Effective & Efficient Access Control in Smart Farms: Opportunities, Challenges & Potential Approaches

Ghadeer I. Yassin and Lakshmish Ramaswamy
Department of Computer Science, University of Georgia, Athens, GA 30602, U.S.A.

Keywords: Access Controls, Smart Farming, Precision Agriculture, IoT.

Abstract: The Internet of Things technologies has revolutionized the sector of farming and agriculture. It also helped it to face the current environmental and societal challenges. IoT technologies are able to assist the farming sector in many different applications including reducing wasted resources, real time monitoring of crops, monitoring environment conditions, precision agriculture, farm data analytics and improving crops quality, while decreasing the number of workers needed to complete farm related tasks. However, the nature of the Smart farms are diverse in terms of the number, type and location of the installed smart devices, the variety of the collected data, the number and type of workers who help in the farm and have access to farm related data and equipment. At the same time, Farmers are very protective of their own data and sometimes refrain from incorporating smart farming technologies to insure the safety of their data. Therefore, in this paper we outline the security challenges in smart framing settings and explain the need for multi-user, multi- device aware access controls in smart farms. We highlight different possible security scenarios that challenge the adoption of IoT solutions in smart farms and discuss possible solutions.

1 INTRODUCTION

The world population is expected to increase to 11.2 billion by the end of the century according to the United Nations (Roser, 2013). With the rapid growth in world population, the food consumption worldwide grows rapidly as well, it is estimated that food production must increase by 70 % to feed this population (Bruinsma et al., 2009). As a consequence farmers are facing a growing demand to produce more food regardless of the struggle they endure because of the climate change, the scarcity of water, the extreme weather conditions and more (aer, 2021). In order to increase the yields of their farms to meet that demand, farmers are turning into smart farming.

"Smart farming" combines traditional agricultural methodologies with actuators, sensors, Internet of Things (IoT), Information and communication technology (ICT) and drones to provide the farmers with precise and accurate information that help in optimizing farming tasks with less labor force, increasing crop yields, improving crops' quality, decreasing the waste in resources such as water, fertilizers and herbicides while increasing farm profitability. Smart farming follows a cycle that includes observing data from the surrounding environment then ensuring it follows a set of predefined rules, identifies any deficiencies and informs the users about them to take the appropriate action if needed.

Smart farms are considered a multi-device environment in the sense that multiple smart devices can be found scattered across the farm such as Drones, Animal's wearable devices, Soil moisture sensors and more. It is also considered a multi-users environment with a significant number of human workers cooperating to monitor the environment data and make informed decisions. In addition to that, There is heterogeneous data related to farms originating from multiple sources such as sensor data, satellite imagery and farm historical data. Each data type has a validity period and a unique value associated to it based on the information derived from this data and how this information can be used. This derived information can have great impact on the livestock health and wellbeing, the farm value and the owners themselves. Therefore, effective access control mechanisms are needed in smart farms to ensure the security of its data considering its diverse nature.

In this paper, we highlight the importance of effective access control mechanisms in smart farms. We compare and contrast smart farm nature with other smart domains as well as the security challenges that

Yassin, G. and Ramaswamy, L.
Effective Efficient Access Control in Smart Farms: Opportunities, Challenges Potential Approaches.
DOI: 10.5220/0010873000003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 445-452
ISBN: 978-989-758-553-1; ISSN: 2184-4356

face smart farms. We discuss which access control mechanisms could be suitable for the smart farm system and discuss some potential solutions and approaches.

2 BACKGROUND INFORMATION

2.1 Smart Farm

A Smart Farm in its simplest form is a combination of computing devices, machine learning (ML), artificial intelligence (AI) and humans integrated into an information driven system that is capable, knowledgeable and a real time-decision maker, therefore," a Smart System". Smart farm's sensors and equipment have a predefined function related to the farm that can be as simple as collecting temperature data or as complicated as harvesting ripened crops and leaving unripened ones behind.

Figure 1 Shows the different entities in smart farms and the interaction that takes place among them. Different sensors collect huge amounts of farm-related data and are connected to gateway devices that perform preprocessing steps such as filtering and analyzing the collected data and transfer only the necessary data to the cloud services where it can be further processed and stored then presented to the user through suitable interfaces.

2.2 Smart Systems

IoT technology and its applications are currently used in multiple smart systems such as smart homes that contain multiple IoT devices connected together and to the internet through a communication protocol and are controlled, accessed and monitored remotely using a mobile application or voice commands issued to a smart assistant. In addition, smart health care refers to completely autonomous and connected healthcare solutions provided for patients along with feedback from doctors. Smart Cities, on the other hand, refers to any city that utilizes modern technologies to convert conventional city's entities into an autonomous entity and consists of a collection of smart services such as city lighting, emergency services, traffic management, water management etc.

2.3 Data Sources & Analytics

Smart farms are majorly driven by data and its analytics. Sensors detect changes and collect data about their environment. While actuators introduce change

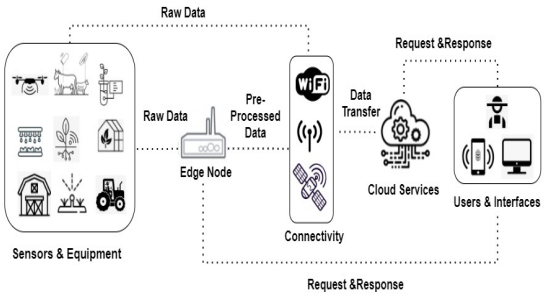

Figure 1: Different Smart Farm Entities' Interaction.

to its environment based on the sensor's collected data. This is a real time process that is mostly automated. There are major domains in smart farms that use the heterogeneous data collected by sensors and apply them in different applications that are capable of providing the farmers with the most accurate analytics to help them improve farm productivity and decrease human interventions as shown in Figure 2.

Precision Farming: Achieved through multiple monitoring and controlling applications including continuous weather monitoring, Crop's health monitoring and Soil analysis which is one of the most important applications of precision farming that helps to easily decide the best type of crops to plant in the soil, the best timing to start sowing etc.

Precision Livestock: Achieved by providing livestock with different monitoring sensors and veterinary wearable devices to continuously detect, analyze and transmit data related to the animal's health and location.

Smart Greenhouse: Enables planting different types of plants anytime of the year regardless of the weather conditions by precisely monitoring and controlling its climate.

2.4 Access Control Policies

Access control refers to processing every request to the system's data and resources, then deciding whether it should be denied or granted. Access controls identify users through verifying their login credentials and then grant them the appropriate access level that is associated with their authenticated credentials.

There are different access control policies that can be used in smart systems based on its requirements including the "RBAC" model that manages the access to the different resources based on hierarchical rights and permissions assigned to various roles. "ABAC" model, on the other hand, shifts from the list of roles to a list of attributes and contextual factors by evaluating requests against the requester's attributes, the required action, and the context. "MAC" model lim-

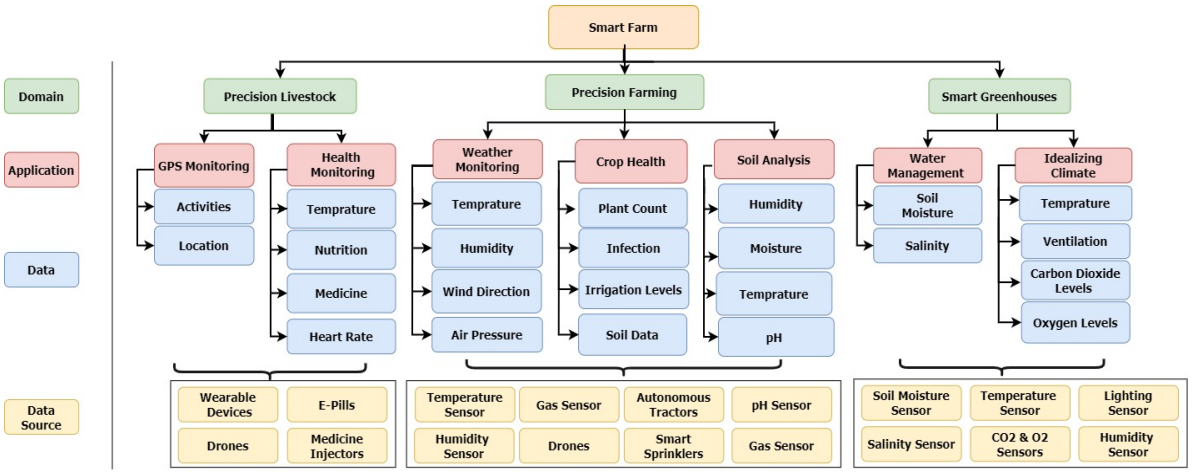

Figure 2: Main Smart Farms' Domains, Applications, Data & Data sources.

its access to system resources based on its sensitivity and the user's authorization to access a resource with that specified sensitivity. "TBAC" enables placing restrictions on the access to resources and its data on the basis of particular time of the day or particular days of a week. Finally, "LBAC" restricts the access to resources based on the location of the user so that the users can access the resource only if they are physically present in the predefined location.

3 MOTIVATION

Many farming systems use insufficient access controls and new smart farming related projects do not consider using them. (De Araujo Zanella et al., 2020). On the other hand, smart farms have a unique nature that requires specialized access control solutions.

3.1 Comparing Smart Farms with Other Smart Systems

There is a wide range of differences and similarities between Smart farms and other Smart systems as shown in Table 1. These differences indicate that security-related countermeasures applied to other Smart systems are not suitable for Smart Farms.

Stakeholders & Security Awareness: In smart farms, The stakeholders range is very wide and the system is very dynamic as the owners usually hire different workers based on the farming season or the scalability of their farm. The stakeholders have different levels of security awareness. Owners are more aware about security since their main goal is to protect their data as it directly affects their profitability if it were to be stolen or leaked to a rival. However, other stakeholders usually have much less awareness about security and might not be concerned about it since it does not directly affect their profit.

Similar to Smart Farms, The stakeholders range in Smart Cities and Smart Healthcare is wide. However, they are usually provided with technical security training on how to protect their data. Those Systems are less dynamic than smart farms as the stakeholders are hired by the government and their change is much less frequent when compared to smart farms.

Data Security: Smart Farming security systems are in their infancy. Very little efforts are being taken to ensure the security of farm data. In addition, farms are mostly self-financed by their owners who do not have enough finance to implement enough security measures. Smart Homes are also self-financed systems but their security measures might not be as costly as Smart Farms and therefore its owner can easily support it. Other systems such as smart healthcare and smart cities are supported by many organizations and a lot of investment is being offered to them.

3.2 Data Validity

Farm data originates from various sources such as sensor's data, satellite data or historical data. Each type of the data has its own validity period; whenever passed, the data is deemed useless. The validity periods range from long validity such as the yearly planted crops in the field to seasonal validity such as season's weather data to short term validity such as soil moisture data that are acted upon immediately. Therefore, the data should be stored and protected during its validity period and erased otherwise. For example, whenever a livestock animal is sold or sent to a slaughterhouse, its data becomes unnecessary to store and therefore should be deleted immedi-

ately while soil data should be deleted once it is analyzed and provided to the farmer etc.

3.3 Farm Ownership

Farms can be owned, rented and operated by different types of owners (Bigelow et al., 2016), (Bigelow, 2019) such as families, non-operator landlords, operator landlords, cooperatives etc.

Family Farms: In family farms, the decision makers are typically the owners of the equity and the assets who usually assign predefined tasks to the other family members. However, a lot of conflicts happen between the family members. Therefore, the family holds a broad meeting to discuss members' roles and responsibilities and negotiate their demands. Therefore, it would be beneficial to propose access control mechanisms that support the negotiations of roles and demands and ensure they are enforced.

Rental Farms: The operator landlords of rented farms usually have conflicts with the tenants due to their involvement in farm decisions as both of them combine their own resources to produce the required farm commodities. Typically, they negotiate their terms and create a farm lease contract describing their agreement that covers the amount of fertilizers that will be used, the time when a specific equipment will be used, the time when the field will be harvested etc. However, the conflicts happen due to the unawareness of the landlord about certain circumstances that affect the execution of the agreement. Therefore, granting access of the farm data to landlords based on a predefined role and agreement will keep them more aware of circumstances and thus eliminate such conflicts.

Partnership Farms: Partners and cooperatives have conflicts over the share of each partner; some farm assets such as livestock or crops might belong to one partner only. Those assets and their related data shouldn't be accessible by the other partners as they are out of the scope of the partnership. Therefore, access controls should be flexible enough to suit assets' data accessibility based on such cases.

3.4 Participants' Profiles

Figure 3 assumes the different in-farm and outside-farm access attempts to different smart devices and sensors. The figure shows 8 different individuals interacting with the smart farm based on their assigned tasks. Both workers A and B are responsible for field sowing and irrigation. Therefore, they have access to plant data and soil data. Worker C is the only worker permitted to monitor the autonomous tractor. Therefore, its accessibility is granted only to him and he is restricted from accessing any other equipment or data in the farm system. On the other hand, Worker D is granted accessibility to the drone when he is present inside the field and is denied accessibility otherwise. Other individuals such as the veterinarian and worker G are involved in occasional animal health monitoring and therefore do not need continuous access to the animal data.

Temporary Labor: It is common to hire temporary labor at the time of harvesting or sowing. The main problem that faces the farm owner with temporary labor are the trust issues. Those workers are mostly coming to work in the farm for the first time and are not trusted as other permanent workers and they might abuse farm related data by uncovering them to a rival or by disrupting the system by modifying sensor's parameters causing it to perform unnecessary actions that leads to profit losses. The accessibility granted to temporary workers should be limited and end by the time their hiring period ends to ensure they will not be able to abuse the system in any form once they are no longer hired.

Labor Working on Multiple Farms: Some workers work in two or more different farms simultaneously. Through those workers, a farm rivalry or a competitor might gain access or insight to the farm data and could use it to develop competing crops to increase their profitability. The data about the owners' farm practices can also be used against them for regulatory enforcement purposes. Therefore, farm owners should decide which and when their data is accessed by workers. For example, owners may choose to automatically notify the worker to turn on/off an irrigation system without receiving soil moisture data from soil sensors. They also may want to limit workers from accessing data outside the daily working hours or to prevent them from receiving full farm's history data.

Other Participants: The range of farm participants is not limited only to farm workers and owners but it also includes government officials, technicians, academic researchers, veterinarians etc. Therefore, The farm owners should be able to control accessibility to their own resources based on what they believe is protecting its security.

3.5 Livestock

Security of livestock's data is often neglected as it is not classified as personal data and hence very little attention is paid to its security. However, Livestock data is a very precious part of farm data.

Livestock Location Data: Livestock location data is continuously collected by GPS-powered wearable devices and drones. This data is used to track the ani-

Table 1: Differences and Similarities between Different Smart Systems.

	Smart Farms	Smart Cities	Smart Healthcare	Smart Homes
Stakeholders' Range	Wide	Wide	Wide	Small
Security Awareness	Lacked	High	High	Medium
System Dynamism	High	Low	Low	Non
Devices Power	Low	High	High	High
Device location	Outdoor	Hybrid	Indoor	Indoor
Maintenance Frequency	Low	High	High	Low
Security Measures	Weak	Strong	Strong	Medium
Connectivity	Unstable	Stable	Stable	Stable
Financed By	Self	Organizations	Organizations	Self

mals when it is left to feed in open areas. However, If adversaries or some untrustworthy workers were incorrectly permitted access to only one animal location data, they can plan to steal the animal and compromise the safety of the whole herd.

Livestock Health Data: It is the most crucial part of the livestock collected data and greatly influences its market prices. Therefore, purchasers can be granted access to the animal's data in order to make an informed decision. General live-stock's data such as previous health conditions might be used to negotiate the offered prices with the owner. In addition, accessibility to the full herd data can lead to inferring information about herd size and value. Therefore, the accessibility should be very limited and only temporary during the purchasing process.

Veterinarians & Assistants: Some veterinarians work with different farms in the same area and can easily anticipate health issues breaking out in that area through monitoring and combining livestock health data from different farms. They can take advantage of such knowledge to propagate exaggerated news about infectious spread and influence the livestock market price and consequently make profit themselves by investing in livestock. Beside that, the assistants and nurses working in the veterinarian's office access livestock health data to prepare health summaries or to assign periodic timing for vaccination. In this case, they should be granted a lower level of accessibility to the data or to be granted accessibility only upon request.

Critical Data: When treating livestock with medications, it is very important to use the appropriate dosage which is generally determined in relation to the animal's weight. Overdosing can cause death while underdosing may lead to drug resistance. Therefore, such data should be secured to prevent adversaries from harming the livestock .

Livestock Environment: The environment where the animals are kept is monitored with different types of sensors to prevent animal sickness and death. If a rivalry gained accessibility to these sensors, they could make adverse conditions inside the barns to affect the yield of the animals or make them sick.

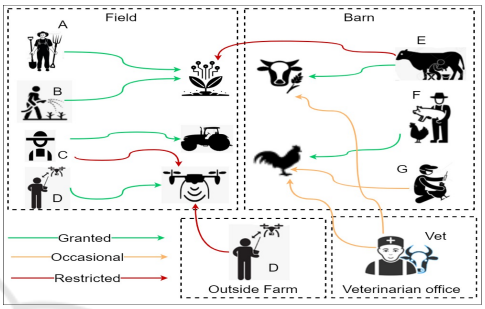

Figure 3: Farm Operations & Accessibility.

3.6 Smart Equipment

Smart farming depends heavily on a large number of smart equipment with various security related aspects that need controlled access control policies.

Leasing, Lending & Borrowing: Smart farm equipment are very expensive. Therefore, farmers turn to leasing them. However, leased equipment can collect sensitive crop yield data, fertilization's application rates, field conditions etc. This data can infer the financial position of the farm and also affect the selling prices of crops. Therefore, leased equipment should be subject to access control negotiations between the farmer and the leasing company. Some farmers also tend to lend and borrow equipment from neighboring farms. Therefore, both farm's data can be combined to infer information about crop health in the area and animal disease outbreaks. Therefore there should be specific access control mechanisms to ensure that the lender and the borrower of the equipment do not obtain data about each other's farms. This can be achieved through policies that ensure data collection is restricted by the location of the equipment as well as the time of the use.

Equipment Repairs: Some companies such as John Deere had made it illegal to repair their farm tractor (Horton and Kirchmeier, 2020). And in case of the

tractor malfunction, the farmer will be forced to repair the tractor at the company which will possibly need access to the tractor sensors and data to identify the source of the malfunction. In this case, the farmer should be dynamically notified of any attempted access to his equipment's data through access control requests and to have power to accept or deny such requests.

Specialized Equipment: Some equipment such as drones can collect a huge amount of data about the food production process, location of critical infrastructure, footage of workers and livestock etc. Those drones might be incorporated from other traditional IoT sectors such as the military sector. This sector's drones are capable of monitoring and identifying their users and tracking their performance and can compromise the security of the whole smart farm system.

Critical Data: The pH levels are very critical to the health of the crops. only specific levels allow the nutrients to be more available and effectively absorbed by the plants. Any tamper of these levels can lead to deficiencies in plant nutrients or plant toxitization if it was not corrected by farmers. It can be corrected by adjusting the ammonium supply levels. If adversaries get insight to this critical type of data, they can plan a physical attack that aims to temper the pH level with required levels of ammonium that ensure that the crops will be damaged.

4 RESEARCH QUESTIONS

There are multiple access control policies that can be applied to smart settings in general as discussed in section 2.4. However, Identifying which of these policies are relevant to smart farms and can be practically applied to it might be tricky. Therefore, we discuss some of the questions that are critical for determining the best access control mechanism that suits farms.

1. Are the Policies based on Devices or Capabilities?

Current access control policies implementations in other smart systems are mostly device-based. That means that the access is either granted or denied per the device itself. However, this implementation is not flexible enough to capture the access control desires that the farmers may think of to protect their data. Therefore, the policies shouldn't be simplified for device control only but rather it should be expanded to involve its capability as well. This is driven by our observation that the majority of smart farm devices combine multiple capabilities with different sensitivities in a single device. For example, Drones are capable of tracking livestock and spraying fields. The sensitivity of livestock tracking might be higher than spraying fields from the farmers point of view. While other capabilities such as erasing sensor's data is very critical and might not be granted to any of the stakeholders. Therefore, a capability-centric model should be designed where the capabilities that can be performed over each smart device can be defined.

2. Which Contextual Factors Affect the Policies?

Some contextual factors might be essential to consider with access control policies such as:

Location of the Devices: Ensures that certain devices' capabilities are used with devices in certain locations.

Location of the Stakeholders: Ensure that stakeholders are restricted from using certain capabilities unless they are connected to the farm network.

Time of Use: Is important especially for tasks that should be timed in advance.

Presence of Others: Is important for some capabilities that require supervision from others.

3. Should Policies Vary based on the Roles?

Since there are many roles assigned to different individuals inside the farm, those roles must play an important factor when deciding the suitable access control policies. For instance, the owner's role differs from a regular worker's role and therefore the individual with the owner role should be able to express access controls over the individual with a regular worker role. Also, a returning temporary worker might be more trusted than a new temporary worker and therefore can be assigned a role with more flexible access controls in the farm system.

4. What happens when Access Controls Fail?

There are consequences for system malfunctions related to access controls including:

False Acceptance: This type of malfunction refers to granting accessibility to some individual who was originally intended to be denied it. The severity of this malfunction depends on who was allowed incorrect access control. For example, a mild false acceptance might be caused by allowing co-owners access to a capability they don't need. A more severe case would happen if a temporary worker was falsely allowed access to a critical capability such as deleting sensor's data. The severest form would be granting access to a 3rd party individual such as a farm rival.

False Rejection: This type of malfunction refers to denying accessibility to some individual who was originally intended to be granted it. The severity of this type of malfunction might be less problematic than the false acceptance malfunction. However, it might disrupt essential work schedules and cause losses of profits.

Continuous Accessibility: This failure comes in the

form of granting continuous accessibility to individuals who were supposed to access the system for a specific period of time. Therefore, a policy expiration option should be provided to allow only temporary access for data and devices for as long as needed and to revoke that access automatically once that period ends in order to avoid any undesired accessibility.

5. How to Design Default Policies?

The process of assigning policies can be simplified through default policies such as:

Default Accept: That can be provided in a very cautious manner to the most trusted roles over some prespecified capabilities. It can also be provided over minor capabilities or data that are considered risk-free.

Default Deny: Should be implemented over critical capabilities such as erasing sensitive data and any administrative capabilities such as adding and removing users and devices to the system.

5 DISCUSSION & POTENTIAL APPROACHES

Reflecting on the research questions, Different Access control policies can be used in smart farm systems.

Role-Based Access Control "RBAC": This model can be used to ensure that stakeholders have access only to the resources they need to complete their jobs. The accessibility can be restricted based on the individual's assigned role as roles can determine the permissions granted to each individual and ensure that no individual can perform higher level operations on farm resources. Hierarchy of the roles allows specific roles to inherit permissions from other roles. This will benefit the higher level roles such as Owners-role to share the responsibility of adding new users to the system, assigning access policies for them and adding or removing smart devices from the system etc.

The different roles that can be implemented in Smart farm system includes: Owner, veterinarian, veterinarian assistant, temporary field worker, regular field worker, purchaser etc. As hierarchy suggests, the role of temporary field worker can inherit some access controls and permissions from the regular field worker role etc.

However, Hierarchical roles might be a major cause of conflicts between stakeholders when they have conflicting access control demands over system resources. Therefore, resolving this kind of conflict should be achieved automatically. The smart system should be aware and able to identify conflicts and resolve them based on the priority of each role in the hierarchical level.

As per the contextual factors that affect access control policies both LBAC and TBAC models can capture the majority of them.

Location-Based Access Control "LBAC": This model can be used to capture the stakeholders' location and determine their accessibility rights based on that location. For example, a drone operator can only operate it when he is connected to the farm network.

Time-Based Access Control "TBAC": This model can be used to ensure that different system resources can be accessed only based on predefined times. For example, a livestock purchasers' access controls to livestock data can be timed in advance to end by the time they make their decision or in another case a regular worker shouldn't access crops data after the working hours.

Attribute-Based Access Control "ABAC": This model can place more limits on the access based on User's attributes, Environment's attributes and Resource's attributes. For Instance, it can be used hierarchically with "RBAC" which can be used first to determine who has access to a resource then "ABAC" determine what they do with the resource based on different attributes.

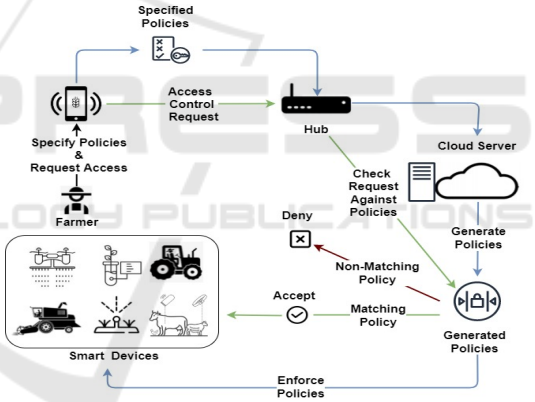

Figure 4: Creation and Enforcement of Access Control Policies.

As different devices have many capabilities, the capabilities must be incorporated in the process of assigning access control policies. Capabilities reflect more fine-grained access control policies than the per-device access controls.

Based on our observation of the smart farm nature, we argue that the smart farm access control system should be multi-user, multi-device aware where farmers can express their system requirements through policies. The system must contain main components as follows:

1. Friendly User Interface: The system should have a unified friendly UI for adding/removing users and devices and assigning policies to them.

2. Expressive Policy Language: Whenever the se-

curity level becomes more complicated, the usability usually drops. However, any complicated process might discourage farmers from using such systems, especially that the security awareness in farms is not high. Therefore, The system should have simple expressive policy language such as roles, time, location, device, capability etc. In addition, It could be beneficial to use policy automation to fill the gap between farmer intuitive policies and the matching detailed technical configurations and rules.

3. Resolving Conflicts: The system should be able to identify and resolve conflicts of access demands.

4. Access Policies: Policies should at least consist of the triplet: <Individual's Role, Device Capability, Contextual Factors>.

5. Policy Creation, Enforcement & Execution: All specified access control policies should be enforced on the system. And access control requests should be evaluated against the enforced policies.

Smart devices are usually managed through a hub device. The hub device is used to facilitate the communication between devices and the cloud. Once the farmer specifies the required access controls, it should be sent through the hub device to the server on the cloud. That server then should generate the required policies and ensure it is enforced over all system resources. Whenever an access control to a system resource is requested, it should be automatically forwarded to the server. The server should check the request against the created policies. If the request is valid it should be accepted on the specified resource, otherwise it should be denied as shown in Figure 4.

6 RELATED WORK

Many researches have started looking into the security and privacy issues in different IoT domains such as (Fan et al., 2019) who designed access controls considering fog computing for providing data confidentiality, variability and attribute based encryption.

However, there have been a limited work exploring specifically the security in smart farming and precision agriculture despite that the U.S. Department of Homeland Security issued a report (Aida Boghossian, 2018) identifying the different threats to precision agriculture and emphasizing the need for more research regarding this area. Most researches were focused on blockchain solutions such as (Kamilaris et al., 2019) who studied the challenges and implications of using blockchain technology projects in the agriculture sector and (Ferrag et al., 2020) who provided the consensus algorithms for the solutions that are based on blockchain and how can they be adapted for smart farming. We omit further blockchain work as its not related to our main focus.

7 PAPER SUMMARY

Smart farming is an emerging sector of IoT applications. It faces many challenges ranging from adoption of its technologies to the security issues that stems from applying it inside the farms. Therefor, an extensive research is required in this area. In this paper we explored different security scenarios that stems form the diverse nature of smart farms. We identified the structure of smart farms and the different stakeholders who are involved in the system. We explored relevant access control policies that can be particularly applied to smart farms.

REFERENCES

2021 Smart farming: How iot-driven precision agriculture helps feed the globe.

Aida Boghossian, S. L. (2018). Threats to precision agriculture,u.s. dept. homeland secur., washington, dc, USA.

Bigelow, D. (2019). Farmland ownership and tenure. *Agricultural Resources and Environmental Indicators, 2019*, 87:84.

Bigelow, D., Borchers, A., and Hubbs, T. (2016). Us farmland ownership, tenure, and transfer. Technical report.

Bruinsma, J. et al. (2009). The resource outlook to 2050: by how much do land, water and crop yields need to increase by 2050. In *Expert meeting on how to feed the world*, volume 2050, pages 24–26.

De Araujo Zanella, A. R., da Silva, E., and Albini, L. C. P. (2020). Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*, page 100048.

Fan, K., Xu, H., Gao, L., Li, H., and Yang, Y. (2019). Efficient and privacy preserving access control scheme for fog-enabled iot. *Future Generation Computer Systems*, 99:134–142.

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., and Maglaras, L. (2020). Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, 8:32031–32053.

Horton, T. J. and Kirchmeier, D. (2020). John deere's attempted monopolization of equipment repair, and the digital agricultural data market-who will stand up for american farmers? *CPI Antitrust Chronicle, Jan*.

Kamilaris, A., Fonts, A., and Prenafeta-Boldý, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science & Technology*, 91:640–652.

Roser, M.(2013). Future population growth. *Our World in Data* https://ourworldindata.org/future-population-growth.