Ontology driven AI and Access Control Systems for Smart Fisheries

Sai Sree Laya Chukkapalli
saisree1@umbc.edu
University of Maryland Baltimore County
Baltimore, Maryland, USA

Shaik Barakhat Aziz
sba6592@uncw.edu
University of North Carolina Wilmington
Wilmington, North Carolina, USA

Nouran Alotaibi
na8103@uncw.edu
University of North Carolina Wilmington
Wilmington, North Carolina, USA

Sudip Mittal
mittals@uncw.edu
University of North Carolina Wilmington
Wilmington, North Carolina, USA

Maanak Gupta
mgupta@tntech.edu
Tennessee Technological University
Cookeville, Tennessee, USA

Mahmoud Abdelsalam
mabdelsalam01@manhattan.edu
Manhattan College
Bronx, New York, USA

ABSTRACT

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, fishery 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.

Therefore in this paper, 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.

CCS CONCEPTS

• **Security and privacy** → *Access control*; • **Computing methodologies** → *Ontology engineering*; *Artificial intelligence.*

KEYWORDS

Smart Fisheries, Ontology, Cybersecurity, Access Control, Artificial Intelligence

SAT-CPS'21, April 28, 2021, Virtual Event, USA
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8319-6/21/04…$15.00
https://doi.org/10.1145/3445969.3450429

ACM Reference Format:
Sai Sree Laya Chukkapalli, Shaik Barakhat Aziz, Nouran Alotaibi, Sudip Mittal, Maanak Gupta, and Mahmoud Abdelsalam. 2021. Ontology driven AI and Access Control Systems for Smart Fisheries. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-physical Systems (SAT-CPS'21), April 28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3445969.3450429

1 INTRODUCTION

With the growing population there arises a need for increasing the food production to avoid food insecurity. This is applicable to produce like fishes which is an important source of food for millions people around the world [1]. Fishing industry is looking for 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. with the intention to increase productivity, quality of produce, etc. Fishery farmers are finding it difficult to meet the needs of growing demand with the application of traditional fishing techniques. Therefore, several fisheries are shifting towards internet connected ecosystems in order to feed the future. In addition, interconnecting the sensors present in fish farms via internet generates huge volumes of data points. These data points further assist the owners of fish farm in analyzing and monitoring the device data in real-time.

However, interconnecting the smart sensors present in the ecosystem have created a security blind spot. 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 [43]. For example, a smart home in Milwaukee was hacked by an attacker where the temperature of room was increased to 90 degrees Fahrenheit by utilizing a thermostat. [2]. Gupta et al. presented [16] 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 growing number of cyber-attacks on critical infrastructures.

In this paper, we introduce a secure smart fisheries ecosystem to protect the internet connected sensors from potential cyber-attacks and propose various AI applications that would aid the owners to effectively manage their fish farms. We design the architecture of smart fisheries ecosystem that has physical entities present in the physical layer, digital twin in the edge layer and 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 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 decision making process, marketing produce, in-depth insights to manage fish farms, early warning alerts, recruiting workers, etc.

The rest of the paper is organized as follows. Section II discusses the related work on various aspects such as smart fisheries, attacks on fisheries, access control solutions and AI applications. Section III explains the architecture, components and their interactions in smart fisheries ecosystem. Smart fisheries ontology is described in Section IV. Section V demonstrates access control decisions of our system in various security use case scenarios. Section VI presents various AI applications that would enhance smart fisheries ecosystem, followed by conclusion in Section VII.

2 RELATED WORK

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

2.1 Smart Fisheries

Smart Fisheries have become more popular in the global seafood market during the 21st century, as it is able to meet the growing demands for sea food and minimize the decline in the amount of fishes. In a project named SMARTFISH H2020 [32], the authors have proposed a system to ensure efficient functioning of the fishery ecosystem while reducing the ecological 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 taking 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 [31] solely from the fishery ecosystem. For example, quality of the water [4] can be evaluated timely for proper water treatment to prevent contamination by monitoring the data collected from the sensors such as the pH levels, temperature, salinity, etc. Another implementation to determine water quality in eel fish aquaculture was done by Salim et al. [38] where they monitor 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 security of the devices in various domains such as smart home [3, 35], smart farms [43], smart manufacturing [44], etc. Such kind of attacks can damage the entire smart infrastructure or incur a partial loss. Frustaci et. al.[14] discussed the vulnerabilities and security challenges faced due to incorporation of IoT devices. For example, the cyber attack on Puerto Rico [12] smart meter utility in 2009 led to 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 against intrusions. Similar kind of attacks can occur in smart fisheries since the sensors deployed are interconnected via Internet. Recently, Northwest Atlantic Fisheries Organization (NAFO) [47] has experienced a ransomware attack where the servers were unavailable for sometime. Additionally, attacks that spread lice and genetic introgression [25] within the stock in aquaculture infrastructure is another possible threat scenario that could bring irrecoverable loss to the ecosystem. Another example of cyber attack on fishery ecosystem occurred in South Korea[37] where hundreds of fishing boats had faced GPS jamming which caused difficulty in locating the nets at sea. Consequentially, reports show that Sunderland Marine [26] has 8,000 insurance policyholders over the world from the aquaculture industry due to the rising number of cyber attacks.

2.3 Access Control Solutions

Minimizing the security risks in the Internet connected devices is significantly important in order to avoid economic loss. Therefore, researchers have started incorporating access control models in their work since they allow or deny access to the devices based on the policy specification. Initially, traditional access control models like Discretionary Access Control (DAC) [29], Mandatory Access Control (MAC) [40] and Role Based Access Control (RBAC) [39] were implemented.

In DAC models, the type of access to the information is determined by the owner based on the users identity or the group to which they belong. A limitation of DAC models is that an unauthorized user can access the information due to the existence of multiple copies. To address this limitation, MAC that works based on a hierarchical model was developed. The access to the information is determined by a central authority (i.e. the administrator) and individual owners cannot assign their own permissions. Users can only access the information based on assigned clearance levels assigned. Furthermore, RBAC is an access control model based on group level permissions granted based on the user roles within an organization. A major disadvantage of RBAC model is what is known as 'role explosion' where the increase of different roles and permissions makes access management a highly complex task.

Attribute Based Access Control (ABAC) [17, 19] addresses the limitations of the aforementioned traditional access control models. In ABAC models, access is granted by evaluating attributes rather than roles. Recently, ABAC models have gained popularity due to its flexibility in grounding the context dependent policies.

Access control models when combined with Web Ontology Language (OWL) [42] describe the entities and their relationships present in the security policies where access control decisions are made by utilizing the power of reasoning. As such, researchers in various domains like smart home, smart farm, healthcare have started incorporating them. For example, Joshi et al. [20] developed a model to evaluate decisions based on rules by utilizing ABAC system in order to determine the access control to critical documents of an organization by considering the end to end encryption of the cloud service provider. Other ontology driven security systems have also been developed [15, 27, 28, 36]. In the agriculture domain, a smart farm ontology [10] based ABAC system was developed in order to evaluate access control requests in a smart farm. Dutta et al. [11] determine the access control for the devices present in smart home environment by utilizing ABAC model.

2.4 Applications of AI in smart fisheries

Recently cyber-physical systems coupled with AI applications have become widely popular as they increase productivity and economic profits. Various CPS domains have started utilizing AI based applications since they provide insights by analyzing large volumes of data from heterogeneous type of devices [8, 41]. For example, activity recognition of an occupant in smart home is implemented by utilizing deep learning model. Data collected from different sensors deployed in the home is the input to the model [46]. Similarly several AI applications that could be developed on a smart farm are mentioned by Chukkapalli et al. [9].

Maintaining ecological balance in the fisheries is quite important to support aquatic life. Therefore, researchers have developed AI based applications for fisheries ecosystem. For example, a low cost computer vision algorithms was developed by Papadakis et al. [33] to monitor the behavior of fishes in the tank where the stress factor is determined based on stocking density. An electronic remote monitoring [24] system was developed by Danish government in order to determine quantity of catch for all the fishermen and also monitor their action. Additionally, AI tools for identifying a hungry fish by the use of vibration based sensors and acoustic signals are developed. For instance, a company known as "eFishery" in Indonesia has developed a system that can dispense the right amount feed at the right time [21]. By using this technology, they can reduce cost of feed by about 21%. Similarly, Parra et al. [34] developed a system that dispenses right amount of feed for the fish by utilizing the sensors that monitor the behavior of the fishes present in the water. Vessel detection by utilizing image recognition algorithm is another example that tracks down illegal fishing was developed by Kanjir et al. [22]. A popular tool named vessel monitoring system [30] tracks fishing activities based on location, speed, etc. and provide it to the fishery management authority.

3 SYSTEM OVERVIEW

With an eye towards providing a secure environment for the fish farm owners, we have outlined a smart fisheries ecosystem shown in Figure 1 where they can cultivate fishes securely in a large scale using a small utility farm. 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 Internet. These insights will help the fish farm owners in the decision making process[18] in order to increase the produce, maintain ecological balance in the fisheries ecosystem, etc.

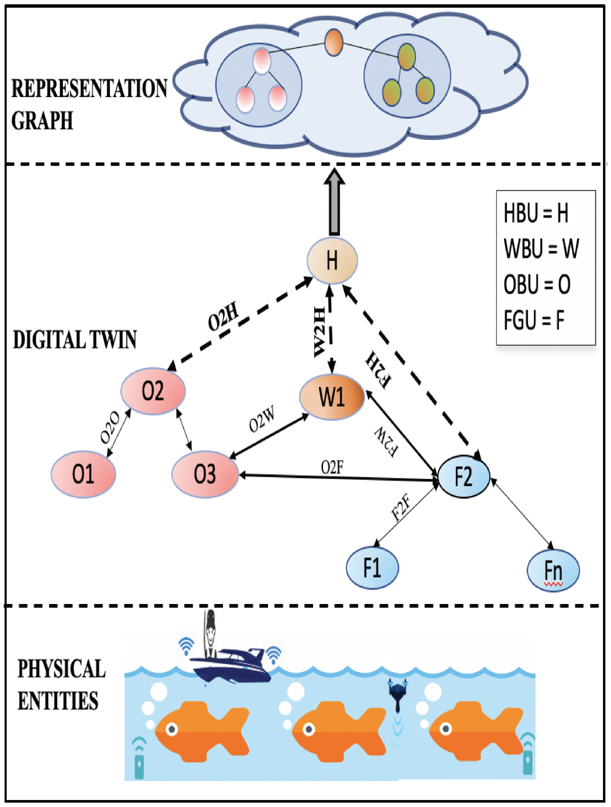

Figure 1: Architecture of our Smart Fisheries Ecosystem.

We have divided this section 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, second layer is the edge layer that performs computations at the node and 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.

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, water color, required amount of feed, plankton monitoring, etc. play 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 take right decisions in real-time scenarios. Sensors such as Arvo-Tec Autofeeders[1], Aqua TROLL Temperature/Conductivity Sensor[2] 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. As 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 an edge computing approach [13] 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 for every 10 seconds. Additionally, 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 offers various services such as data pre-processing, identifying abnormal patterns in the data and predicting outcomes such as quantity of feed, downtime of machinery, etc. based on historical data present in the cloud. The insights generated by these applications are communicated to fish 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 the 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 belong to any of the three layers such as physical layer, edge layer and cloud layer of the architecture.

3.2.1 Physical Entities. The physical entities that are depicted in the Figure 1 determine various interactions that happen in a 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 sensor, 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 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 others units like FGU, OBU, WBU and HBU present in the fish farm are stored as representation graph in the cloud units.
- *Worker Based Units (WBU)*: The workers employed to perform different tasks for the fish farm are represented as WBU. They utilize mobile or computer platform to monitor, communicate and operate FGUs and OBUs. There are two types of workers namely permanent and temporary workers. Fishery farm owners hire the workers based on their requirements to manage the farm. The level of access and role of each type of worker are described below:
  - Permanent Workers : Permanent worker are those workers that have a permanent access to the whole system or a part of system depending on the capabilities of worker 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 such as netting, catching fishes during the peak season. These workers are given a limited authorization in order to keep security robust, have minimum human error and avoid data leakage.
- *Home Based Unit (HBU)*: A centralized hub that is setup by the fish farm owner to interconnect all the units present in the fish farm is represented as Home Based Unit. The HBU is connected to the cloud via internet. Fish farm owner 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 is 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 a machinery in advance to reduce downtime by training machine learning models. Digital twins can also be utilized for maintaining the data security and privacy which is an added advantage. For example, unauthorized transmission of data can be avoided with the help of 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 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 top most 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 representation graph which has all the interactions like OBU-OBU, FGU-FGU, FGU-WBU, OBU-HBU, etc. that happen between the nodes. Also, the representation graph is immediately updated whenever communication happens between the nodes. For example, WBU tries to

[1] https://pentairaes.com/arvo-tec-robot-feeding-system.html
[2] https://in-situ.com/us/aqua-troll-temperature-conductivity-sensor

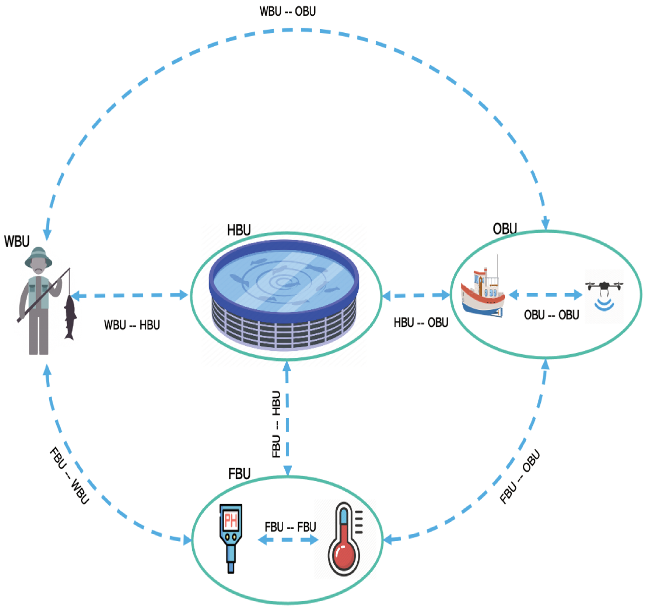

Figure 2: Interactions in a smart fisheries ecosystem.

know the readings of temperature sensor present in water. Information exchange happens between FGU and WBU that is automatically stored in the representation graph. Owners of the fishery farms can visualize all the interactions that happen in the fisheries ecosystem with the help of HBU.

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

3.3 Interactions

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

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 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 status of OBUs.

OBU-FGU: Interaction between OBUs and FGUs happen whenever an OBU wants to know the status of FGUs before performing an action. For example, 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 interaction between the OBU and FGU are stored in the representation graph that can be accessed by the fishery 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 are 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 recent interaction between OBU and WBU that can be viewed by the fishery farm owners. When the WBUs access to the equipment present in the fishery 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 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 take 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 which can be access by the HBU whenever required.

WBU-HBU: The HBU employs workers to work on the fishery farms who could either be permanent workers or temporary workers. The temporary workers get only temporary access to the 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.

4 SMART FISHERIES ONTOLOGY

A philosophical compilation of data is made to envelope all concepts and and its subcategories called as Ontology where properties describe the attributes of the concepts and relationships between them. Various domains such as security [45], medicine [6], finance [5], manufacturing [49], etc. have been utilizing ontologies for knowledge representation since they enable reuse of domain knowledge. As 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, class named Books represents all books where the book named "The Secret" would be an instance of this class. In the field of security itself there are multiple ontologies that are already existing to monitor their cyber physical ecosystems

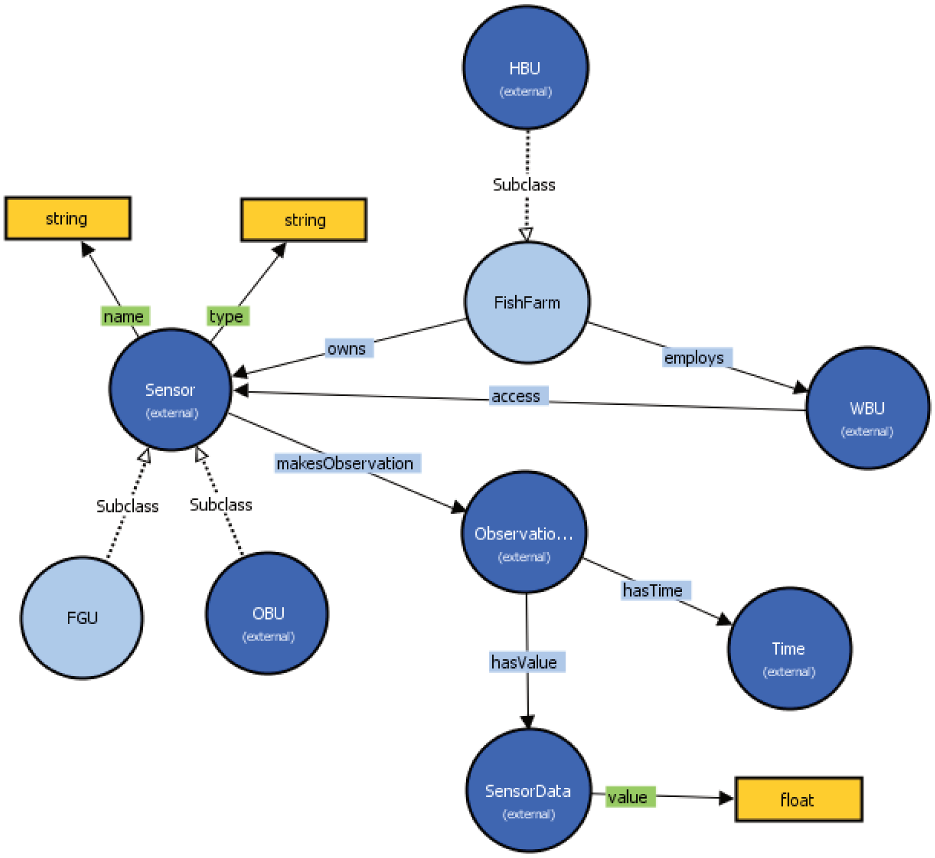

Figure 3: Smart Fisheries Ontology.

(CPS) such as smart home ontology [23], smart farm ontology [10], smart city ontology [7], etc. Considering the benefits and effectiveness of the above ontologies in securing their ecosystems, we planned to create an ontology for fisheries ecosystem.

Therefore, we have developed a smart fisheries ontology shown in Figure 3 by utilizing the architecture, components and interactions of the smart fisheries ecosystem described in Section III. We utilize this ontology for capturing data from the information exchange discussed in Section III-C between various sensors. Furthermore, access control of smart fisheries ecosystem in multiple use case scenarios mentioned in Section V can be determined based on our ontology. Also, various AI applications described in Section VI are built with help of this ontology. Our smart fisheries ontology consists of six main classes where the FishFarm class represents the owner of the fisheries ecosystem that maintains the fish farm, WBU class represents workers employed in the fish farm, Sensor class represents the devices owned by the fish farm, Observation class represents data collected, SensorData class represents a data value and Time class represents timestamp. Some of the important classes and relationships present in our ontology are described below:

4.1 Classes

- 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 smart fisheries ecosystem.
- HBU class: This class is represented as hub setup that keeps track of the information exchange between the sensors present in the fish farm. Moreover, HBU class assists the owners of the fish farm in taking key decisions by providing necessary information like status of the sensors for a specified time period.
- 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.
- 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.

- 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.
- OBU class: Movable machinery like vessel monitoring systems, drones, etc are treated as instances of this class. Information about change in status or current status of the devices can be obtained from this class.
- Observation class: This class has information such as data points, timestamp of the FGU and OBU class whenever there is change in status.
- SensorData class: This class represents observation value of movable and immovable sensors located in the smart fisheries ecosystem.
- Time class: This class provides the timestamp whenever an observation is recorded due to change in status of device (FGUs) or an action being performed on them(OBUs).

4.2 Relationships

- *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 Sensor class is the object entity.
- *employs*: This link provides information about current workers working in the fish farm. The subject entity is FishFarm class and object entity is WBU class.
- *makesObservation*: This property indicates that sub-classes of Sensor class has a new observation. Here, the subject entity is Sensor class and the object entity is Observation class.
- *hasData*: This relationship provides us with data value recorded by the physical sensors for every few seconds. The subject entity is Observation class and the object entity is SensorData class.
- *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 object entity is Time class.
- *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 object property is Sensor class.

5 ACCESS CONTROL USE CASES

In order to secure smart fisheries ecosystem, we utilize our developed smart fisheries ontology described in Section IV to develop Attribute Based Access Control (ABAC) framework. ABAC model 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 fishery farm is determined. To process the access requests based on context we include context class in our framework. We also included *Platys* ontology [48] to get details like time, data, location, etc. of sensors present in the farm. We discuss below the rules for multiple access control scenarios built on our ontology.

5.1 Scenario 1 - Permission to access FGU data

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

```
# 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 in 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)

5.2 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 fishery farm needs to be immediately updated to the owner. This way owner will have an idea about the current status of workers to grant future 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 follows:

```
# 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 every minute whenever there is a change in status of the WBU. This policy rule makes use of Platys ontology. The property named Duration states time interval at which the owner is updated about actions of Worker_1.

5.3 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 is completely in the control of the HBU. Therefore, authorized workers employed in the fish farm can operate only the allocated devices.

```
# 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_12020* can operate the drone(OBU) present in 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.

5.4 Scenario 4 - Access Permission to workers based on location

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

```
# 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 moves far away from the fish farm, it would immediately loose access.

6 AI ASSISTED APPLICATIONS

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

6.1 Decision Support System

Decision Support System is an important real time application in the smart fisheries ecosystem. Typically, data collected from sensors in smart fisheries ecosystem are stored in the cloud. Based on the analysis of such data, AI tools can take decisions or provide recommendations regarding the amount of feed for the fish, resource usage, operational scheduling, etc. This helps in reducing the production costs for the ecosystem while increasing the productivity. For example, fishery farmers can decide the right time and optimal quantity of feed needed for the fish by analyzing the previously collected data stored in the cloud. In this way, contamination of water can be avoided that is caused due to excessive feed present in the fisheries ecosystem.

Similarly, fishery farmers can make decisions in advance regarding purchasing or borrowing an 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. Also, fishes death due to power failure, pipe clogging, excessive amount of unwanted contents in the water, etc. can be avoided with advance strategic planning. For example, quantity of filtration units required to be present can be purchased prior to harvesting by the HBUs as it is a necessary equipment that regulates ammonia and nitrate content in the tanks.

6.2 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. Specially, data collected from the smart fisheries ecosystem can also be utilized for marketing the quality of the product. For example, fishery farm owner can get USDA Organic seafood certification for the produce by utilizing data obtained from FGUs and OBUs. Acquiring this certification before marketing the product will be beneficial since it will attract consumers due to the transparency maintained by the fisheries. Also, recommendations for growing certain species based on environmental conditions and demand for the product in the market can also be provided to the HBUs. In this way, fishery farmers have an idea on what type of species to grow in their fishery farms depending on the nature of the geographical area. For example, based on the recommendations, HBUs can select fish species suitable to grow in their region.

Additionally, AI tools can be used to increase the sales and avoid wastage of produce by tracking down daily range of sales or previous sales history during 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.

6.3 Vision based Insight Generation

In-depth analysis such as recognizing the defects in fishes (e.g., shrink in size or length of the fish) 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. Such insights can aid the fish 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 utilizes 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 to identify environmental changes in the ecosystem and provide HBU with insights to better manage the fish farms.

6.4 Early Warning System

An early warning system for the fisheries ecosystem will ensure the survival of the aquatic life by alerting the fishery 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 growth of aquatic life. Therefore, data collected from the sensors such as FGUs and 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 early warning system is predicting downtime of machinery, such as OBUs and FGUs, that are utilized in managing the fisheries ecosystem. Identifying and tracking down the abnormal behavior of sensors by utilizing predictive maintenance application can help reduce heavy maintenance costs incurred due to failure 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. In this case, it minimizes the unexpected and sudden failure of machinery.

6.5 Worker Hiring 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 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 the fish farms only during the harvesting period. Such tool can assist the fishery farm owners as they can avoid conflict when there is high demand for labor which could delay the harvest. Additionally, it can also help in employing both temporary and permanent workers in that particular geographical area who would match the expertise required by the fishery farm owners.

7 CONCLUSION

The increase in popularity of cyber-physical systems as they can interconnect various smart sensors via internet has led to the rise of smart ecosystems in various sectors such as 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 above benefits, fishery farmers have started adopting smart fisheries technology in order to increase the quality and quantity of produce for maximizing their profits. Additionally, smart fisheries ecosystems also enables the fishery farmers to monitor the interactions, control their devices remotely, etc. However, interconnecting these devices through 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 paper, we developed a secured smart fisheries ecosystem that would be beneficial to the fishery farmers and also prevent attackers from exploiting the ecosystem that could incur huge losses. The paper 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 have 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 few use case scenarios to show how access controls requests are handled. Furthermore, we mention AI applications that could assist fishery farmers in maintaining the fish farms.

REFERENCES

[1] [n.d.]. An inventory of new technologies in fisheries. https://www.oecd.org/greengrowth/GGSD_2017_Issue%20Paper_New%20technologies%20in%20Fisheries_WEB.pdf.

[2] 2019. Felt so violated:'Milwaukee couple warns hackers are outsmarting smart homes. https://www.fox6now.com/news/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes.

[3] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. 2020. 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*. 207–218.

[4] Kofi Sarpong Adu-Manu, Cristiano Tapparello, Wendi Heinzelman, Ferdinand Apietu Katsriku, and Jamal-Deen Abdulai. 2017. Water quality monitoring using wireless sensor networks: Current trends and future research directions. *ACM Transactions on Sensor Networks (TOSN)* 13, 1 (2017), 1–41.

[5] Duygu Altinok. 2018. An ontology-based dialogue management system for banking and finance dialogue systems. *arXiv preprint arXiv:1804.04838* (2018).

[6] Timothy W Bickmore, Daniel Schulman, and Candace L Sidner. 2011. A reusable framework for health counseling dialogue systems based on a behavioral medicine ontology. *Journal of biomedical informatics* 44, 2 (2011), 183–197.

[7] Paolo Brizzi, Dario Bonino, Alberto Musetti, Alexandr Krylovskiy, Edoardo Patti, and Mathias Axling. 2016. 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)*. IEEE, 1–7.

[8] Nitu Kedarmal Choudhary, Sai Sree Laya Chukkapalli, Sudip Mittal, Maanak Gupta, Mahmoud Abdelsalam, Anupam Joshi, et al. 2020. YieldPredict: A Crop Yield Prediction Framework for Smart Farms. (2020).

[9] S. S. L. Chukkapalli, S. Mittal, M. Gupta, M. Abdelsalam, A. Joshi, R. Sandhu, and K. Joshi. 2020. Ontologies and Artificial Intelligence Systems for the Cooperative Smart Farming Ecosystem. *IEEE Access* 8 (2020), 164045–164064.

[10] Sai Sree Laya Chukkapalli, Aritran Piplai, Sudip Mittal, Maanak Gupta, Anupam Joshi, et al. 2020. A Smart-Farming Ontology for Attribute Based Access Control. In *6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020)*.

[11] Sofia Dutta, Sai Sree Laya Chukkapalli, Madhura Sulgekar, Swathi Krithivasan, Prajit Kumar Das, Anupam Joshi, et al. 2020. Context Sensitive Access Control in Smart Home Environments. In *6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020)*.

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

[13] Joao C Ferreira and Ana Lucia Martins. 2019. Edge computing approach for vessel monitoring system. *Energies* 12, 16 (2019), 3087.

[14] M. Frustaci, P. Pace, G. Aloi, and G. Fortino. 2018. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal* 5, 4 (2018), 2483–2495.

[15] Aditi Gupta, Sudip Mittal, Karuna P Joshi, Claudia Pearce, and Anupam Joshi. 2016. Streamlining management of multiple cloud services. In *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)*. IEEE, 481–488.

[16] Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* 8 (2020), 34564–34584.

[17] Maanak Gupta and Ravi Sandhu. 2016. The GURA$_G$ Administrative Model for User and Group Attribute Assignment. In *International Conference on Network and System Security*. Springer, 318–332.

[18] H.Poor. 1985. An Introduction to Signal Detection and Estimation. (1985).

[19] Xin Jin, Ram Krishnan, and Ravi Sandhu. 2012. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. (2012), 41–55.

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

[21] VV Jothiswaran, T Velumani, R Jayaraman, et al. 2020. Application of Artificial Intelligence in Fisheries and Aquaculture. *Biotica Research Today* 2, 6 (2020), 499–502.

[22] Urška Kanjir, Harm Greidanus, and Krištof Oštir. 2018. Vessel detection and classification from spaceborne optical images: A literature survey. *Remote sensing of environment* 207 (2018), 1–26.

[23] Ji Eun Kim, George Boulos, John Yackovich, Tassilo Barth, Christian Beckel, and Daniel Mosse. 2012. Seamless integration of heterogeneous devices and access control in smart homes. In *2012 Eighth International Conference on Intelligent Environments*. IEEE, 206–213.

[24] Lotte Kindt-Larsen, Eskild Kirkegaard, and Jørgen Dalskov. 2011. Fully documented fishery: a tool to support a catch quota management system. *ICES Journal of Marine Science* 68, 8 (2011), 1606–1610.

[25] Richard Green Lawrence Baker. [n.d.]. Cyber Security in UK Agriculture.

[26] Sunderland Marine. 2019. Cybersecurity: a growing concern.

[27] Sudip Mittal, Anupam Joshi, and Tim Finin. 2017. Thinking, fast and slow: Combining vector spaces and knowledge graphs. *arXiv preprint arXiv:1708.03310* (2017).

[28] Sudip Mittal, Anupam Joshi, and Tim Finin. 2019. Cyber-all-intel: An AI for security related threat intelligence. *arXiv preprint arXiv:1905.02895* (2019).

[29] Tawfik Mudarri, Samer Al-Rabeei, and Samer Abdo. 2015. SECURITY FUNDAMENTALS: ACCESS CONTROL MODELS. *Interdisciplinarity in theory and practice* (08 2015).

[30] S Nguyen-Khoa, Matthew McCartney, S Funge-Smith, L Smith, SS Sellamuttu, and M Dubois. 2020. Increasing the benefits and sustainability of irrigation through integration of fisheries: A guide for water planners, managers and engineers.

[31] EDF Oceans. 2020. Smart Fisheries for the 21st Century.

[32] Hüseyin Özbilgin. [n.d.]. Smart fisheries technologies for an efficient, compliant and environmentally friendly fishing sector–SMARTFISH H2020. *Mediterranean Fisheries and Aquaculture Research* 1, 2 ([n. d.]), 98–99.

[33] Vassilis M Papadakis, Ioannis E Papadakis, Fani Lamprianidou, Alexios Glaropoulos, and Maroudio Kentouri. 2012. A computer-vision system and methodology for the analysis of fish behavior. *Aquacultural engineering* 46 (2012), 53–59.

[34] Lorena Parra, Laura García, Sandra Sendra, and Jaime Lloret. 2018. The use of sensors for monitoring the feeding process and adjusting the feed supply velocity in fish farms. *Journal of Sensors* 2018 (2018).

[35] Aritran Piplai, Sai Sree Laya Chukkapalli, and Anupam Joshi. 2020. NAttack! Adversarial Attacks to bypass a GAN based classifier trained to detect Network intrusion. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE, 49–54.

[36] Vishal Rathod, Sandeep Narayanan, Sudip Mittal, and Anupam Joshi. 2018. Semantically Rich, Context Aware Access Control for Openstack. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 460–465.

[37] REUTERS. 2016. South Korea Revives GPS Backup After Cyber Attack.

[38] Taufik Ibnu Salim, Triya Haiyunnisa, and Hilman Syaeful Alam. 2016. Design and implementation of water quality monitoring for eel fish aquaculture. In *2016 International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 208–213.

[39] Ravi S Sandhu, Edward J Coyne, Hal L Feinstein, and Charles E Youman. 1996. Role-based access control models. *Computer* 29, 2 (1996), 38–47.

[40] Ravi S Sandhu and Pierangela Samarati. 1994. Access control: principle and practice. *IEEE communications magazine* 32, 9 (1994), 40–48.

[41] H. Sedjelmaci, F. Guenab, S. Senouci, H. Moustafa, J. Liu, and S. Han. 2020. Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems. *IEEE Network* 34, 3 (2020), 6–7.

[42] Nitin Kumar Sharma and Anupam Joshi. 2016. Representing attribute based access control policies in owl. In *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)*. IEEE, 333–336.

[43] Sina Sontowski, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, and Ravi Sandhu. 2020. Cyber Attacks on Smart Farming Infrastructure. *UMBC Student Collection* (2020).

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

[45] Bill Tsoumas and Dimitris Gritzalis. 2006. Towards an ontology-based security management. In *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, Vol. 1. IEEE, 985–992.

[46] TLM Van Kasteren, Gwenn Englebienne, and Ben JA Kröse. 2010. Activity recognition using semi-Markov models on real world smart home datasets. *Journal of ambient intelligence and smart environments* 2, 3 (2010), 311–325.

[47] Cliff White. [n.d.]. Northwest Atlantic Fisheries Organization hit by ransomware attack.

[48] Laura Zavala, Pradeep K Murukannaiah, Nithyananthan Poosamani, Tim Finin, Anupam Joshi, Injong Rhee, and Munindar P Singh. 2015. Platys: From position to place-oriented mobile computing. *Ai Magazine* 36, 2 (2015), 50–62.

[49] Jiehan Zhou and Rose Dieng-Kuntz. 2004. Manufacturing ontology analysis and design: towards excellent manufacturing. In *2nd IEEE International Conference on Industrial Informatics, 2004. INDIN'04. 2004.* IEEE, 39–45.