TRUST IN THE ADOPTION OF INTERNET OF THINGS FOR SMART AGRICULTURE IN DEVELOPING COUNTRIES

Tsitsi Zengeya[1], Paul Sambo[1] and Nyasha Mabika[2]

[1]Great Zimbabwe University, Department of Mathematics and Computer Science, Zimbabwe
[2]Great Zimbabwe University, Department of Livestock, Wildlife and Fisheries, Zimbabwe

ABSTRACT

Trust in online environments is based on beliefs in the trustworthiness of a trustee, which is composed of three distinct dimensions - integrity, ability, and benevolence. Zimbabwe has slowly adopted Internet of Things for smart agriculture as a way of improving on food security in the country, though there is hesitancy by most farmers citing trust issues as monitoring of crops, animals and farm equipment's would be done online through connecting several devices and accessing data. Farmers are facing difficulties in trusting that the said technology has the ability to perform as expected in a specific situation or to complete a required task, i.e. if the technology will work consistently and reliably in monitoring the environment, nutrients, temperatures and equipment status. The integrity of the collected data as it will be used for decision making. There is a growing need to determine how trust in the technology influence the adoption of IoT for smart agriculture in Zimbabwe. The mixed methodology was used to gather data from 50 A2 model farmers randomly sampled in Zimbabwe. The findings revealed that McKnight etal. trust in technology model can be used to influence the adoption of IoT through trusting that the technology will be reliable and will operate as expected.Additional constructs such as security and distrust of technology can be used as reference for future research.

KEYWORDS

Internet of Things, Adoption, Smart Agriculture, Trust, Trust in Technology

1. INTRODUCTION

The adoption of Internet of Things for Smart Agriculture in Zimbabwe will see an increase in food production resulting in improved food security and minimizing food imports such as maize, wheat and soya beans as revealed through research by[1]. The introduction of technology in agriculture has boosted food production in some of the developed countries especially in the United States of America (USA) and other developing countries. Although the Zimbabwean farmers are gradually adopting smart agriculture because of its perceived usefulness and perceived ease of use which are the key determinants of IoT use in agriculture. Farmers are facing challenges in trusting IoT farming systems as the technology has failed to perform as expected in a specific situation or to complete a required task. Also farmers need to trust the integrity of the collected data as it will be used for decision making.

Five agro-ecological regions in Zimbabwe are classified as natural regions. These regions are categorized according to the amount of rainfall, soil quality, vegetation, climatic conditions among other factors. Zimbabwe's rainfall pattern ranges from 550 to 900 millimeters across the

five regions. Most of the Zimbabwean farmers rely on rainfall for crop farming and some of the A1 and A2 farms largely rely on irrigation[2]. Zimbabwe has slowly adopted IoT for smart agriculture citing trust issues.The rapid use of IoT in agriculture has brought in new risks thus farmers losing trust in the adoption of the smart technology. Potential cyber threats paused by the Internet has led farmers to be skeptical in the implementation of IoT in agriculture.

2. LITERATURE REVIEW

Internet of Things is defined as a network of interconnected devicessuch as sensors and communication networksconnected through the internet to transfer information without human intervention[3].IoT has managed to change the traditional method of farming, by aiding farmers with the use of technology. This has transformed the agricultural sector from precision farming into smart farming[4].A farmer can monitor their field with the use of sensors and drones. The type of sensors that are used with IoT are: location sensors, optical sensor, electro-chemical sensors, mechanical sensors, dielectric soil moisture sensors and airflow sensors. Location sensors are used by farmers to identify or locate a specific area using Global positioning Systems (GPS) or manned or unmanned aerial devices. Optical sensors are used to understand the properties of the soil and crop through analyzing the amount of reflected light on the growing parts of the plant in real time. The optical sensors are used to examine moisture and plant nutrients such as Nitrogen content. Electro-chemical sensors are used to monitor the pH level of the soil such as the levels of Phosphorous, Potassium, Calcium, Sodium, Nitrogen, Copper and Iron. Mechanical sensors are used to monitor plant growth such as the amount of force that roots exert when absorbing water. Dielectric soil moisture sensors are used to monitor the soil moisture. Airflow sensors determines the properties of the soil, its compaction, moisture holding and capacity.

The sensors gives an opportunity for a farmer to plan watering times and areas that need to be irrigated the most. Sensors can also be used to monitor and alert the farmer on the movement of pests in the field. IoT allows farmers to remotely control farm activities, processing, and logistic operations by the use of sensors and actuators, e.g. it allows for accuracy in the application of pesticides and fertilizers or robots for automatic weeding. IoT can be used to monitor food quality during transportation by remotely accessing and controlling the geographic location and conditions of shipments and products.

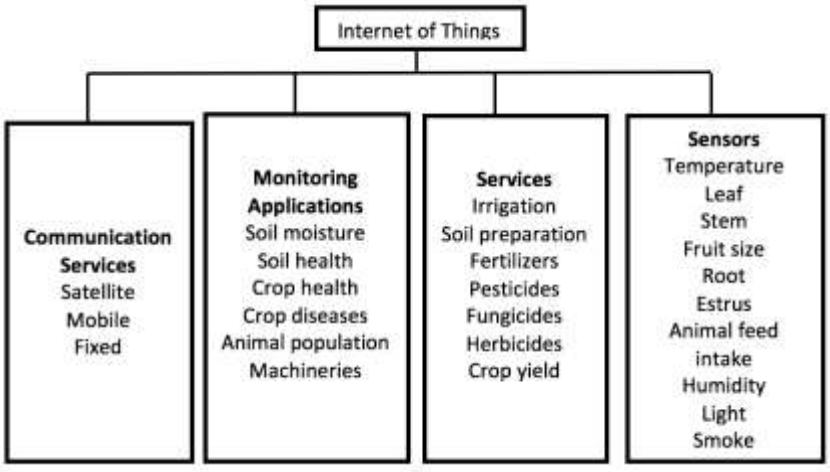

Figure 1. Illustration of Internet of Things in agriculture[1]

Figure 1 illustrates the application of the Internet of things in agriculture which is composed of four elements, communication services, monitoring applications, services, and sensors. Communication services include network services for Internetdata that can be offered through satellite, mobile fixed networks[5]. Data transmission of IoT devices varies and can be supported with 2G-5G cellular networks. Internet-linked devices enable farmers to collect and exchange data without human involvement. The monitoring applications can be used to monitor soil moisture, soil health, crop health, crop diseases, and animal population[6]. Machinery such as combine harvesters, tractors, irrigation equipment, and drones can be fitted with sensors[7], for example, Hello Tractor developed a low-cost monitoring device that can be used to monitor the condition of the tractor[8].IoT canbe applied through an agricultural drone which is a relativelyinexpensive device fitted with a mechanism that provides farmers with information about the status of the crops which can result in an increasein yields and reduce crop damage.The drone can also be used to track and monitor the movement of animals and check if there is any danger being paused in their area[9]. IoT can also be used with irrigation equipment where water usage can be monitored. The services include the detection of soil nutrients andthe amount of fertilizer required. The services for IoT in agriculture vary from crop yield to, detection of pests and herbs affecting the growth of the crop. Sensor devices play a pivotal role in the collection of data about the status of the land, crop, or animal, for example, the devices can be used to determine fruit size, moisture,or nutrient content[10].

With the adoption of IoT, farmers will be able to control the internal processes and thereby decrease production risks. The availability of data allows farmers to foresee the output of production and allows for better planning especially crop management and product distribution. With enhanced control over overproduction, waste levels canbe reduced and costs can be more effectively managed. Knowledge about any anomalies or challenges in the rate of crop growth or the health of livestock allows farmers to mitigate the risk of diminished yield or even crop failure[11].

Current agricultural trends have seen the adoption of novel strategies of crop production such as greenhouses, hydroponics, vertical farming, and phenotyping to increase crop yield[10]. Crop production in greenhouses is done in a controlled environment which allows for seasoned and unseasoned crops to be grown anywhere at any time. Wireless communication, mobile devices, and other Internet devices are used in the greenhouse to monitor humidity, temperature, light, and pressure. Hydroponics allows farmers to grow seasonal and unseasonal crops in water under controlled conditions without a soil medium and the nutrients are applied through the irrigation system. Wireless devices connected through the Internet are used to monitor the water level, nutrients, and fertilizers used for crop production. Vertical farming allows farmers to grow crops in a controlled environment on a small piece of land. This type of farming is commonly used in Japan[12]. The use of IoT in vertical farming permits the control of moisture and groundwater using computers or cellular devices such as tablets and smartphones. Phenotyping *"is an advanced genetic engineering technique and biotechnology which correlates the genetic sequences of crops for agronomical and physiological aspects"*[13]. In this approach, IoT is used to determine and analyzethe characteristics of genetic engineering and biotechnology of the crops[3].

IoT is also being used to improve the sustenance of food production in aquaculture. Aquaculture is an agricultural activity where farmers focus on producing fish, water plants, and diverse oceanic organisms[14].Devices can be used to monitor the water, oxygen and nutrients levels and transmit this data through the Internet. Aquaponics is a sustainable agriculture in a symbiotic environment by combining aquaculture and hydroponics[15]. The water system should flow on

the planting medium periodically to ensure the plants get the nutrients, while the water can be filtered properly by the medium.

IoT can be used with cloud computing which resolves some of the limitations of the devices and sensors, by providing storage solutions and computing power for analysis. Cloud computing also offers farmers an opportunity to obtain valuable information about markets, especially seeds, fertilizers, equipment, and farming methods. Cloud computing can also facilitate the use of Big Data analytical tools forfarmers[16][17].

Trust in technology is defined as a willingness to depend on the specific technology in a given situation in which negative consequences are possible[18]. For farmers to adapt to IoT smart farming, they need to trust the technology for example, believing that the technology is performing to the expected standards, considering that the data/information collected will be critical for decision making.

The theoretical framework of this research is based on the [19] model which has three constructs: Propensity to Trust General Technology, Institution – Based Trust in Technology and Trust in Specific Technology. The relationship of the three constructs are shown in Figure 2.

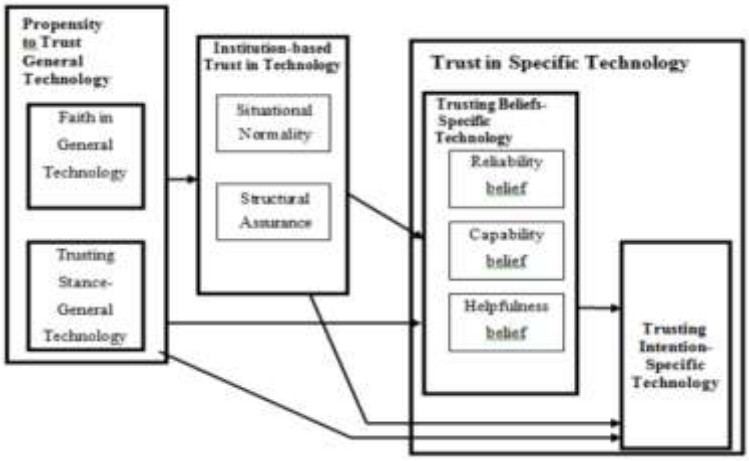

Figure 2 Relationship among Technology-Related Constructs[18]

In the ‘Propensity of Trust in General Technology’ two aspects are involved which are ‘Faith in General Technology’ and ‘Trusting Stance in General Technology’. Faith in General Technology claims that if farmers have faith in general technology they assume that the IoT technology is consistent, reliable, functional and can provide the help required, while Trusting Stance in General Technology is when a farmer trust a technology until it provides a reason not to be trusted.

Institution-based Trust in Technology involves ‘Situational Normality’ and ‘Structural Assurance’. Situational Normality gives a belief that success with a specific technology is likely when farmers feel comfortable using the general type of technology. While Structural Assurance is when farmers believe that enough support - be it as legal such as contractual obligations or physical such as replacing faulty equipment really do exist to ensure successful use of IoT technology.

Trust Intention on Specific Technology involves beliefs about the context and features of technology were farmers expects the IoT technology to work consistently and reliably with the capacity to complete the required task, as well as Trusting Intention- Specific Technology were farmers express a willingness to depend on a specific technology in uncertain or risky situations. Trust can be affected by security issues such as privacy, confidentiality, integrity, availability, authenticity and non-repudiation factors as shown in Table 1.

Table 1: Overview of possible attacks per security aspect in agricultural cybersecurity[20]

Security Aspects	**Example of Attacks**	**Agricultural Consequences**	**Studies**
Privacy	Physical Attack Replay Attack Masquerade Attack	The collection of information regarding the type and possible usage of devices concerning agriculture projects. These security leaks can be used in order to get access to infrastructure and production standards as well as getting privacy data and compromising the privacy of the system. Theft and vandalism purposes can be the outcome of possible violation of privacy	[[21][22][23][24][25][26]
Confidentiality	Tracing attack Brute force attack Known-Key Attack	The usage of various communication devices in a smart farming or an agricultural system based on ICT can outcome into data travelling through several interconnected devices and protocols from source to destination. Possible confidentiality problems can lead to the persistence, on many occasions, of loss of privacy and data or information breaches. The unauthorized access to important data as a result of the confidentiality loss could lead to theft of key information and also cause serious threats over the involved agriculture system users' confidential information	[27][21][23][28][29]
Integrity	Forgery Attack Man-In-The-Middle Attack (MTM) Biometric template attack Trojan Horse Attack	This can be as a result of an unauthorized or improper changes in the trustworthiness of data or resources, information between agriculture Information Communication Technology (ICT) or smart farming system can no longer be reliable or accurate. The transmitted information or data between the devices and/or people/farmers/stakeholders involved in an agricultural business or even a process can lead to possible financial or authentication frauds due to the assurance that the information is sufficiently accurate for its purpose.	[21][23][26][20][30]
Availability	Denial of service (DoS) Attacks (SYN Floods, Ping of Death, Botnets	A smart farming environment is meant for real or near real-time operations in order to keep a real world impact. An attacker can suspend the activities of the installed smart network, or even establish the service unavailable to the farmers. The lack of availability of the provided services can lead to business disruption, possible customer's loss of confidence and revenue.	[21][23][31][32][33]
Authenticity	Attack against Authentication 9dictionary attack, Session	Authenticity ensures the authentication of certain information provided from a valid/authorized source. Forged attackers' identities can mimic legal/authorized persons and gain access to the smart farming system. Possible results can be the data breach/loss and/or alternation, service unavailability, loss of devices connectivity or even smart farming agriculture system corruption and/or destruction.	[21][23][34][35][36]

	Hijacking, Spoofing)		
Non-Repudiation	Malicious code Attack Repudiation Attack	During the authentication process, a commonly known service that provides proof of the integrity as well as the origin of data, both in an unforgeable relationship, and can be verified by any third party at any time with high assurance and genuineness, is non-repudiation. The repudiation of information an attacker to repudiate all the power consumption, generated information and production processes of an agricultural ICT system, which can lead to a situation of refusing services, authentication information or data transmission through the codes of the system.	[21][23][37][38]

Trust plays a crucial role in IoT for smart agriculture as it shapes technology related-beliefs and behaviour of farmers and help improve the adoption rate of IoT for smart agriculture in developed countries. Trust in technology was necessitated by various security threats and risks that are associated with the use of technology which prompts farmers to really want to be assured of whether IoT technology for smart agriculture would perform as expected, work properly and whether the collected data is reliable so that it can be used for decision making. This paper investigated howtrust can be used to influence the adoption of IoTin agriculture in developing countries such as Zimbabwe.

3. RESEARCH METHODOLOGY

This research examined how trust can influence the adoption of IoT in developing countries such as in the Zimbabwean agricultural sector.The mixed methodology was used in this research involving the collection of qualitative data through interviews and this was also supported by documentation and literature from the Internet.50 farmers from A2 model farms in the five agro-ecological regions were interviewed online due to the Covid- 19 restrictions. The data was collected about how trust influences the adoption of IoT developed countries. Farmers who had access to the Internet and Social media platforms were identified through purposive sampling. The three constructs of[19] model was used as guidance for this research. Data was systematical analyzedand factors that influence trust in the adoption of IoT in Zimbabwean agriculture were identified.

.

4. FINDINGS

From the interviews held online, farmers expressed different views on trust in the adoption of IoT in agriculture.The views were categorized into classes: Propensity to trust general technology, institution based trust in technology, trust specific technology and other issues raised by farmers concerning trust.

4.1. Propensity to Trust General Technology

During the interviews, some of the farmers who had adopted IoT had faith in the services provided. The farmers indicated that the services provided were reliable, consistent and functional and had back up power facilities during outages. Other farmers indicated that as long as IoT farming system is providing the expected results they have a reason to trust the technology until such a point when the system performs otherwise.

4.2. Institution Based Trust in Technology

In the situational normality beliefs farmers expected that service providers of IoT (Internet services, devices, applications and installations) During the interviews,some farmers were knowledgeable about IoT, but are still adopting the technology. The reasons that were given by the farmers for not adopting such technology were cost, lack of proper infrastructure, poor internet connectivity, and the requisite skill to adopt such systems. The farmers stated that adopting such technology using the existing mobile or fixed networks had challenges during access, uploading, and downloading dataas services were poor and not accessible in some other areas. The other alternative which is satellite services were said to be costly in Zimbabwe.

4.3. Trust Specific Technology

During the interviews, some of the farmers revealed that they had adopted IoT and the benefits were quite enormous. The farms that had adopted IoT,were able to monitor soil nutrients, moisture, water usage, temperature, humidity, light, weed, and pests. Some of the farms had sensors in their greenhouses to monitor the environmental parameters for example the sensors were able to monitor temperatures, humidity, soil nutrients, and light. In one of the farms, the farmer installed global tracking devices on some of the bull cattle. This assisted the farmer in animal management i.e. ability to locate the animals if they had been lost or stolen.

The following benefits were highlighted on the farms that were adopting IoT in Zimbabwe: enhanced decision making, savings in electricity, preservation of water, better yields, and reduced labour. The farmers indicated that they were able to monitor their fields or animals remotely and could make faster decisions especially if they had challenges on the farm. The farmers also stated that electricity was saved due to constant monitoring of the moisture content of the soil rather than physically checking the wetness of the ground. The farmers also revealed that water usage was reduced because only areas that needed to be irrigated would get the required amount of water. There was an improvement in the yields as farmers were able to monitor the growth of their plants especially the soil nutrients and other adverse weather conditions. Labour costs were also reduced as the farmers did not have to send someone to the field to physically check the temperatures, moisture, or nutritious content. This data would be remotely transmitted to the farmer.

4.4. Other Issues Raised by Farmers Concerning Trust

The majority of the farmers interviewed were not aware of the IoT technology and its benefits and it was their first time to be introduced to such technology. Some of the farmers who did not know about the existence of such technology revealed that they were eager to embrace this innovative technology. But, some of the farmers, although made aware of IoT in agriculture through this interview said they would not adopt such technology due to the perceived security threats and risks.

The security issues raised by the farmers includes: confidentiality, privacy, authenticity, availability of the services, integrity and non-repudiation as major concerns. The farmers felt that data transmitted or received through the Internet may be subjected to attacks such as Denial of Service (DoS) attacks, malicious code attacks and sniffing attacks. Because of these security concerns the farmers had distrust in the adoption of IoT in agricultural activities.

5. DISCUSSION AND ANALYSIS

Trust plays a significant role in the adoption of IoT in Zimbabwe. Many benefits come with the adoption of IoT by Zimbabwean farmers such as remote monitoring of farming activities and enhancing the decision-making process. Although the benefits of IoT in agriculture are enormous, some farmers were concerned about security issues in the adoption of such systems as the risks perceived from the threats of their data transmitted over the Internet outweighs the benefits of adopting such systems.The security concerns can lead to data loss, link failures or even loss of login credentials such as passwords as shown in Table 2.

Table 2: Security threat in IoT for smart farming [20]

Layer	Security threat	Smart farming effects	Solution
Application	Data thefts Access Control Attacks Service Interruption Attacks Malicious Code Injection Attacks Sniffing Attacks Reprogram Attacks	The top of the stack in the already mentioned IoT layer architecture. Possible effects or problems could be considered the lack of delivery of services between the respective users from various domains such as farmers, retailers and/or other stakeholders. Accessibility problems for the involved users and lack of security and privacy are also major issues.	[21][23][20][16][39]
Middleware		This layer operates in two way mode. More specifically, this layer stands between (in the middle) of the application and the hardware layer and also acts as an interface between them. Major problems that come as a result of attacks on this layer can affect data and/or device (nodes installed into the agriculture infrastructure and other types of issues such as device information discovery, access control by users and data analysis as well.	[21][23][16][11]
Internet		The most crucial layer concerning the establishment of the communication between the distinct endpoints such as device to device, device to cloud, device-to-gateway, and back-end data sharing. In case of failure the communication is being disrupted and the IoT system is practically out of service. Improper communication service services and/or and lack of automatic updates could lead to privacy concerns among the user' private information (e.g. access credentials).	[21][23][16][40]
Access gateway		Access Gateway layer contributes to the handling of the very fast data as well as to bridging the gap between the client (farmers, stakeholders, retailers) and the end point (node or device). Message routing, identification and subscribing problems between the IoT system nodes could be possible outcomes to the client	[21][23][16][39][41]

		side concerning the final form of the received message. This message may also include the desired information as well as transport encryption/integrity verification, so sensitive data could easily then be intercepted.	
Edge Technology		This layer is consisted of majority of hardware parts (e.g. sensors, Radio-Frequency Identification (RFID) tags) and have a significant role for the communication between the involved devices as well as the data collection within the network and the servers that are installed for the IoT farming system. Possible attacks on the entities of this layer could lead to important problems of monitoring or sensing various phenomena. Additionally, information thefts and or tampering could also be possible results.	[21][23][16][39][11]

Farmers should not doubt about who they share the IoT data/information with on the Internet. To win trust on the adoption of IoT in agricultural activities service providers (Internet, device, application, cloud service)have to ensure that the data/information that they provide to farmers is shared ina transparency manner. The service providers should also enable farmers to analyze and act on data in real-time without too much interference.

Data confidentiality/loss prevention plays a critical role in the building of trust in the adoption of IoT by farmers. The critical information collected through the interconnected IoT platform should be encrypted at the transport layer and at the rest state using strong encryption, data integrity checksums, and data loss prevention mechanism. This will help ensure the confidentiality and completeness of the sensitive datathereby increasing the trust belief.

Some of the farmers who were computer illiterate may fail to trust the system as they feel that the system is not user friendly. This can be exacerbated by complex user interfaces which some of the framers are not able to understand especially the elderly. Some IoT devices lack application and/or human user interfaces for device management, leading to inability to acquaint concerned individuals to provide meaningful consent for processing their Personal Identification (PI). This situation is worsened due to lack of universally accepted standards for IoT APIs, thus fostering interoperability among IoT devices.

By using smart agriculture technology, Zimbabwean farmers will gain better control of farmingactivitiessuch as the rearing of livestock and growing crops, bringing about massive efficiencies of scale, cutting costs, and helping save scarce resources such as water.As Zimbabwe is often affected by droughts, IoT will allow the country to preserve water. With the adoption of IoT, Zimbabwe will be able to provide smart solutions in agriculture.

6. CONCLUSIONS

Trust is an important aspect in the adoption of IoT in agriculture in developing countries. The use of IoT has immense benefits to Zimbabwean food security as farmers will be able to make faster decisions thereby boosting agricultural productivity. IoT will enable framers to monitor soil nutrients, environmental parameters, water usage andenabling farmers to be well informed about agricultural activities in their fields regardless of geographic area.

However, it is important to note that some of the farmers concerns on security such as the use of the Internet of Things and what the technology is expected to transmit and receive should be adequately addressed. It is recommended for further research on security of IoT in agriculture.

7. ACKNOWLEDGEMENTS

This paper was inspired by the research that has beendone about IoT in the Zimbabwean agriculture sector.

REFERENCES

[1] T. Zengeya, P. Sambo, and N. Mabika, "The Adoption of the Internet of Things for SMART Agriculture in Zimbabwe," in 5th Conference on Networks and Communications (NET 2021), 2021, pp. 99–106.
[2] FAO, Fertilizer use by crop in Zimbabwe. 2004.
[3] N. Khan, R. L. Ray, G. R. Sargani, M. Ihtisham, M. Khayyam, and S. Ismail, "Current progress and future prospects of agriculture technology: Gateway to sustainable agriculture," MDPI, vol. 13, no. 9, pp. 1–31, 2021.
[4] V. Saiz-Rubio and F. Rovira-Más, "From smart farming towards agriculture 5.0: A review on crop data management," MDPI, vol. 10, no. 2, 2020.
[5] J. E. Sierra, B. Medina, and J. C. Vesga, "Management system in intelligent agriculture based on Internet of Things," Espacios, vol. 39, no. 8, 2018.
[6] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: A review," MDPI, vol. 17, no. 8, 2017.
[7] FAO, "Agriculture 4.0: Start Agricultural robotics and automated equipment for sustainable crop production," 2020.
[8] Hello Tractor, "Hello Tractor, Break Ground, Drive Change."
[9] R. Giacomo and G. David, E-Argriculture in action: Drones for agriculture. 2018.
[10] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. H. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," IEEE Access, vol. 7, pp. 129551–129583, 2019.
[11] R. A. Acharige, M. N. Halgamuge, H. A. H. S. Wirasagoda, and A. Syed, "Adoption of the Internet of Things (IoT) in Agriculture and Smart Farming towards Urban Greening : A Review," Int. J. Adv. Comput. Sci. Appl., no. April, pp. 10–28, 2019.
[12] K. Benke and B. Tomkins, "Future food-production systems: vertical farming and controlled-environment agriculture," Sustain. Sci. Pract. Policy, vol. 13, no. 1, pp. 13–26, Jan. 2017.
[13] N. Khan, R. L. Ray, G. R. Sargani, M. Ihtisham, M. Khayyam, and S. Ismail, "Current progress and future prospects of agriculture technology: Gateway to sustainable agriculture," Sustain., vol. 13, no. 9, 2021.
[14] U. Acar et al., "Designing An IoT cloud solution for aquaculture," Glob. IoT Summit, GIoTS 2019 - Proc., no. June, 2019.
[15] C. Li et al., "Prospect of aquaponics for the sustainable development of food production in urban," Chem. Eng. Trans., vol. 63, no. August, pp. 475–480, 2018.
[16] G. Vitali, M. Francia, and M. Golfarelli, "Crop Management with the IoT : An Interdisciplinary Survey," MDPI, pp. 1–18, 2021.
[17] S. Nandhini, S. Bhrathi, D. D. Goud, and K. P. Krishna, "Smart Agriculture IOT with Cloud Computing, Fog Computing and Edge Computing," Int. J. Eng. Adv. Technol., vol. 9, no. 2, pp. 3578–3582, 2019.
[18] H. McKnight, M. Carter, and P. Clay, "Trust in Technology: Development of a Set of Constructs and Measures," Digit 2009 Proc. - Diffus. Interes. Gr. Inf. Technol., p. 12, 2009.
[19] D. H. Mcknight, L. L. Cummings, and N. L. Chervany, "Trust formation in new organizational relationships," Acad. Manag. Rev., vol. 23, no. 3, pp. 473–490, 1998.
[20] K. Demestichas, N. Peppes, and T. Alexakis, "Surveys on Security Threats in Agricultural IoT and Smart Farming," MDPI, vol. 20, p. 17, 2020.

[21] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," IEEE Access, vol. 8, pp. 34564–34584, 2020.
[22] P. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, "The Effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved.," IEEE Internet Things, vol. 6, pp. 1606–1616., 2019.
[23] M. A. Ferrag, L. E. I. Shu, S. Member, and X. Yang, "Security and Privacy for Green IoT-Based Agriculture : Review , Blockchain Solutions , and Challenges," IEEE Access, vol. 8, pp. 32031–32053, 2020.
[24] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," ACM Trans. Cyber-Physical Syst., vol. 1, no. 2, 2017.
[25] E. C. Ametepe, A.F.; Ahouandjinou, S.A.R.M.; Ezin, "Secure encryption by combining asymmetric and symmetric cryptographic method for data collection WSN in smart agriculture.," in In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), pp. 93–99.
[26] M. S. Mekala and P. Viswanathan, "A Survey: Smart agriculture IoT with cloud computing," in 2017 International Conference on Microelectronic Devices, Circuits and Systems, ICMDCS 2017, 2017, vol. 2017-Janua, no. August 2017, pp. 1–7.
[27] C. Kamienski et al., "Smart water management platform: IoT-based precision irrigation for agriculture," Sensors (Switzerland), vol. 19, no. 2, 2019.
[28] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture," Comput. Electron. Agric., vol. 157, no. November 2018, pp. 218–231, 2019.
[29] K. Yu, S.; Lou, W.; Ren, "Data Security in Cloud Computing," in In Handbook on Securing Cyber-Physical Critical Infrastructure Das, S.K., Kant, K., Zhang, N., M. Kaufmann:, Ed. Boston, 2012, pp. 389–410.
[30] G. Codeluppi, A. Cilfone, L. Davoli, and G. Ferrari, "LoraFarM: A LoRaWAN-based smart farming modular IoT architecture," Sensors (Switzerland), vol. 20, no. 7, 2020.
[31] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective," IEEE Sens. J., vol. 21, no. 16, pp. 17591–17607, 2021.
[32] L. Benos, A. C. Tagarakis, G. Dolias, R. Berruto, D. Kateris, and D. Bochtis, "Machine learning in agriculture: A comprehensive updated review," Sensors, vol. 21, no. 11, pp. 1–55, 2021.
[33] F. Bisogni, S. Cavallini, and S. D. I. Trocchio, "Cybersecurity at European Level: The Role of Information Availability," Commun. Strateg., vol. 1, no. 81, pp. 105–124, 2011.
[34] T. Palm, "Impact of authenticity on sense making in word problem solving," Educ. Stud. Math., vol. 67, pp. 37–58.
[35] and M. National Academies of Sciences, Engineering, "Policy and Global Affairs; Government-University-Industry Research Roundtable. Whitacre, P., Ed.;," in Authenticity, Integrity, and Security in a Digital World: Proceedings of a Workshop–In Brief, 2019.
[36] N. Bothe, A.;Bauer, J.;Aschenbruck, "RFID-assistedContinuoususerauthenticationforIoT-basedsmart farming," in In Proceedings of the 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA), pp. 505–510.
[37] W. McCullagh, A., & Caelli, "Non-repudiation in the digital environment. First Monday, 5(8)," 2000.
[38] A. M. Holkar, N. S. Holkar, and D. Nitnawwre, "Investigative analysis of repudiation attack on MANET with different routing protocols routes information to get destination that it needs to send," Int. J. Emerg. Trends Technol. Comput. Sci., vol. 2, no. 3, pp. 356–359, 2013.
[39] A. Triantafyllou, D. C. Tsouros, P. Sarigiannidis, and S. Bibi, "An architecture model for smart farming," Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019, no. May, pp. 385–392, 2019.
[40] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas," IEEE Internet Things J., vol. 5, no. 6, pp. 4890–4899, 2018.
[41] M. Ryu, J. Yun, T. Miao, I. Y. Ahn, S. C. Choi, and J. Kim, "Design and implementation of a connected farm for smart farming system," 2015 IEEE SENSORS - Proc., no. January 2018, 2015.

AUTHORS

Tsitsi Zengeya is a Computer Science lecturer at Great Zimbabwe University. She holds an Msc degree in Computer Science. Areas of research interest are: Artificial Intelligence, Data Science & Ontologies.

Dr. Paul Sambo is a lecturer at Great Zimbabwe University's Computer Science department. He has wealth of experience in the Information Communication Technology industry. He holds a PhD in Information Systems and his research areas are: Information systems, Data Communication, Artificial Intelligence and Software Engineering**.**

Nyasha Mabika is a lecturer at Great Zimbabwe University, Department of Livestock, Wildlife and Fisheries. He has vast experience in biological techniques and fishery sciences. He is a PhD holder with an interest in fish health and biomonitoring.