Final Project Literature Review

For the last two decades, the world has been populated with internet connected devices; starting with the smart phone, moving through the household from toothbrushes to vacuum cleaners, from wristwatches to lighting. The proliferation of such devices has enabled data to flow in new and unexpected ways, not restricted to the home but also allowed for increased automation and monitoring of the natural environment, notably in the agriculture industry. Previously, I have written ( in the CM3040 module ) on how small scale smart technology can be introduced into everyday gardening. In this paper, I am investigating how IoT can be integrated into existing designs, to build new and harden existing smart agriculture solutions in a security conscious way. This is an urgent topic because if we rely on internet connected technologies to grow our food, we must ensure that the supply of our food is not vulnerable to a catastrophic technology induced failure.

The smart devices that make up the internet of things (commonly referred to as IoT devices, or just IoT) have begun to transform the agriculture industry, with the potential for a similar impact upon society as the plough made thousands of years ago. This new age of farming was coined “Agriculture 4.0” by a global consulting firm (De Clercq, Vats and Biel, 2018) as part of research conducted in the last decade,[[1]](#footnote-0) describing a “food security” issue in terms of the correlation of worldwide population growth and the subsequent increasing demand for food, posing this as an issue to be solved by the technology sector.[[2]](#footnote-1) Although many technologies are mentioned, including; drone technology, artificial intelligence, 3D printing, automated hydroponics, vertical farming, and data analytics - the Internet of Things is not identified as something that is foundational to the success of Agriculture 4.0. Rather, IoT is included in the long list, as if it was but another module, interchangeable with AI.[[3]](#footnote-2) This early article is indicative of the ongoing situation, where commercial solutions offer technology to an industry under pressure to adapt and adopt, where farmers are being promised efficiency and profits, using the threat to food security as a weapon without considering how the technologies themselves could be weaponised.

Technical or cyber security is not marketed as the highest priority for the target audience for many of the consumers of these IoT devices, but the devices themselves are well placed to be secured. In agriculture, many of the IoT devices are sensors that are able to take measurements, record and store data, and send them to a central server (Singh et al., 2022).[[4]](#footnote-3) The sensors are high precision, can be calibrated to defined tolerances, and will report their findings in real time.[[5]](#footnote-4) These are all shared features with good security monitoring tools, such as those deployed in secure buildings, and indeed those already used to protect farms and crops against pests and other physical threats.[[6]](#footnote-5) Therefore, there is an opportunity to build some strong foundations for the development of a secure network, though it is clear that this must be as automated and user friendly as possible, as much of the online literature in the smart agriculture sector references only the most basic security tips; such as recommending the use of passwords.[[7]](#footnote-6) This is not to say that there are no complex IoT farming systems, quite the opposite, research published in China detail both the the improvements that precision feeding offers to the farm’s output efficiency and cost while also tracking the performance of the IoT platform in terms of usability of the system and packet loss (Xia et al., 2023).[[8]](#footnote-7)

By tracking the error rate of the precision equipment against the baseline error recorded when humans did not use technology, the researchers found that the IoT system performed at last as well as humans at delivering a quantity of feed to animals.[[9]](#footnote-8) However, the system was severely limited, while there were a great deal of child nodes providing either monitoring data or controlling servo motors, the parent node - a handheld Personal Digital Assistant (PDA) - was a bottleneck for the data.[[10]](#footnote-9) This suggests that while usability in the form of a handheld device was prioritised for the research in order to record accurate data, in the event that two child nodes attempted to send data to the PDA at the same time, packet loss became inevitable and so therefore the data could not be recorded.[[11]](#footnote-10) This causes significant concern for a system that prioritises security of the system as information must have good integrity, and must be recorded accurately for fear of triggering a security alert or an alarm. This also highlights the need for a number of human machine interfaces, to prevent the kind of system failure described above - it is clear from this source that a single PDA will not suffice for a complex operation. With a number of administration nodes and personal devices, comes the need for secure user authentication and role based policy access that come along with it.

As the number of nodes increase, so does the visible attack surface, increasing the risk of compromise from device hijacking and the risk of data loss as described in (Alruwaili et al., 2024).[[12]](#footnote-11) It is therefore vital to properly secure the network that the devices operate within using standard methods, but also enforce rigorous security methods for the devices, the users, and the gateway that acts as interface between the user and the device infrastructure.[[13]](#footnote-12) There are a number of different access control frameworks that have been proposed; including “physically secure”[[14]](#footnote-13) “unclonable functions” (PUFs) that are hardcoded into the devices themselves,[[15]](#footnote-14) and access control policies that are able to meet the demands of a non-static network of devices with multiple users and potentially different ways to view data travelling across the network.[[16]](#footnote-15) The data travelling across the network may be traffic like simple sensor readings being updated in real time, or it could be commands issued by the users that control various robotic functions such as the delivery of animal food,[[17]](#footnote-16) irrigation or camera position.[[18]](#footnote-17) Therefore, I pose that the risk associated with device hijacking directly relates to the ability of the land to continue to produce efficiently. As a result, the system must offer security, observability, and also a level of alerting for when errors or anomalies are detected.

Security is an issue for IoT, which is often by definition exposed to the open internet, or running numerous devices and services on smaller local networks, which makes it necessary to consider the difficulty of updating device software or firmware.[[19]](#footnote-18) This offers inherent weaknesses when relying on IoT devices, which may have persiant and unpatched vulnerabilities. (Chaudhry et al., 2020) notes that alongside this risk of vulnerability exploitation, the limited processing resource available to the microcontrollers commonly used in IoT devices expose these systems to catastrophic denial of service attacks.[[20]](#footnote-19) These devices are often powered by internally small batteries, as IoT can support very low power consumption, however this limits the resilience that these devices offer, as described in (Deva Shahila et al., 2024).[[21]](#footnote-20) The paper demonstrates why “effective safeguards” are needed when developing IoT products, and poses a “System on Chip”[[22]](#footnote-21) approach to designing hardware for IoT networks that are at risk of tamper, or compromise. However, despite the clear need for such secure hardware and firmware in order to deploy hardened and resilient IoT, this is a novel approach that does not address the reality that many IoT devices are already on the market. Therefore reinstallation of a new system architecture onto a wide range of devices for the sake of security is simply not realistic - if only because it would be very inconvenient.

Therefore, policy based access control is the most reasonable solution for both user access and for device control. By ensuring that access is granted and continuously validated it will allow safe and secure transmission of data, and will also trigger alerts in the event of a policy based failure. This kind of security feature will prevent several prominent cyber attacks including physical capture, malicious device deployment and on path attacks.[[23]](#footnote-22) We can rely on rule evaluation in order to set the triggers for such alerting or trigger more severe security features. Typically in an agricultural internet of things network we will see monitoring for temperature, moisture levels, or humidity within certain parameters. It is possible to adapt the same rules to communicate fluctuations in network traffic or to monitor for unauthorised access. (Chaudhry et al., 2020) proposes improvements to the existing “lightweight access control and key agreement (LACKA-IoT)” system that enforces an access control policy during the registration phase, and also provides continual security analysis to authenticate the legitimacy of device to device communication.[[24]](#footnote-23) In the event a device or agent fails a control check, it would be possible to trigger an alert on the network, **or indeed to trigger an on-device security control that would isolate the device from the network.**

While rule based policy and automation are key features for secure IoT environments, these systems must be readable and accessible by people. Ideally these people would not have to be IT experts, or network administrators to operate the systems properly. Other IoT systems (without emphasis on security) employ visual interfaces in order to display data, and control functionality. In (Xia et al., 2023) there is an emphasis on how a graphical user interface helps a person to select an animal to be fed, by touching a screen and remotely trigger the delivery of food,[[25]](#footnote-24) while in (Huet et al., 2022) the environmental controls of a beehive are displayed and updated in real time on a dashboard.[[26]](#footnote-25) While the first example shows a snapshot of the current moment at any time, the second dashboard shows change over time in the form of a graph,m and includes an algorithmic projection of what the expected future reading would ideally be.[[27]](#footnote-26) This kind of visual feedback is particularly useful, as while a system might be operating within accepted parameters, a person might be able to simply identify by sight anomalies in the readings too subtle for the system - or indeed recognise if the system’s parameters are incorrectly configured or malfunctioning.

The literature here has sought to address general IoT security principles, authentication protocols, hardware security, and IoT’s broad applications into agriculture. There is a generally accepted view in the literature that monitoring, control and prediction of data is a positive step forward and treated as if this is a step into the future, as “Agriculture 4.0”. However this is often without reference to secure data handling, despite discussion of technology failures by many of the researchers. One of the key issues I wish to face is the trade off between security and convenience for smaller or less well off farmers who choose to adopt IoT technology. Instead of considering IoT devices as single function objects, as only environmental sensors or control panels, my project looks to integrate these devices into a network where each node actively participates in the security of the system.

# Bibliography

Alruwaili, O., Mohammed Alotaibi, F., Tanveer, M., Chaoui, S. and Armghan, A., 2024a. PSAF-IoT: Physically Secure Authentication Framework for the Internet of Things. *IEEE Access*, [online] 12, pp.78549–78561. https://doi.org/10.1109/ACCESS.2024.3407353.

Alruwaili, O., Tanveer, M., Alotaibi, F.M., Abdelfattah, W., Armghan, A. and Alserhani, F.M., 2024b. Securing the IoT-enabled smart healthcare system: A PUF-based resource-efficient authentication mechanism. *Heliyon*, [online] 10(18), p.e37577. https://doi.org/10.1016/j.heliyon.2024.e37577.

Anon. 2022a. *Ukraine war spotlights agriculture sector’s vulnerability to cyber attack*. [online] Cisco Talos Blog. Available at: <https://blog.talosintelligence.com/ukraine-and-fragility-of-agriculture/> [Accessed 10 June 2025].

Anon. 2022b. *Why Ukraine’s agriculture sector could be set to attract cyberattacks*. [online] euronews. Available at: <https://www.euronews.com/next/2022/08/24/the-war-in-ukraine-has-threatened-its-vital-agriculture-now-it-could-be-crippled-by-a-cybe> [Accessed 10 June 2025].

Anon. 2025a. *BS 8646:2023 | 30 Jun 2023 | BSI Knowledge*. [online] Available at: <https://knowledge.bsigroup.com/products/use-of-autonomous-mobile-machinery-in-agriculture-and-horticulture-code-of-practice> [Accessed 10 June 2025].

Anon. 2025b. *CEMA - European Agricultural Machinery - Agriculture 4.0*. [online] Available at: <https://www.cema-agri.org/priorities/agriculture-4-0> [Accessed 11 June 2025].

Anon. 2025c. *Guidance to support safe and secure use of crop robots in farming*. [online] BSI. Available at: <https://www.bsigroup.com/en-GB/insights-and-media/media-centre/press-releases/2023/june/guidance-safe-secure-use-crop-robots-farming/> [Accessed 10 June 2025].

Anon. 2025d. *Smart Farming: How Technology is Enhancing Agricultural Security*. [online] Available at: <https://www.agritecture.com/blog/smart-farm-security-technology> [Accessed 11 June 2025].

Anon. 2025e. *The Complete Guide to Smart Farming & Agriculture*. [online] Available at: <https://smartertechnologies.com/guides/the-complete-guide-to-smart-agriculture-farming/> [Accessed 10 June 2025].

Anon. n.d. *12 Climate-smart technologies that could transform the way we grow food*. [online] World Economic Forum. Available at: <https://www.weforum.org/stories/2023/10/12-climate-smart-technologies-that-could-transform-the-way-we-grow-food/>.

Anon. n.d. *How the Russian invasion of Ukraine has further aggravated the global food crisis*. [online] consilium.europa.eu. Available at: <https://www.consilium.europa.eu/en/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/>.

Whiting, A., 2019. The UK senses a smart farming revolution. *Transform Industry*. Available at: <https://transformindustry.com/sensors/the-uk-senses-a-smart-farming-revolution/> [Accessed 10 June 2025].

Chaudhry, S.A., Yahya, K., Al-Turjman, F. and Yang, M.-H., 2020. A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems. *IEEE Access*, [online] 8, pp.139244–139254. https://doi.org/10.1109/ACCESS.2020.3012121.

Anon., 2025. *Shielding the supply: Cybersecurity in food and agriculture*. [online] Cybersecurity Guide. Available at: <https://cybersecurityguide.org/industries/food-and-agriculture/> [Accessed 10 June 2025].

De Clercq, M., Vats, A. and Biel, A., 2018. Agriculture 4.0: The Future of Farming Technology. [online] Available at: <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/apr/agriculture-4-0-the-future-of-farming-technology.pdf>.

Deva Shahila, D.F., Suresh, Dr.L.P., Aruna Jeyanthy, P., Stephen, V. and R M, A., 2024. Designing and Analyzing Secure SoC Architecture for IoT Devices. In: *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*. [online] pp.1893–1899. https://doi.org/10.1109/ICCPCT61902.2024.10673314.

García-García, J.I., Marín-Aragón, D., Maciá, H. and Jiménez-Cantizano, A., 2021. Viñamecum: A Computer-Aided Method for Diagnoses of Pests and Diseases in the Vineyard. *Applied Sciences*, [online] 11(10), p.4704. https://doi.org/10.3390/app11104704.

Gerlée, K., 2023. IoT in agriculture – 6 smart farming examples. *Freeeway*. Available at: <https://freeeway.com/iot-in-agriculture-6-smart-farming-examples/> [Accessed 10 June 2025].

Holmberg, A., 2024. Food security in light of the war in Ukraine: food studies meets defence studies. *Defence Studies*, [online] 24(4), pp.543–558. https://doi.org/10.1080/14702436.2024.2378793.

Huet, J.-C., Bougueroua, L., Kriouile, Y., Wegrzyn-Wolska, K. and Ancourt, C., 2022. Digital Transformation of Beekeeping through the Use of a Decision Making Architecture. *Applied Sciences*, [online] 12(21), p.11179. https://doi.org/10.3390/app122111179.

Adamson, J., 2023. TuberScan undergoes UK testing. *Crop Production Magazine*. Available at: <https://www.cpm-magazine.co.uk/news/tuberscan-undergoes-uk-testing/> [Accessed 10 June 2025].

Joseph, M., Matthew, B., Lee, W., Jim, M., Richard, G. and Edwin, H., 2025. *Research - Tuberscan: Using deep learning and data science to improve agronomy decisions in the potato industry*. [online] Available at: <https://www.harper-adams.ac.uk/research/project/1285/tuberscan-using-deep-learning-and-data-science-to-improve-agronomy-decisions-in-the-potato-industry> [Accessed 10 June 2025].

Leal Filho, W., Fedoruk, M., Paulino Pires Eustachio, J.H., Barbir, J., Lisovska, T., Lingos, A. and Baars, C., 2023. How the War in Ukraine Affects Food Security. *Foods*, [online] 12(21), p.3996. https://doi.org/10.3390/foods12213996.

Lewis, V., 2023. *BSI release guidance on use of AMM in agriculture and horticulture*. [online] News from AA Farmer. Available at: <https://s45854.p1721.sites.pressdns.com/news/bsi-release-guidance-on-use-of-amm-in-agriculture-and-horticulture.html> [Accessed 10 June 2025].

Lin, F., Li, X., Jia, N., Feng, F., Huang, H., Huang, J., Fan, S., Ciais, P. and Song, X.-P., 2023. The impact of Russia-Ukraine conflict on global food security. *Global Food Security*, [online] 36, p.100661. https://doi.org/10.1016/j.gfs.2022.100661.

Plexal, n.d. *CYBER SECURITY AND OUR FOOD SYSTEM*. [online] Available at: <https://www.plexal.com/wp-content/uploads/2022/05/Cyber-security-and-our-food-system-4.pdf>.

Shahila, D.F.D., Prathaban, B.P., Stephen, V., Jeyanthy, P.A. and Evangelin, D.L., 2023. Novel Biometric ATM User Authentication and Real-Time Secure Clickbait for Multi-Bank Transactions. In: *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*. [online] pp.1–7. https://doi.org/10.1109/ICCEBS58601.2023.10448889.

Shalimov, A., 2023. *IoT in Agriculture: 9 Technology Use Cases for Smart Farming (and Challenges to Consider)*. [online] Eastern Peak - Technology Consulting & Development Company. Available at: <https://easternpeak.com/blog/iot-in-agriculture-technology-use-cases-for-smart-farming-and-challenges-to-consider/> [Accessed 10 June 2025].

Sharp, N., 2025. *7 types of agricultural sensors driving the smart farming revolution*. [online] Available at: <https://www.escatec.com/blog/7-types-of-agricultural-sensors-driving-the-smart-farming-revolution> [Accessed 10 June 2025].

Singh, R., Singh, R., Gehlot, A., Akram, S.V., Priyadarshi, N. and Twala, B., 2022a. Horticulture 4.0: Adoption of Industry 4.0 Technologies in Horticulture for Meeting Sustainable Farming. *Applied Sciences*, [online] 12(24), p.12557. https://doi.org/10.3390/app122412557.

Singh, R., Singh, R., Gehlot, A., Akram, S.V., Priyadarshi, N. and Twala, B., 2022b. Horticulture 4.0: Adoption of Industry 4.0 Technologies in Horticulture for Meeting Sustainable Farming. *Applied Sciences*, [online] 12(24), p.12557. https://doi.org/10.3390/app122412557.

Torres-Sanchez, R., Zafra, M.T.M., Soto-Valles, F., Jiménez-Buendía, M., Toledo-Moreo, A. and Artés-Hernández, F., 2021. Design of a Distributed Wireless Sensor Platform for Monitoring and Real-Time Communication of the Environmental Variables during the Supply Chain of Perishable Commodities. *Applied Sciences*, [online] 11(13), p.6183. https://doi.org/10.3390/app11136183.

Welsh, C., 2024. Russia, Ukraine, and Global Food Security: A Two-Year Assessment. [online] Available at: <https://www.csis.org/analysis/russia-ukraine-and-global-food-security-two-year-assessment> [Accessed 10 June 2025].

Xia, J., Xu, J., Zeng, Z., Lv, E., Wang, F., He, X. and Li, Z., 2023. Development of a Precision Feeding System with Hierarchical Control for Gestation Units Using Stalls. *Applied Sciences*, [online] 13(21), p.12031. https://doi.org/10.3390/app132112031.

1. De Clercq, M., Vats, A. and Biel, A., 2018. Agriculture 4.0: The Future of Farming Technology. [online] Available at: <<https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/apr/agriculture-4-0-the-future-of-farming-technology.pdf>>. p.5. [↑](#footnote-ref-0)
2. Ibid. p.12. [↑](#footnote-ref-1)
3. Ibid. p. 16. [↑](#footnote-ref-2)
4. Singh, R., Singh, R., Gehlot, A., Akram, S.V., Priyadarshi, N. and Twala, B., 2022. Horticulture 4.0: Adoption of Industry 4.0 Technologies in Horticulture for Meeting Sustainable Farming. *Applied Sciences*, [online] 12(24), p.12557. https://doi.org/10.3390/app122412557. [↑](#footnote-ref-3)
5. Ibid. [↑](#footnote-ref-4)
6. Anon. 2025. *Smart Farming: How Technology is Enhancing Agricultural Security*. [online] Available at: <https://www.agritecture.com/blog/smart-farm-security-technology> [Accessed 11 June 2025]. [↑](#footnote-ref-5)
7. Ibid. [↑](#footnote-ref-6)
8. Xia, J., Xu, J., Zeng, Z., Lv, E., Wang, F., He, X. and Li, Z., 2023. Development of a Precision Feeding System with Hierarchical Control for Gestation Units Using Stalls. *Applied Sciences*, [online] 13(21), p.12031. https://doi.org/10.3390/app132112031. [↑](#footnote-ref-7)
9. Ibid. p.4. [↑](#footnote-ref-8)
10. Ibid. p.5. Figure 10. [↑](#footnote-ref-9)
11. Ibid. p.5. [↑](#footnote-ref-10)
12. Alruwaili, O., Mohammed Alotaibi, F., Tanveer, M., Chaoui, S. and Armghan, A., 2024. PSAF-IoT: Physically Secure Authentication Framework for the Internet of Things. *IEEE Access*, [online] 12, pp.78549–78561. <https://doi.org/10.1109/ACCESS.2024.3407353>. p.1. [↑](#footnote-ref-11)
13. Ibid. p.4. [↑](#footnote-ref-12)
14. Ibid. p.1 [↑](#footnote-ref-13)
15. Alruwaili, O., Tanveer, M., Alotaibi, F.M., Abdelfattah, W., Armghan, A. and Alserhani, F.M., 2024. Securing the IoT-enabled smart healthcare system: A PUF-based resource-efficient authentication mechanism. *Heliyon*, [online] 10(18), p.e37577. <https://doi.org/10.1016/j.heliyon.2024.e37577>. p.4. [↑](#footnote-ref-14)
16. Chaudhry, S.A., Yahya, K., Al-Turjman, F. and Yang, M.-H., 2020. A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems. IEEE Access, [online] 8, pp.139244–139254. <https://doi.org/10.1109/ACCESS.2020.3012121>. p.2. [↑](#footnote-ref-15)
17. Xia, J., Xu, J., Zeng, Z., Lv, E., Wang, F., He, X. and Li, Z., 2023. Development of a Precision Feeding System with Hierarchical Control for Gestation Units Using Stalls. *Applied Sciences*, [online] 13(21), p.12031. <https://doi.org/10.3390/app132112031>. p 5. [↑](#footnote-ref-16)
18. Singh, R., Singh, R., Gehlot, A., Akram, S.V., Priyadarshi, N. and Twala, B., 2022. Horticulture 4.0: Adoption of Industry 4.0 Technologies in Horticulture for Meeting Sustainable Farming. *Applied Sciences*, [online] 12(24), p.12557. <https://doi.org/10.3390/app122412557>. p.2 [↑](#footnote-ref-17)
19. García-García, J.I., Marín-Aragón, D., Maciá, H. and Jiménez-Cantizano, A., 2021. Viñamecum: A Computer-Aided Method for Diagnoses of Pests and Diseases in the Vineyard. Applied Sciences, [online] 11(10), p.4704. <https://doi.org/10.3390/app11104704>. P.2. [↑](#footnote-ref-18)
20. Chaudhry, S.A., Yahya, K., Al-Turjman, F. and Yang, M.-H., 2020. A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems. *IEEE Access*, [online] 8, pp.139244–139254. <https://doi.org/10.1109/ACCESS.2020.3012121>. p.1. [↑](#footnote-ref-19)
21. Deva Shahila, D.F., Suresh, Dr.L.P., Aruna Jeyanthy, P., Stephen, V. and R M, A., 2024. Designing and Analyzing Secure SoC Architecture for IoT Devices. In: *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*. [online] pp.1893–1899. <https://doi.org/10.1109/ICCPCT61902.2024.10673314>. p.5. [↑](#footnote-ref-20)
22. Ibid. p.2 [↑](#footnote-ref-21)
23. Chaudhry, S.A., Yahya, K., Al-Turjman, F. and Yang, M.-H., 2020. A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems. IEEE Access, [online] 8, pp.139244–139254. https://doi.org/10.1109/ACCESS.2020.3012121. p.3. [↑](#footnote-ref-22)
24. Ibid. p.5. [↑](#footnote-ref-23)
25. Xia, J., Xu, J., Zeng, Z., Lv, E., Wang, F., He, X. and Li, Z., 2023. Development of a Precision Feeding System with Hierarchical Control for Gestation Units Using Stalls. *Applied Sciences*, [online] 13(21), p.12031. <https://doi.org/10.3390/app132112031>. p.5. [↑](#footnote-ref-24)
26. Huet, J.-C., Bougueroua, L., Kriouile, Y., Wegrzyn-Wolska, K. and Ancourt, C., 2022. Digital Transformation of Beekeeping through the Use of a Decision Making Architecture. Applied Sciences, [online] 12(21), p.11179. <https://doi.org/10.3390/app122111179>. p.16. [↑](#footnote-ref-25)
27. Ibid. Fig. 11. [↑](#footnote-ref-26)