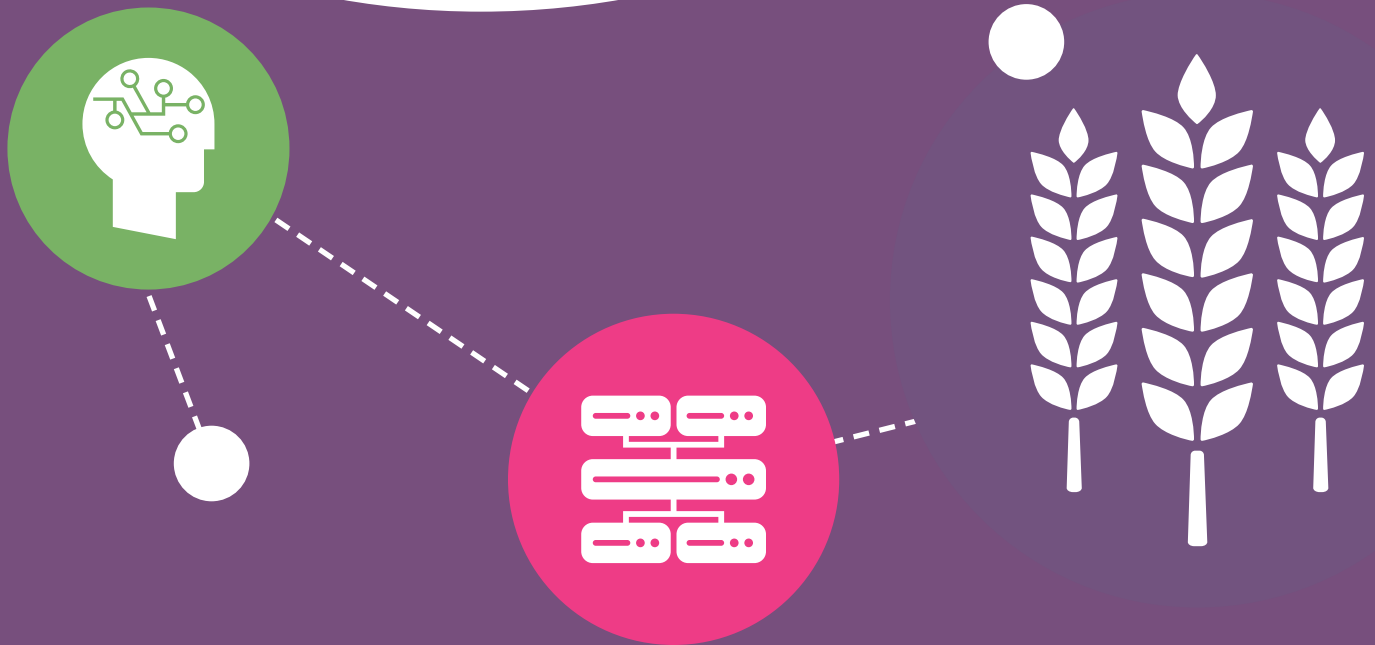
PETRAS

Industry Briefing

Cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech Sector

Dr Monica Racovita



About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 16 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate and the University of Warwick.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

The wider PETRAS community has played a role in creating this report - in particular Professor Awais Rashid from the University of Bristol for his critical role in review, and Caroline Wijnbladh and Emilie Didier from the PETRAS Business Development Team for their editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Racovita, M. 2021. *Industry Briefing: Cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech Sector,* PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI:

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech Sector. This is the second in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, AgriTech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the AgriTech sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

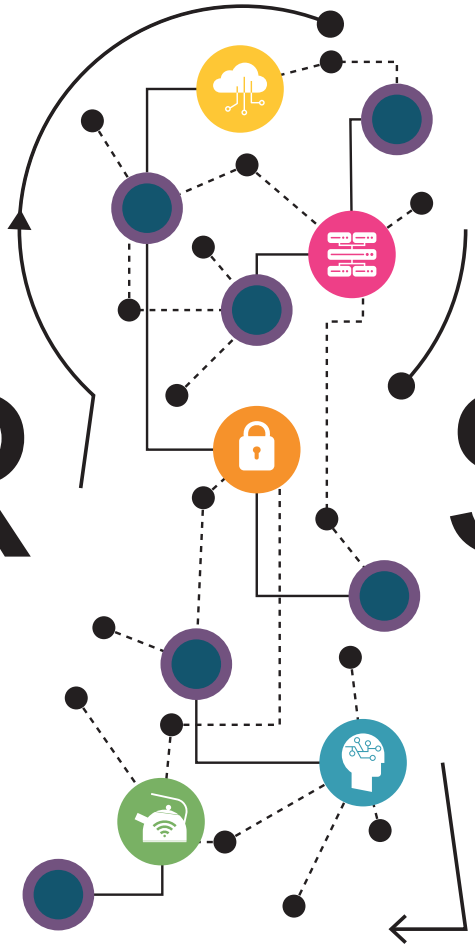
Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

UKRI Engineering and Physical Sciences Research Council

Contents

PETRAS

THE PETRAS NATIONAL
CENTRE OF EXCELLENCE
FOR IoT SYSTEMS
CYBERSECURITY



Executive Summary

The PETRAS National Centre of Excellence[1] aims to ensure that technological advances in the Internet of Things (IoT) and Artificial Intelligence (AI) are developed and applied safely, and securely by considering social and technical issues in a variety of sectors.

AgriTech is an umbrella term for a variety of cutting-edge technologies used in agriculture, such as digital tools, Internet of Things (IoT), edge computing, and Artificial Intelligence (AI). The market for such technologies is undergoing a rapid, albeit uneven, growth with the US having the biggest market share.

Benefits of IoT

IoT can supply a variety of benefits for farmers. By real-time monitoring crop and livestock, IoT can allow farmers to reduce waste and costs, achieve a more sustainable environmental impact, as well as reach a higher productivity with a smaller workforce.

The application of AI to agriculture is an exciting field as fully autonomous systems can learn from experience and adapt to the continuously changing agricultural environment.

IoT cybersecurity challenges

The market for smart agriculture is rapidly growing, as IoT devices are set to become more ubiquitous. As the adoption at the farm level increases, so do cybersecurity threats due to an increase in attack surfaces.

Specific technical challenges for IoT cybersecurity in agriculture stem from the **variety of harsh conditions** (high variation in temperature, humidity, physical shock, PH, mobility) in which devices need to be placed and function, and which need to be balanced with **device limitations** (size, energy consumption, memory) and **requirements for cybersecurity best practices** (for example, software security updates or good networking architectures).

Socio-technical threats to cybersecurity relating to perceptions of cybersecurity issues and on data sharing practices can also leave systems and data open to attack. Movements such as the “Right to

Repair", which are increasingly becoming requirements in certain jurisdictions, can also bring complex cybersecurity challenges to farmers, industry and regulators, where differing perceptions of risk are difficult to reconcile.

These technical and social considerations on cybersecurity, in challenging environmental conditions, highlight the question of whether the AgriTech sector should be covered under cyber protection policies or certification schemes.

The UK is becoming a major destination for global AgriTech companies but it is also offering a supporting environment for agrifood tech start-ups. UK public research centres are conducting world leading research in, among other, digital agriculture, automation or sensor technology.

Introduction

Scope of this brief

This brief offers a summary of the general trends, challenges and opportunities in cybersecurity and associated policy for the Internet of Things (IoT) and artificial intelligence (AI) in the AgriTech sector in the UK, the EU and globally in 2020. The brief concludes with insights into UK research landscape activities and business development opportunities with PETRAS.

The brief is constructed as a primer for discussion, and the target audiences for this brief include:

- government organisations involved in food and supply chain security,
- companies that provide IoT solutions to the AgriTech sector,
- companies that provide cybersecurity solutions to IoT in the AgriTech sector,
- AgriTech companies looking for cybersecurity solutions,
- and researchers involved in the AgriTech cybersecurity sector,

who would like to gain insight into PETRAS work and collaboration opportunities.

Here, IoT devices are seen as a component of an ecosystem together with data communication, data aggregation and processing, data analytics and inference, and data visualisation.

This brief considers IoT and AI deployment in agricultural settings including horticulture and aquaculture, but excluding capture fisheries. It focuses on technology usage by primary producers, excluding storage, food safety and other elements of the Agri-Food supply chain.

Within AgriTech this brief looks at the deployment of IoT and AI in smart farming, precision farming, robotics and automation, vertical farming, big data and AI, and the use of drones and satellites.

Sector background

AgriTech is associated with different emerging technologies, especially digitisation, the cloud, the Internet of Things, edge computing, and artificial intelligence, that are increasingly being used in farming, horticulture, aquaculture, and other forms of food and drink production. This cluster of technologies is sometimes called AgriTech, agtech, foodtech, precision farming, precision agriculture, farming 4.0, digital farming, or smart farming, although some of these denominations are better suited as subsectors of AgriTech.

A 2020 MarketandMarkets report indicates a rapid growth of the global smart agriculture market, from 13.8 billion USD (10 billion GBP) in 2020 to 22.0 billion USD (16 billion GBP) by 2025, due to farmers' need to increase yields, improve livestock production and reduce management costs to meet a growing demand for food, in particular protein-rich food[2]. The Americas are projected to maintain the largest market share, with US and Canada expected to maintain their grip on the market and Argentina and Brazil to adopt smart agriculture technologies at a rapid rate. The report identifies the industry key players in this field.

IoT can supply high-resolution, real-time data from remote automated sensor systems about plants, animals, workers, or machines, on plant and animal growth, wellbeing, location, environmental conditions (temperature, pressure, humidity, water/nutrient intake), or soil composition. By better managing inputs, they can allow farmers to reduce waste, decrease overall costs and have a better, more sustainable, environmental impact [3].

IoT sensors together with connected robotic/automated IoT actuators can also help farmers achieve a higher productivity with a smaller workforce. This is particularly sensitive for countries like the UK which not only has a low productivity growth, but also needs to face challenges like the changing climate, reducing greenhouse emissions and Brexit[4].

Artificial intelligence, machine learning (ML), deep learning (DL), High-Performance Computing (HPC), big data analytics, and the cloud are together focused on knowledge-gathering, analysis, and prediction. The most popular AI applications in agriculture, currently in development, belong to three main categories: agricultural robots, crop and soil monitoring, and predictive analytics[5].

The majority of currently deployed robots in agriculture are not led by AI, and just perform automated tasks that have been set up in advance (sometimes with a limited degree of autonomy). Yet, the next generation of agricultural robots will be expected to be fully autonomous, learn from experience and adapt to a continuously changing environment. There is also a hope that these future generations of robots will deliver a much wanted and needed sustainable intensification alongside food security[6].

FAO indicates the need to reduce costs, including labour costs, as a major driver for automation in agriculture[7]. Labour availability plays no small role, painfully obvious during the COVID-19 pandemic which saw severe labour shortages around the world[8]. Yet economic implications of the use of robots and automation in agriculture, including labour demands and risk/benefit analyses, remain insufficiently addressed, in particular in the developing world[9].

Key market players identified by MarketsandMarkets[2]: Deere & Company (US), Trimble, Inc (US), Topcon Positioning Systems (US), DeLaval (Sweden), Heliospectra (Sweden), Antelliq (France), Afimilk Ltd. (Israel), AKVA Group (Norway), InnovaSea Systems (US), LumiGrow (US), AG Leader Technology (US), Raven Industries (US), AgJunction (US), The Climate Corporation (US), Nedap NV (The Netherlands)

Internet of Things and AI Cybersecurity

With a wider adoption of internet-connected devices and AI in agriculture comes an increase in vulnerabilities and exposure to cyber attacks[10]. It is worth noting that the IoT are a type of cyber-physical systems (CPS), which “integrate computational and physical components to implement a process in the real world”[11]. CPS also have security challenges that emerge from the need to have a reliable, predictable and safe interaction with the physical environment, even when the physical world behaves unpredictably or consists of harsh conditions[11]. Agriculture has no shortages of unpredictable events or harsh conditions.

The IoT deployed at farm level becomes a part of vast networked food systems which may contain components which are not cyber secure, and which would make such food systems vulnerable to “hybrid warfare tactics of both state and non-state actors”, according to the Canadian Cyber Science Lab[12]. From a general business process point of view, the IoT integration in business processes can raise issues, as “the process perspective is often neglected and coordination of [IoT] devices is realised in an ad-hoc way using custom scripts”[13].

Security vulnerabilities in smart farming

Gupta et al. summarise the main security and privacy issues in smart farming[10]:

DATA ON EDGE

- Within smart farms, the presence of data on the edge enhances the agility of the system but also poses security risks due to increase in attack surfaces in IoT devices with sometimes poor security. In addition, with websites like Shodan, finding the IP addresses of edge endpoints becomes much easier. Compromised 3rd parties, like agronomy analytics, can also be security weak points and they are more challenging as they are difficult to detect.

AUTHORISATION AND TRUST

- Various smart applications on the farm communicate via communication protocols such as Message Queue Telemetry Transport (MQTT) or Constrained Application Protocol (CoAP). These devices need to ensure that messages come from trusted authorised entities (farmers or trusted 3rd parties).

AUTHENTICATION AND SECURE COMMUNICATION

- Devices need to be authenticated before being connected. As such, legacy solutions would bring significant risks. Possible solutions reviewed by Gupta et al. include cryptography solutions (which unfortunately utilise much of the limited power of edge devices), lightweight cryptography, or quantum-based cryptography (the last, not yet evaluated in real-world scenarios).
- Other authors like Bonneau et al. look at legacy systems and the challenges they pose to AgriTech. New vulnerabilities and risks are introduced as the industry mechanises then digitises. Partial digitisation and interaction with legacy 'built to last' analogue equipment is common as agricultural tech lifespans are longer than communication tech lifespans e.g. the average tractor age in Germany is 27.5 years (and this is rising, in part due to long equipment life and high purchase costs of up to 150k EURO/130k GBP), with 60-70% of existing machinery in use still analogue, and 30-40% fitted with digital technology[14]. This need to retrofit causes further risks. There are many old operating systems not updated or patched.

COMPLIANCE AND REGULATIONS

- **Contracts and agreements:** data privacy, security, and intellectual property clauses are routinely incorporated in contracts with technology vendors. Yet, as Gupta et al. note, certain devices like self-driving tractors can have specific clauses and farmers can request, in theory, strong compensation and limitations of liability clauses (see the Socio-technical issues section of this brief for the John Deere and the "right to repair" movement case).
- **Data security and privacy:** agreements with technology providers need to include specific clauses with regards to data security and privacy.
- **IP (Intellectual Property):** data itself cannot be IP protected yet. But copyright provisions with technology providers can be used to set up safeguards
- **Cybersecurity insurance:** existing offers have limited coverage. Insurance companies like HSB have started offering cybersecurity insurance for agriculture, covering both farm and personal vulnerabilities[12]. Yet the offers still fall short of the demand. Researchers like Jahn et al. argue that the reasons for the lack of coverage reside in the rapid development of technologies, which makes it difficult for insurance companies to predict and project future risks; the small number of claims filled to date; difficulties in characterizing threat, vulnerability, reliability and liability; the lack of a good understanding of risk on both sides, farmers and insurance companies[16].

Gupta et al. also summarise the main types of cyber-attacks in smart farming classified according to the IoT system layer they affect[10]:

ON DATA	• Insider data leakage of confidential data • Cloud data leakage: if the data is stored in other countries, it might be less secure (due to less strict security laws) • False data injection attacks: falsify data for real-time decisions (e.g. wrong information on soil moisture levels can lead to too much or too less water delivered to crops) • Misinformation attacks: endanger data integrity (e.g. falsely reporting a disease)
ON NETWORKING AND EQUIPMENT	• Radio frequency jamming attack • Malware injection attack • Denial of service attack: disrupts normal functions at different module • Botnet: several compromised IoT devices controlled by a malicious system • Side-channel attack: exploiting weakness from how a system is implemented
OTHER	• Compliance and regulation: inject false data to impact compliance certification process • Cyber terrorism • Cloud computing: cloud is increasingly becoming a desirable target (e.g. auto-scaling means virtual machines are similarly configured and when a malware exploits a vulnerability it can infect all similar virtual machines).

Authors like Nikander et al indicate that cybersecurity can also include unintentional threats due to human errors, natural cases, including extreme weather, power or signal failure as well as device malfunctions[17].

In addition, attack vectors in the form of physical interaction with devices and subsequent tampering resulting in their replacement with a compromised device or one that would enable a remote connection are a real possibility due to farms being open and often remote spaces. Yet this cybersecurity aspect is noticeably missing from the specialised literature.

A report for the US Homeland Security identifies key cyber threats to precision agriculture and warns that potential threats are often not understood or not taken seriously[18]:

- **Threats to Confidentiality:**
  - Intentional theft of data collected through decision support systems (DSS) or the unintentional leakage of data to third parties
  - Intentional publishing of confidential information from within the industry
  - Access to unmanned aerial system data
  - Sale of confidential data
- **Threats to Integrity**
  - Intentional falsification of data to disrupt crop or livestock sectors.
  - Introduction of rogue data into a sensor network which damages a crop or herd
  - Insufficiently vetted machine learning modelling
- **Threats to availability**
  - Timing of equipment availability
  - Disruption to positioning, navigation and timing (PNT) systems – space ground based
  - Disruption to communication networks
  - Foreign supply chain access

to equipment used in precision agriculture
- Smart livestock production facility failure

Best practices for precision agriculture recommended by the UD Department for Homeland Security report include[18]:

- baseline security controls employed in other sectors can also be used in precision agriculture, such as email and web browser protections, or levels of access for authorised users.
- specific data security controls for precision agriculture include data recovery capabilities, data protection (through database management tools, encryption, and access control) and understanding who owns what data.
- implementing physical controls and incident response and management to increase resilience in the case of an attack.

In the UK, according to a NCC Group white paper, cybersecurity threat scenarios are unlikely to be of great severity for agricultural edge devices in the near future[16]. However, there is a potential for **financial harm and negative impacts for livestock**. There is also a high concern from farmers on data ownership, privacy and security when big data is concerned (for AI/ML/DL applications). Other security concerns include physical theft (with a cybersecurity component) and attacks from animal rights activists. The mitigation of current risks, the report further states, could be done by standard approaches and business processes. For the future, the report concludes, as the number of IoT devices and AI applications is likely to increase, cybersecurity might pose more serious challenges, even threatening food security.

Box 1. New business model - "farming as a service"

An informal interview conducted with a representative from the British AgriTech start-up Small Robot Company revealed a new type of business model, increasingly popular with agricultural robotic companies in the UK, that addresses many of the security concerns presented above, called "farming as a service". Through it, farmers pay a per-hectare subscription for services offered by the company through its robotic machinery rather than purchasing the equipment. The business model, developed following consultations with farmers, simplifies the use of automation on farms, gives farmers a higher degree of autonomy and safety, places technology risks (including cybersecurity) with the company that provides the service, and reduces the amount of data that would need to be gathered and processed by robots acting on information present in the field at operation time. Measures that provide additional cybersecurity protection include the use of an open-source operating system with built-in security with data being sent there manually and mainly processed on the edge.

Policy and Regulations

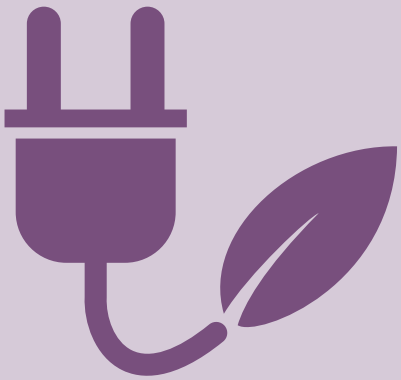
In the area of security and cybersecurity, UK has few specific regulations for AgriTech. The Department for Environment, Food and Rural Affairs (DEFRA) in collaboration with Food Standards Agency and the British Standards Institution produced PAS 96, an overall and general guide for the food industry on how to protect against various types of attacks including cybersecurity[20]. There are no current governmental assurance schemes, good practices or certifications specific for agriculture.

Challenges

AgriTech policy challenges indirectly related to security and cybersecurity of IoT and AI ecosystems in the UK could include:

- An insufficiently addressed regulatory regime and skills gap in general (identified in the 2013 “A UK Strategy for Agricultural Technologies”[21]);

- Within robotics and autonomous systems (RAS)[9]:
    - A narrow human resource capacity;
    - An insufficient basic research base;
    - Potential missing links between the RAS community, industry and academia;
    - A lack of a coordinated and integrated Agri-Food research policy.



Regulations

At the time of writing this brief, it seems unclear whether Brexit would have a significant impact on AgriTech policies in the area of security and cybersecurity, in particular concerning data privacy and data sharing. Up to maximum 6 months from the beginning of the Specified Period (1 January 2021) flow of data between UK and EU can still follow the GDPR rules[22]. After the end of that period (or before if specific regulations are passed) it is not yet clear what data protection legal framework will guard data flow between UK and the EU.

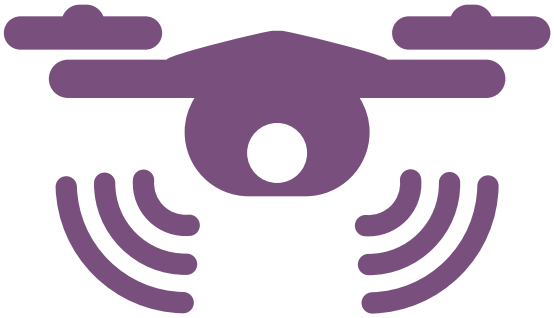
At the EU level, regulatory gaps regarding security and cybersecurity in precision agriculture include[23]:

- **General security and safety regulations** e.g. anonymise data, safeguards on privacy, data encryption, transfer or change of data fully traceable, enhance cybersecurity, liability and insurance instruments for the use of automated technologies;

- **Special rules for small drones** e.g. to prevent attacks, contingency procedures, predictable behaviour, 3rd party liability, insurance, security.

Although data processing in agriculture seems to be an issue of great importance for the EU (European Commission announced the intension to establish a Common European agriculture data space in 2020[24]), cybersecurity for agricultural devices does not seem to receive the same amount of attention. The 2019 Cybersecurity Act does not contain any specific references for agriculture[25].

Cybersecurity in agriculture receives comparatively more attention in the US than in Europe. The Federal Bureau of Investigation (FBI) warned in 2016 the food and agriculture sector of cybersecurity risks associated with smart farming[26]. Additionally, the US Department of Homeland Security identified technologies and cyber threat scenarios related to precision agriculture[18]. The main threats identified by the US Department of Homeland Security concern confidentiality, integrity and availability.



Socio-technical issues

Technical research challenges follow the dual nature of cyber-physical systems (CPS), namely focusing on both computational and physical challenges.

Research

Some of the main current computational challenges are summarised by Ferrag and colleagues [27] as:

- machine learning techniques for intrusion detection systems (a protection system against cyber-attacks using encryption); challenges include: selecting the right machine learning technique and selecting the right dataset for IoT based scenarios;
- use of blockchain-based solutions: currently in their infancy, but future blockchain-based solutions would need to consider aspects such as scalability (increasing number of IoT-based participating nodes) and the effectiveness of the consensus algorithm;
- design of practical and compatible cryptographic protocols, for which the resource and power constraints of IoT in agriculture are some of the major challenges;
- resiliency against specific attacks in the context of low-resource IoT devices;
- counter measures against 5G network slicing (partitioning physical and network resources to optimise the traffic) threat: security leakages, authentication for privileged users;
- a changing agricultural environment brings interference in the communication between nodes and thus challenges for novel duty-cycle control, sampling and scheduling, data reconstructions, as well as data storage and query, intelligent control, and other solutions.

In addition, research is expected to find solutions to physical challenges for IoT security:

- withstand sensor degradation and communication failure due to harsh environmental conditions[28];
- physical tampering, due to theft or animal attacks[28] or tampering that would result in the replacement of devices with compromised ones;
- balance the need to have up-to-date security protocols with limited memory, low communication capabilities, and low energy consumption[28];
- physical consequences of cyberattacks resulting in human, animal or plant harm.

Society

A particular emerging issue for the security of AgriTech devices is the **“right to repair”**.

AgriTech companies such as John Deere (US) have started stipulating in their End User Licence Agreement (EULA) that farmers are forbidden to conduct repairs or modifications to AgriTech devices[29]. As a result, Wanstreet reports instances of farmers using illegal Ukrainian software to hack their own Deere tractors.

Concerns for cybersecurity are raised on both industry and farmer sides according to Waldman and Mulvany[30]. Farmers are worried that by having the right to turn off a tractor remotely, companies like John Deere are a security risk for farmers, because if companies become the target of hackers thousands of tractors can be affected at the same time. John Deere representatives are worried that by hacking their own tractors, in the name of the “right to repair”, farmers can introduce vulnerabilities in the systems. Representing the interests of farmers, the Repair Association aims to see, according to Waldman and Mulvany, the passing of a law similar with a 2012 Massachusetts auto-industry law, which had a spill-over effect at the federal level requiring the car industry to offer car owners and independent mechanics the same software for repairs they provide their own dealers. In Europe, according to an NCC Group white paper, EU has rules on the “right to repair”, but they do not cover agricultural equipment[19].

A further social challenge is that the **perceptions of cybersecurity issues and practices of data sharing can be dependent on the socio-cultural context** as well as the type of stakeholder[31]. Van der Linden and colleagues find that in Israel data is routinely shared among farmers as the Israelian agriculture is still heavily influenced by the kibbutz culture (collective communities)[31]. As such, farmers see real-time data as less important and data in general as not commercially sensitive. Israeli technology vendors however, are concerned about cyberattacks on data that could come from small scale cybercriminals, and less from nation states, focusing on the IT layer rather than operational one. Technology vendors also list lateral attacks through insecure configurations as a high security risk.

In Australia, Wiseman and colleagues find low willingness from farmers towards data sharing, which, the researchers argue, is due to a lack of trust between farmers and third party companies who collect and analyse the data[32].

However, there is little research done at the moment on the importance of socio-cultural context in cybersecurity perceptions and data sharing attitudes in agriculture.

Additional challenges in the UK, according to a NCC Group white paper[19], **include farm and farmer characteristics:** small average farm size, increasing farmer average age and low awareness of cybersecurity. Due to these challenges, the responsibility for implementing and monitoring cybersecurity measures cannot be left with farmers.

Opportunities

With the explicit recognition of AgriTech in 2013[21] came the acknowledgement of opportunities in this field: technology revolution, growing markets, UK placed to become a centre for international R&D, growing investments in applied research.

The freshly minted Agriculture Act 2020 sets up a new system in UK that pays farmers for producing public goods such as better quality of air, water and soil, healthier plants and animals and tackle the effects of climate change[33]. Technology, while not being the ultimate silver bullet, can help farmers produce these health and environmental public goods as well as tackle other systemic problems faced by the agriculture of the 21st century[34]:

- Reducing greenhouse gas emissions
- Managing food losses
- Managing scarce natural resources, like land and water
- Managing demographic and income trends, like population growth, urbanisation, or ageing
- Adapting to changes in consumption patterns

In the UK, a NCC Group white paper assessed the severity of cybersecurity threats for agricultural edge devices as low[19]. But with an increase of deployment of technologies such as IoT devices and AI applications, the report warns, cybersecurity might pose more serious challenges.

The warning is starker for the US. The US currently dominates, and is expected to continue to do so, the world market in this sector until 2025 according to a MarketsandMarkets report[2]. Yet cybersecurity measures are low on the industry side, due to low awareness or driven by the need to reduce costs, warns a joint notification from Federal Bureau of Investigation and the US Department of Agriculture[26]. Yet as a result of cyber attacks, more seed and farm equipment started investing more in cybersecurity, the same report states.

PETRAS in the UK Research Landscape

The UK is becoming a major destination for major AgriTech companies including agricultural equipment companies like JCB and Denso and animal health companies like Elanco, Merck and Zoetis reports AgFunder[35]. According to AgFunder data the UK is also offering a supporting environment for AgriTech start-ups, in 2017 being the third most active country for agrifood tech start-up funding.

Notable start-ups include The Small Robot Company[36], Hands Free Farm[37], Dogtooth Technologies[38], and LettUs Grow[39].

Key UK public research centres that support IoT and AI adoption in the AgriTech sector are presented in Table 1.

PETRAS is represented in this research landscape by Cybersecurity for Food Security (CyFoo) project, led by Prof. Awais Rashid, University of Bristol. The project aims “to develop a risk analysis framework and policy guidelines to support users in understanding and mitigating the cybersecurity risks from sensor-driven digital infrastructure (Agritech)”[47].

Table 1. UK research centres and programmes

Research centre/programme	Focus
Centres for Agricultural Innovation, including Agrimetrics, Centre for Crop Health and Protection (CHAP), Centre for Innovation Excellence in Livestock (CIEL), and Agricultural Engineering Precision Innovation Centre (Agri-EPI)	A new collaborative model between the AgriTech sector and government. Collectively, the centres aim to: "improve the economic performance of UK farming through the development and uptake of technologies, knowledge, and practices; recreate UK leadership in this area by joining-up existing excellence; resolve challenges that no one part of the sector can address alone; open up opportunities for transformational change in the sector not possible in current structures".[40]
Lincoln Institute for Agri-Food Technology (LIAT)	Investigates the integration of 3D imaging and automation to harvesting and weeding and has current projects in robotics and automation, energy efficiency and sustainability, soil, water and crop science, and food safety and security.[41]
Cranfield University, Centre for Environmental and Agricultural Informatics	The centre specialises in transformational informatics technology, sensor tech, informatics and data sciences applied to "air quality and climate change, soil quality, crop growth and monitoring, natural capital, ecosystem goods and services and on urban systems".[42]
National Centre for Precision Farming (NCPF) based at the Agricultural Engineering Innovation Centre at Harper Adams University (HAU)	NCPF is known as an innovator in the field of engineering in the AgriTech sector. The role of the centre focuses on the promotion and evaluation of technology in AgriTech as well as providing a focal point for the industry. Current research centres on the implementation and technical specifications of edge solutions in agriculture.[43]
University of Bristol, the Cabot Institute for the Environment	Bristol has a project to identify the vulnerabilities of the increasingly digital food system which asks to what extent the introduction of connected technology to the supply chain impacts the integrity of that system, and how aware are farmers of these potential threats and how they could minimise them.[44]
Agriforwards CDT, established by the University of Lincoln in collaboration with the University of Cambridge and University of East Anglia	World's first EPSRC Centre for Doctoral Training (CDT) in Agri-Food Robotics.[45]
Ceres Agri-Tech Knowledge Exchange Partnership, a collaboration of 5 Universities (Reading, Cambridge, East Anglia, Hertfordshire and Lincoln) and 3 research institutes (NIAB, Rothamsted and the John Innes Centre)	The 3-year project aiming to establish a regional AgriTech knowledge exchange cluster.[46]

Table 2. PETRAS projects in cybersecurity in AgriTech

Project	Partners	Description	Industrial relevance
Cybersecurity for Food Security (CyFoo) (ongoing)	• The University of Bristol	• To develop a risk analysis framework and policy guidelines to support users in understanding and mitigating the cybersecurity risks from sensor-driven digital infrastructure.	• AgriTech cybersecurity

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Glossary

AI (Artificial Intelligence) "A branch of computer science that attempts to both understand and build intelligent entities, often instantiated as software programs"[48]

ML (Machine Learning) "A field of computer science that uses algorithms to identify patterns in data"[48]

DEEP LEARNING involves training an artificial neural network with big datasets .

PRECISION FARMING is a farming management concept that measures the evolution of crops or livestock and uses technologies, such as the global positioning system (GPS) and geographical information systems (GIS).

SMART FARMING goes beyond precision farming to use past and real-time data to provide a rich, heterogeneous context.

VERTICAL FARMING is the practice of growing crops inside in vertically stacked layers.

End Notes

1. PETRAS (2021). https://petras-iot.org.

2. MarketsandMarkets (2020) Smart Agriculture Market by Agriculture Type (Precision Farming, Livestock, Aquaculture, Greenhouse), Hardware (GPS, Drones, Sensors, RFID, LED Grow Lights), Software, Services, Application, Farm Size, and Geography - Global Forecast to 2025. https://www.marketsandmarkets.com/PressReleases/smart-agriculture.asp. Accessed 25 Jan 2021

3. Finger R, Swinton SM, El Benni N, Walter A (2019) Precision Farming at the Nexus of Agricultural Production and the Environment. Annual Review of Resource Economics 11:313–335. https://doi.org/10.1146/annurev-resource-100518-093929

4. Birnie & Associates Consulting (2020) Agricultural Productivity Working Group Report. Agricultural Productivity Working Group, Food and Drink Sector Council

5. Faggella D (2020) AI in Agriculture - Present Applications and Impact. In: Emerj. https://emerj.com/ai-sector-overviews/ai-agriculture-present-applications-impact/. Accessed 21 Sep 2020

6. UK-RAS (2018) Agricultural Robotics: The Future of Robotic Agriculture

7. Santos Valle S, Kienzle J (2020) Agriculture 4.0 Start Agricultural robotics and automated equipment for sustainable crop production. Integrated Crop Management 24, Rome, FAO:

8. Naik G (2020) Global farming suffers from falling prices, labor shortages as virus spreads. In: S&P Global Market Intelligence. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/global-farming-suffers-from-falling-prices-labor-shortages-as-virus-spreads-57836793. Accessed 13 Apr 2021

9. Lowenberg-DeBoer J, Huang IY, Grigoriadis V, Blackmore S (2020) Economics of robots and automation in field crop production. Precision Agric 21:278–299. https://doi.org/10.1007/s11119-019-09667-5

10. Gupta M, Abdelsalam M, Khorsandroo S, Mittal S (2020) Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access PP:1–1. https://doi.org/10.1109/ACCESS.2020.2975142

11. Serpanos D (2018) The Cyber-Physical Systems Revolution. Computer 51:70–73. https://doi.org/10.1109/MC.2018.1731058

12. Dehghantanha A, Karimipour H (2020) Cybersecurity in Smart Farming: Canada Market Research. Cyber Science Lab, University of Guelph - Canada

13. Friedow C, Völker M, Hewelt M (2018) Integrating IoT Devices into Business Processes. In: Matulevičius R, Dijkman R (eds) Advanced Information Systems Engineering Workshops. Springer International Publishing, Cham, pp 265–277

14. Bonneau V, Copigneaux B, Probst L, Pedersen B (2017) Industry 4.0 in agriculture: Focus on IoT aspects. European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs

15. Farm Cyber Insurance | HSB. https://www.munichre.com/hsb/en/products/personal-lines-insurers/farm-cyber-insurance.html. Accessed 9 Nov 2020

16. Jahn DMM, Oemichen WL, Treverton DGF, et al (2019) Cyber Risk and Security Implications in Smart Agriculture and Food Systems. University of Wisconsin–Madison College of Agriculture and Life Sciences

17. Nikander J, Manninen O, Laajalahti M (2020) Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture 179:105776. https://doi.org/10.1016/j.compag.2020.105776

18. Champion S, Linsky, Mutschler P, et al (2018) Threats to Precision Agriculture (2018 Public-Private Analytic Exchange Program Report). Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS)

19. Baker L, Green R (2019) Cyber Security in UK Agriculture. NCC Group

20. DEFRA, Food Standards Industry, British Standards Institution (2017) PAS 96: Guide to protecting and defending food and drink from deliberate attack. British Standards Institution

21. HM Government (2013) UK agricultural technologies strategy. Department for Business, Innovation & Skills, Department for Environment, Food & Rural Affairs, and Department for International Development

22. Hunton Andrews Kurth (2020) EU-UK Trade Deal: What It

Means For Post-Brexit Data Flows. In: Privacy & Information Security Law Blog. https://www.huntonprivacyblog.com/2020/12/28/eu-uk-trade-deal-what-it-means-for-post-brexit-data-flows/. Accessed 2 Feb 2021

23. Kritikos M (2017) Precision agriculture in Europe: legal, social and ethical considerations. EPRS European Parliamentary Research Service, Scientific Foresight Unit (STOA), Brussels

24. European Commission (2020) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A European strategy for data. European Commission, Brussels

25. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION (2019) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

26. FBI, US Department of Agriculture (2016) Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector

27. Ferrag MA, Shu L, Yang X, et al (2020) Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. IEEE Access 8:32031–32053. https://doi.org/10.1109/ACCESS.2020.2973178

28. Elijah O, Rahman TA, Orikumhi I, et al (2018) An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. IEEE Internet of Things Journal 5:3758–3773. https://doi.org/10.1109/JIOT.2018.2844296

29. Wanstreet R (2018) America's Farmers Are Becoming Prisoners to Agriculture's Technological Revolution. https://www.vice.com/en_us/article/a34pp4/john-deere-tractor-hacking-big-data-surveillance. Accessed 15 Sep 2020

30. Waldman P, Mulvany L (2020) Farmers Fight John Deere Over Who Gets to Fix an $800,000 Tractor. Bloomberg.com

31. van der Linden D, Michalec OA, Zamansky A (2020) Cybersecurity for smart farming: socio-cultural context matters. IEEE Technology and Society Magazine (fothcoming)

32. Wiseman L, Sanderson J, Zhang A, Jakku E (2019) Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming. NJAS - Wageningen Journal of Life Sciences 90–91:100301. https://doi.org/10.1016/j.njas.2019.04.007

33. Francis J (2020) The Agriculture Act 2020 - What it means for Farmers. In: Josiah Hincks Solicitors. https://www.josiahhincks.co.uk/2020/11/17/agriculture-act-2020/. Accessed 25 Jan 2021

34. Kirova M, Montanari F, Ferreira I, et al (2019) Megatrends in the agri-food sector: global overview and possible policy response from an EU perspective. European Parliament, Policy Department for Structural and Cohesion Policies, Brussels

35. (2018) How the UK is Becoming a Global Leader in Agritech. In: AgFunderNews. https://agfundernews.com/how-the-uk-is-becoming-a-global-leader-in-agritech.html. Accessed 29 Oct 2020

36. Small robot company. In: Small Robot Company. https://www.smallrobotcompany.com/meet-the-robots. Accessed 28 Oct 2020

37. Martin R (2020) Hands Free Farm completes first major operation despite Covid delays. In: Agriland.co.uk. http://www.agriland.co.uk/farming-news/hands-free-farm-completes-first-major-operation-despite-covid-delays/. Accessed 28 Oct 2020

38. Hodge K (2020) Coronavirus accelerates the rise of the robot harvester. Financial Times

39. Editorial Team Bristol-based agritech startup LettUs Grow bags €2.76M to develop new future for farming out of thin air. In: Silicon Canals. https://siliconcanals.com/crowdfunding/agritech-startup-lettus-grow-bags-e27-6m-to-develop-new-future-for-farming/. Accessed 27 Oct 2020

40. Centres for Agricultural Innovation. In: Department for Business, Energy & Industrial Strategy. https://www.gov.uk/government/publications/centres-for-agricultural-innovation/centres-for-agricultural-innovation. Accessed 28 Oct 2020

41. Lincoln Institute for Agri-Food Technology | College of Science | University of Lincoln. https://www.lincoln.ac.uk/home/liat/. Accessed 28 Jan 2021

42. Centre for Environmental and Agricultural Informatics. https://www.cranfield.ac.uk/centres/centre-for-environmental-and-agricultural-informatics. Accessed 1 Apr 2021

43. The National Centre for Precision Farming | Harper Adams University. https://www.harper-adams.ac.uk/research/ncpf/. Accessed 1 Apr 2021

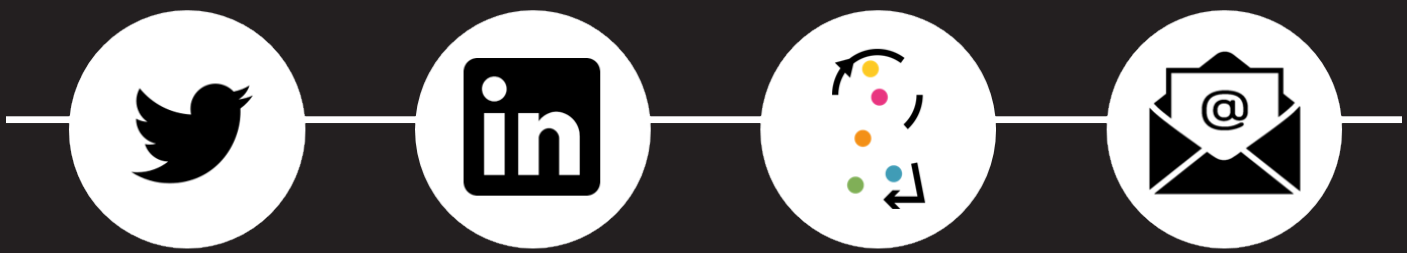
44. Bristol U of cyber-security-food-security | Cabot Institute for the Environment | University of Bristol. https://www.bristol.ac.uk/cabot/what-we-do/cyber-security-food-security/. Accessed 1 Apr 2021

45. Agriforwards CDT. https://agriforwards.eng.cam.ac.uk/. Accessed 1 Apr 2021

46. (2018) Ceres Agri-Tech Knowledge Exchange Partnership. In: IFNH. https://research.reading.ac.uk/ifnh/2018/09/04/school-of-agriculture-policy-and-development-partner-in-the-ceres-agri-tech-knowledge-exchange-partnership/. Accessed 1 Apr 2021

47. PETRAS Petras - – Cybersecurity for Food Security (CyFoo). https://petras-iot.org/project/cybersecurity-for-food-security-cyfoo-2/. Accessed 28 Jan 2021

48. Yu K-H, Beam AL, Kohane IS (2018) Artificial intelligence in healthcare. Nature Biomedical Engineering 2:719–731. https://doi.org/10.1038/s41551-018-0305-z



TWITTER
@PETRASiot

LINKEDIN
linkedin.com/
school/petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.ac.uk