

2020

**University of North Carolina Wilmington
Master of Science in
Computer Science and Information Systems
Proceedings**

<https://csbapp.uncw.edu/mscsis>

SECURE SMART FISHING USING ATTRIBUTE BASED ACCESS CONTROL

Shaik Barakhat Aziz

A Thesis Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2020

Approved by

Advisory Committee

Ulku Clark

Gulustan Dogan

Sudip Mittal, Chair

Accepted By

Dean, Graduate School

LIST OF TABLES

Table	Page
ABSTRACT	iv
CHAPTER I: INTRODUCTION	1
CHAPTER II: RELATED WORK AND BACKGROUND	4
2.1 SMART FISHERY	4
2.2 ATTACKS ON SMART FISHERIES	5
2.3 ACCESS CONTROL SOLUTIONS	6
2.4 APPLICATIONS OF SMART FISHERIES	7
CHAPTER III: SYSTEM OVERVIEW	9
3.1 ARCHITECTURE.....	10
3.2 COMPONENTS	12
3.3 INTERACTIONS	15
CHAPTER IV: SMART FISHERIES ONTOLOGY	19
4.1 CLASSES	21
4.2 RELATIONSHIPS	22
4.3 ACCESS CONTROL USE CASES	23
CHAPTER V: AI ASSISTED APPLICATIONS.....	27
5.1 DECISION SUPPORT SYSTEM	27
5.2 MARKETING AND DISTRIBUTION OF PRODUCE.....	28
5.3 VISION BASED INSIGHT GENERATION.....	29
5.4 EARLY WARNING SYSTEM.....	29
5.5 WORKER RECRUITING TOOL	30
CHAPTER 6: CONCLUSION	31
BIBLIOGRAPHY	32

LIST OF FIGURES

Figure		Page
1	The architecture of our Smart Fisheries Ecosystem.....	10
2	Interaction in a smart fisheries Ecosystem.....	15
3	Smart Fisheries Ontology	20
4	SWRL code of “Permission to Access FGU Data”.....	24
5	SWRL code of “HBU monitoring WBU to rant Accesses”.....	25
6	SWRL code of “Access permission to operate OBU”	25
7	SWRL code of “Access Permission on Worker Based Location”	26

ABSTRACT

Secure Smart Fishing using Attribute based Access Control

Shaik Barakhat Aziz, 2019. Thesis document, University of North Carolina Wilmington.

The increasing number of internet-connected devices has paved a path for smarter ecosystems in various sectors such as agriculture, aquaculture, manufacturing, healthcare, etc. Especially, integrating technologies like big data, Artificial Intelligence (AI), blockchain, etc. with internet-connected devices has increased efficiency and productivity. Therefore, aqua farmers have started adopting smart fisheries technologies to better manage their fish farms. Despite their technological advancements smart fisheries are exposed and vulnerable to cyber-attacks that would cause a negative impact on the ecosystem both physically and economically. As less emphasis is laid on securing the smart sensors that are connected through the internet. Therefore, in this document, we present a smart fisheries ecosystem where the architecture describes various interactions that happen between internet-connected devices. We develop a smart fisheries ontology based on the architecture and implement Attribute Based Access Control System (ABAC) where access to resources of smart fisheries is granted by evaluating the requests. We also discuss how access control decisions are made in multiple use case scenarios of a smart fisheries ecosystem. Furthermore, we elaborate on some AI applications that would enhance the smart fisheries ecosystem.

CHAPTER I: INTRODUCTION

With the growing population, there arises a need for increasing food production in order to avoid food insecurity. This includes produce like fish which is an important source of food for millions of people around the world [1]. Therefore, the fishing sector is also looking forward to every possible opportunity to improve resource efficiency for all fishing related activities. For instance, incorporating new technologies like AI, big data, cyber-physical systems (CPS), blockchain, etc. would help in increasing productivity, quality of produce, etc. Since traditional methods are finding it difficult to meet the needs of growing demand. Therefore, several fisheries are shifting towards internet-connected ecosystems in order to feed the future. Moreover, interconnecting the sensors present in fish farms via the internet generates huge volumes of data points. These data points further assist the owners of the fish farm in analyzing and monitoring the device data in real-time.

However, interconnecting the smart sensors present in the ecosystem has created a security blind spot. Thus, attackers can easily damage the smart fisheries ecosystem causing huge economic loss since they are exposed to similar security threats that have happened in other IoT domains.

For example, a smart home in Milwaukee was hacked by an attacker where the temperature of the room was increased to 90 degrees Fahrenheit by utilizing a thermostat. [7]. Gupta et al. presented [3] several security and privacy issues in a smart farming ecosystem. Therefore, measures to protect the smart fisheries ecosystem from attackers is more necessary now than before due to the growing number of cyber-attacks.

In this document, a secured smart fisheries ecosystem is introduced in order to protect the internet-connected sensors from potential cyber-attacks and present various AI applications that would aid the owners to effectively manage their fish farms. We design the architecture of a smart fisheries ecosystem that has physical entities present in the physical layer, digital twins in the edge layer, and a representation graph in the cloud layer. Static sensors deployed in the fish farm, movable machinery equipment, workers, and owner are represented as physical entities. We describe in detail the physical entities and information exchange that happens between them. Based on the domain-specific information obtained from the smart fisheries architecture related to fish farm sensors and their interactions we create a smart fisheries ontology. We utilize the developed ontology to implement Attribute Based Access Control (ABAC) for securing the fish farm and also discuss how access control decisions are made in various security use case scenarios. We present some AI applications that would immensely benefit the fish farm owners in multiple aspects such as the decision-making process, marketing produce, in-depth insights to manage fish farms, early warning alerts, recruiting workers, etc.

The rest of the document is organized as follows:

- Chapter II discusses the related work on various aspects such as smart fisheries, attacks on fisheries, access control solutions, and AI applications for smart fisheries.
- Chapter III explains the architecture, components, and their interactions in the smart fisheries ecosystem.
- Smart fisheries ontology is described in Chapter IV.
- Chapter V demonstrates access control decisions of our system in various security use case scenarios.
- Chapter VI we present various AI applications that would enhance smart fisheries

ecosystem.

- Finally, Chapter VII draws a conclusion to this research document.

CHAPTER II: RELATED WORK AND BACKGROUND

In this chapter, we discuss some important works relevant to smart fisheries, attacks on smart fisheries, access control approaches. We also present some existing AI applications in the smart fisheries ecosystem.

2.1 SMART FISHERY

Smart Fisheries are becoming more popular in the global seafood market during the 21st century. As it is able to meet the growing demands for seafood and also manages to minimize the decline in the number of fishes. In the project named SMART FISH 2020 [4], the authors have proposed a system to ensure the efficient functioning of the fishery ecosystem while reducing the environmental impact in the European Union fishing sector. They have incorporated the recent technological advancements in the field of big data, machine learning, artificial intelligence, etc. to assist the fishermen in making informed decisions. Interconnecting the IOT devices that are deployed in the fisheries has helped the fisherman to exploit the IOT applications in a wider range. In the next 30 years, it is predicted that advanced analytics can bring over an annual profit of 60 billion dollars [5] solely from the fishery ecosystem. For example, the quality of the water [6] can be evaluated timely for proper water treatment and also to prevent contamination by monitoring the data collected from the sensors that contain the pH levels, temperature, salinity, etc. Another implementation to determine water quality was done by Salim et al. [7] measures the water quality in eel fish aquaculture where it monitors data from dissolved oxygen (DO), acidity (pH), and temperature sensors.

2.2 ATTACKS ON SMART FISHERIES

The number of attacks on interconnected devices is increasing at a rapid rate as less emphasis is laid on the security of the devices in various domains such as smart homes [8], smart farms [9], smart manufacturing [10], etc. Such kinds of attacks can damage the entire smart infrastructure or incur a partial loss. For example, a cyber-attack on Puerto Rico [11] smart meter utility in 2009 led to the loss of hundreds of millions of dollars due to False Data Injection (FDI) that could alter the power consumption units. It was reported that the smart meters lacked sufficient security controls to protect from an intrusion. Similar kinds of attacks can happen in smart fisheries since the sensors deployed are interconnected via the internet. Reports show that Sunderland Marine [12] has 8,000 insurance policyholders over the world from the aquaculture industry due to the rising number of cyber-attacks. Recently, the Northwest Atlantic Fisheries Organization (NAFO) [13] has experienced a ransomware attack where the servers were unavailable for some time. Frustaci et. al. [14] discussed the vulnerabilities and security challenges faced due to the incorporation of IOT devices. Attacks that spread lice and genetic introgression [15] within the stock in aquaculture infrastructure is another possible threat scenario that could bring irrecoverable loss to the ecosystem. Another example of a cyber-attack on the fishery ecosystem happened in South Korea [16] where hundreds of fishing boats had faced GPS jamming which caused difficulty in locating the nets at sea.

2.3 ACCESS CONTROL SOLUTIONS

Joshi et al. [17] have developed a model to evaluate decisions based on rules by using ABAC system that analyzes end attributes of the data. The system was determining the access control to critical documents of an organization by considering the end to end encryption of the cloud service provider. Wai Sze [18] has referenced in his document that instead of using a two-factor Authorization, authenticating beyond physical access with minimal interaction would benefit to preserve the privacy of users' access and the temporal routine profile mechanisms. this can enable us to have minimal interaction with maintained security and decreased human interaction [19]. In order to obtain that following process, high-level encryption is used to define the roles, and the second layer to access the cloud server and retrieve information is assessed [20]. A fundamental concept of minimizing security risk and implemented to a business or organization. While a secure facility needs to rely on the credentials or access levels. Instead of having security for individual entry to individual systems, it is better to have secured control access to all aspects [21]. Although many accept that an access control system is needed but they are unable to implement the accurate adaptability with the sophisticated methodologies [22] mentioned about other access control models and cite them Different Organizations prefer using Different types of Access Controls. There are many different types such as Mandatory Access Control [23], Discretionary Access Control [24], Role-Based Access Control [25], Rule Based Access Control, Attribute Based Access Control [26]. With the ontology-based access control, the assertions obtained according to the updates are fetched and then provided access, or any operation required is performed [27]. The use of such automated tools will help in the detection and prevention of Insider as well as outsider information [28]. In this document, we will be reading more about ABAC Access controls challenges for web

services and systematic approaches based on objects and environmental approaches which uses ABAC Authorization and formulation of architecture [29]. An ABA ABAC can be seen as an Externalized Authorization management, Dynamic Authorization management, and Fine-grained Authorization. ABAC currently used in XAMCL also called as Extensible Access control Markup Language. It is currently used in the world in big corporations and even in military based units using the basic IF/AND/Else conditions which being supported by Boolean logic defined by the user having the right to access a certain part of it. [30]. Using ABAC methodologies has provided great accomplishments to further provide research analysis and hence has given a wide range of expertise in accomplishing an integral management tool which has further encompassed people to achieve the mapping of Indigenous areas and accomplish a basis to implement necessary actions [31]. It has also seen to be used to create an environment or a framework to indict the rules according to the organization and help mitigate the resources and access levels effectively [32]. Creating formal attributes and access controlled to specific users might be a bit hindrance but the attributes involved are constrained to the categories that are implemented.

2.4 APPLICATIONS OF SMART FISHERIES

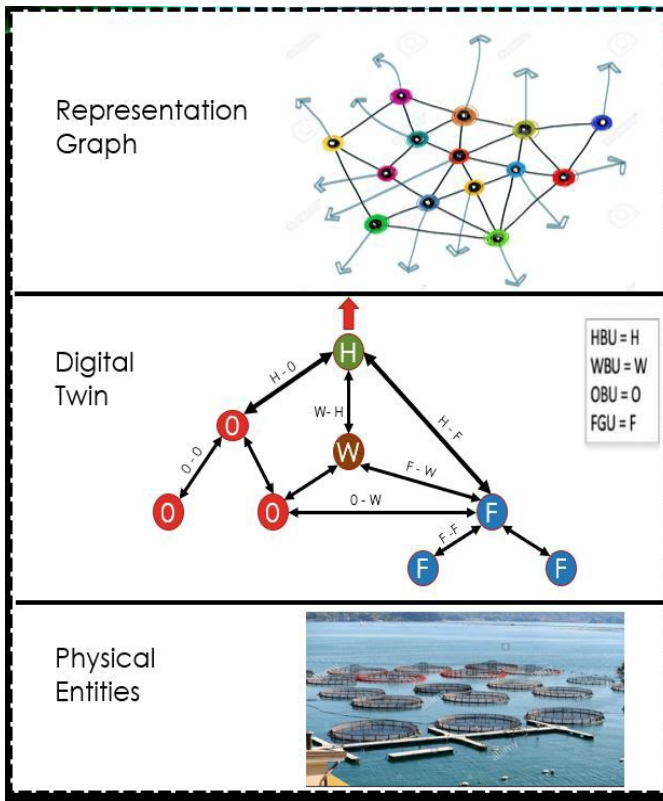
Recently cyber-physical systems coupled with AI applications have become widely popular as they would increase productivity and bring in economic profits. Various CPS domains have started utilizing AI based applications since they provide insights by analyzing large volumes of data from a heterogeneous type of devices [33]. For example, activity recognition of an occupant in a smart home is implemented by utilizing a deep learning model. Data collected from different sensors deployed in the home is the input to

the model [34]. Similarly, several possible AI applications that could be developed on a smart farm are mentioned by Chukkapalli et al. [35] Maintaining ecological balance in the fisheries is quite important to support aquatic life. Therefore, researchers have developed some AI-based applications for the fisheries ecosystem. For example, low-cost computer vision algorithms were developed by Papadakis et al. [36] to monitor the behavior of fishes in the tank where the stress factor is determined based on stocking density. An electronic remote monitoring [37] system was developed by the Danish government to determine the quantity of catch for all the fishermen and also monitor their actions. Additionally, an AI tool for differentiating a hungry fish from that of a full by the use of vibration-based sensors and acoustic signals is developed. For instance, a company known as “e-Fishery” in Indonesia has developed a system that can dispense the right amount of feed at the right time [38]. By using this technology, they can reduce the cost of feed by about 21%. Another example is vessel detection by utilizing an image recognition algorithm in order to track down illegal fishing was developed by Kanjir et al. [39]. A popular tool named vessel monitoring system [40] tracks fishing activities based on location, speed, etc., and provides it to the fishery management Architecture of our Smart Fisheries Ecosystem authority. Parra et al. [41] developed a system that dispenses the right amount of feed for the fish by utilizing the sensors that monitor the behavior of the fishes present in the water.

CHAPTER III: SYSTEM OVERVIEW

In order to provide a secure environment for the owners to cultivate fishes on a large scale using a small utility farm, we have outlined a smart fisheries ecosystem shown in Figure 1. Our proposed ecosystem can give multiple insights to the fish farm owners by analyzing the collected data obtained by interconnecting the sensors present in the fish farm via the Internet. These insights will help the fish farm owners in the decision-making process [42] in order to increase the produce, maintain ecological balance in the fisheries ecosystem, etc. We have divided this chapter into three modules for a better understanding of our smart fisheries ecosystem. The first module describes the architecture of our system that has three layers. The first layer is the physical layer that contains all the physical sensors deployed in the fish farm, the second layer is the edge layer that performs computations at the node and the third layer contains cloud where large volumes of data generated is stored in the form of a representation graph to support AI applications. The second module discusses the functionality of physical entities, digital twins, and representation graph. The third module describes all the interactions that happen between different types of sensors.

FIG 1: The Architecture of our Smart Fisheries Ecosystem



3.1 ARCHITECTURE

3.1.1 PHYSICAL LAYER

In this layer, we have real-time sensors where the information obtained while monitoring is captured to store and further analyze the data using AI techniques. Information such as temperature, oxygen concentration, salinity, pH levels, watercolor, the required amount of feed, plankton monitoring, etc. plays a vital role in balancing the aquatic life and managing the smart fisheries ecosystem. Therefore, devices are deployed to monitor various features in the fisheries ecosystem and assist the fisheries farmers to make the right decisions in real-time scenarios. Sensors such as YCS-2000 dissolved oxygen sensor, Arvo-Tec Auto feeder, Aqua TROLL Temperature/Conductivity Sensor are few examples that are utilized in the fisheries ecosystem.

3.1.2 EDGE LAYER

This layer processes the generated data from the sensors near the edge instead of transmitting it into the cloud. Continuous transmission of data to the cloud unit is expensive because satellites are utilized for communication purposes. Therefore, transmission costs are reduced with the help of edge computing as it eliminates the need for transferring large volumes of real-time data. For example, a vessel monitoring system that incorporated the edge computing approach [43] has shown a reduction in communication costs that ranged from 70 % to 90 %. As data was transmitted to the cloud only when an abnormal scenario is detected even though data was collected more frequently like every 10 seconds. Additionally, the edge computing layer supports real-time applications such as monitoring, data analysis, predict downtime of sensors, etc.

3.1.3 CLOUD LAYER

This layer secures all the sensor data received from the edge layer by storing it in a distributed file system. The cloud layer follows Platform as a Service as the architecture model since it provides resources to build and run applications. These applications offer various services such as data pre-processing, identifying abnormal patterns in the data, and predicting outcomes such as the quantity of feed, downtime of machinery, etc. based on historical data present in the cloud. The insights generated by these applications are communicated to aqua farmers through a mobile application that would assist them in better managing their farms as it can help them take a better course of action like changing the food, recycling the water, etc. In recent times, IBM Cloud, Microsoft Azure, Google-Cloud, and AWS are the popular ones that offer cloud-based AI services by providing secured access to the users for accessing and analyzing their data even remotely.

3.2 COMPONENTS

We describe various components present in the smart fisheries ecosystem that could belong to any of the three layers such as the physical layer, edge layer, and cloud layer of the architecture.

3.2.1 Physical Entities

The physical entities that are depicted in Figure 1 determine various interactions that happen smart fisheries ecosystem. They are divided into various categories based on their functionality which are described below:

- **Fishery Ground Unit (FGU):** Static physical sensors like temperature sensors, pH Tester, automated feeders, etc. deployed on the fish farms are represented as FGU. The data collected from these smart devices are stored in the cloud that could be retrieved by fish farm owners to take decisions like maintaining the temperature of water in order to balance the aquatic life.
- **On-Board Unit (OBU):** Movable machinery like vessel monitoring systems, drones, etc. are represented as OBU. The OBUs can interact with other OBUs and FGUs while being operated. Information exchange that happens with the OBUs and the other units like FGU, OBU, WBU, and HBU present in the fish farm is stored as a representation graph in the cloud units.
- **Worker Based Units (WBU):** The workers employed on the farm to perform different tasks are represented as WBU. They utilize mobile or computer platforms to monitor, communicate, and operate FGUs and OBUs. There are two types of workers namely permanent and temporary workers which is determined by the fish

farm owners based on their requirements to manage the farm. The level of access and role of each type of worker are described below:

- ***Permanent Worker***: Permanent workers are those workers that have permanent access to the whole system or a part of the system depending on the capabilities of workers and requirements of the fish farm owners. Usually, permanent worker roles are given to an Owner or someone with similar authentication.
- ***Temporary Workers***: Temporary workers are given temporary access to operate, monitor, and control the FGUs and OBUs. The access can be given on a daily basis or weekly or dependent on a specific time duration in order to perform tasks in peak season such as harvesting. These workers are given limited authorization in order to keep security robust, have a minimum human error, and avoid data leakage.
- **Home Based Unit (HBU)**: The centralized hub that is set up by the fish farm owner to interconnect all the units present in the fish farm is represented as a Home Based Unit. The HBU is connected to the cloud via the internet. Fish farm owners with the help of HBU can monitor all the sensors (FGU, OBU, and WBU) and also determine access permissions of WBU. HBU can also access all the information exchange that happens between the units which are stored in the cloud.

3.2.2 Digital TWIN

The virtual replicas of the physical sensors deployed in the farm are represented as digital twins. They monitor the data generated from the physical sensors and notify the fish farm owners about a breakdown of machinery in advance to reduce downtime by training machine learning models. Digital twins can also be utilized for maintaining data security and privacy which is an added advantage. For example, unauthorized transmission of data can be avoided with the help of a digital twin whenever a temporary worker tries to access previous data of the sensors present in the fish farm. Additionally, digital twins when coupled with AI techniques helps in increasing the operational efficiency of the physical sensors deployed. Insights such as the required amount of feed for the fish, quantity, and quality of fish, etc. are provided to the fish farm owner by analyzing large volumes of generated data.

3.2.3 Representation Graph

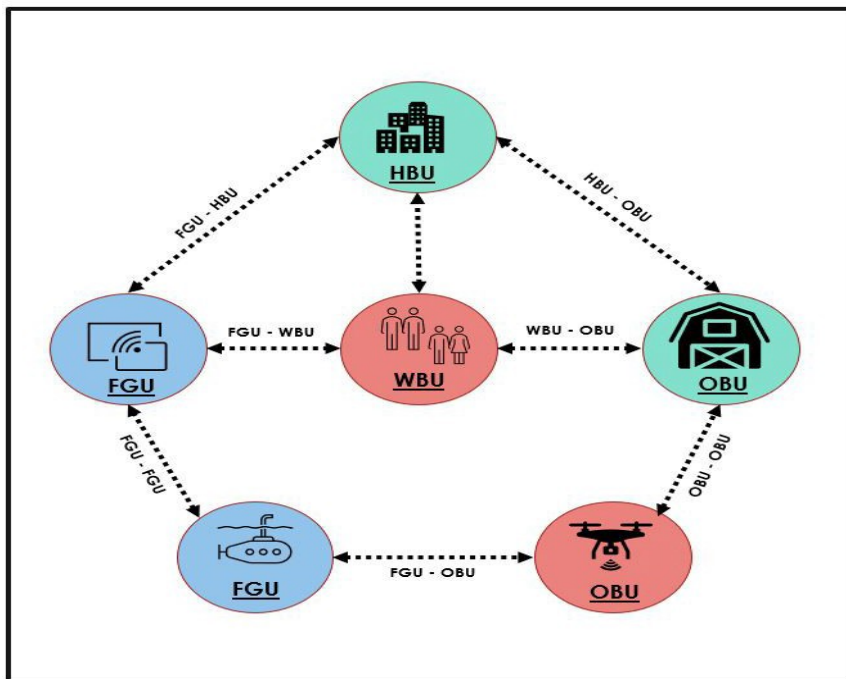
The representation graph is present in the topmost layer of our smart farm ecosystem architecture that contains nodes and edges. The physical devices are represented as nodes and information exchange between nodes are represented as edges. The cloud stores the information collected from the representation graph which has all the interactions like OBU-OBU, FGU-FGU, FGU-WBU, OBU-HBU, etc. that happen between the nodes. The representation graph is immediately updated whenever communication happens between the nodes. For example, WBU tries to know the readings of the temperature sensor present in water. Information exchange happens between FGU and WBU that is automatically stored in the representation graph. Owners of the fish farms can visualize all the interactions that happen in the fisheries ecosystem with the help of HBU.

In order to eliminate redundant interactions, the representation graph is optimized in the cloud layer. To have a secured smart fisheries ecosystem, HBU monitors the status of the sensors with the help of data obtained from the representation graph with an intention to detect anomalous events. For example, HBU blocks the interaction of a temporary worker (WBU) with the OBU which is considered an abnormal event if the contract of the temporary worker expires.

3.3 INTERACTIONS

In this chapter, we elaborate below on various interactions that could happen between sensors deployed in the smart fisheries ecosystem. Figure 2 provides a visual representation of these interactions.

FIG 2: Interaction in a smart fisheries Ecosystem



- **FGU-FGU:** Several static sensors deployed in the fish farms communicate with each other since they are interconnected. The information exchange between them contains details such as the status of the sensors, timestamp, etc. that are stored in the representation graph. OBUs, WBUs, and HBUs can monitor or retrieve information from the FGUs to perform certain actions in the fish farms. Only HBUs have the control to give access permissions for operating the FGUs present in that particular fish farms.
- **OBU-OBU:** Various interactions that happen between movable machinery like vessel monitoring systems, drones, filtration units, etc. are collected and stored in the cloud. The HBUs authorize the WBU to operate them whenever required for a specific period of time. Any status change or actions being performed on the OBU are immediately updated. Therefore, fish farm owners with the help of HBUs can monitor the status of OBUs.
- **OBU-FGU:** Interaction between OBUs and FGUs happens whenever an OBU wants to know the status of FGUs before performing an action. For example, a vessel monitoring system (OBU) interacts with the various FGUs to retrieve information from them in order to identify the right time to feed the fish. These interactions between the OBU and FGU are stored in the representation graph that can be accessed by the fish farm owner with the help of HBU.
- **FGU-WBU:** An interaction between the FGUs and WBU happens whenever the WBU wants to know the status of FGUs prior to performing an action. The WBUs can communicate with the FGUs only when they are authorized by the HBU. All the interactions that happen between FGU and WBU are stored in

representation graph. Change in status of FGU is always notified to the authorized WBU in order to keep them updated.

- **OBU-WBU:** Authorized WBUs can control or operate OBUs for that specified time period. The representation graph contains automatically updated information about a recent interaction between OBU and WBU that can be viewed by the fish farm owners. When the WBUs access to the equipment present in the fish farm expires they would no longer be able to interact or retrieve information from the OBUs.
- **FGU-HBU:** The HBU is the central unit that has permanent access to all the FGUs present in the fish farm. Also, HBU contains a complete list of all the interactions that happen with FGUs stored in a representation graph. Therefore, fish farm owners can access the past data of the FGU with the help of HBU in order to make certain decisions that would be beneficial to the fisheries ecosystem.
- **OBU-HBU:** The HBU gets automatically updated whenever there is an action being performed on the OBUs that belong to the fish farm. It keeps track of operations being performed by the OBUs and who is performing them. All the interactions that involve OBU are stored in the representation graph that can be accessed by the HBU whenever required.
- **WBU-HBU:** The HBU employs workers to work on the fish farms who could either be permanent workers or temporary workers. The temporary workers get only temporary access to operate the equipment in the fish farm or retrieve data only for a particular time period specified by the HBU. Information

exchange between the WBUs and HBUs are also stored in a representation graph for future reference.

CHAPTER IV: SMART FISHERIES ONTOLOGY

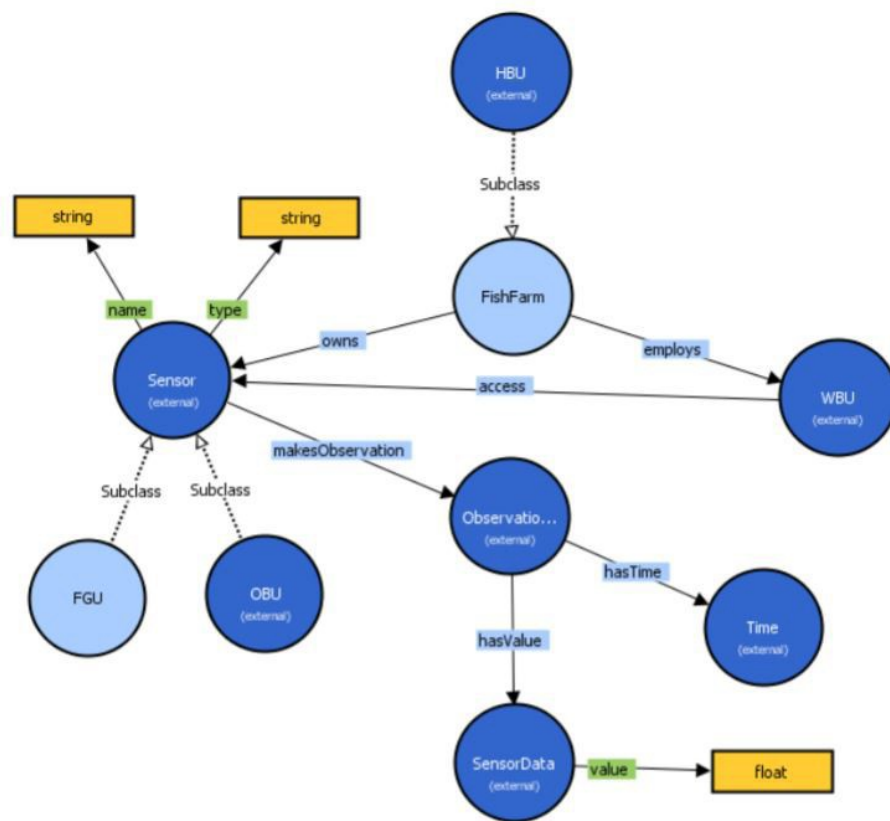
A philosophical compilation of data is made to envelop all concepts and their subcategories called Ontology where properties describe the attributes of the concepts and relationships between them. Various domains such as security [44], medicine [45], finance [46] manufacturing [47], etc. have been utilizing ontologies for knowledge representation since they enable the reuse of domain knowledge. Various concepts present in the domain are represented as classes and individual elements that belong to a particular class are represented as instances. For example, a class named Books represents all books where a book named "The Secret" would be an instance of this class. In the field of security itself, multiple ontologies are already existing to monitor their cyber-physical ecosystems (CPS) such as smart home ontology [48] smart farm ontology [49], smart city ontology [50], etc. Considering the benefits and effectiveness of the above ontologies in securing their ecosystems, we planned to create an ontology for the fisheries ecosystem.

Therefore, we have developed a smart fisheries ontology shown in figure 3 as described below by utilizing the architecture, components, and interactions of the smart fisheries ecosystem described in Chapter III. We utilize this ontology for capturing data from the information exchange discussed in Chapter III-C between various sensors. Furthermore, access control of the smart fisheries ecosystem in multiple use case scenarios mentioned in Chapter V can be determined based on our ontology. Also, various AI applications described in Chapter VI are built with help of this ontology. Our smart fisheries ontology consists of six main classes where the Fish Farm class represents the owner of the fisheries ecosystem that maintains the fish farm, the WBU class represents workers employed in the

the fish farm, Sensor class represents the devices owned by the fish farm, Observation class represents data collected, Sensor Data class represents a data value and Time class represents the timestamp.

Some of the important classes and relationships present in our ontology are described below:

FIG 3: Smart Fisheries Ontology



4.1 CLASSES

1. **FishFarm class:** This is an important class as it has details about various physical sensors and working employees present in the fisheries ecosystem. It has HBU as its subclass. It provides information about the operations that are being performed in order to manage the smart fisheries ecosystem.
2. **HBU class:** This class is represented as a hub setup that keeps track of the information exchange between the sensors present in the fish farm. Moreover, the HBU class assists the owners of the fish farm in taking key decisions by providing necessary information like the status of the sensors for a specified time period.
3. **WBU class:** This class contains details such as name, type of access, hours of operation about the employed workers in the fish farm. Workers can access the device data to operate or monitor devices owned by the fish farm only when the owners of the fish farm grant permission.
4. **Sensor class:** The class contains information about the functionality of the equipment owned by the member farm. It has sub-classes named FGU and OBU. Data collected from the physical sensors can be accessed from this class based on access permissions.
5. **FGU class:** This class contains details about the immovable equipment present in the fish farm. Devices such as temperature sensor, recycling unit, food dispensary unit, dissolved oxygen sensor are represented as individuals of this class.
6. **OBU class:** Movable machinery like vessel monitoring systems, drones, etc. are treated as instances of this class. Information about change in status or the current status of the devices can be obtained from this class.

7. **Observation class:** This class has information such as data points, timestamp of the FGU, and OBU class whenever there is a change in status.
8. **Sensor Data class:** This class represents the observation value of movable and immovable sensors located in the smart fisheries ecosystem.
9. **Time class:** This class provides the timestamp whenever an observation is recorded due to a change in the status of the device (FGUs) or action being performed on them (OBUs).

4.2 RELATIONSHIPS

- I. **owns:** This property provides the list of physical sensors such as FGUs and OBUs owned by the smart fisheries ecosystem. The FishFarm class is the subject entity and the Sensor class is the object entity.
- II. **employs:** This link provides information about current workers working on the fish farm. The subject entity is FishFarm class and the object entity is WBUclass.
- III. **makesObservation:** This property indicates that the sub-classes of the Sensor class has a new observation. Here, the subject entity is the Sensor class, and the object entity is the Observation class.
- IV. **hasData:** This relationship provides us with data value recorded by the physical sensors for every few seconds. The subject entity is the Observation class, and the object entity is SensorData class.
- V. **hasTime:** This link indicates the temporal information of the sensors such as when a particular data was recorded. The subject entity is Observation class and the object entity is Time class.

VI. **access:** This property states whether a worker of the WBU class can operate or monitor the physical sensors that belong to the fish farm. The subject property over here is WBU class and the object property is Sensor class.

4.3 ACCESS CONTROL USE CASES

In order to secure our smart fisheries ecosystem, we utilize our smart fisheries ontology described in Chapter IV to develop Attribute Based Access Control (ABAC) framework. As ABAC framework dynamically evaluates access requests based on various attributes information. Considering the ABAC framework, we present the rules written in Semantic Web Rule Language (SWRL) for multiple access control scenarios where access to various resources present in the fish farm is determined. In order to process the access requests based on the context, we include context class in our framework. We also included Platys ontology [51] to get details like time, date, location, etc. of sensors present on the farm. We discuss below the rules for multiple access control scenarios built on our ontology:

4.3.1 Scenario 1 - Permission to access FGU data

For this scenario, the owner of the fish farms utilizes HBU to grant access for the temporary worker (WBU) employed in the fish farm where the worker can analyze the data from the temperature sensor (FGU) for a certain time interval. The rule for this case is represented as follows in figure 4:

FIG 4: SWRL code of “Permission to Access FGU Data”

```
# Authorization Policy for accessing data collected
#from temperature sensor based on day/time.
{ ?A a abac:RequestedAction;
  abac:subject ?S;
  abac:object data :Temperature;
  abac:permission ?P;
  abac:context ?C.
?P rdfs:label "access"^^xsd:String.
?S abac:sRole ?r.
?C abac:contextActivity ?cAct.
?cAct abac:occursOnDay ?d.
?d list:in
("Tuesday" "Thursday").
?cAct platys:occurs_when ?t.
data:Temperature ?t
acadDomain:workHour1 time:includes ?t.
} => { ?A a abac:PermittedAction }.
```

Here the temporary worker (WBU) based on Unit S creates a request A to access the temperature data of a deployed physical sensor from 09:00 AM to 11:00 AM (workHour1). The policy rule permits this action where the temporary worker can only access data on Tuesday and Thursday (occursOnDay) for a particular time interval(workHour1)

4.3.2 Scenario 2 - HBU monitors actions of WBUs to grant further access permissions

Important information such as actions being performed by the worker (WBU) in the fish farm needs to be immediately updated to the owner. This way owner will have an idea about the current status of workers to grant further access permissions. Therefore, in this scenario, the HBU is updated about WBU for every minute. We write the SWRL rule for the above scenario as figure 5:

FIG 5: SWRL code of “HBU monitoring WBU to rant Accesses”

```
# Owner receives data for every minute whenever
# there is change in action of WBU
{ ?A a abac:RequestedAction;
  abac:subject ?S;
  abac:object data:workerAction;
  abac:permission ?P;
  abac:context ?C.
  ?P rdfs:label "sendImmediate"^^xsd:String.
  ?S abac:sRole ent:Worker_1.
  ?C abac:contextActivity ?cNetAct.
  ?cNetAct netwok:hasReceiver ?id.
  ?id enthost:belongsTo ent:HBU.
  data:workerAction data:lastModifiedOn ?t.
  ent:Duration time:includes ?t.
} => { ?A a abac:PermittedAction }.
```

The above policy rule states that HBU receives data for every minute whenever there is a change in the status of the WBU. This policy rule makes use of Platys ontology. The property named {Duration} states the time interval at which the owner is updated about the actions of Worker.

4.3.3 Scenario 3 - Access permission to operate OBU

In this scenario, an instance of the worker class having worker id can operate the drone (OBU). The device allocation and workers' authorization are completely in the control of the HBU. Therefore, authorized workers employed in the fish farm can operate only the allocated devices as described in figure 6:

FIG 6: SWRL code of “Access permission to operate OBU”

```
# Authorization Policy for WBU to operate OBU
# based on worker id.
{ ?A a abac:RequestedAction;
  abac:subject ?S;
  abac:object data:Drone;
  abac:permission ?P;
  abac:context ?C.
  ?P rdfs:label "access"^^xsd:String.
  ?C abac:contextActivity ?cAct.?cAct
  platys:has_participant ?p.
  ?p platys:has_worker ?u.
  ?u platys:owns "Worker_12020".
} => { ?A a abac:PermittedAction }.
```

From the above policy, the WBU having worker id as Worker can operate the drone (OBU) present on the farm. If the worker id is not similar to the one requested, then the WBU will no longer be able to operate the OBU.

4.3.4 Scenario 4 - Access Permission to workers based on location

For this scenario, the employed workers utilize their mobile devices for connecting to the fish farm wireless network. This way the employed workers' monitor, control sensors present on the farm. Therefore, access is denied if the location of the worker does not match with the location address of the fish farm. The SWRL rule for this scenario is presented in figure 7:

FIG 7: SWRL code of “Access Permission on Worker Based Location”

```
# Authorization Policy for accessing the sensors
# based on location
{ ?A a abac:RequestedAction;
  abac:subject ?S;
  abac:object ?O;
  abac:permission ?P;
  abac:context ?C.
  ?P rdfs:label "access"^^xsd:String.
  ?S abac:sRole ?r.
  ?O abac:Role ?r.
  ?C abac:contextActivity ?cAct.
  ?cAct platys:haslocation ?p.
  ?p platys:farm_location data:FishFarm1.
} => { ?A a abac:PermittedAction }.
```

In the above policy, the owner of the fish farm named FishFarm1 allows the authorized WBU to access OBU and FGU only if they are present in the vicinity of the fish farm. Once the WBU move far away from the fish farm, he would immediately lose access.

CHAPTER V: AI ASSISTED APPLICATIONS

Integrating AI and cyber-physical systems that facilitate interaction and communication with their surroundings makes the ecosystem smarter and insightful. In this chapter, we present a few AI application scenarios that will be beneficial for managing the fisheries ecosystem and also support fisheries dependent communities.

5.1 DECISION SUPPORT SYSTEM

Decision Support System is an important real-time application in the smart fisheries ecosystem. As data collected from sensors in the smart fisheries ecosystem are stored in the cloud as representation graphs that help in analyzing requirements such as the amount of feed for the fish, resource usage, operational scheduling, etc. using AI tools. In this way, the production costs for the ecosystem can be optimized while increasing their productivity. For example, aqua farmers can decide the right time and the required quantity of feed needed for the fish by analyzing the previously collected data stored in the cloud. By doing this contamination of water can be avoided that is caused due to excessive feed present in the fisheries ecosystem.

Similarly, aqua farmers can make decisions in advance regarding purchasing or borrowing equipment like food dispensary units for feeding the fish, fish pumps, and elevators for loading the truck, back-up generators, filtration equipment, etc. whenever required. In order to avoid the risk of killing the fishes during harvesting due to power failure, pipe clogging, an excessive amount of unwanted contents in the water, etc. For example, the number of filtration units required to be present can be purchased prior to harvesting by

the HBUs as it is necessary equipment that regulates ammonia and nitrate content in the tanks.

5.2 MARKETING AND DISTRIBUTION OF PRODUCE

An AI-based application can be used to track the nearby markets that offer better price value for the produce. The data collected from the smart fisheries ecosystem can also be utilized for marketing the quality of the product. For example, the aqua farmer can receive an USDA Organic seafood certification for the product by utilizing data obtained from FGUs and OBUs.

While marketing the product, acquiring this certification will be beneficial since it will attract consumers due to the transparency of fisheries. Also, recommendations for growing certain species based on environmental conditions and demand for the product in the market can be provided to the HBUs. In this way, aqua farmers have an idea of what type of species to grow in their fisheries according to that particular geographical area. For example, HBUs based on the recommendations can select species of fish suitable to grow in their present climate.

Additionally, AI tools can be used to increase the sales and avoid wastage of produce by tracking down the daily range of sales or previous sales history during the distribution of produce to the markets. Consequently, aqua farmers will have information regarding the required quantity of produce and avoid over-harvesting of the produce.

5.3 VISION BASED INSIGHT GENERATION

In-depth analysis such as recognizing the defects like shrink in size of the fish, length of the fish, etc. can be performed by utilizing AI based techniques like computer vision algorithms to monitor and track characteristics of the fish with the help of real-time images. Therefore, insights generated from the analysis can aid the aqua farmers in keeping the fish healthy. For example, HBUs can receive insights on how to increase the quality and quantity of the fishes present in the ecosystems with the help of vision-based algorithms that utilize images captured from the drones deployed underwater. Additionally, monitoring the behavior of the fish in the ecosystem can also be done by recording the movements or behavioral patterns like swimming patterns or feeding patterns of the fish. These patterns can help the aqua farmers to increase the quality of the ecosystem by reducing fish diseases. For example, changes in behavioral patterns of the fish can be detected from the video clips that could help the aquatic farmers to identify environmental changes in the ecosystem and provide HBU with insights to better manage their fish farms.

5.4 EARLY WARNING SYSTEM

An early warning system for the fisheries ecosystem will ensure the survival of the aquatic life by alerting the aqua farmers whenever there are unusual events like fluctuations in water, color, temperature, salinity level, carbon dioxide concentration, oxygen concentration, etc. This safety application plays a huge role in maintaining a balanced environment for the fisheries ecosystem in order to support the growth of aquatic life. Therefore, data collected from the sensors such as FGUs, OBUs can be utilized for analyzing abnormal events with the help of various AI tools. For example, HBUs get an

alert when sudden changes in temperatures are observed as fishes cannot handle temperature fluctuations.

Another aspect of an early warning system is predicting downtime of machinery like OBUs and FGUs that are utilized in managing the fisheries ecosystem. Identifying and tracking down the abnormal behavior of sensors by utilizing predictive maintenance applications can help reduce heavy maintenance costs incurred due to the breakdown of machinery. For example, an early warning alert about a minor repair can be sent to HBU when an abnormal behavior of the OBU is detected that is quite different from the regular behavior of the equipment. In this case, it minimizes the unexpected breakdown of machinery and unwanted interruptions.

5.5 WORKER RECRUITING TOOL

The owners of the fisheries can use AI tools to hire temporary or permanent workers whenever required. As it helps in automatically scheduling workers to work on fish farms for a certain time period based on specific requirements such as expertise, availability, etc. For example, workers (WBU) can be hired in advance to work temporarily on fish farms only during the harvesting period. This tool is an added advantage to the fish farm owners as they can avoid conflict when there is a high demand for labor which could delay the harvest. Additionally, AI models also help in employing both temporary and permanent workers in that particular geographical area who would match the expertise required by the fish farm owners.

CHAPTER 6: CONCLUSION

The increase in popularity of cyber-physical systems as they can interconnect various smart sensors via the internet has led to the rise of smart ecosystems in various sectors such as homes, agriculture, aquaculture, etc. Especially, they paved a path for the integration of technologies like artificial intelligence, big data, blockchain, etc. since the ecosystems generate large volumes of data. Considering the benefits, aqua farmers have started adopting smart fisheries approaches to increase the quality and quantity of produce for maximizing their profits. Additionally, smart fisheries ecosystems also enable the aqua farmers to monitor the interactions, control their devices remotely, etc. However, interconnecting these devices through the internet has unlocked several security threats and attacks like data breaching, denial of service, etc. that would impact the overall functionality of the smart fisheries ecosystem.

In this document, we developed a secured smart fisheries ecosystem that would be beneficial to the aqua farmers and also prevent attackers from exploiting the ecosystem that could incur huge losses. The document first describes the functionality of each layer in the smart fisheries architecture.

We define the components such as physical entities, digital twin, and representation graph present in the ecosystem. Also, we explain possible interactions that happen between the physical entities. Then we developed a smart fisheries ontology based on architecture and the interactions. Finally, we implemented an Attribute Based Access Control system that determines the access to resources in the fish farm based on smart fisheries ontology. We also present a few use case scenarios to show how access controls requests are handled. Furthermore, we mention AI applications that could assist aqua farmers in maintaining fish farms.

BIBLIOGRAPHY

- [1] An inventory of new technologies in fisheries.
<https://www.oecd.org/greengrowth/GGSD2017Issue%20DocumentNew%20technologies%20in%20FisheriesWEB.pdf>.
- [2] Felt so violated: Milwaukee couple warns hackers are outsmarting smart homes.
<https://www.fox6now.com/news/felt-so-violatedmilwaukee-couple-warns-hackers-are-outsmarting-smart-homes>.
- [3] Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, 8:34564–34584, 2020.
- [4] Huseyin Ozbilgin. Smart fisheries technologies for an efficient, compliant and environmentally friendly fishing sector—smartfish h2020. *Mediterranean Fisheries and Aquaculture Research*, 1(2):98–99.
- [5] EDF Oceans. Smart fisheries for the 21st century, February 20 2020.
- [6] Kofi Sarpong Adu-Manu, Cristiano Tapparello, Wendi Heinzelman, Ferdinand Apietu Katsriku, and Jamal-Deen Abdulai. Water quality monitoring using wireless sensor networks: Current trends and future research directions. *ACM Transactions on Sensor Networks (TOSN)*, 13(1):1–41, 2017.
- [7] Taufik Ibnu Salim, Triya Haiyunnisa, and Hilman Syaeful Alam. Design and implementation of water quality monitoring for eel fish aquaculture. In *2016 International Symposium on Electronics and Smart Devices (ISESD)*, pages 208–213. IEEE, 2016.
- [8] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac.

Peek-a-boo: I see your smart home activities, even encrypted! In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pages 207–218, 2020.

[9] Sina Sontowski, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, and Ravi Sandhu. Cyber attacks on smart farming infrastructure. UMBC Student Collection, 2020.

[10] Logan D Sturm, Christopher B Williams, Jamie A Camelio, Jules White, and Robert Parker. Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. stl file with human subjects. Journal of Manufacturing Systems, 44:154–164, 2017.

[11] Elizabeth. Puerto rico smart meters believed to have been hacked – and such hacks likely to spread, April 12 2012.

[12] Sunderland Marine. Cybersecurity: a growing concern, May 01 2019.

[13] Cliff White. Northwest atlantic fisheries organization hit by ransomware attack.

[14] M. Frustaci, P. Pace, G. Aloï, and G. Fortino. Evaluating critical security issues of the iot world: Present and future challenges. IEEE Internet of Things Journal, 5(4):2483–2495, 2018.

[15] Richard Green Lawrence Baker. Cyber security in uk agriculture.

[16] REUTERS. South korea revives gps backup after cyber attack, February 05 2016.

[17] Maithilee Joshi, Sudip Mittal, Karuna P Joshi, and Tim Finin. Semantically rich, oblivious access control using abac for secure cloud storage. In 2017 IEEE international conference on edge computing (EDGE), pages 142–149. IEEE, 2017.

[18] Khutso Lebea and Wai Sze Leung. A model for context-driven authentication in physical access control environments. In Kuinam J. Kim and Hye-Young Kim, editors,

Information Science and Applications, pages 319–328, Singapore, 2020. Springer Singapore.

[19] Fredrik Einberg, Phillip Hoyer, Julian Lovelock, and Robert Rowe. Method and system for automated physical access control system using biometric recognition coupled with tag authentication, June 6 2019. US Patent App. 16/323,199.

[20] Supriya Raywade, Ayushi Dixit, Shruti Jain, and Deepali Jain. Enabling authentication and access control-based data sharing with personal information hiding for secure cloud storage. *CLIO An Annual Interdisciplinary Journal of History*, 6(4):143–149, 2020.

[21] Kathleen Richards and Sharon Shea. Access controls. 2019.

[22] Kathleen Richards and Sharon Shea. Online access controls. 2018. [23] Online access controls. 2018.

[24] Discretionary access controls. 2019.

[25] Margaret Rouse. Role based access controls. 2020. [26] 1 * Se-Ra Oh, 1 Young-Gab Kim and Sanghyun Cho². An interoperable access control framework for diverse iot platforms based on oauth and role. 2018.

[27] Francesco Fabrizi, Angelo Littera, Frank G Marbello, and Claudio Valant. Ontology based control of access to resources in a computing system, January 23 2020. US Patent App. 16/042,657.

[28] Teresa F Lunt. A survey of intrusion detection techniques. *Computers & Security*, 12(4):405–418, 1993.

[29] J. Tong E. Yuan. Attributed based access control (abac) for web services. 2005.

[30] Tomas Cerny Michal Trnka and Nathaniel Stickney. Survey of authentication and authorization for the internet of things. 2018.

- [31] Lorenzen K. McGrath D. G. Almeida, O. Fishing agreements in the lower amazon: For gain and restraint. *fisheries management and ecology*. 2009.
- [32] Xin Jin, Ram Krishnan, and Ravi Sandhu. A unified attribute-based access control model covering dac, mac and rbac. pages 41–55, 2012.
- [33] H. Sedjelmaci, F. Guenab, S. Senouci, H. Moustafa, J. Liu, and S. Han. Cyber security based on artificial intelligence for cyber-physical systems. *IEEE Network*, 34(3):6–7, 2020.
- [34] TLM Van Kasteren, Gwenn Englebienne, and Ben JA Krose. Activity “ recognition using semi-markov models on real world smart home datasets. *Journal of ambient intelligence and smart environments*, 2(3):311–325, 2010.
- [35] S. S. L. Chukkapalli, S. Mittal, M. Gupta, M. Abdelsalam, A. Joshi, R. Sandhu, and K. Joshi. Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. *IEEE Access*, 8:164045– 164064, 2020.
- [36] Vassilis M Papadakis, Ioannis E Papadakis, Fani Lamprianidou, Alexios Glaropoulos, and Maroudio Kentouri. A computer-vision system and methodology for the analysis of fish behavior. *Aquacultural engineering*, 46:53–59, 2012.
- [37] Lotte Kindt-Larsen, Eskild Kirkegaard, and Jørgen Dalskov. Fully documented fishery: a tool to support a catch quota management system. *ICES Journal of Marine Science*, 68(8):1606–1610, 2011.
- [38] VV Jothiswaran, T Velumani, R Jayaraman, et al. Application of artificial intelligence in fisheries and aquaculture. *Biotica Research Today*, 2(6):499–502, 2020.
- [39] Urska Kanjir, Harm Greidanus, and Kristof Ooster. Vessel detection and classification from spaceborne optical images: A literature survey. *Remote sensing of environment*, 207:1–26, 2018.

- [40] S Nguyen-Khoa, Matthew McCartney, S Funge-Smith, L Smith, SS Sellamuttu, and M Dubois. Increasing the benefits and sustainability of irrigation through integration of fisheries: A guide for water planners, managers and engineers.
- [41] Lorena Parra, Laura Garc'ia, Sandra Sendra, and Jaime Lloret. The use of sensors for monitoring the feeding process and adjusting the feed supply velocity in fish farms. *Journal of Sensors*, 2018, 2018.
- [42] H.Poor. An introduction to signal detection and estimation. 1985.
- [43] Joao C Ferreira and Ana Lucia Martins. Edge computing approach for vessel monitoring system. *Energies*, 12(16):3087, 2019.
- [44] Bill Tsoumas and Dimitris Gritzalis. Towards an ontology-based security management. In *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, volume 1, pages 985–992. IEEE, 2006.
- [45] Timothy W Bickmore, Daniel Schulman, and Candace L Sidner. A reusable framework for health counseling dialogue systems based on a behavioral medicine ontology. *Journal of biomedical informatics*, 44(2):183–197, 2011.
- [46] Duygu Altinok. An ontology-based dialogue management system for banking and finance dialogue systems. *arXiv preprint arXiv:1804.04838*, 2018.
- [47] Jiehan Zhou and Rose Dieng-Kuntz. Manufacturing ontology analysis and design: towards excellent manufacturing. In *2nd IEEE International Conference on Industrial Informatics*, 2004. *INDIN'04*. 2004, pages 39– 45. IEEE, 2004.
- [48] Ji Eun Kim, George Boulos, John Yackovich, Tassilo Barth, Christian Beckel, and Daniel Mosse. Seamless integration of heterogeneous devices and access control in smart homes. In *2012 Eighth International Conference on Intelligent Environments*, pages 206–213. IEEE, 2012.

- [49] Sai Sree Laya Chukkapalli, Aritran Piplai, Sudip Mittal, Maanak Gupta, Anupam Joshi, et al. A smart-farming ontology for attribute based access control. In 6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020), 2020.
- [50] Paolo Brizzi, Dario Bonino, Alberto Musetti, Alexandr Krylovskiy, Edoardo Patti, and Mathias Axling. Towards an ontology driven approach for systems interoperability and energy management in the smart city. In 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pages 1–7. IEEE, 2016.
- [51] Laura Zavala, Pradeep K Murukannaiah, Nithyananthan Poosamani, Tim Finin, Anupam Joshi, Injong Rhee, and Munindar P Singh. Platys: From position to place-oriented mobile computing. *Ai Magazine*, 36(2):50–62, 2015.