Mini-Project: M19: Exploring smart-farming ontology for attribute-based access control

Zak Chambers Hale
Department of Computer Science
Swansea University
Swansea, Wales
Email: 951548@swansea.ac.uk

Mariam Kiryakos
Department of Computer Science
Swansea University
Swansea, Wales
Email: 2031543@swansea.ac.uk

***Abstract*—The immense growth in the world population has increased the need for food and thereby the efficiency of farming and agriculture to be able to meet the demands. IoT Technology and Artificial Intelligence automates a lot of the farming work that is usually done manually. However, to get the most benefits out of Smart Farming. The whole infrastructure must be secured against cyber-attacks. In this paper, we discuss the Smart farming architecture, possible security threats and how our project aims at eliminating a few threats through Attribute Based Access Control aided by an Ontology.**

I. Introduction

The supply and demand of food around the world has, in general, been satisfied quite well with Earth's population doubling in size between the years of the 1960s and 2000s. But this does not take away from the fact that the demand of crops and livestock will continue to steadily increase, as according to the Food and Agriculture Organisation (FAO) of the United Nations (UN). [1]

With the population expected to grow, new and improved systems to effectively cultivate crops are a necessity, especially with climate change and global warming posing serious difficulties to farms around the world.

Luckily, the emergence of new technologies and concepts, such as sensors, drones or the Internet of Things (IoT), have been implemented to bring the creation of smart farms, also known as smart agriculture. These smart farms allow information to be provided extremely quickly and remotely, increasing effectiveness of crop placement and decreasing resources lost such as water and energy. The incorporation of machine learning and artificial intelligence also facilitates the analysing of crops to find any potential pests or illnesses.

The combination of all these devices and concepts lets the agriculture industry cultivate and grow their crops, to satisfy the population's demand, in the ideal environment for each particular season to maximise the results. This, however, also brings risks due to the technologies still being susceptible to cyber threats, if not implemented correctly.

To do this, the industry must pay special attention, and put in place a series of policies and security measures to avoid and, in unavoidable cases, minimise the damage to the system.

This project aims to provide of such measures in the form of Attribute Based Access Control (ABAC). This concept, represented by an ontology, will significantly reduce the risk of unauthorised access and accidental tampering by employees.

II. Ontology

Ontologies were created to satisfy the need for better representation of information in the various fields of computer science. In other words, an ontology is a simple representation method to easily display the important properties of a given system by defining the characteristics and concepts that constitute it. This brings an easier way to understand a possibly almost incomprehensible system, if it were explained exactly as the computer instructions define it and allows others to comprehend its characteristics without complications.

This becomes especially useful when dealing with multiple systems that could possibly have represented similar, or equal, concepts very differently. In this case, an ontology helps transfer the necessary information to avoid confusion as it gives a more general definition. It also allows developers to independently implement the same, or similar, concept to fulfil their own requirements for a given system.

III. Attribute Based Access Control

Attribute-Based Access Control (ABAC) is a security measure employed by companies and/or enterprises to permit or deny accessibility to specific data resources and or functions. This is implemented to specify what information each possible individual that comes into contact with the application can read or write. [2]

In other words, it allows users to access certain information and, if needed, give them any and all rights requested if said user satisfies the prerequisite attributes.

These attributes are decided based on the requirements of the system, i.e. what equipment is being used, the type of data kept, the number of employees and how they expect customers or clients to interact. Developers of the ABAC must come up with policies to fulfil these requirements in a way that ensures the organisation's resources and clientele are kept safe and secure.

To do this, policies are expected to include any and all possible influencing attributes such as user, resource, environment or object attributes. [2] Access control can also be boiled down to deciding on whether or not a user or resource can access a

particular piece of information and, therefore, can be defined with Boolean logic with the help of If, Then statements, e.g. If the user is an Administrator, then allow read/write access. [3]
The main components of attribute based access control systems as described in [2] are:

1) Subjects: Users and/or processes that would be given or denied access.
2) Objects: Units such as files, folders, programs, entities or pages to which subjects would request access.
3) Actions: different types of way to operate objects (for example: read-only, edit, run)
4) Privileges: The permissions given to subjects with regards to certain objects.
5) Access policies: A set of rules for the access control decision making.
6) Attributes: Properties of subjects, objects and actions.

ABAC policies give or deny access based on the attributes. There is therefore no need to reference subjects and objects in the policies, which is why ABAC is so efficient when there are unlimited subjects and objects in a system. [2]
One of the most popular ABAC languages is the eXtensible Access Control Markup Language (XACML) which was introduced by OASIS in 2003. XACML is based on XML but still adds features within its framework to enable access control. [4]

IV. Smart Farming and Agriculture

Agriculture has played a huge part in the development of human beings and society dating back to the ancient times of human civilisation when we were beginning to drift away from the nomadic lifestyle and entering a more sedentary oriented one. [5] This allowed people to begin focusing on tasks other than hunting and gathering for survival and begin the development of the first civilisations.

As time went on, new inventions arose to help increase efficiency of those that were dedicated to keeping and maintaining farms and crops, some examples of these are ploughs, automated irrigation systems and tractors to name a few. The emergence of new technologies are still prevalent in today's day and age where networks and virtually instant global communication reign supreme, these new facets of human innovation have naturally been incorporated into one of the most important businesses in our society.

If we analyse a modern smart farm, we would easily find electronic systems put in place to monitor and track the production of each specific aspect of the farm, i.e. the amount of produce ready to be sent to a local supermarket, the growth rate of certain crops and the temperature, humidity and illumination levels they are kept at among many other aspects. But these would just be the tip of the iceberg as, due to the advancements in computer science and technology, other topics such as machine learning and artificial intelligence have been incorporated into specific aspects of agriculture to quickly detect and, in some cases, make decisions to better help the system and ease the workload for employees. [6] [7]

Although farming and agriculture has come a long way in recent history, the current state of smart farming is relatively new and still provides its challenges. However, its results provided at such a young age proves that smart farming has still got a lot of potential and will probably grow to be a key component in society. [8]

V. Smart Farming Architecture

Smart farms often are defined through the means of an architecture which describes the various components and how they are connected. To do this, many have found the use of layers to be useful, separating the various parts of the ecosystem based on their properties and functions. Common layers are defined as the perception or physical layer, the cloud layer, the edge layer, network layer and, in some cases an application layer. [9]
The physical layer is composed of all devices that the farm may have such as humidity or temperature sensors or drones capable of acquiring some form of data. They are in charge of collecting real time information and sending it to the edge or cloud layers for further processing which, in turn, will contribute to smart farming procedures. An example of this could be a humidity sensor in charge of notifying any change in humidity levels to the corresponding system that will automatically change to meet the required levels of humidity without the need of a human worker to be present. Possible security threats that are relevant to this layer involve a malicious third party attempting to take control of one or more of the devices found in the farm, such as automated vehicles or drones with the aim of disrupting or damaging the environment or even taking control of sensors to alter the measuring of data or deactivating them entirely, ultimately damaging the production of the crops or cattle. [10]
The cloud layer is usually an offsite centre which connects to the smart farm via the internet. The farm uses the services provided by the cloud similarly to that of Platform as a Service (PaaS) where the organisation pays a fee to use the cloud and its services to reduce complications within the smart farm. As the cloud is an external feature used by the smart farm, its security risks are in the hands of the service provider. In other words, the responsibility to ensure the security of the cloud is down to the organisation in charge of handling the servers that keep and act on the data gathered by the smart farm. For this reason, the smart farm system is vulnerable to any vulnerability that the cloud may be susceptible to. Damage from these situations could possibly be reduced by having a different service provider for different aspects of the system, but this can also lead to an increased amount of vulnerabilities, should the different providers have various embedded exploits. [11]
The edge layer contains devices that can perform a multitude of tasks, some may be in charge of simply retransmitting data from one point to another while others might be tasked with multiple tasks such as filtering data and decision-making depending on the system and device. To be more concrete, this layer is of significant importance as it encompasses real

time decision making, usually based on machine learning algorithms, data capturing and security measures.

Due to the interconnectedness of this particular layer, the security risks involved are critical to the safety of the system. The security risks found in the edge layer can be both physical or through the internet by a malicious third-party attacker as a cause of it being connected to both the physical layer and cloud layer. This means that attackers could possibly gain access through the cloud servers by posing as trusted gateways and, in turn, modify or delete collected data. It is also possible for an attacker to gain access by introducing some form of malicious code, such as a worm or trojan, through physical means, e.g. a USB, and compromising the entire system. [10] [11]

The network layer is the basis for communication between layers and utilises the concept known as the Internet of Things (IoT). It is an essential piece in the smart farm's architecture as it allows the various devices present in the system to communicate with each other in real time. The network layer is susceptible to many, if not all, vulnerabilities associated with IoT such as a man-in-the-middle attack when unencrypted information is being sent through the network. This case can lead to an attacker intercepting, possibly crucial, information that is meant to be hidden from the public. [11]

The final layer to be taken into account is the application layer. This layer's security risks mostly come from external factors whose prevention can only be attempted in the sense that measures can be put in place to minimise the frequency to the point that, if enforced correctly, would never see one of these problems arise. However, these problems are due to human error and as such can never be fully discarded. Examples of these problems are phishing or Denial of Service attacks which can happen due to unforeseeable external factors. [12]

VI. Security Threats

Every business or organisation can be susceptible to some form of security threat, a bank could have poor security measures in place and accidentally allow its clients personal information to be leaked to the public, or a hacker gaining access and deleting important and sensitive data. Whatever the case may be, security threats are to be taken very seriously and require appropriate security measures to be put in place wherever they are needed.

In the case of smart farming, there exists various aspects that could be considered vulnerable to some form of attack if not prepared adequately and could still be affected by a number of uncontrollable factors such as a third party's network failing. The security measures and policies should therefore aim to be compatible between the various pieces that comprise the system and keep damage to a bare minimum in aspects that are out of their control.

In the following we list some of the known threats focusing mainly on those that are not under the responsibility of a third party.

In the physical layer, the sensors could be moved or deformed in ways that would alter the way data is being collected and make measurements inaccurate. To stop sensors from taking measurements, apart from stealing or damaging them, a series of requests can be sent so that the battery could get drained and not let the sensors sleep while the farmer is not using them. Another threat is that an attacker could gain control over sensors, drones, etc. and start giving malicious commands that could harm the crops or simply access private data and passing it onto competitor farms. [12]

As mentioned in the previous section, the cloud layer is the responsibility of the could service provider (CSP) and therefore the security threats associated as well. From a farm's point of view the main responsibility would be to avoid getting tricked by social engineering attacks claiming to be their CSP or offering additional services that could be built on their current Cloud service pack.

The Edge layer is between the cloud and the physical layer and as a result attacking it could jeopardise the physical layer as well as the cloud. This layer handles data transmission between the cloud and the physical layer and be used to send malicious messages. Most of the attacks involve the attacker posing as a sensor or as the cloud and sending messages with forged signatures to install backdoors on sensors or overload them to cause a DoS attack. Another threat is to pose a sensor and gain access to the cloud. The edge is also vulnerable to Man-in-the-Middle attacks and unauthorized access the latter being the result of non-robust authentication and access control mechanisms. [12] [10]

Communication within the Edge layer and between Edge and Cloud layer is handled by the Network layer and intercepting it could result in critical losses. Since the network is connected to the internet, attacks on this layer include phishing attempts and DoS. Other ways to attack it would be by routing the information elsewhere, in that case the attacker would be gathering information on the farm and never sending it to the cloud service of that farm. Furthermore, malicious code can be injected through this layer to devices on the Edge enabling the attacks on the Edge layer described previously. [11] [13]

The application layer is vulnerable to the general attacks on applications such as unauthorised access or DoS. Specifically, in smart farming, an unauthorized user could steal data or even change the behaviour of the application by injecting pieces of code. Any areas of the application that allow user input are also vulnerable to cross-side scripting as well. Another threat worth mentioning the possibility of passwords being cracked if they are not strong enough. [12] [13]

VII. Smart Farm Ontology

This section of the paper will describe the proposed ontology to develop ABAC for a smart farming system. The ontology is created by taking into account the previously mentioned factors, to produce an effective access control for the theoretical smart farm.

After describing the various layers that form the smart farm architecture, we can see that not all of them have properties that require access control to function. Therefore, access control shall only be implemented in those layers that

are deemed necessary for the security of the system, namely the physical layer, the cloud layer, the edge layer and the network layer.

The ontology created to implement the ABAC follows a straightforward pattern, in which users are given access to certain functions and/or resources based on their position in the organisation. Users are expected to be employees of the organisation that own the smart farm and so, for that reason, users are split into different possible types.

Each user will be tasked with specific instructions based off of their job description, but ABAC does not know each individual's task. Instead, ABAC decides whether or not a user is granted access to a particular resource based on the attributes assigned to each type of user.

In the case of this ontology, farmers will be granted access to the crops and cattle they are assigned to. In other words, a farmer will be assigned attributes that will allow them to access any and all necessary devices and their functionalities with the aim to fulfil their instructed task, but any rights needed to change any settings that do not directly involve their objectives are not given.

The same applies to maintenance workers, who would be able to access specific aspects of the system at times that maintenance checks or repairs are needed but would be unable to alter those of which they are not tasked with.

An example of this situation would be a farmer accessing an irrigation system to check on growing crops and noticing a sensor not connecting to the network properly, they would then notify a maintenance worker that would then work on fixing the problem. Here the farmer would have access to the irrigation system and its properties as it is their task, they then have to rely on another employee to fix the problem. This avoids possible complications such as either worker tampering and accidentally altering and subsequently damaging the overall system.

Another aspect to take into account are the managerial and administrator roles. Managers are expected to have access to not just the smart devices that concern them, but also the cloud service to analyse and monitor the data stored there. Administrators on the other hand also have administrative rights to all devices and network settings, making them the most influential user type in the system. For this reason, the administrative roles should be kept to a minimum, as having many users capable of altering settings only available to administrators is a security risk.

This is evident in the case that a third party learns the credentials to access the administrator user. Having a smaller number of these user types is easier to handle than a large multitude due to good security measures labelling all of them unusable after a security breach. [14]

The timeframe at which specific workers may access resources should also be defined, i.e. an employee should not be able to interact with devices and functions outside of work hours so that an individual that has gained unauthorised access to the system, for instance by keylogging an employee's password, cannot access the system in their personal time. This reduces the timeframe of possible attacks and therefore increases the security. It should be mentioned that this would not apply to the administrator user type, as there should always be a way to access key resources in the event of an emergency.

VIII. Conclusion

Agriculture has been an incredibly important concept and practise in human civilisation and has found itself many a times in need of innovation to continue to satisfy the population's demand. Smart agriculture helps increase production and efficiency by incorporating smart devices and concepts such as IoT to create adjustable environments for the crop's growth.

Smart farms require high levels of cybersecurity to avoid attacks from malicious third parties, due to the interconnectedness of the system.

This project defines an ontology that represents an Attribute Based Access Control system to avoid unauthorised access to the various sections of the system by limiting the accessible resources that an individual may access at a given time.

References

[1] FAO, "Long-term Perspectives - The outlook for agriculture," http://www.fao.org/3/y3557e/y3557e06.htm, online; accessed 28 April 2021.

[2] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, "Xacml for building access control policies in internet of things." in *IoTBDS*, 2018, pp. 253–260.

[3] S.-K. Chin, *Access control, security, and trust : a logical approach / Shiu-Kai Chin, Susan Older.*, ser. Chapman & Hall/CRC cryptography and network security, 2011.

[4] Y. Zhang and B. Zhang, "A new testing method for xacml 3.0 policy based on abac and data flow," in *2017 13th IEEE International Conference on Control Automation (ICCA)*, 2017, pp. 160–164.

[5] N. Greenfieldboyce, "When Humans Quit Hunting And Gathering, Their Bones Got Wimpy," https://www.npr.org/sections/health-shots/2014/12/22/372441550/when-humans-quit-hunting-and-gathering-their-bones-got-wimpy?t=1619364527675, online; accessed 25 April 2021.

[6] A. D. Stefano, "Why Machine Learning Is Agriculture's New Best Friend," https://apro-software.com/machine-learning-agriculture/, online; accessed 25 April 2021.

[7] Sciforce, "Machine Learning in Agriculture: Applications and Techniques," https://medium.com/sciforce/machine-learning-in-agriculture-applications-and-techniques-6ab501f4d1b5, online; accessed 25 April 2021.

[8] Á. Regan, "'smart farming' in ireland: A risk perception study with key governance actors," *Njas-wageningen Journal of Life Sciences*, p. 100292, 2019.

[9] A. Triantafyllou, D. Tsouros, P. Sarigiannidis, and S. Bibi, "An architecture model for smart farming," 05 2019, pp. 385–392.

[10] S. S. L. Chukkapalli, S. Mittal, M. Gupta, M. Abdelsalam, A. Joshi, R. Sandhu, and K. Joshi, "Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem," *IEEE Access*, vol. 8, pp. 164 045–164 064, 2020.

[11] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[12] A. Zanella, E. da Silva, and L. C. Albini, "Security challenges to smart agriculture: Current state, key issues, and future directions," *Array*, vol. 8, p. 100048, 12 2020.

[13] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural iot and smart farming," *Sensors*, vol. 20, no. 22, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/22/6458

[14] City of Dublin Education and Training Board, "Data breach protocol," no. 14, 2018. [Online]. Available: https://pearsecollege.ie/wp-content/uploads/2018/11/Data-Breach-Protocol.pdf