Kalpa Publications in Computing

Volume 12, 2019, Pages 95–104

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019

IoT Security and Privacy: Turning on the Human Firewall in Smart Farming

Tapiwa Gundu[1] and Vimbai .L. Maronga [2]

[1] Sol Plaatje University, Kimberley, South Africa

[2] Urban-Econ Development Economists, Port Elizabeth, South Africa.

tapgun@gmail.com, vimlin@gmail.com

Abstract

Agriculture is central to the economy of the world, with sixty percent of the population depending on it for survival. Farmers are adopting smart farming technics to make agricultural practices more efficient. Smart farming takes advantage of Internet of Things (IoT) technologies for performing tasks such as moisture sensing, weeding, keeping vigilance, spraying, bird and animal scaring, smart irrigation controls, the use of real time field data for intelligent decision making and smart warehouse management which includes theft detection and temperature and humidity maintenance of the warehouse. Smart devices such as watches, computers or cellphones connected to the internet can then be used to control the smart farming system. Smart farming being at nascent stage, its privacy and security needs to be researched and explored as its future partially dependent on the resolution of the privacy and security issues associated. This paper comprehensively reviews various security and privacy issues and challenges associated with IoT deployments in smart farming. Following a structured approach, a framework for smart farming security and privacy was developed in an attempt to address challenges experienced/expected. This framework can also be used for future directions for any IoT related privacy and security initiatives.

1 Introduction

The growth in global population is leading to increased food requirement needs of the modern-day civilization requires increased food production. Unfortunately, traditional farming methods with low yields for fruit and crops are still predominantly used. But wherever automation has been implemented, yield improvement has been evident (Gondchawar & Kawitkar, 2016). This highlights the need to introduce modern technologies to the agriculture sector to achieve better yields.

The new technologies and solutions being implemented in agriculture increase efficiency in methods for gathering and processing data while enhancing net productivity (Ray, 2017). On the other hand, the

water crisis and alarming climate change require new and improved methods of farming. Automation and intelligent decision making technologies are therefore also important in accomplishing this mission (Fan TongKe, 2013). Amongst technologies that are making it possible are; IoT, remote sensing, ubiquitous computing, cloud computing, Radio Frequency Identifier and wireless and sensor networks (Ray, 2017).

However, this study only focuses on IoT, which is "a collection of many interconnected objects, services, humans, and devices that can communicate, share data, and information to achieve a common goal in different areas and applications. IoT is fast tracked by the rapid growth in nanotechnology which enables production of small and cheap sensors. This has brought about great potential towards faster decision making and automation in the agriculture industry in the following smart farming techniques: (automated irrigation scheduling (Reche, Sendra, Díaz, & Lloret, 2015), precision agriculture (Barcelo-Ordinas, Chanet, Hou, & García-Vidal, 2013; Ray, 2017), optimization of plant growth (Hwang, Shin, & Yoe, 2010), green-house monitoring (Mao, Miao, He, Li, & Liu, 2012), farm land monitoring (Corke et al., 2010), and farming production process management (Dong, Vuran, & Irmak, 2013)). This rapid development in the Internet of Things in agriculture has propelled the phenomenon that is called Smart Farming (Sundmaeker, Verdouw, Wolfert, & Freire, 2016).

Although smart farming promotes the increase of yields, reduces operating costs, and increases agility, its unique architecture raises numerous security and privacy concerns. The huge amounts of data that are shared in IoT-enabled environments can be harnessed by malicious applications that can use to the disadvantage of some aspect of smart farming. Thus, understanding and minimization of these security and privacy risks by the development of efficient and effective cybersecurity solutions is critical for the success of smart farming initiatives. Since both IoT and smart farming are relatively new phenomena, their knowledge concerning security and privacy implications is not widespread as expected. Some authors have labeled these technologies as "technology hypes that may fail to materialize." (Fenn & LeHong, 2011).

This research paper provides insight into smart farming and goes on to identify the most important security and privacy challenges they expose farmers to. Lastly, we introduce a framework to help mitigate the smart farming security and privacy challenges exposed. We acknowledge both technical and human security and privacy challenges, however, the paper mainly focuses on the human aspect of privacy and security in smart farming because it seems as though not enough research has been done. In line with that, this paper seeks to answer the following research questions:

1. What are the privacy and security issues in IoT?
2. How do humans affect the privacy and security of IoT initiatives?
3. How can the impact of human weakness in the privacy and security of IoT be reduced?

The remainder of this paper is structured as follows; firstly, it will highlight the contribution of this study, it will then discuss a review of related literature after which it will provide the brief methodology for the research followed by a description of the proposed framework. The last section will conclude and provide recommendations for further research and actions.

2 Related Literature

Agriculture has seen three revolutions already, from plants animal domestication a few thousand years ago, systematic crop rotational methods of a few hundred years ago and the "green revolution" which came with the use of fertilizers, pesticides, genetic modifications and introduction of systematic breeding a few decades ago (Walter, Finger, Huber, & Buchmann, 2017). We suggest that agriculture

is undergoing a fourth revolution triggered by the increasing population that in turn is increasing the demand of food. Ray (2017) warns that the growth rate in food production is not at par with the food required by the growing population. The Food and Agriculture Organization of the United Nations (*How to Feed the World in 2050*) recently published a report showing a prediction of global food requirements reaching 3 billion tons by 2050 from 1.5 billion in 2015. This calls for an exploration of new and modern technologies that can be used in agricultural applications to achieve the target. As a result, this is accelerating the incorporation of sensors and IoT into agriculture, giving birth to smart farming.

2.1 Internet of Things (IoT)

IoT is rapidly gaining momentum in modern wireless telecommunications. The basic IoT concept lays around connection and use of a variety of technologies (such as Radio-Frequency IDentification (RFID) tags, sensors, computers, actuators, smart watches, mobile phones, etc.). These technologies interact with each other through unique addressing schemes to achieve common goals (Pecorella, Pierucci, & Nizzi, 2018). The integration of IoT with humans can take advantage of collaboration and technical analytics to achieve real-time decision making (Angelini, Mugellini, Abou Khaled, & Couture, 2018; Ray, 2017). IERC ('IERC-European Research Cluster on the Internet of Things', 2014) which seems to have the most cited definition, defines IoT as follows: "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, often communicate data associate with users and their environments."

2.2 Smart Farming

Smart farming is the use of modern technology to improve the amount and quality of agricultural products. Walter et al (Walter et al., 2017) advocates that, apart from the use of intelligent sensors, smart farming also encompasses the use of robotic vehicles (e.g. for application of fertilizer, weeding and fruit harvesting). They also elaborate that the drones with autonomous flight control, bundled with powerful hyperspectral and high-resolution cameras are also being used to calculate biomass development and fertilization status of crops, is another form of sophisticated smart farming. Another common form of smart farming innovation is virtual fencing technologies which assist cattle herd management by the use of Global Positioning System Sensors (GPS) sensors attached to the livestock and monitored on computer or smart phones. This management can also be achieved by the use of real time remote-sensing signals. Combined, these technical improvements discussed constitute a technical revolution that can generate positive changes in agricultural practices. These trends for farming are not only applicable to developed countries but also to developing countries, especially where deployments in ICT (e.g., use of smart phones, access to the Internet) are being adopted at a rapid pace. The rapid decrease in price for IoT based sensors for smart farming solutions is also opening a possibility for smart faming initiatives in emerging economies as the farmers can also afford them (Ray, 2017).

Smart farming reduces the ecological footprint of farming due to efficient site-specific application of inputs, such as fertilizers and pesticides. This makes agriculture more profitable for the farmer as resource inputs would have been decreased. It also assists with mitigation of leaching problems as well as greenhouse gas emissions (Mahmoud, Yousuf, Aloul, & Zualkernan, 2015) and increase reliability of spatially explicit data which will ultimately reduce farming risks. Optimal, yield projections, site-

specific weather forecasts, and diseases and disasters probability maps based on weather and climate data will help plan and optimize cultivation of crops (Walter et al., 2017). With the IoT, it is possible to create a sensor network allowing for almost continuous monitoring of the farm reducing the time needed for surveillance.

In principle, optimization of farming activities due to smart farming should lead to better product quality (e.g., watering an orchard when the moisture level has not dropped too much, produces better juicier fruits or better-quality milk produced by individualized feeding of cattle). Better quality products are not only healthier but also generate more profits as they sell at higher prices.

Because there are numerous players in smart farming, this introduces a challenge of accountability for malpractice or mistakes that may lead to environmental and/or economic consequences. For example, it is difficult to establish the source of the problem if a consumer gets sick from eating harvested fruits that still had traces of fertilizer or pesticides because it was applied too late. Should the blame be on the farmer, or the software vendor, or the network provider, or the manufacturer of the sensor? As at the time of publishing of this paper, there is no straightforward answer to address such an incident. Another challenge is that smart farming can lead to serious disease outbreaks if not monitored properly. Efficient use of fungicide in a smart farming environment may delay disease outbreaks which then increases the risk of creating fungicide resistant traits which is even more devastating.

Contrary to the view that the automation in smart farming eliminates the need of human labor therefore increases the unemployment rate, this whole process will always require humans however at a much higher intelligent level. Machines will only conduct the monotonous and tiring operational activities (Walter et al., 2017).

2.3 Security and Privacy

We will discuss the security and privacy challenges of smart farming as well as those of IoT in general as they also filter into smart farming. These challenges can be broadly divided into technological challenges and human challenges (Gundu, Flowerday, & Renaud, 2019; Mahmoud et al., 2015). The technological challenges in smart farming mainly arise due to its heterogeneous and ubiquitous nature. If magnified closer, these challenges have to do with wireless technologies, scalability and energy. The human challenges are related to the awareness and knowledge of principles and functionalities that should be followed to achieve and maintain a secure smart farming environment. These human challenges evolve around the ability to ensure security by authentication, confidentiality, end-to-end security, integrity etc. (Mahmoud et al., 2015).

In the recent years, there has been a lot of effort attempting to address security and privacy issues smart paradigms (Alaba, Othman, Hashem, & Alotaibi, 2017; Cho, Cho, Shin, Park, & Lee, 2012; Corke et al., 2010; Fagade & Tryfonas, 2016; Granjal, Monteiro, & Sa Silva, 2015; Hwang et al., 2010; Oleshchuk, 2009; Pecorella et al., 2018; Zhou, Cao, Dong, & Vasilakos, 2017). Collectively, the authors touch on trust management, authentication, intrusion detection systems, privacy issues, data security, network security, access control systems, fault tolerance and digital forensics. An IoT project requires some form of trust, privacy, and security model implementation. This model should address data integrity, confidentiality and end-to-end communication issues. To probe into data misuse, the model should also address access policies and encrypting mechanisms to be used.

The classic security goals of Confidentiality, Integrity and Availability (CIA) of any cyber system also apply to IoT. However, IoT based smart systems have other restrictions and limitations. These are

primarily due to computational power limitations of the devices and the heterogonous and ubiquitous nature of IoT. To address that, we suggest authentication, lightweight solutions, heterogeneity, policies and key management systems to be added to the traditional CIA triad, which will be discussed below.

Security and privacy issues that may arise due to weaknesses of the human in smart farming are interception, node capture attack, dos attack, man-in-the-middle attack and data theft. Technological issues include compatibility, wireless signal strength, storage capacity, power consumption, and computation capability. In general, when designing IoT applications it is important to take the following into account: how will different users interact with the devices, how much data will be revealed and who will be managing the applications. Therefore, users should have tools that control data to be disclosed, by whom and when (Mahmoud et al., 2015).

3 Contribution

This paper contributes to the body of knowledge as follows.

- Analysis of the advantages of smart farming.
- Analysis of privacy and security issues related to IoT and smart farming deployments with respect to the human aspect.
- Development of a framework that can be followed to reduce the effect of the human weakness in terms of privacy and security of smart farming.

4 Methodology

In order to address the research questions outlined in the Introduction, we reviewed literature from January 2009 to January 2019. This review period was chosen due to the fact that IoT and smart farming are recent phenomena, hence as a practical consideration we did not expect to access older studies within articles prior to 2009. Apart from inclusion by period of publication, we also used two other inclusion criteria for the literature search. These encompassed whether it was a full article publication and its relevance to the research questions. Exclusion of previous literature was also based on two different criteria: either the articles were not published in English or the articles focused solely on technological designs. The literature survey was undertaken using the following systematic approach: a search on two major bibliographical databases was carried out, on Science Direct and Scopus. This search was conducted using a combinations of keywords which were separated into two groups, the first addressing Smart Farming (i.e. precision farming, agri-food, sensor-driven innovation, technologies in farming, internet of things, IoT) and the second group focusing on cybersecurity (i.e. human centered security, awareness campaigns, training). The choice of the two databases was based on their wide coverage of relevant literature and their capability to suggest related articles or citations. A total of 359 peer-reviewed articles were retrieved from the two databases. These were filtered by scanning for relevance. This involved identifying sections of the text that address the research questions. Followed by screening, where, the search function was used to locate the paragraphs containing the key words. We then analyzed the text to identify links to our research questions.

We used Zotero reference management software to manage the articles and eventually, 21 articles were considered as very relevant and 93 as relatively relevant. The remainder of the articles were irrelevant and excluded from this analysis because they did not speak to smart farming or cybersecurity. The number of relevant peer reviewed literature was very low; however, this was not surprising as IoT and Smart Farming are relatively new concepts. Their applications are rapidly evolvingpeer reviewed articles are lagging behind as usually the case with most technologies. This led to the decision to also include grey literature into the review. This comprised using Google Scholar and LexisNexis search engine. Thus, we managed to obtain magazines, reports, blogs, and other web-items. This resulted in 213 magazine articles, 4 reports, 119 blogs and 19 items on twitter. Each of the 119 blogs had their title and sentences scanned for relevance and duplicated blogs were removed. As a result, 21 blogs were selected for additional evaluation through further reading. Eventually, 7 blogs were considered as containing relevant information for our study. Each of the 213 magazine articles was similarly evaluated and 9 articles were considered as containing relevant information. The analysis and synthesis of the literature led to the development of the framework presented in the next section.

5 Proposed Framework

This paper argues that for the technological security measures put in place to be effective, the user of the system should be aware of the security risks associated and how to behave securely. Technology should complement and supplement the human element not the other way around. The technological/physical firewall can be deemed useless if the 'human firewall' is not turned on, as it is the human who controls the technology. In summary, we suggest that the human element is at the Centre of any security and privacy initiative.

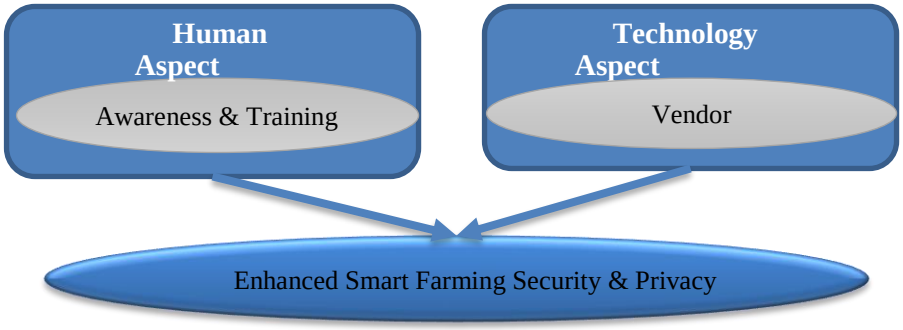

Figure 1: A privacy and security framework for smart farming

The proposed privacy and security framework for smart farming in figure 1 has constructs guided by how literature seems to address the human and technological aspects of privacy and security attempts to highlight that enhanced security and privacy can only be achieved by considering both technological and human aspects.

5.1 Technology Aspect

Appropriate technological infrastructure is essential in making smart farming systems function. Although literature does not have much information on infrastructures being used, the few mentioned are supplied by large venture capital vendors such as AGCO, John Deere, KAA IoT, ThingsWorkx, Blue River Technologies, Thingsboard.io and Monsanto. However, the demands of the fourth industrial

revolution particularly smart farming are now attracting organizations that were previously not active in traditional agriculture. For example, a Japanese technology firm (Fujitsu) now hosts cloud-based farming systems. In North America, there are several initiatives for example the facilitation of data acquisition via an open-source hardware platform and software libraries known as the ISOBlue project and the Open Ag Toolkit (OpenATK) (Ray, 2017) In Europe, FIWARE was developed. It is for cloud hosting, data management, provision of IoT services, cybersecurity and analysis of Big Data (Wolfert, Ge, Verdouw, & Bogaardt, 2017).

Since, devices (sensors, computers, cellphones, routers, etc.) in smart farming are manufactured and distributed by different vendors, trust should be established between them and the farmers. For this to happen the devices they supply should be technically secure. This leaves the aspect of the technological aspect of privacy and security primarily on the vendors. However, these vendors should train the farmers on the use of their devices and advise them on possible risks and how to use the devices securely.

5.2 Human Aspect

The challenge for smart farming is to ensure awareness of security and privacy to the farmers and their employees and also to ensure that they are trained on how to implement safety in their daily routines in a consistent manner. Technical security controls may only assist in reducing the threat of malicious people such as hackers, competitors or disgruntled employees. However, the defense against naïvetés and lacking understanding necessary to safeguard the smart farming system may be achieved by vigorous security awareness and training programs.

The trusted human (employee) typically has unregulated access to some part or else parts of the smart farming system. This makes it possible for a naive farmer or employee to breach security and privacy measures put in place from within the system's perimeter defenses without triggering the perimeter defenses alarm (Gundu, 2012). On the other hand, outside attackers attempt to gain access inside a network either by attacking the system directly or by exploiting the weaknesses of an employee. This research study focused on insiders only. The reason for this segregation was that the insider threat is usually taken for granted and smart farming often has limited measures in place to minimize the risk to which insiders expose the farm as compared to that posed by outsiders with firewalls and physical security being used to guard against intruders. The hour it takes an employee to view an awareness presentation may be the difference between a secure organization and a multimillion Dollar breach of security.

What should be given great attention is that most farmers and farm workers are not Information and Communication Technology (ICT) specialists. Hence, they might not be aware of the risks involved in a smart farming environment, and how those risks can be reduced. Farmers and farm employees with 'little-to-no' prior cyber security training or experience may suddenly be responsible for hundreds of networked IoT devices generating large amounts of data some which might be sensitive as part of their job The weaknesses humans present can never be completely avoided, however, a properly structured cybersecurity awareness campaign can lower the risk to tolerable levels (Flowerday & Von Solms, 2005; Gundu, 2017).

In a smart farming environment, everyone requires cybersecurity awareness training just as in the armed forces, every soldier, regardless of their role, have to complete elementary training. Hence, cybersecurity awareness among human users (farmers and farm workers) is an important security measure for the success and growth of smart farming. If humans lack awareness, they can make

mistakes such as using default passwords that come with devices making it easy for hackers to conduct attacks against the whole network (Mahmoud et al., 2015).

6 Conclusions and recommendations

With the global population prediction of 9.6 billion by 2050, extreme weather condition challenges, climate change, and resulting environmental impact, there is great need to embrace IoT. Effective farming practices can address these issues. Currently, literature reports smart farming applications are taking place primarily in Europe and North America. However, it reveals keen interest from Africa and Asia whose economies are primarily based on agriculture.

Ensuring security and privacy is one of the biggest challenges of smart farming governance to date. This challenge might end up inhibiting developments because farmers may be reluctant to share data as they begin to fear that their data may end up in their competitors' hands. Hence, strong access controls might be a starting point for vendors to build trust with farmers.

In this paper a literature review on security and privacy in smart farming was conducted. It was concluded that IoT in smart farming applications is still premature based on the limited peer reviewed publications. However, it is evident that humans remain the weak link in smart farming security and privacy initiatives. Some farmers are lulled into a false sense of security by IoT device vendors who vogue that technology is the total barrier to breaches. Hence, this paper develops a framework to try to reduce the risk the human exposes smart farming initiatives to. As we believe, it will be the most effective way of switching on the human firewall that is making the human part of the solution and not the problem. The next step for this study is conduct action research to test the effectiveness of the proposed model. Our main recommendation for future research lies within analyzing whether Africa is ready for smart farming in terms of security and privacy.

References

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Angelini, L., Mugellini, E., Abou Khaled, O., & Couture, N. (2018). Internet of Tangible Things (IoTT): Challenges and Opportunities for Tangible Interaction with IoT. *Informatics*, *5*(1), 7. https://doi.org/10.3390/informatics5010007

Barcelo-Ordinas, J. M., Chanet, J. P., Hou, K.-M., & García-Vidal, J. (2013). A survey of wireless sensor technologies applied to precision agriculture. In J. V. Stafford (Ed.), *Precision agriculture '13* (pp. 801–808). Wageningen Academic Publishers.

Cho, Y., Cho, K., Shin, C., Park, J., & Lee, E.-S. (2012). An Agricultural Expert Cloud for a Smart Farm. In J. J. (Jong Hyuk) Park, V. C. M. Leung, C.-L. Wang, & T. Shon (Eds.), *Future Information Technology, Application, and Service* (pp. 657–662). Springer Netherlands.

Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., & Moore, D. (2010). Environmental Wireless Sensor Networks. *Proceedings of the IEEE*, *98*(11), 1903–1917. https://doi.org/10.1109/JPROC.2010.2068530

Dong, X., Vuran, M. C., & Irmak, S. (2013). Autonomous precision agriculture through integration of wireless underground sensor networks with center pivot irrigation systems. *Ad Hoc Networks*, *11*(7), 1975–1987. https://doi.org/10.1016/j.adhoc.2012.06.012

Fagade, T., & Tryfonas, T. (2016). Security by compliance? A study of insider threat implications for Nigerian banks. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 128–139. Springer.

Fan TongKe. (2013). Smart Agriculture Based on Cloud Computing and IOT. *Journal of Convergence Information Technology*, *8*(2), 210–216. https://doi.org/10.4156/jcit.vol8.issue2.26

Fenn, J., & LeHong, H. (2011). Hype cycle for emerging technologies. *Gartner, Stamford*.

Flowerday, S., & Von Solms, R. (2005). Real-time information integrity= system integrity+ data integrity+ continuous assurances. *Computers & Security*, *24*(8), 604–613.

Gondchawar, N., & Kawitkar, R. S. (2016). IoT based Smart Agriculture. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*(6), 838–842.

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver Security Awareness Training, then Repeat: Deliver; Measure Efficacy. *2019 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. https://doi.org/10.1109/ICTAS.2019.8703523

Gundu, T. (2012). *Towards an information security awareness process for engineering SMEs in emerging economies*. University of Fort Hare.

Gundu, T. (2017). *An information security policy compliance reinforcement and assessment framework*. University of Fort Hare.

How to Feed the World in 2050. (2015). Retrieved from http://www.fao.org/fileadmin/templates/wsfs/docs/expert_paper/How_to_Feed_the_World_in_2050.pdf

Hwang, J., Shin, C., & Yoe, H. (2010). A Wireless Sensor Network-Based Ubiquitous Paprika Growth Management System. *Sensors*, *10*(12), 11566–11589. https://doi.org/10.3390/s101211566

IERC-European Research Cluster on the Internet of Things. (2014). Retrieved 30 March 2019, from http://www.internet-of-things-research.eu/about_iot.htm

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

Mao, X., Miao, X., He, Y., Li, X., & Liu, Y. (2012). CitySee: Urban CO2monitoring with sensors. *2012 Proceedings IEEE INFOCOM*, 1611–1619. https://doi.org/10.1109/INFCOM.2012.6195530

Oleshchuk, V. (2009). Internet of things and privacy preserving technologies. *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology*, 336–340. https://doi.org/10.1109/WIRELESSVITAE.2009.5172470

Pecorella, T., Pierucci, L., & Nizzi, F. (2018). "Network Sentiment" Framework to Improve Security and Privacy for Smart Home. *Future Internet*, *10*(12), 125. https://doi.org/10.3390/fi10120125

Ray, P. P. (2017). Internet of things for smart agriculture: Technologies, practices and future direction. *Journal of Ambient Intelligence and Smart Environments*, *9*(4), 395–420. https://doi.org/10.3233/AIS-170440

Reche, A., Sendra, S., Díaz, J. R., & Lloret, J. (2015). A Smart M2M Deployment to Control the Agriculture Irrigation. In M. Garcia Pineda, J. Lloret, S. Papavassiliou, S. Ruehrup, & C. B. Westphall (Eds.), *Ad-hoc Networks and Wireless* (pp. 139–151). Springer Berlin Heidelberg.

Sundmaeker, H., Verdouw, C., Wolfert, S., & Freire, L. P. (2016). Internet of Food and Farm 2020. *Digitising the Industry-Internet of Things Connecting Physical, Digital and Virtual Worlds*, 129–151.

Walter, A., Finger, R., Huber, R., & Buchmann, N. (2017). Opinion: Smart farming is key to developing sustainable agriculture. *Proceedings of the National Academy of Sciences*, *114*(24), 6148–6150. https://doi.org/10.1073/pnas.1707462114

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). Big Data in Smart Farming – A review. *Agricultural Systems*, *153*, 69–80. https://doi.org/10.1016/j.agsy.2017.01.023

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26–33. https://doi.org/10.1109/MCOM.2017.1600363CM