**IAIoT-SmartFarm**

The proposed work to develop is a research based on machine learning for cyber security purposes in an IoT (Internet of Things) system on a general Smart farm environment, this way It is of most importance to make a global study about topics mentioned then go to deeper knowledge and detail.

In this case some topics correlated to the proposed work about Smart farm, IoT, Cybersecurity, Artificial intelligence and Machine learning will be approached, some aspects will be discussed with more importance depending on its relevancy for the proposed work.

Later tests will be made to exploit the problems studied and solutions to the problem will be tested.

**1.Smart Agriculture**

**1.1-Definition**

Smart agriculture concept has been growing exponentially in the past decade in which involve traditional agriculture with advanced technology that help an agriculture environment to ensure its main goal: to increase agricultural output quantity while maintaining efficiency, productivity, and cost effectiveness.

They ease agriculture complexity by reducing human labor on certain activities, which need constant supervision and monitoring or help in tasks that cannot be handled by human hand replacing it with a solid building and interactive system.

There are used diversified types of technology overall, from physical devices and automated machines that operate in the field such as sensors, actuators, automated robots to information monitoring and remote access platforms that can visualize and monitor the farming environment,

**1.2-Real case example of a Smart Farm robot device**

For example: in paper [1] a modular automated, precisive agricultural robot was developed with the objective of applying selective types of pesticides with diverse quantity accordingly to the need in analyzed grapevines in a Farm, with possible remote access and control. All the components of the robot were integrated through electronics and communication framework architectures, It incorporates a robotic arm with a modulated design addressing multiple configurations for multiple applications and a precision spraying end-effector containing pesticide liquid spray generated based on real time data and configurated algorithms , the robot is provided with a disease sensing system that use several sensors for optical and Multispectral scanning purposes, this robot also has own operating system installed allowing connection and communication of the whole infrastructure and connectivity of all parts: a real time remote control unit hosted exteriorly with accessible interface, disease sensing system and manipulator robot arm. This modular agricultural robot is a demonstration example of what Smart Farm is, by providing automation, precision and efficiency on the field, also different levels of information and technology can interact to provide a better performance with software, hardware, networking, and data analysis support.



Figure-Modular agricultural robot executing functionalities on a vineyard

**1.3- Smart Farm environment technology**

Therefore, a smart farm architecture adopts an advanced infrastructure and innovative use of today´s existing technology to achieve and get more accurate and precisive approach to traditional farming.

Connection and communication from physical equipment or devices, to end users or remote interface platforms and internet, through heterogenous connections and communication protocols. Making what today´s technological trending that is nominated as IoT (Internet of Things).

In today´s agriculture environments it has been a growing on adaptation of this technology in agriculture, therefore physical devices, communication devices, connection devices, servers, information, data stored, communications established, and overall technologies used in Smart farming agriculture are vulnerable in Security in functionality and information integrity to the outsiders.

In consequence, there are and will be more challenges providing safe and secure application methods in smart agriculture sector in multiple ways due to the heterogenous types of devices and technology it constitutes.

**1.3- IoT technology on a Smart Farm**

There are enormous types of cyberattacks to different IoT systems, the ones redirected to a Smart Farm environment will be studied, with finality of finding a possible pattern in cyberattacks in this infrastructure,

posteriorly a possible solution will be attempted to be implemented with help of artificial intelligence methods and machine learning algorithms.

In a Smart Farm architecture there are certain layers with different functionalities and operate in different sequential and hierarchical domains. All of them are connected to making it an overall consistent Smart Farm environment.

All those layers combined make applications and services in an IoT Smart environment.

IoT information can be assembled or computed in distinct ways, it can be used local data processing devices such as: SoC (Single board Computers), microcontrollers machines that has processing capabilities and functionality to acquire information from hardware (sensors and readers) to process in field, generally end users are also able to interface with physically and extract data or input operation commands locally. That information combined with data exchanged from Network domain, allows sending and receiving information remotely to user entities on ethernet example, data can also be stored and analyzed in data centers and processed to Network. Those connections, communications, interactions, and data in a single point is nominated Gateway Node.

**2.IoT architecture**

A typical IoT architecture is configurated in a way of dividing and categorizing diverse types of technologies with different focus and functionalities. In a Smart Farm environment typical configuration of layer infrastructure design does not differ much from a general IoT System.

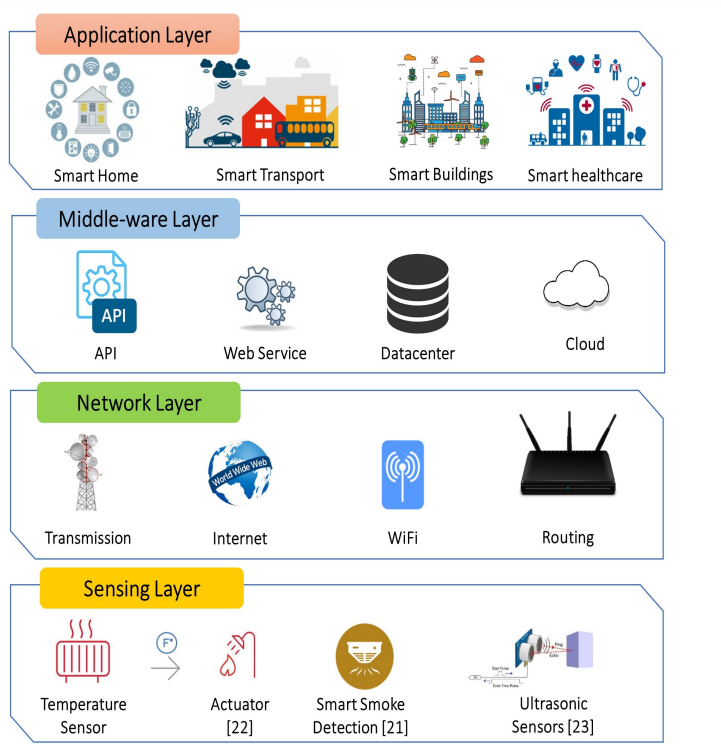


Figure- Typical 4 Layer architecture in an IoT System

On different IoT systems equivalent layer hierarchy can be referred in designation differently but, in the end, having similar or equal functionalities, a layer can even be divided into more layers, this way adopting a functionality of lower- or upper-layers hierarchy thus having a more concrete function in the system. In [2] layer names differ from [3] and [4] but layer order characteristics are very similar and have the same purpose in ecosystem. For example, in different articles some layers like “edge layer” is nominated “link layer”, “application layer” is similarly mentioned “service layer” or “sensing layer” referenced to “physical layer”, all in different papers.

In this analysis will be considered and proposed an infrastructure layer architecture with similarities to [3], also based on [2],[4].

In this article a 4-layer typology architecture will be used, that way information can be addressed in a convenient manner while covering system architecture with more details and functioning's than in a 3-layer basic IoT architecture.

*Smart farm layers can be divided into: Physical layer, Network layer, Processing layer and Application layer*.

More information and different topologies of IoT layer architecture can be find in [5].

**2.1-Physical layer:**

It consists of front-end hardware components that are used IoT system such as sensors, actuators, receivers, transmitters, controlled and automotive devices that operate directly with farm environment. Making connection controller devices that are responsible for operating field sensors.

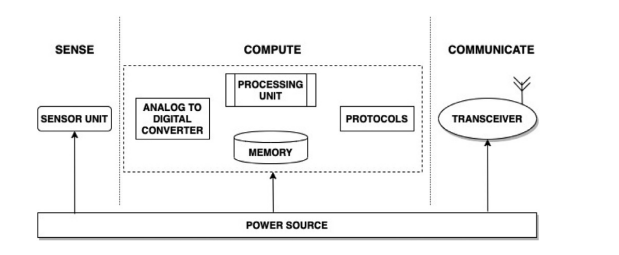
Physical parameters are measured directly providing environment measures such as Humidity, Precipitation, temperature, gas, etc.

Alternatively, information that is directly acquired can be processed or computed locally as well as providing local interface, leading to relieve processing power of upper layers in decisions making or processing certain farming inputs into data.

Generally, this layer is directly connected to Network Layer to where data is transmitted and received.

Bellow an illustration of a common physical Node sensor described in [2].

Where sensing is the sensors' function, compute is the controller device function locally and communicate to a Node Network.



**Figure-block diagram of local node sensor with 3 different tasks**

**2.2-Network layer:**

This layer is directly connected to physical, cloud layer and application layer being the main goal connectivity and communication between all layers.

There are used different data types of communications and different protocols and devices with ways of data transfer, where this layer is very important to establish connectivity in cross-layer manner between different devices.

Different nodes are established on certain sub-areas of Smart Farm where different nodes have different data aggregations and information on environment, typically coming from physical layer. Network Layer is responsible for communicating with nodes and layers establishing data sharing in a compatible way for all devices and data frames of Smart farm ecosystem.

**2.3-Processing layer:**

It is generally virtualized (not physically present) infrastructure and support Internet of things needs on data storage, data analysis and developing applications or security.

Smart Farm data and resources can be processed and managed in a way that physically would not be so convenient, allowing big data processing and extra external information gathering, also more heavy applications can be executed whereas in other layers it is not possible or convenient because of lack of resources or harder access.

In cloud it is also harder for information about the Smart farm to be accessed by unauthorized third parties due to internet and advanced protocol securities.

Cloud also has the functionality to provide remotely interaction and monitoring for the end user thus improving service quality and ensure that user have the whole Farm under surveillance with any device that support internet connection.

**2.4-Application layer:**

This layer is the closest to the end user and communicates providing services and interface by operating other layers ensuring that the user manages Smart farm through monitoring and controlling applications accessible in monitoring hardware or any supportable and compatible user end device.

This is example is a Scada (Supervisory Control and Data Acquisition) system with integrated wireless instrumentation [6] and exposed to the IoT environment, reducing their operational costs and related expenses

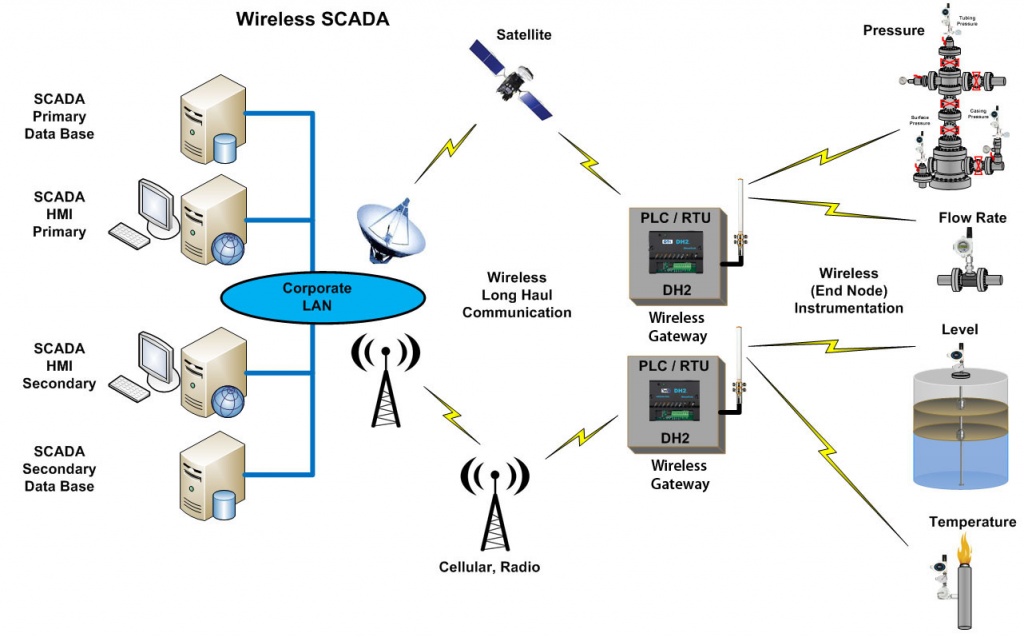


Fig- Scada system through Wireless Network Transmission involving multiple layers

**3.Communication and interaction between layers**

In each layer there are several types of devices, communications protocols, and overall connectivity between different layers, making possible automation, remote control, and monitoring on the entire ecosystem.

Below an example of a complete system that incorporates all layers categorized.

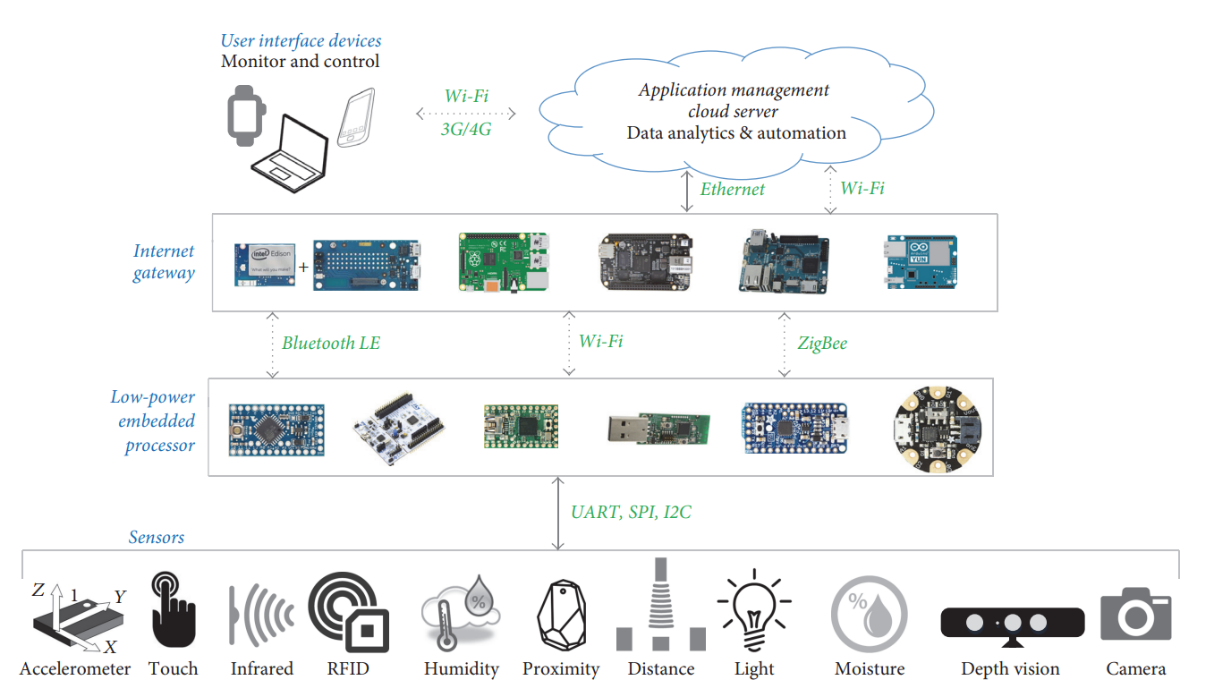


Fig-Proposed Layer architecture and connectivity in IoT [6.1]

**3.1-Standard protocols IoT:**

**3.1.1-COAP** (Constraint over the air protocol)-It is a lightweight protocol mainly used by soft hardware to communicate with wider internet services. Use Rest model architecture and use **UDP** protocol, and it is designed to easily translate to HTTP protocol for simplified integration with the web. It adopts DTLS (Datagram Transport Layer Security) similarly to **TLS** that will be talked further.

**3.1.2-MQTT** (Message queue Telemetry Transport): It is a lightweight Protocol that is based on a Publish/Subscribe mechanism architecture that allow multiple clients to connect to a broker and subscribe to multiple topics and publish messages getting access to that topic messages, it is also possible to subscribe to multiple topics in same broker It is often used in exchange between constrained devices and server applications scenarios, it also has the functionality of end-to-end communication and it has different levels of quality of service.

It is used **TCP/IP** transport protocol and can be secured through **TLS** (Transport Layer Security) encryption that will be talked further.

**3.1.3-HTTP** (Hyper Text Transport Protocol): It is a heavier protocol than MQTT and COAP but transmit larger size data payloads, It use Request and Response architecture between client and server, it does not guarantee message quality of service on message delivery. It is better used for web messaging in higher layers than to limited constraint devices. It also uses encryption standard like **TLS**

**3.2-Layer communications**

The most relevant and important communications made inside exterior or between layers will be briefly talked about due to the importance of it in pretended final developing work.

**3.2.1- Physical layer Communications:**

Several types of sensors actuators and general operating devices also use communications to acquire data or communicating with other local processing devices can on peer-to-peer connection.

Examples:

* RFID (Radio Frequency Identification Transmission)
* BLE (Bluetooth low energy)
* NFC (Near Field Coupling)

**3.2.1-Network layer Communications:**

Network layer is where the majority and important communications occur in an IoT ecosystem being the bridge that connects devices and services over transport protocols allowing connectivity of all layers to services and devices, further Fog layer architecture will also be one of the main focus on providing communication and data flow between layers, in this topology data is exchanged with physical, processing and application layers.

Important devices used for communication: Routers, Aggregators, Gateways, Repeaters, processing units with network capabilities

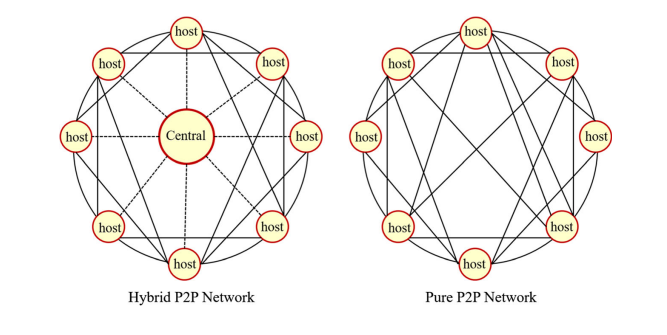
* Standards used: IEEE802.3, PLC, IEEE802.15.4, IEEE802.15.4e, IEEE802.15.4, Wi-Fi, 3G/4G/5G
* Wired connections: DSL, CAN, Optic fiber, Ethernet
* WSN (Wireless Sensor Networks) receiving data from physical or Processing layer Forming a Network node that does not need wired connections.
  + examples: WiFi, LAN, Bluetooth, BLE, Lora, Zigbee, Sigfox.

**3.3- Machine to Machine(M2M):** Can be used to describe any technology that enables networked devices to exchange information from a point to another and perform actions without need of human intervention.

Internet of things need M2M technology to operate and can use peer to peer connection to communicate (P2P) without any need of client-server connection.

**3.3.1 - Peer to Peer (P2P):** IT is a network architecture established by several protocols where connected devices have similar priorities being clients forming nodes and use a secure device authentication to communicate with each other, in this case it can be either device to device **authentication** or node to a single device.

It often uses encryption on an end-to-end connection.



*Fig-P2P Network configurations from [8]*

**4.Secure device authentication:**

Authentication is of most importance for communication between devices, servers and other devices in order to make it more secure by providing secure identity credential for the device to communicate in a system. Authentication attacks can be performed on such Smart Farm devices, or to the gateway server, this way a security breach on a supposed trustworthy environment is a serious problem on a smart farm environment due to the multiple and heterogeneous devices.

So ideally devices need to be authenticated first to get connected to various services on a smart farming system to neglect a botnet type attack that will be also aborded later on.

**4.1-Cryptography:** It is a technique to secure communications between sender and receiver with the finality of hiding the content in a communication, this way offering confidentiality, integrity, and secure authentication method through secure keys that both entities have use of and can manage.

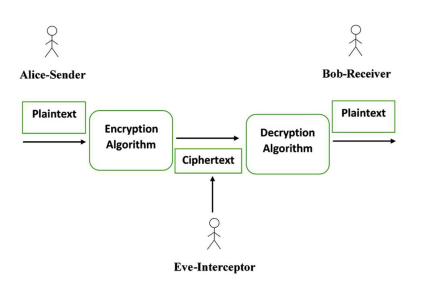


Fig-Cryptography process retired from [9]

**4.1.1-Cryptographic Key**- It is digital word composed of Strings of characters generated from encryption algorithms, they have the functionality in encryption to generate an encrypted message from merging the key to the actual data transmitted and can also decrypt it.

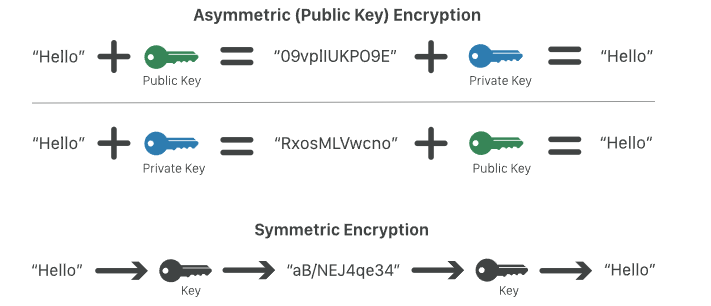


Fig-Two-way types of encryptions

**4.1.1-Symmetric encryption**: There is only one key, that is private in which both entities exchanging data have access to it, use of a public key is not needed.

Each communication session between the sender and receiver are generated different private keys called session keys that is different for different messages on internet.

* Example: **AES** (Advanced Encryption standard): It is an advanced encryption standard with symmetric encryption method.

**4.1.2-Public key encryption**: Pair of two keys, one private and other public, private key can generate signature and a signature cannot be generated any other way and it is unique for each communication so called session, Entity who have public key can authenticate that signature made by private key and verify if it is genuine, verifying trustworthy of the user. In [9] [10] are mentioned huge disadvantage on resource constraint IoT devices implementing this, because it puts a lot of computing load on limited processing and battery drain hardware.

* example: **RSA (Rivest Shamir Adleman):** It is well known protocol for public key encryption, it is heavier to execute than protocol compared to symmetric cryptography protocols, it is commonly used along with other protocols making a public key authentication method

**4.1.3- Common IoT encryption protocols [9][10]:**

**4.3.1.1-EEC** (Elliptic Curve Cryptography): It uses key authentication and Rivest–Shamir–Adleman (RSA) algorithm and mathematics of elliptic curves.

**4.3.1.2-ECDH** (Elliptic Curve Diffie-Hellman): public-key based cryptographic protocol that utilizes PUF-derived keys as the root-of-trust

* **4.3.1.2.1 -DHKE** (Diffie-Hellman-Key-exchange): Type of key exchange between two parties required that they first exchange keys based on key generated by physical device chip (SRAM PUF), It is used in ECDH cryptography
  + SRAM PUF: is based on the behavior of standard SRAM memory that is available in any digital chip making it a PUF based on SRAM memory, those are unique in its hardware lifetime, it is used as a root of trustfunctioning as vault with a cryptographic root key onto a device in some protocols such as DHKE
    - PUF (physical unclonable function): Each chip has its unique identity measured by variations that occur naturally during semiconductor production
    - SRAM (Static Random Access Memory) memory that store and erase data once power is shut down SRAM is powered.

**4.3.1.3- TLS/SSL (Transport Layer Security**): It is the principal protocol for encryption on Internet and serve to verify server identity if it is safe or not for the host to connect.

SSL uses both asymmetric encryption and symmetric encryption.

It can be used to covert a website on internet from HTTP to HTTPS, turning it secured with TLS/SSL authenticity.

SSL was further upgraded to TLS (Transport Layer Security) with this designation but with similar purpose, it is still used nowadays to secure communications but was replaced by TSL on newer versions, it also uses **TLS Handshake** method**.**

* **Cipher Suits:** cryptographic algorithms used on TLS protocol on a TLS handshake.
* **SSL certificate:** It is given by trustworthy certificate authorities from outside the server organization signed with their own key and deployed on the server, making it HTTPS secure.

It contains several important information needed to establish a trustworthy connection between server and client in order to verify server identity authenticating client and server connection in the TLS Handshake protocol.

* **TLS Handshake** is a set of datagrams exchanged between clients and servers that establish communication parameters for further message exchange such as authenticity through SSL certificate checking.

Firstly, a message from the client is sent to the server, server sends a message important information such as cipher suits and TLS version supported along with other random bytes known as client random.

The server receives the message and send back to the client the chosen cypher suit, SSL certificate and random bytes known as server random

Client verifies the authenticity of the server through **SSL certificate**

For a second time random bytes are sent front the client to the server known as premaster secret, client encrypt it with public key got from the server with **SSL certificate**.

Premaster secret can be decrypted with server private key that is confidential to the server. So decrypting client random, server random and premaster secret by both client and server is possible using the opposite key that encrypted those messages.

If public key is used to encrypt a message, the secret key is used by other entity to decrypt it, and vice-versa, having in total 3 keys (2 private and 1 public).

The authenticity is done successful if both client and server are able to generate simultaneous results for client random, server random and premaster key.

Further Client and Server communications will have symmetric encryptions for each communication session they begin, existing only 1 temporary key for each session.

**4.3.1.4-HTTP** (Hypertext Transfer Protocol). A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web (WWW) without TLS encryption protocol thus making it less secure.

**4.3.1.5-HTTPS** (Hypertext Transfer Protocol Secure). A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web (WWW) with TLS encryption protocol becoming HTTPS. It uses public key encryption therefore SSL encryption is used for this protocol.

**5- Fog Layer Architecture**

The main task of fog computing is to handle data generated by IoT devices, it is implemented on lower layers of the architecture, and it is executed by physical devices.

Before exchanging information to cloud computing or services on processing or application layer level by executing simpler processing tasks and leaving more complex decisions or processes to processing layer and cloud.

It can also be accesses directly by the user or local data management, and latency is reduced compared with Cloud storage.

it is considered a complementation and assistance of cloud computing, not a replacing entirely [6].

Function and use of FOG layer was also described generally at physical and Network layers of this article, but not mentioned. Fog architecture is implemented around those layers and serves as an additional assistance to them.

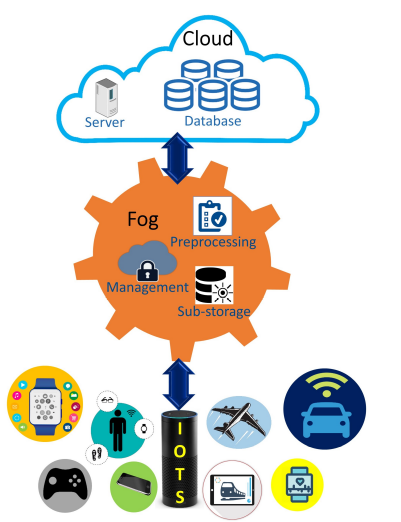
A fog node can be any device like a router, switch, or a video surveillance camera which has computing, storage, and network connectivity.

Fog layer must be able to decide the duration for which the data should be retained and when the data should be discarded or shifted to the cloud for prolonged storage, it can also provide services to end user without evolving processing layer.

The finality of mentioning and going to details about this infrastructure is to study the several devices, protocols and communications vulnerabilities related in several papers, it is one of the main targets of cyberattacks, it is closer to lower end devices and gateways with less protection making it easier to exploit vulnerabilities compared to security of higher layers.

After studying fog architecture, it is pretended to study several possible attacks on this layer and analyze network traffic in those circumstances, further detecting certain anomalies on data traffic studied,

Several types of attacks could be analyzed and applied detection methods using Artificial intelligence, such attacks are most likely attacks that can shift, delete, insert reprogram or try to access data. The final objective is to solve issues by applying machine learning algorithms that detect and learn attack patterns on the Network traffic.



Fog Computing Architecture of [11]

**6.Blockchain**

Blockchain contains digital data information about Smart Farm encrypted and distributed across the Network in form of blocks.

Advantages of Blockchain aspects from [11] that can possibly be studied and used machine to learning can be further developed:

Blockchain can enhance the security of IoT systems because it eliminates the centralized cloud servers and makes the network peer-to-peer, and data becomes not centralized

Communication in blockchain takes place using the public and private keys, and therefore only the intended party or node can access the data.

The data can be stored, rather than storing the actual data. The actual data can be stored on the cloud and the hash key can be mapped with the original data. If there is any change in the data, the hash of the data will change.

Connected to the cloud to enable IoT applications to be used from any location, can act as a suitable solution to store and transmit data.

It can avoid the risk of being a single point of failure as is faced by various IoT applications based on the cloud

If any device updates data, the system rejects it automatically.

**5.Cyber security risks**

*5.1- Vulnerabilities categories in Smart Farm*

Smart Farm is a vast ecosystem with a complex architecture that incorporates heterogenous types of technologies such as internet connected devices, different data types and communications.

It leads to greater risks for cybercrimes to strike due to the increase in opportunities of vulnerabilities it offers with the integration of IoT technology in agriculture sector.

The practice of cybercrimes can have multiple reasons for being executed and can be targeted on different Smart Farm infrastructures and technologies and can be executed in different ways. Further information will be provided with more details about this topic about several topologies of cyberattacks and categorize them in a Smart farm environment.

Disrupting Smart Farm environment can lead to human health problems, concerns for farmers, companies, or government in financial or data confidentiality matters.

Due to the number of devices on field, sensors and Network nodes, gateways, and hardware in general, it is there the possibility that the main cybersecurity's threats focus are around physical and Network layer or fog architecture, so threats related to those layers will be studied with more relevance.

It is possible that there are not sufficient security solutions to those threats because of the vast area it englobes, therefore the attacks correlated that are most likely to happen in a Smart Farm environment will be talked.

It is of great importance to keep studying, researching, developing, and implementing possible solutions to prevent cybersecurity breaches in Smart farm environment without the use of current large scale cybersecurity methods on low power constraint devices.

The requirements that Cybersecurity propose can be many, in this case some of them are more important on a Smart farm environment than others and will be approached with more relevancy, they can be categorized into authenticity, availability, confidentiality, integrity and privacy correlated attacks.

Authenticity attacks are driven to cyber-attacks trying to get access to the Smart Farm environment through any meaning based on a falsification identity, pretending to be one of the devices on the field or an authorized person or server.

Availability attacks deny any service or hardware on smart farm and compromise data acquisition or deny information and services, not providing the full service, access or control to the client or internal environment process that need a resource.

It affects the ecosystem by not keeping it entirely operating as it should.

Confidentiality attacks that try to get access to Farming private information or correlated Farming resources, it can lead to several problems such as public sharing of private and confidential data about the Farm that can lead to data leakage.

Integrity attacks try to change, inject, or delete important data, information or resources that are exchanged through Smart farm, this way misinform important smart farm identities affecting the overall trustworthy of the ecosystem.

Privacy attacks try to get Smart farm identities private information or get unauthorized access on the Smart Farm property.

*5.2- Cyberattacks in Smart Farm Environment*

* **Man in the middle** –

This attack can take multiple forms to be executed and can be categorized as a violation to all cybersecurity requirements since it can affect several layers. This attack consists in interception and infiltration on internal Smart Farm system through any possible path (other possible cyberattacks), this way this attack can get access to multiple information inside the Network and can also lead to the possibility of doing multiple other cybercrimes.

This attack is one of the mainstreams in IoT environments and it is referenced in [3],[6],[12],[14],[13],[15],[18].

* **Routing attack-**

This attack intention is to intercept current routing direction by applying a malicious node on the Network that can redirect data path to a different location, therefore the attacker can have access to the information transmitted, the data can be received late, changed, or not received at all. It is referenced in [6],[12],[13],[14].

This attack can be divided into:

* + **Sinkhole attack**-The attacker inserts a fake shortest path on a communication between existing nodes, therefore the routing methodology chooses the closest path to travel, that is fake one, this way the attacker gains access and control to the traffic.
  + **Wormhole attack**- this attack can be executed without any detection or compromise of the system, and it is aimed at sending the information intercepted on Network to the outside.
* **Side Channel attack-**

This attack is performed from the outside of the system, and it is implemented exploit vulnerabilities of the system with several techniques that are not implemented through the Network or digital access, it is generally aimed at physical layer.

* + It can be briefly talked in some papers [3],[12],[15],[18] some attacks that involve side channel attacks such as: Hardware glitching, timing attacks, electromagnetic attacks, power consumption attacks.
* **Sleep Deprivation Attack**-

This attack is performed against devices with limited battery power, the objective of this attack is to prevent a computing device from entering sleep mode, this state is set when there is no data on the device to be processed, acquired or exchanged with other nodes, this attack try to deny the device or node from entering this state by constantly interacting with it, through one malicious node are sent legitimate, thus requests that are not considered hostile by the receiving device or security, for this reason it is of high difficulty to detect such type of passive attacks . This attack is analyzed in [16] and briefly talked in [3],[12],[13],[15].

* **DoS (Denial of Service)**- This attack any target the system communication, devices, gateways nodes or other components that are crucial to the functioning of the ecosystem, making a service or application unavailable for the users.

It can also become a DDoS (Distributed DoS) in case other similarly devices on the system get infected with malware and send requests to the server simultaneously, this form of attack is called botnet attack.

DoS is referenced in most cyber security papers. [3],[6],[12],[14],[13],[15],[18],.

* **Node capture-** This attack consists of hostile identity physically changing a node device or replace it with another fake one so that it can enter the Network system then it can modify, delete or generate false data.

Once the Node is captured it can lead to implementation of other attacks through node such as fake node attacks and becoming a man in the middle attack, can also potentially trigger DoS or DDoS through a botnet or a similar attack. It is referenced in [4],[6],[12],[14],[15].

* **Flooding attack**- This attack is considered a type of DoS.

It sends a large number of continuous requests to the system Network overloading it, consequently overloading the traffic and diminishing the quality of services or even shut down. Generally, affect Network layer and application layer where the user cannot access to the service or device. It is referenced in [4],[6], [12],[14].

*There are also other interesting attacks that can affect a Smart farm environment:*

* + **Brute force** **attack**: Targeted to application layer where an authenticity attack is tried through several continuous attempts to break down a password in order to obtain legitimate access to the system as a user. It is mentioned and described in [17] as a possible threat than can be executed even from an inside malware compromised device.
  + **Eavesdropping:** This type of attack is targeted to collect system information without the attack being detected through intercepting an unprotected communication, gaining access to the data, It is briefly talked in [6],[12] as a smart farm potential cyberattack specified at [15].
  + **Jamming attacks:** In a Smart farm environment some devices use Radio Frequency transmissions to communicate, like sensing devices or communication edge devices, those communications can be intercepted and shut down by distortion of the radio frequency band by the attacker with jamming signals [3],[13],[18].

**6-Smart Farm environment perspectives**

Smart farming can have indetermined environment architectures, they can consist in different devices, technologies, and different layer architectures, depending on the environment.

Overall, they all incorporate IoT technology plus other modern technology for assistance, this way a traditional Farm becomes Smart with these applications.

Commonly Smart farms are meant to be efficient, providing support and decision-making increasing productivity, automation and decrease laboring tasks.

***6.1-Proposed work***

As mentioned before, several Smart farm environment topologies need to be considered in order to discover vulnerabilities, in the next chapters, related papers about Smart Farm architecture topologies and potential cyberattacks vulnerabilities need to be addressed. The next step is to study based on those architectures data traffic on the Network in order to analyze and apply certain filters to detect considered anomalies based on sets of that information.

A generated dataset can be detected through certain patterns. Further AI cybersecurity papers related to that matter will also be a priority.

6.2- Smart Farm different environments categories

It is specified in [2] several applications, sensors and services that will assist in describing the Smart farm scenarios and which characteristics are usual on such environment category that will be proposed.

In [20] a common greenhouse topology is specified explaining in detail how they work without any real case example.

6.2.1-Controled environment

***Greenhouse environments****-* Greenhouse buildings are the most traditional farming methodology for precision, cost and effectiveness consisting of private indoor building that provide weather safety, monitoring, automatic control, plant growth and pest control management [19].

At [20] It is specified common smart greenhouse architecture explaining in detail how they work.

They use a variety of sensors as (temperature, humidity, soul moisture, gas, light, pressure…) and actuators in physical layer for controlling the environment parameters settings to achieve more efficient and precise control. Further there is the possibility of implementation of several automated devices such as monitoring or actuating robots to make parameters gathering and embedded sensors for monitorization throughout the greenhouse field.

Connectivity between devices is made by a wireless Network that range all the devices nodes on the greenhouse, processing can be made through called Fog computing architecture providing local or remote-control trough a gateway to the outside of greenhouse Network.

Typically, a Smart greenhouse is just a fraction of an overall Smart Farm ecosystem, where there can also exist outside Smart farms or similar greenhouses provided with mutual connectivity to each other and to core Network described in [17] that communicate with Fog layer architecture that is responsible for local data acquisition and processing.

The following image is a typical greenhouse IoT environment that is present at [20]:

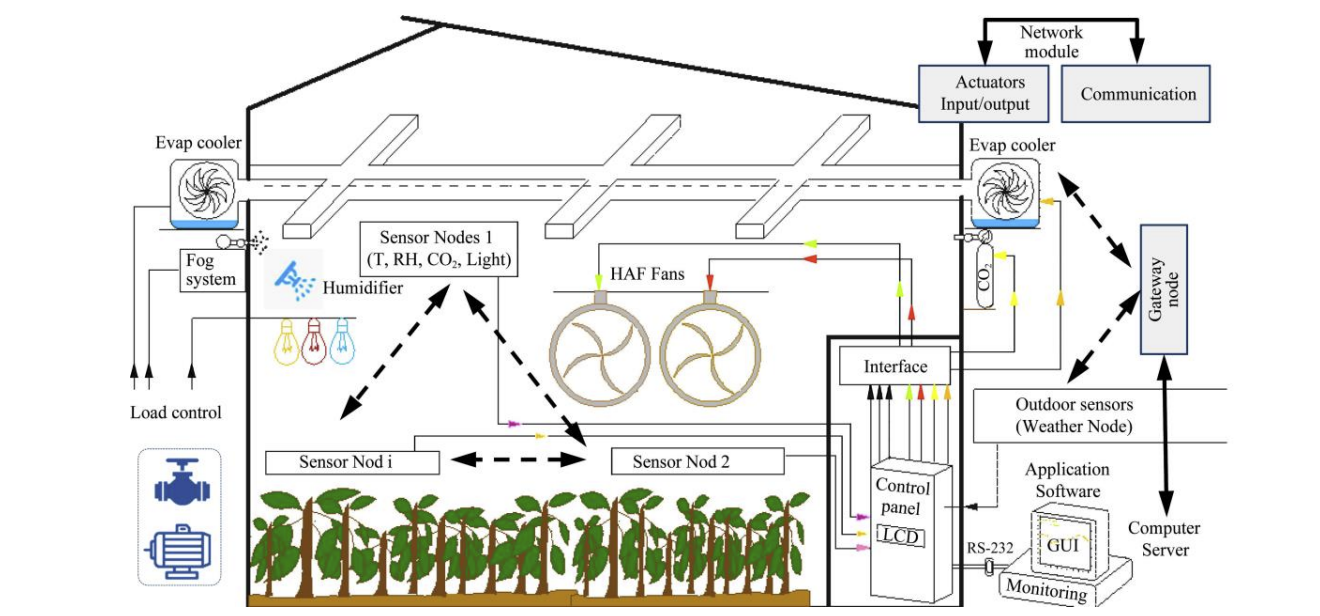


Fig-Standard IoT based greenhouse cited from <https://www.adaptiveagrotech.com/>

13-05-2022

***Environmental tecnhonolgy: Multiple scenarios and examples about particular examples of greenhouses***

**Name of paper** [27] “Greenhouse Automation Using Wireless Sensors and IoT Instruments Integrated with Artificial Intelligence”

**Communication Technologies**

* WIFI
* LORA
* Sigfox

Low level:

* I2C
* SPI

**Equipment:**

High end:

* IoT automation system constituted with: controller, 2 wifi modules, relays, motor drivers, lorawan sensor
* Arduino Microcontrollers types: (ESP32, Atmega328P), expansion board
* Raspberry pi computer
* Router systems
* GSM modems

Low end:

* Leaf Wetness sensor(ADP-AgroTech ADP-LWS2020)
* Ground temperature sensor( ds18b20, pt100)
* Soil moisture(SX239, SZYTF MOISTURE,10hs,EC-5)
* Distance sensor(SR04)
* Air temperature sensor(DHT11 ,ah10,sht20,bme280)
* Luminosity sensor(LDR Photoresistor, TSL2561, SQ-110 sensor)
* PH sensor
* SD card(for local monitoring

**Name of paper** [28] “Model-based evaluation of greenhouse microclimate using IoT-Sensor data fusion for energy efficient crop production”

**Communication Technologies**

* WIFI
* Sigfox
* Zigbee

Low level:

* SPI
* I2C
* Other Serial wired connection

**Equipment:**

High end:

* Arduino Microcontrollers types: (Atmega328P, ESP8266), expansion board

Low end:

* SD CARD
* Humidity (DHT-22)
* Ground parameters(xtech SD800,nashuah)- acquisition systems
* Solar radiation (might be the same as luminosity sensors)
* Air temperature sensor(DHT11 ,ah10,sht20,bme280, DHT-22)
* Luminosity sensor(LDR Photoresistor, TSL2561, SQ-110 sensor, LM393)
* RTC(DS3231)

Actuators

* DC actuators(can be cooling systems most likely and ventilation),
* Relays controller
* Motor drivers

Many IoT technologies incorporated in Agriculture and farms are arranged through centralized companies that have their own build in equipment and sensors with microcontrollers adapted to mainboards and embedded devices , making it a complex task to follow or simulate such IoT environment for not having access or having to pay in order to obtain that equipment that are fabricated and launched by certified big brands, such as: M5STACK, AgriTech.

One of the solutions proposed is to build just a simulation with basic sensors, actuators and computer processing that can be used in simple commonly smart farm uses and IoT uses, therefore several examples and applications of not centralized smart farm ecosystems will be explored, even smart farms with centralized solutions with platforms certain companies will be also explored to get a leverage of its specific technology specially in physical ,fog and Network layer, in order to elaborate an accurate simulation on our own...

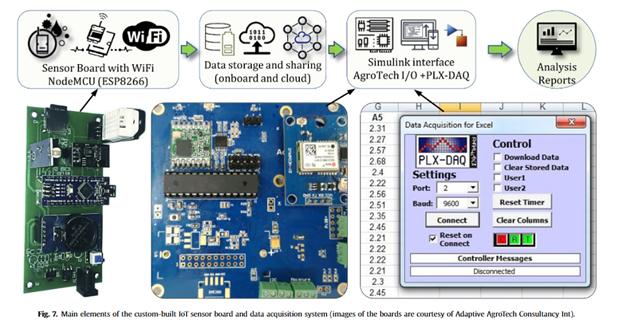


Figure-Custom built IoT sensor board from certified companies

Examples of integrated centralized Farming IoT solutions and equipment:

<https://m5stack.com/solution?id=2>

https://www.agritechtomorrow.com/

Both[29],[30]provide a concept and developed a IoT service platform decentralized, similarly in this work we might also need to develop a self-platform to where the physical data is monitored and processed locally fog layer, posteriorly to cloud storage.

**[29] “A Creative IoT agriculture platform for cloud fog computing”**

Equipment:

* Raspberry pi
* Service gateway
* Cloud platform (amazon ec2)
* Farm equipment

Protocols:

* MQTT
* Wifi

Sensor:

* Monitoring camera (pest detection)
* Temperature, humidity, PH data monitoring

Actuator:

* Water and fertilizer ground device

**[30]” Smart farming IoT platform based on edge and cloud computing”**

Parameters monitored:

* Temperature, Humidity, PH, solar radiation, co2 level

Custom parameters actuators with greenhouse equipment:

* Level control
* Liquid counter
* Flow meter
* Osmosis equipment
* Ventilation
* Air cooling
* Roof top panel for adjusting light
* Fog system(humidity control)

Microcontrollers or local computer processing

* IPex16 controller(CPS controller)
* CPS(CYBER PHISIC SYSTEM): It is an integrated solution whereas the whole system is autonomous and controlled through an intelligent and integrated algorithm present in the whole system providing autonomous control over environment settings for both acquisition or actuation, it provides higher accuracy than a generic IoT architecture, it also incorporate nodes and server instruction using Network Functions Virtualized(NFV) that provide communication and services between intelligent nodes , devices, Network, gateways, cloud, it is more autonomous and processed based system than a general IoT system.

Communication:

* MQTT
* CoAP
* 6LowPAN

6.2.2-Open field environment:

Open field environments can be diverse in configuration scenarios and purposes, there can be a vast number of physical devices due to the extensivity of the field different type of crop cultivated its main objective is to heavy produce crop.

The standard tasks executed in open field environment are environment monitoring, crop growth development, crop disease detection and precision agriculture, that is provided in previous papers, [22] about different smart farm ontologies cooperation and integration of units between the Smart farm ecosystems. It could also compromise the whole ecosystem in case of data breaches on just a particular domain.

There are also several technologies to assist in certain tasks like drones flying in the air, autonomous tractors, other autonomous devices.

6.2.3-Precision Agriculture

Precision agriculture concept is one of the main tasks performed in nowadays in agriculture environment and it is related to Smart farming on most of the aspects such as common technologies and purposes, frequently its definition deviates from Smart agriculture for the number of devices connected to a Network crop yield increase and reduced labor costs due to the number of devices it uses to make a precise evaluation. Smart Farm leverages internet of things in a way of providing more connectivity between the environment and external devices. Both are equally risked to cybersecurity related attacks,[17],[18] makes good definition and comparison of both infrastructures.

Possible Precision farm scenarios:

Attacks to these environments: all mentioned in the section of cyber-attacks in smart farm are attacks and even more can be executed.

6.2.4-Livestock breeding environment

This is not the main environment of study, but it is related to Smart farming and make part of industry 4.0, currently using several IoT technologies for physical layer interactions and use of multiple ICT technologies, it also adjusts environment parameters or concrete in-farm actuators for better animal livestock. The common tasks of those technologies in such an environment is disease monitoring, feeding details, identification, and positioning of each animal, with several biometrical sensors attached to them, with also GPS that require a wireless internet connection.

6.1.5- Centralized IoT platform for Smart farm

There are also multiple platforms that can provide IoT building support and offer data management and storage, being part of all smart farm layers. There are several examples of platforms in [21] that are classified based on functionalities, data management and edge device compatibility for data acquisition.

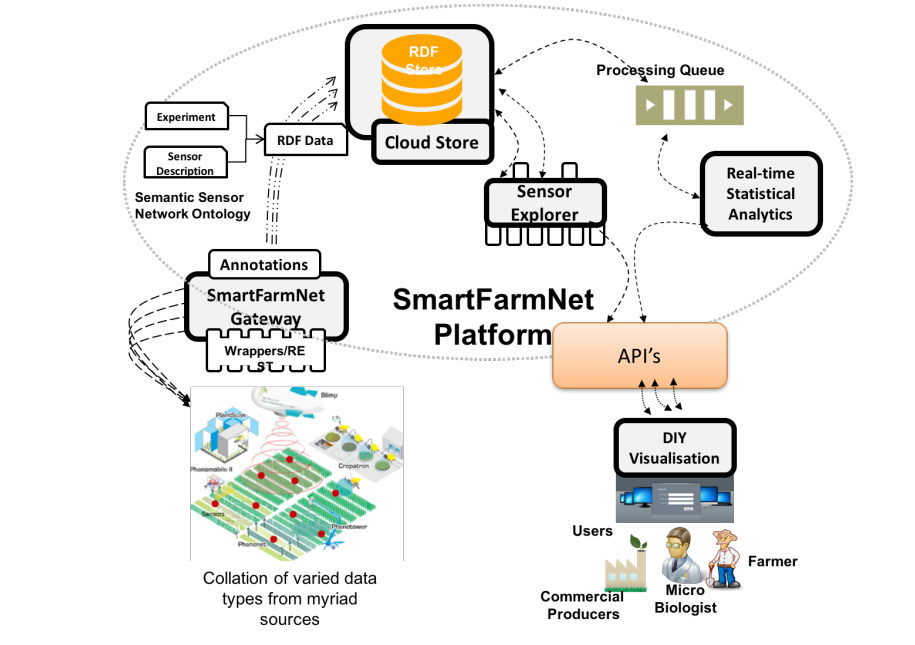


Figure-Smart farm example with SmartFarmNet platform

For example *SmartFarmNet* is a IoT platform for farming that incorporates Bring-Your-Own sensor principle and supports virtually any IoT device provided by any standard company that include several functionalities to users such as providing statistics, data storage, data analytics other user interactions for users or collaborators to monitor visualized information.

**7-Artificial intelligence and machine learning**

**Other Related work that focusses on methods of cybersecurity in Smart Farm envrionments**

The idea of this work is not to find innovative solutions to cybersecurity attacks but implementing algorithms based on several already invented techniques , and apply it on smart farm environments in order detect cyber-attacks on a Smart farm environment.

There are not sufficient studies on cybersecurity field to follow the burst if innovation and insurgency of IoT technologies in Agriculture, therefore with this work a proposed implementation of machine learning techniques with additional tools in order to open new research opportunities fulfilling reduced knowledge or implementations in this sector.

In this section it is pretended to make a leverage of currently already implemented solutions to cyberattacks proof in this environment, several topologies of attacks have been studied in this paper so far, now it is pretended to find related vulnerabilities registered and related to Smart Agriculture environments.

Articles [3],[14][22],[23] described and referenced several papers that propose solutions to cybersecurity problems in Smart Farm environment. However, on this article the objective is to focus on implementing machine learning techniques, a field inside artificial intelligence.

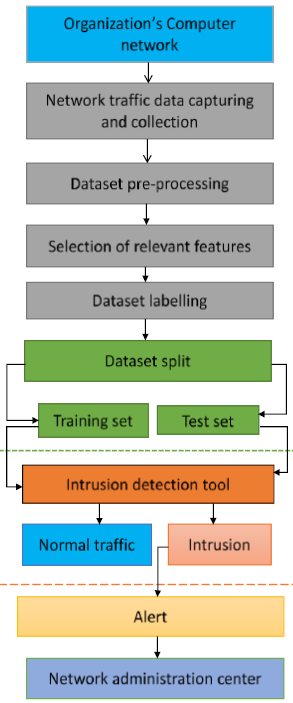
**7.1-Important definitions related to IDS, machine learning and datasets**

Artificial intelligence is a concept that address several methodologies to simulate human behavior that correspond similarly to human intervention decision and used in several areas of study. It plays a flawless role in cybersecurity industry and can have several methodologies and qualifiers [23].

Machine learning is a subset of Artificial intelligence where several techniques and algorithms are performed to apply self-learning functionalities becoming an intelligent system that does not need human intervention to execute tasks.

Deep learning is even a more complex and recent field under artificial intelligence and machine learning that opened recently due to new technologies and advancements. It consists of machine learning and expected behavior similar to that of human consciences performing actions based on it.

Intrusion Detection Systems (IDS) are computing defense systems that generally use datasets from Network traffic to identify threats or different patterns that suggest malicious intents to a system.



Generic constitution block of a Network IDS [23]

They can be modulated through several ways [23,25,26,28], for example they can be implemented in parallel with other cybersecurity methods in a Network system. A lot of technologies techniques and configurations integrate an IDS or combine with it to make the system even more secure, such as data mining [27]. A detailed and complete approach to IDS is made at [25] describing it completely through discussion, examples, and references.

Machine learning is one of the highlights discussed helping to develop an IDS, deep learning is extremely discussed as well.

Several datasets that were used to perform IDS evaluations and classifications are also discussed with moderate detail, all related to Agriculture 4.0 scenarios also referencing several layer levels of framework.

They can be classified based on metrics making distinction between them on different scenarios.

The classification is related to security and performance: Where security is a set of parameters that qualify an IDS based on its detection capabilities and rate of success in a detection, for that, several performed tests are made where intrusive and non-intrusive approaches are made to the system to qualify the output based on the input [23],[25],[27]. The output for a binary classification of intrusion/non-intrusion can be:

*True positive*: A malicious intent attack is performed to the system and IDS correctly detects an intrusion.

*True negative:* A legitimate interaction is performed to the system and IDS correctly detecting it a non-intrusion action.

*False positive:* A legitimate interaction is performed to the system and IDS incorrectly detecting it an intrusion action.

*False negative:* An illegitimate interaction or malicious attack is performed to the system and IDS incorrectly detects it a non-intrusion action.

The classification of an IDS on performance is related to the resources used by the system for implementing detection functionality and its efficiency at processing that information.

**7.2-Importance of datasets**

Data traffic is agglomerated and anomalies suggesting cyberattacks can be detected, machine learning is a tool that can facilitate in recognizing anomaly pattern of data and it is described in [23] and implemented in [25] under Smart Agriculture environments and can be part of an IDS.

In connected environments such as Smart farms data is used and transported to the Network. Making or acquiring a dataset of information is one crucial requisition for study and conducting security research in any system.

The pretended work is to obtain access to datasets for posteriorly analyzing and studying its content pretending to detect anomalies that deviate from the common pattern of information present on that data, knowing that they exist.

Datasets can be accessed through online access publications or simulated computationally through software mimicking a smart farm ecosystem composed with all technology and devices present like in a standard or concrete smart farm environment. Posteriorly through several software tools, data traffic on the Network will be filtered, analyzed, and grouped forming the dataset.

Several scenarios need to be considered and intentional cyberattacks made. There are multiple datasets online but there is not a dataset to each smart farm potential scenario infrastructure.

Commonly used public datasets:

Network related:

NSL-KDD

NSLD-KDD

KDD CUP 1999

UNSW-NB15

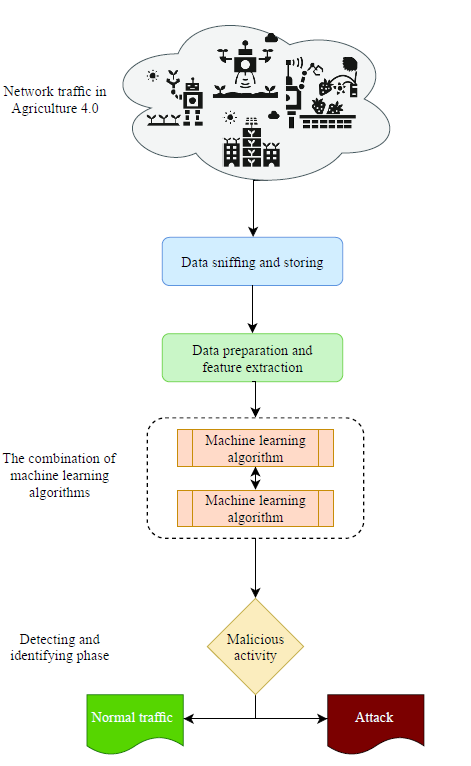
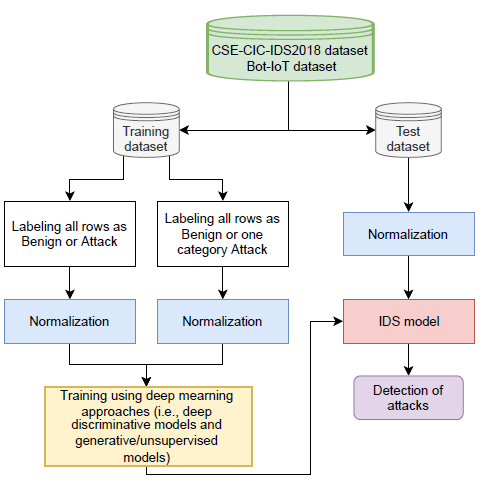
**7.3-Anomalies detection in datasets and appliance of machine learning algorithms**

Machine learning can be used and incorporated in an IDS that analyses datasets, further instructions are executed based on the status of analysis.

Data mining is a crucial part of the machine learning field although it is not considered artificial intelligence or machine learning technology.

It is used to find statistics in certain patterns in large quantity of data and provide association, classification, clustering, and prediction [25], that in conjunction with other tools and human execution developing machine learning.

In the figure bellow there are two illustrations of IDS, the first refers to a generic IDS mechanism based on a certain dataset of bot IoT where two datasets based on original are forged, one of the datasets is split in two objects in order to develop a detection technique by injecting and comparing both objects meanwhile making use of deep learning and other tools developing a detection technique. Posteriorly after the model for detection is made then system tests are performed , to evaluate detection model created The other illustration is an example of an IDS on Agriculture environment with machine learning implementation as detection technique.



Figures-IDS implementation topologies [27],[25]

**Different types of machine learning techniques:**

*Supervised learning*

*Unsupervised Learning*

**Commonly used algorithms:**

K-Nearest Neighbor

Support Vector Machine

Deep belief Networks

Artificial Neural Networks

Decision tree

Convolutional neural networks

Random forest

Restricted Boltzmann machine

Deep Neural Network

Recurrent neural network

Self-Organizing Maps

**8-Setting up a smart agriculture scenario for the proposed work**

Firstly general approach will take place by getting about the ecosystems because there can be infinite configurations possible.

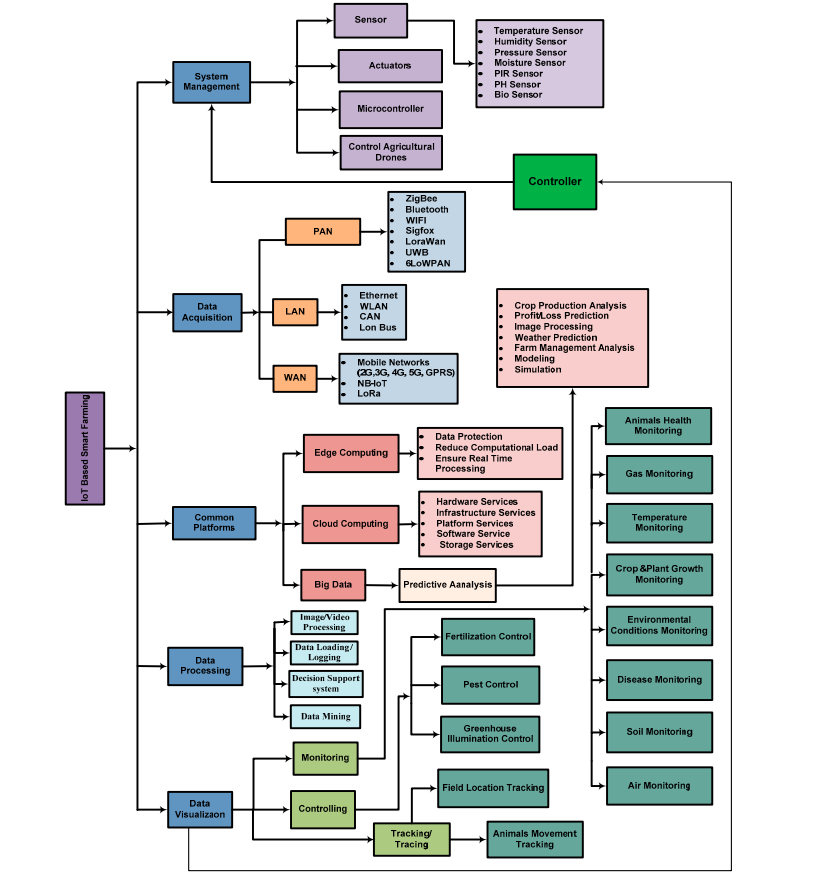


Figure- A complete framework of deployable IoT platform ecosystem for a smart farm [31]

An IoT environment will be implemented in Farming and agriculture environment, for that a simulation and a real scenario implementation need to have decent coherency compared to real ecosystems of Smart Farms and smart agriculture, therefore a small and accurate deployable IoT system will be developed to make the studies in the more accurate way.

Multiple articles will be reviewed, and ecosystems analyzed to make the best possible detailed leverage.

Many IoT technologies incorporated in Agriculture and farms are arranged through centralized companies that have their own build in equipment and sensors with microcontrollers adapted to mainboards and embedded devices , making it a complex task to follow or simulate such IoT environment for not having access or having to pay in order to obtain that equipment that are fabricated and launched by certified big brands ,normally those companies don´t sell their equipment only but their services as well.

Such companies as: M5STACK, AgriTech.

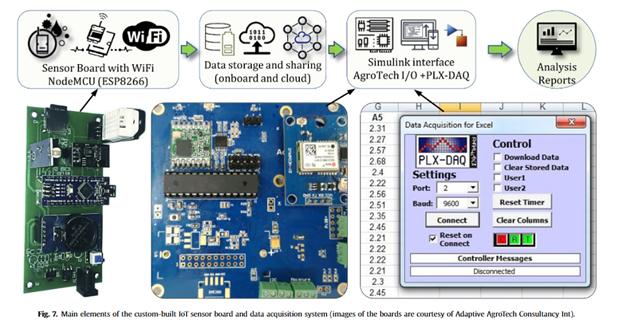


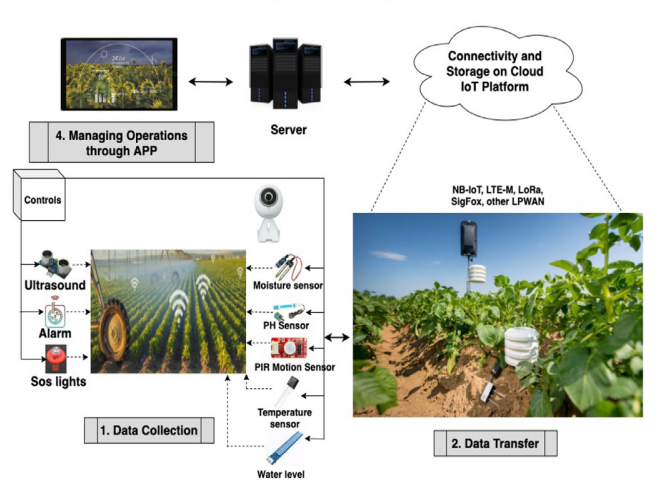
Figure-Custom built IoT sensor board from certified companies

One of the solutions proposed is to build just a simulation with basic sensors, actuators and computer processing that can be used in simple commonly smart farm uses and IoT uses, therefore several examples and applications of not centralized smart farm ecosystems will be explored, even smart farms with centralized solutions with platforms certain companies will be also explored to get a leverage of its specific technology specially in physical ,fog and Network layer, in order to elaborate an accurate simulation on our own...

Examples of integrated centralized Farming IoT solutions and equipment:

<https://m5stack.com/solution?id=2>

https://www.agritechtomorrow.com

Several IoT hardware for agriculture is highlighted and described, smart farm roles, processes, IoT platforms and functionalities.

Technology highlighted that can be easily deployed:

* Microcontrollers: ESP8266, PIC microcontroller
* GSM module (Use of RS232)
* Sensors: LM35, DHT11- Temperature, humidity, gas, PH, motion, solar radiation soil moisture, wind speed sensor, RTC (Real time clock)
* Also highlights: Proteus 8 software for simulation.

[31] Role of IoT Technology in Agriculture: A Systematic Literature Review is a survey of IoT technology addressed in domain of agriculture and provide a leverage of several papers and its application for agriculture, some of papers that are considered and consulted for this work implementation are described by this paper as well.

This paper also talks about ontologies of implementations of smart farms and sub-domains like field tasks, environmental parameters measured, data transmitted, company services ,cloud computing communications used, making a current state of art about use of IoT in agriculture.

Besides papers that are discussed in this article it also talks about

Communication protocols:

* WSN (WIFI)
* ZIGBEE
* WiMAX (Worldwide Interoperability for Microwave Access)- Mainly used for wide long-range communication with more speed than Wifi.
* Bluetooth
* Sigfox
* RFID
* Lora
* GPRS(GSM driven)

Sensors used:

* Soil moisture
* Temperature
* PH
* UV
* Motion
* CO2
* Pressure
* Location (RFID, UWB, GPS)
* Luminosity

Possible subsystems:

* UAV
* Farm management
* Disease monitoring and controlling
* irrigation

**Environmental technology: Multiple scenarios and examples about particular examples of greenhouses**

**Name of paper** [28] “Greenhouse Automation Using Wireless Sensors and IoT Instruments Integrated with Artificial Intelligence”

**Communication Technologies**

* WIFI
* LORA
* Sigfox

Low level:

* I2C
* SPI

**Equipment:**

Hardware:

* IoT automation system constituted with: controller, 2 Wi-Fi modules, relays, motor drivers, Lora wan sensor
* Arduino Microcontrollers types: (ESP32, Atmega328P), integrated expansion board
* Raspberry pi computer
* Router systems
* GSM modems

Sensors:

* Leaf Wetness sensor (ADP-AgroTech ADP-LWS2020)
* Ground temperature sensor(ds18b20, pt100)
* Soil moisture (SX239, SZYTF MOISTURE,10hs,EC-5)
* Distance sensor (SR04)
* Air temperature sensor (DHT11 ,ah10, sht20, bme280)
* Luminosity sensor (LDR Photoresistor, TSL2561, SQ-110 sensor)
* PH sensor
* SD card (for local monitoring

**Name of paper** [28] “Model-based evaluation of greenhouse microclimate using IoT-Sensor data fusion for energy efficient crop production”

**Communication Technologies**

* WIFI
* Sigfox
* Zigbee

Low level:

* SPI
* I2C
* Other Serial wired connection

**Equipment:**

High end:

* Arduino Microcontrollers types: (Atmega328P, ESP8266), expansion board

Sensors:

* Humidity (DHT-22)
* Ground parameters (xtech SD800,nashuah)- acquisition systems
* Solar radiation (might be the same as luminosity sensors)
* Air temperature sensor(DHT11 ,ah10,sht20,bme280, DHT-22)
* Luminosity sensor(LDR Photoresistor, TSL2561, SQ-110 sensor, LM393)
* RTC(DS3231)

Actuators

* DC actuators(can be cooling systems most likely and ventilation),
* Relays controller
* Motor drivers

Both [29],[30] provide a concept and developed a IoT service platform decentralized, similarly in this work we might also need to develop a self-platform to where the physical data is monitored and processed locally fog layer, posteriorly to cloud storage.

**[29] “A Creative IoT agriculture platform for cloud fog computing”**

Equipment:

* Raspberry pi
* Service gateway
* Cloud platform (amazon ec2)
* Farm equipment

Protocols:

* MQTT
* Wifi

Sensor:

* Monitoring camera (pest detection)
* Temperature, humidity, PH data monitoring

Actuator:

* Water and fertilizer ground device

**[30]” Smart farming IoT platform based on edge and cloud computing”**

Parameters monitored:

* Temperature, Humidity, PH, solar radiation, co2 level

Custom parameters actuators with greenhouse equipment:

* Level control
* Liquid counter
* Flow meter
* Osmosis equipment
* Ventilation
* Air cooling
* Roof top panel for adjusting light
* Fog system(humidity control)

Microcontrollers or local computer processing

* IPex16 controller(CPS controller)
* CPS(CYBER PHISIC SYSTEM): It is an integrated solution whereas the whole system is autonomous and controlled through an intelligent and integrated algorithm present in the whole system providing autonomous control over environment settings for both acquisition or actuation, it provides higher accuracy than a generic IoT architecture, it also incorporate nodes and server instruction using Network Functions Virtualized(NFV) that provide communication and services between intelligent nodes , devices, Network, gateways, cloud, it is more autonomous and processed based system than a general IoT system.

Communication:

* MQTT
* CoAP
* 6LowPAN

**OBJETIVOS**

* **~~Pesquisar e estudar cenários de simulação de ambiente Smart Farm que poderemos abordar~~**
* **Estudar IDS e relacionar com inteligência artificial-tentar fazer até dia 11**
* **Uso de inteligência artificial em trabalhos (como usam:” usa ou não usa?” e que conjunto de dados são usados, apresentado a fonte)- tentar fazer até dia 11.**
* **Que tipo de anomalias são comuns em rede e que tipo de algoritmos machine learning são usadas ( camadas neuronais, arvore de decisão…).-Tentar fazer até dia 11 de Maio**
* **Elaboração de um esquema para analise com os tópicos estudados nomeadamente-Até 18 de Maio**
  + **Escolha do dataset**
  + **Escolha do tipo de algoritmo machine learning**
  + **Programas a usar(wireshark, cisco packet tracer,tcpdump… ?**
  + **Ferramentas auxiliares**

Dúvidas para os orientadores:

1-IDS usam vários métodos de deteção nos quais machine learning/deep lerarning é um deles… abordo também esses aspetos? Nomeadamente: Fuzzy Gaussian mixture-based e Hybrid machine learning. Também como referenciado nos artigos é possível o uso em paralelo ou incorporado em certos mecanismos ou técnicas de cybersegurança existentes que apenas auxiliam na sua segurança.

No meu trabalho terei de fazer uma IDS deste modo será necessário eventuais ferramentas extra sem ser machine learning ?

References

[1] B. Basso, B. Dumont, D. Cammarano, A. Pezzuolo, F. Marinello, and L. Sartori, ‘‘Environmental and Economic benefits of variable rate nitrogen fertilization in a nitrate vulnerable zone,’’ Sci. Total Environ., vols. 545–546, pp. 203–215, Mar. 2016.

[2] Muhammad Ayaz ,“Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk”,Digital Object Identifier 10.1109/ACCESS.2019.2932609

[3] Maanak Gupta, Mahmound Abdelsalam, Sajad Korsandroo, Sudip Mittad,” Security and Privacy in Smart Farming: Challenges and Opportunities”, Digital Object Identifier 10.1109/ACCESS.2020.2975142

[4] Bam Bahadur Sinha , R. Dhanalakshmi "Recent advancements and challenges of Internet of Things in smart agriculture: A survey", Future Generation Computer Systems vol:126 pp. 169–184 (2022)

[5]Nallapaneni Manoj Kumara , Pradeep Kumar Mallick “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers” (ICCIDS 2018), Procedia Computer Science 132 (2018) 109–117

[6] VIKAS HASSIJA , VINAY CHAMOLA , VIKAS SAXENA , DIVYANSH JAIN , PRANAV GOYAL and BIPLAB SIKDAR "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures “DOI 10.1109/ACCESS.2019.2924045, IEEE Access

[6.1] Kumar Yelamarthi, Md Sayedul Aman, and Ahmed Abdelgawad , “An Application-Driven Modular IoT Architecture”, College of Science and Engineering, Central Michigan University, Mount Pleasant, MI 48859, USA

[7] Haji Akhundov, Erik van der Sluis, Said Hamdioui, and Mottaqiallah Taouil “Public-Key Based Authentication Architecture for IoT Devices Using PUF”, rXiv:2002.01277v1 [cs.CR] 4 Feb 2020

[8] Cheol-Joo Chae1 & Han-Jin ,“Enhanced secure device authentication algorithm in P2P-based smart farm system” Cho Peer-to-Peer Networking and Applications (2018) 11:1230–1239

[9] Huanhao Xu , Kutub Thakur , Abu S. Kamruzzaman , Abu S. Kamruzzaman ,“Applications of Cryptography in Database”, 978-1-6654-4067-7/21/$31.00 ©2021 IEEE

[10] Haji Akhundov , Erik van der Sluis , Said Hamdioui , and Mottaqiallah Taouil, “Public-Key Based Authentication Architecture for IoT Devices Using PUF”, arXiv:2002.01277v1 [cs.CR] 4 Feb 2020

[12] Angelita Rettore de Araujo Zanella, Eduardo da Silva, Luiz Carlos Pessoa Albini,” Security challenges to smart agriculture: Current state, key issues, and future directions”, Array 8 (2020) 100048

[13] Bam Bahadur Sinha , R. Dhanalakshmi ,” Recent advancements and challenges of Internet of Things in smart agriculture: A survey”, Future Generation Computer Systems 126 (2022) 169–184

[14] Konstantinos Demestichas \* , Nikolaos Peppes and Theodoros Alexaki,” Survey on Security Threats in Agricultural IoT and Smart Farming”, Institute of Communication and Computer Systems, Zografou, 15773 Athens

[15] Richa Sarma, Ferdous Ahmed Barbhuiya “Internet of Things: Attacks and Defences”, 2019 7th International Conference on Smart Computing & Communications (ICSCC)

[16] MATTHEW PIRRETTI, SENCUN ZHU, N. VIJAYKRISHNAN, PATRICK MCDANIEL, and MAHMUT KANDEMIR ,“The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense”, DOI:10.1080/1550132060064271

[17] MOHAMED AMINE FERRAG , LEI SHU, (Senior Member, IEEE), XING YANG , ABDELOUAHID DERHAB , AND LEANDROS MAGLARAS ,” Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges”, 10.1109/ACCESS.2020.2973178

[18] Abbas Yazdinejad , Behrouz Zolfaghari , Amin Azmoodeh , Ali Dehghantanha , Hadis Karimipour , Evan Fraser , Arthur G. Green , Conor Russell and Emily Duncan,” A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures”, Appl. Sci. 2021, 11, 7518. <https://doi.org/10.3390/app11167518>

[19] Junhu Ruan, Yuxuan Wang, Felix Tung Sun Chan, Xiangpei Hu, Minjuan Zhao, Fangwei Zhu, Baofeng Shi, Yan Shi, and Fan Lin ,“A Life Cycle Framework of Green IoT-Based Agriculture and Its Finance, Operation, and Management Issues”, 10.1109/MCOM.2019.1800332

[20] Redmond Ramin Shamshiri , Fatemeh Kalantari , K. C. Ting , Kelly R. Thorp , Ibrahim A. Hameed , Cornelia Weltzien , Desa Ahmad , Zahra Mojgan Shad “Advances in greenhouse automation and controlled environment agriculture: A transition to plant factories and urban agriculture”, DOI: 10.25165/j.ijabe.20181101.3210

[21] Prem Prakash Jayaraman , Ali Yavari , Dimitrios Georgakopoulos , Ahsan Morshed , Arkady Zaslavsky, “Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt”,doi:10.3390/s16111884

[22] Abeer Alshammari , Qamra Alharbi, Rawan Alonazi , Nora Aljomaih , Zainab Malik , “Smart Agriculture and Cybersecurity”, International Journal of Engineering and Information Systems (IJEAIS) ISSN: 2643-640X Vol. 5 Issue 6, June - 2021, Pages: 24-31

[23] Maniriho, Pascal, et al. "Detecting intrusions in computer network traffic with machine learning approaches." *International Journal of Intelligent Engineering and Systems* 13.3 (2020): 433-445.

[24] Xin, Yang, et al. "Machine learning and deep learning methods for cybersecurity." *Ieee access* 6 (2018): 35365-35381.

[25] Ferrag, Mohamed Amine, et al. "Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions." *IEEE/CAA Journal of Automatica Sinica* 9.3 (2021): 407-436.

[26] Osman, Abdullahi Sidow. "Data mining techniques." (2019).

[27] Ferrag, Mohamed Amine, et al. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." *Journal of Information Security and Applications* 50 (2020): 102419.

[28] “Greenhouse Automation Using Wireless Sensors and IoT Instruments Integrated with Artificial Intelligence”

[29] “A Creative IoT agriculture platform for cloud fog computing”

[30]” Smart farming IoT platform based on edge and cloud computing”

[31]Muhammad Shoaib Farooq, Shamyla Riaz , Adnan Abid, Tariq Umer and Yousaf Bin Zikria, ”Role of IoT Technology in Agriculture: A Systematic Literature Review”, Electronics 2020, 9, 319doi:10.3390/electronics9020319

[32] Ravi Kishore Kodali and Borade Samar Sarjerao”A Low Cost Smart Irrigation System Using MQTT Protocol”, Department of Electronics and Communication Engineering National Institute of Technology Warangal, India

<https://www.visma.com/cloud-technology/cloud-computing-layers/>

https://oleumtech.com/what-is-scada

https://www.cloudflare.com/learning/