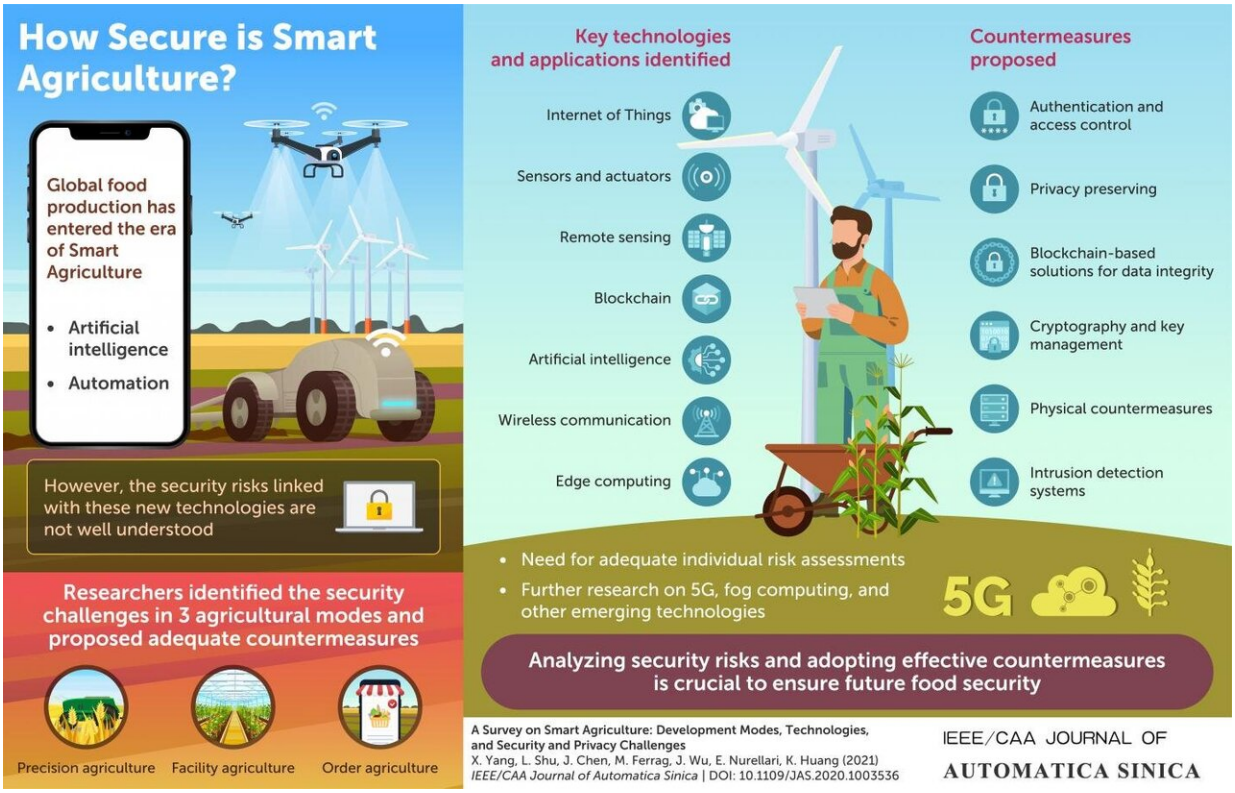
Sustainable but smartly: Tackling security and privacy issues in smart agriculture

February 23 2021



Scientists discuss the emerging security challenges that come with integrating technology in modern agriculture and suggest measures to tackle them Credit: *IEEE/CAA Journal of Automatica Sinica*

According to recent estimates, there will be roughly 10 billion people to feed in 2050. Agricultural production will need to increase by almost

56% to guarantee food security globally, without converting more land for agriculture (in line with environmental and climate targets). This unprecedented challenge has ushered in the era of 'smart agriculture,' which promises to revolutionize food production by combining agricultural techniques with information technology, automation, and artificial intelligence. This new era, called 'Agriculture 4.0,' could ensure sustainable food production for the entire world. However, as communities gradually embrace smart agriculture, it is important to understand how to manage the security and privacy risks associated with the integration of information technology into agriculture.

To this end, in a new survey published in *IEEE/CAA Journal of Automatica Sinica*, researchers from China, Algeria, and the UK have performed a comprehensive analysis of the risks involved in current technologies used in smart agriculture and identified potential countermeasures. Lei Shu, a Professor from Nanjing Agricultural University in China and University of Lincoln in UK, the leading author of the paper, and Xing Yang from Nanjing Agricultural University in China, the first author of the paper, say, "Smart agriculture provides solutions for agricultural intelligence and automation. Both intellectual and unmanned operations are the development goals of smart agriculture."

The researchers also state that the field of smart agriculture is ripe with the risks of information theft and cyberattacks. To prevent these risks from putting global food supply in jeopardy, Yang and his team identified and proposed adequate countermeasures to the risks, based on the context (or "mode") of agricultural production. Commenting on their approach, Yang explains, "Security countermeasures based on urban conditions may not be suitable for rural conditions." They categorized the agricultural system into three modes: precision agriculture, facility agriculture, and order agriculture. Each of these modes has its own distinctive features (scale, climate, infrastructure, equipment, and

technology) that makes it vulnerable to distinct types of risks requiring equally distinct countermeasures.

After laying this groundwork, the researchers set out to analyze the various security challenges involved in the three modes. First, they identified key technologies involved in each mode and their applications. The Internet of Things (IoT), which is arguably the most important technology in smart agriculture, is used in every mode, but has different applications depending on what specific tasks need to be performed. For instance, it is used in field agriculture to record environmental variables and analyze trends to predict optimal fertilizer input, while it can be used to automate environmental conditions in greenhouses and aquaculture. In each case, the way in which the technological architecture is set up exposes it to widely varying types of security challenges. For example, extreme environmental conditions can damage sensing equipment outside, while unauthorized access and malicious cyberattacks can compromise data integrity and site security, tamper with automated equipment, and lead to severe financial costs and a loss in food production. To better assess the solutions needed in each case, the researchers classified the challenges they identified as belonging either to agricultural production or information technology.

Reviewing each technology and their current applications, the researchers proposed six general countermeasures. These include technological solutions such as intrusion detection systems, authentication and access control, and privacy-preserving, blockchain-based solutions for data integrity, as well as physical countermeasures. Their study goes into great detail about how each solution can be applied in different contexts and how they address each of the challenges identified for smart agriculture.

After this comprehensive review, the scientists went one step further and pointed out that little is known about the potential security risks for

agricultural equipment, such as sensors and tractors. They portray this lack of knowledge using a case study of one piece of equipment: a solar insecticidal lamp based on an IoT architecture (SIL-IoT). Their experiments showed that this lamp can cause electromagnetic interference and might even cause wireless sensor networks to malfunction. In this case, a simple physical separation distance was enough to address the security risk; however, the researchers advise caution.

As agriculture becomes more technologically complex, so will the challenges of ensuring its security. To this end, the researchers discussed other emerging technologies (such as 5G networks and VR/AR simulation) and the need for further research on their security impacts as their integration in smart agriculture becomes inevitable in the near future.

As we move towards a sustainable future with smart agriculture, let's also learn take a step back from time to time to check how we could become truly smart about it.

More information: Xing Yang et al. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges, *IEEE/CAA Journal of Automatica Sinica* (2020). DOI: 10.1109/JAS.2020.1003536

Provided by Chinese Association of Automation