# SWAMP

Kamienski, Carlos; Kleinschmidt, João Henrique; Soininen, Juha-Pekka; Kolehmainen, Kari; Roffia, Luca; Visoli, Marcos; Maia, Rodrigo Filev; Fernandes, Stenio

*Published in:*
Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018

*DOI:*
10.1109/DSN-W.2018.00024

Published: 01/01/2018

*Document Version*
Peer reviewed version

| | |
|---|---|
| Title | SWAMP: Smart Water Management Platfrom Overview and Security Challenges |
| Author(s) | Kamienski, C., Kleinschmidt, J. H., Soininen, J., Kolehmainen, K., Roffia, L., Visoli, M., Maia, R. F., Fernandes, S. |
| Citation | Paper presented at IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, Luxembourg City, Luxembourg |
| Date | 27.6.2018 |
| Rights | © 2018 IEEE |

# SWAMP: Smart Water Management Platform Overview and Security Challenges

Carlos Kamienski[1], João Henrique Kleinschmidt[1], Juha-Pekka Soininen[2], Kari Kolehmainen[2], Luca Roffia[3], Marcos Visoli[4], Rodrigo Filev Maia[5], Stenio Fernandes[6]
*cak@ufabc.edu.br, joao.kleinschmidt@ufabc.edu.br, Juha-Pekka.Soininen@vtt.fi, Kari.Kolehmainen@vtt.fi, luca.roffia@unibo.it, marcos.visoli@embrapa.br , rfilev@fei.edu.br, stenio@cin.ufpe.br*
[1]*Federal University of the ABC, Santo André/Brazil*
[2]*VTT Technical Research Centre of Finland, Oulu/Finland*
[3]*University of Bologna, Bologna/Italy*
[4]*Brazilian Agricultural Research Corporation (EMBRAPA), Campinas/Brazil*
[5]*Centro Universitário da FEI, São Bernardo do Campo/Brazil*
[6]*Federal University of Pernambuco, Recife/Brazil*

***Abstract* — The intensive use of technology in precision irrigation for agriculture is getting momentum in order to optimize the use of water, reduce the energy consumption and improve the quality of crops. Internet of Things (IoT) and other technologies are the natural choices for smart water management applications, and the SWAMP project is expected to prove the appropriateness of IoT in real settings with the deployment of on-site pilots. At the same time, the more intense the use of technology is, agriculture turns new security risks, which may affect both crop development and the commodities market. A security breach may irreversibly compromise a crop and data eavesdropping may compromise price and contracts exposing sensitive data such crop quality, development or management. This paper discusses security challenges and technologies for the application of IoT in agriculture and indicates that one of the most relevant challenges to be handled in SWAMP project is dealing with the multitude of behaviors from IoT application and what would be considered as normal and what would be considered as a threat.**

***Keywords - Internet of Things, Smart Water Management, Precision Irrigation***

## I. INTRODUCTION

Food security calls for the intensive use of irrigation in agriculture at the same time that water is increasingly becoming a precious and scarce asset for mankind. Irrigation for agriculture is the most significant consumer of freshwater in the world, amounting to 70% of freshwater [5]. In an attempt to avoid loss of productivity by under-irrigation, farmers feed more water than is needed and as a result not only productivity is challenged but also water and energy is wasted. The Internet of Things (IoT) [2] and other related technologies can be used for that purpose, but it faces several challenges such as the lack of easy-to-use software tools and platforms, communication constraints in rural areas and sensor integration issues. Such technological features in agriculture also bring severe security risks, since some machines have autonomous systems and data generated by IoT devices could expose critical aspects of the production or even they may be manipulated to support wrong conclusions about crop development.

The SWAMP[1] project develops IoT based methods and approaches for smart water management in precision irrigation domain and to pilot the approaches in four places, two pilots in Europe (Italy and Spain) and two pilots in Brazil. The same underlying SWAMP platform can be customized to different pilots considering different countries, climate, soil, and crops. The SWAMP architecture may be implemented in a range of deployment configurations involving the use of smart algorithms and analytics in the cloud, fog-based smart decisions located on the farm premises and possibly mobile fog nodes acting in the field (e.g., drones or in the central pivot irrigation mechanisms).

The four SWAMP pilots are based on the similar technical solutions and deal with different crops and have different primary goals.

1. CBEC Pilot (Bologna/Italy): the main objective of the Consorzio di Bonifica Emilia Centrale (CBEC) pilot is optimizing water distribution to the farms.
2. Intercrop Pilot (Cartagena/Spain): Intercrop Iberica addresses several challenges since production is in a dry area, and a considerable amount of water comes from a desalination plant. The primary goal for Intercrop is using water more rationally.
3. Guaspari Pilot (Espírito Santo do Pinhal / Brazil): The Guaspari Winery transfers the wine grape harvesting to the winter season (June-August) using irrigation techniques. The main goal for Guaspari is improving wine quality.
4. MATOPIBA Pilot (Barreiras/Brazil): The Rio das Pedras Farm is located in the MATOPIBA region, and irrigation is mostly performed by center pivots. This main pilot goal is to implement and evaluate a smart irrigation system based on Variable Rate Irrigation (VRI) for center pivots in soybean production and save energy used in irrigation.

## II. IOT IN PRECISION IRRIGATION FOR AGRICULTURE

The SWAMP project is being built upon existing research such as FIWARE that is EU-funded IoT solution library used for smart applications [8] and precision irrigation [7]. SWAMP shares several features with other precision irrigation initiatives such as FIGARO project [4] that aims at increasing

[1] swamp-project.org

water productivity and improving irrigation practices through a cost-effective precision irrigation management platform not directly involving IoT. SWAMP intends to use IoT combined with cloud-based services and big data analytics and conduct experiments in real settings. Brewster et al. discuss the deployment of large-scale pilots for IoT in agriculture and describe technologies that might be present in some agrifood domains [3].

## III. Security Challenges for IoT in Agriculture

In general, IoT has many security requirements, such as data privacy, confidentiality and integrity, authentication, authorization and accounting, and availability of services [6]. The security mechanisms have to be energy efficient, since many IoT devices are limited in power, processing, and memory resources. There is no unified vision on security in the IoT [1][6], but many security solutions are being proposed and may be used in smart agriculture and irrigation.

Water is a critical resource and an attacker may take control of the system and a whole crop would be decimated, due to lack or excess of irrigation. A DoS (Denial of Service) attack in the sensors, irrigation actuators or in the distribution system may affect the availability of the system. Changes in the values of some sensors are also a threat that may cause systems or decision makers to take wrong actions and compromise months of efforts and production goals. If an attacker takes control of the actuators, the irrigation and water distribution is compromised, wrongly irrigating some crop. Using eavesdropping, intruders may have access to private data about the farm and crop yield information and even manipulate the commodity markets, which is even a more extensive threat. Autonomous vehicles, such as drones and tractors, used for collecting images and crop monitoring, must also be secured. An unauthorized node in the network (sensor node or drone) may send false information about the crop. A drone or sensor node performing the Sybil attack could send fake images and false measurements, leading to the incorrect interpretation of the actual soil conditions, incorrect calculation of the NDVI (Normalized Difference Vegetation Index), and the like.

The SWAMP architecture must deal with the control of data by the farmers or producers, ensuring that each owner controls their data and decides the access control to the data and the services. The distribution of water between users is very sensitive issue also addressed by SWAMP. Trust, privacy and security must be the basis of information exchange. Data anonymization is another helpful technique for data governance and even some regulation and legal frameworks for agriculture are being discussed by governments. There are also many innovative proposals in the literature for security solution in various domains of IoT [7][8], including 6LoWPAN networks. SDN (Software Defined Networking) architecture for IoT allows administrators to have a centralized view of the IoT system [8] and to implement security services. A disruptive technology in security is blockchain, which will have great importance in the security of IoT [7]. One possible application is in the supply chain and lifecycle of an IoT device. For instance, it is possible to track all the attributes, relationships and events related to a device. The use of smart contracts is also a promising mechanism to be used in new methods for authentication, authorization, and privacy of IoT devices [6].

One of the most relevant security challenges for IoT in agriculture is not only the integration of technologies but also to understand and correlate the expected sequence of events and behavior of agriculture applications. SWAMP has a multitude of characteristics to be evaluated and a baseline must be created to promote security effectiveness. Regardless of the data acquisition rate, or the number of installed sensors, the system will probably have a partial view of the environment. As a consequence, applications may create a partial profile of the crop and related environment, which does not necessarily correspond to that crop. Therefore, inadvertent use of a given profile may cause harm to a crop, and security mechanisms should take this into account when producing their results.

The SWAMP project deals with many of these challenges and requirements. The platform must provide efficient authentication, authorization and access control mechanisms. It is important to keep data apart from farms in our pilots. The access to the platform must be allowed only for identified and authorized users, using FIWARE security generic enablers (GE) and the OAuth 2.0 protocol. The confidentiality of the data must be provided using state of the practice cryptography. Wireless and wired communications must use existing security features of the underlying technology and existing security protocols. The availability of the platform must be provided even in case of Internet disconnections using local components (fog computing) to keep the platform running properly.

## IV. Conclusion

SWAMP intends to use IoT to improve the use of water resources in heterogeneous pilots, each one with its own characteristics and challenges. The adoption of an open-source platform as FIWARE as the basis of SWAMP platform development has advantages but the use of IoT in agriculture also brings several security challenges, since a multitude of threats may cause severe and irreversible damages to the crop. In order to protect IoT devices and cloud systems, the SWAMP platform should not only deal with device security, data confidentiality and authentication mechanisms, but also with mechanisms to avoid fake data. The latter may result in misunderstandings about crops or may allow eavesdropping that may cause manipulation of commodity markets.

## References


[1] Alaba, F. A., et al., “Internet of Things security: a review”, Journal of Network and Computer Applications”, 88, pp. 10-28, June 2017.

[2] Atzori, L., Iera, A., Morabito, G., "The Internet of Things: A survey", Computer Networks, 54(15), October 2010.

[3] Brewster, C. et al., "IoT in Agriculture: Designing a Europe-Wide Large-Scale Pilot", IEEE Comm. Mag., September 2017.

[4] Doron, L., "Flexible and Precise Irrigation Platform to Improve Farm Scale Water Productivity", Impact, 2017(1), January 2017.

[5] FAO, “AQUASTAT: Water Uses”, http://www.fao.org/nr/water/aquastat/water_use, 2016, Accessed February 2018.

[6] Khan, M. A., Salah, K., “IoT security: Review, blockchain solutions, and open challenges”, Future Generation Computer Systems, 82, pp. 395-411, May 2018.

[7] López-Riquelme, J. A., "A software architecture based on FIWARE cloud for Precision Agriculture", Agricultural Water Management, March 2017.

[8] Ramparany. F., et al., “Handling smart environment devices, data and services at the semantic level with the FI-WARE core platform”, IEEE Intl. Conference on Big Data, October 2014.