmat, and G. A. Shah, 'A multi-layer industrial-iot attack taxonomy: Layers, dimensions, techniques and application', *Proc. - 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020*, pp. 1820–1825, 2020, doi: 10.1109/TrustCom50675.2020.00249.

[10] G. Kamieniecky and J. Bennet, 'Emerging use of Industrial Internet of Things (IIoT)', 2019.

[11] European Environment Agency, 'Environment in the European Union at the turn of the century- 3.1. Greenhouse gases and climate change', pp. 79–98, 1999.

[12] C. International, 'Carbon emission tax', *2018*, 2018. [Online]. Available: https://cuts-lusaka.org/carbon-emission-tax/. [Accessed: 02-Mar-2022].

[13] H. Panchasara, N. H. Samrat, and N. Islam, 'Greenhouse gas emissions trends and mitigation measures in australian agriculture sector—a review', *Agric.*, vol. 11, no. 2, pp. 1–16, 2021, doi: 10.3390/agriculture11020085.

[14] Y. S. Kalinin, E. K. Velikov, and V. I. Markova, 'Design of Indoor Environment Monitoring System Using Arduino', *Int. J. Innov. Sci. Mod. Eng.*, no. 7, pp. 2319–6386, 2015.

DOI: 10.31695/IJASRE.2022.8.4.9

[15] J. Kalunga and S. Tembo, 'Development of Fingerprint Biometrics Verification and Vetting Management System', *Am. J. Bioinforma. Res.*, vol. 6, no. 3, pp. 99–112, 2016, doi: 10.5923/j.bioinformatics.20160603.01.

[16] P. Samarati and S. De Capitani, 'Access Control : Policies , Models , and', pp. 137–196, 2001.

[17] I. Indu, P. M. R. Anand, and V. Bhaskar, 'Identity and access management in cloud environment: Mechanisms and challenges', *Eng. Sci. Technol. an Int. J.*, vol. 21, no. 4, pp. 574–588, 2018, doi: 10.1016/j.jestch.2018.05.010.

[18] S. Ameer, J. Benson, and R. Sandhu, 'An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach', *Information*, vol. 13, no. 2, p. 60, 2022, doi: 10.3390/info13020060.

[19] G. Feulner, 'Global Challenges: Climate Change', *Glob. Challenges*, vol. 1, no. 1, pp. 5–6, 2017, doi: 10.1002/gch2.1003.

[20] J. Kalunga, 'INTEGRATING FINGERPRINT BIOMETRICS SYSTEM INTO THE', University of Zambia, 2015.

[21] K. M. Baina a, Deswart Y, 'Chapter 14 COLLABORATIVE ACCESS CONTROL FOR CRITICAL INFRASTRUCTURES', *Int. Fed. Inf. Process.*, vol. 290, no. Critical Infrastructure Protection II, pp. 189–201, 2008.

[22] R. Belguechi, E. Cherrier, V. Alimi, P. Lacharme, and C. Rosenberger, 'An Overview on Privacy Preserving Biometrics', *Recent Appl. Biometrics*, no. July, 2011, doi: 10.5772/19338.

[23] K. Dragerengen, 'Access Control in Critical Infrastructure Control Rooms using Continuous Authentication and Face Recognition', no. June, 2018.

[24] H. L. Gawand, A. K. Bhattacharjee, and K. Roy, 'Online Monitoring of a Cyber Physical System Against Control Aware Cyber Attacks', *Procedia Comput. Sci.*, vol. 70, pp. 238–244, 2015, doi: 10.1016/j.procs.2015.10.079.

[25] D. Belfadel, M. A. Rodriguez, M. Zabinski, and R. Munden, 'Use of the Arduino platform in fundamentals of engineering', *ASEE Annu. Conf. Expo. Conf. Proc.*, 2019, doi: 10.18260/1-2--33491.

[26] H. Timmis, *The Process of Arduino Engineering. In: Practical Arduino Engineering.* CA, 2012.

[27] B. Aston, '10 Best Requirements Management Tools & Software Of 2022', *2022*, 2022. [Online]. Available: https://thedigitalprojectmanager.com/tools/requirements-management-tools/. [Accessed: 29-Mar-2022].

[28] N. Nhede, 'Industry believes IIoT applications "essential to sustainability"', *Feb 11, 2022*, 2022. [Online]. Available: https://www.smart-energy.com/industry-sectors/iot/industry-believes-iiot-applications-essential-to-sustainability/. [Accessed: 18-Feb-2022].

[29] A. Ben Youssef, 'How Can Industry 4.0 Contribute to Combatting Climate Change?', *cain.Info*, 2020. [Online]. Available: https://doi.org/10.4000/rei.8911. [Accessed: 25-Aug-2021].

[30] M. A. Moritz *et al.*, 'Climate change and disruptions to global fire activity', *Ecosphere*, vol. 3, no. 6, p. art49, 2012, doi: 10.1890/es11-00345.1.

[31] A. M. Abhilash Panda, nicholas j Ramos, 'Making Critical Infrastructure Resilient Ensuring Continuity of Service Making Critical Infrastructure Resilient', *UNDRR*, 2020.

[32] H. Derhamy, 'Architectural Design Principles For Industrial Internet of Things', Lulea University of Technology, 2018.

[33] M. Burhan and R. A. Rehman, 'IoT Elements , Layered Architectures and Security Issues : A Comprehensive Survey', pp. 1–37, 2018, doi: 10.3390/s18092796.

[34] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, 'IoT elements, layered architectures and security issues: A comprehensive survey', *Sensors (Switzerland)*, vol. 18, no. 9, 2018, doi: 10.3390/s18092796.

[35] R. de Oliveira Albuquerque, L. J. García Villalba, A. L. Sandoval Orozco, F. Buiati, and T. H. Kim, 'A layered trust information security architecture', *Sensors (Switzerland)*, vol. 14, no. 12, pp. 22754–22772, 2014, doi: 10.3390/s141222754.

[36] A. Henderson, 'The CIA Triad: Confidentiality, Integrity, Availability', *2019*, 2019. [Online]. Available: http://panmore.com/the-cia-triad-confidentiality-integrity-availability. [Accessed: 29-Jun-2021].

[37] J. Al-Jaroodi, I. Jawhar, A. Al-Dhaheri, F. Al-Abdouli, and N. Mohamed, 'Security middleware approaches and issues for ubiquitous applications', *Comput. Math. with Appl.*, vol. 60, no. 2, pp. 187–197, 2010, doi: 10.1016/j.camwa.2010.01.009.

DOI: 10.31695/IJASRE.2022.8.4.9

[38] GeeksForGeens, 'Unified Modeling Language (UML) | Activity Diagrams', *GeeksForGeens*, 2018. [Online]. Available: https://www.geeksforgeeks.org/unified-modeling-language-uml-activity-diagrams/. [Accessed: 10-Sep-2020].

[39] B. Li, Q. Zhou, S. Peng, and Y. Liao, 'Recent Advances of SnO2-Based Sensors for Detecting Volatile Organic Compounds', *Front. Chem.*, vol. 8, no. May, pp. 1–6, 2020, doi: 10.3389/fchem.2020.00321.

[40] Q. Zhang, Q. Zhou, Z. Lu, Z. Wei, L. Xu, and Y. Gui, 'Recent advances of SnO2-based sensors for detecting fault characteristic gases extracted from power transformer oil', *Front. Chem.*, vol. 6, no. AUG, pp. 1–7, 2018, doi: 10.3389/fchem.2018.00364.

[41] P. Education and P. Addison-wesley, 'Chapter 9 Outline Relational Database Design Using ER-to- Relational Mapping Mapping EER Model Constructs to Relations', 2011.

[42] L. Louis, 'Working Principle of Arduino and Using it as a Tool for Study and Research', *Int. J. Control. Autom. Commun. Syst.*, vol. 1, no. 2, pp. 21–29, 2016, doi: 10.5121/ijcacs.2016.1203.

[43] M. Mahbub, 'Toxic and hazardous gas detection , measurement and monitoring system for safety assurance in home and industrial application of wireless sensor node Toxic and hazardous gas detection , measurement and monitoring system for safety assurance in home and in', *Eng. Technol. Res.*, no. August, pp. 089–098, 2019, doi: 10.15413/etr.2019.0108.

[44] T. Chennai, 'Humidity and Temperature Monitoring System using IoT', *Int. J. Eng. Adv. Technol.*, vol. 9, no. 2, pp. 1353–1356, 2019, doi: 10.35940/ijeat.b2569.129219.

[45] Asahi Kasei, 'Gas Sensors types and mechanism', *Asahi Kasei Microdevices Corporation*, 2018. [Online]. Available: https://www.akm.com/eu/en/products/co2-sensor/tutorial/types-mechanism/. [Accessed: 03-Oct-2021].

[46] S. Campbell, 'Python Tutorial for Beginners: Learn Programming Basics', *February 23, 2022*, 2022. [Online]. Available: https://www.guru99.com/python-tutorials.html. [Accessed: 23-Feb-2022].

[47] J. A. Langbridge, 'Arduino Sketches: Tools and Techniques for Programming Wizardry', *January 2015*, 2015. [Online]. Available: https://www.wiley.com/en-us/Arduino+Sketches%3A+Tools+and+Techniques+for+Programming+Wizardry-p-9781118919606. [Accessed: 23-Feb-2022].

[48] L. R. Team, 'IoT and Big Data: Understanding the relationship between these two technologies', *May 18, 2021*, 2021. [Online]. Available: https://ryax.tech/iot-and-big-data-understanding-the-relationship-between-these-two-technologies/. [Accessed: 04-Mar-2022].

[49] A. J. Kornecki, 'Safety and security in industrial control Safety vs . Security in Industrial Control', no. October, 2015.

DOI: 10.31695/IJASRE.2022.8.4.9