Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Review of the techniques and mechanisms for enhancing trust in internet of things for smart agriculture

Martin Otieno *

School of Informatics and Innovative Sciences, Jaramogi Oginga Odinga, University of Science and Technology, Kenya.

Global Journal of Engineering and Technology Advances, 2023, 15(01), 050–063

Publication history: Received on 01 March 2023; revised on 16 April 2023; accepted on 19 April 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.15.1.0070

Abstract

Smart agriculture is an emerging technology that has been developed from innovative information technologies such as AI, IoT, ML, smart vehicles in order to maximize outputs while optimizing farm inputs for better production and profit. However, these innovations have several vulnerabilities, especially, given that most of agriculture is practiced in open fields, exposed to harsh, unprotected environments. Studies have been conducted on its security issues and how to mitigate the threats from the vulnerabilities along with some studies in data privacy in smart agriculture. However, studies on trust issues of farmers on these technologies are absent. This paper looks at the security issues and how they impact on farmers' trust on these technologies. It finally offers direction on hoe to enhance their trust on the smart farming technologies.

Keywords; Trust; Smart agriculture; Threats; Vulnerabilities; Privacy

1. Introduction

Smart Agriculture (SA) is the effort to integrate IoT and AI into agricultural practices in order to enable farmers to make efficient and effective use of agricultural inputs for maximum profits [1]- [3]. SA has attracted attention from both the agriculture industry as well as the research community [4]. Agriculture is a primary industry globally, spanning over several centuries and it plays an important role in social stability and economic development [5]. With the exponential growth in global populations, the need to increase yields has motivated technological advances in agriculture. It has attracted an increasing interest of both industry and academic researchers on SA. This is due to the fact that the use of these technologies has led to rapid improvements in animal and crop production in both quantity and quality, along with efficient use of resources. These innovative technologies have also exported vulnerabilities and threats [6], [7] associated with them into farming industry. Smart agriculture provides solutions for agricultural intelligence and automation but is laden with information security issues that cannot be ignored [8]. The Internet of Things (IoT) is a universe of things that are seamlessly integrated into the networks of networks as active participants, exchanging data about themselves and their perceived surrounding environments over a web-based infrastructure [9]. The use of the Internet of Things (IoT) in agriculture helps farmers improve their productivity through better prediction, real-time monitoring, and efficient management of crops [10]-[12].

Internet of Things (IoT)-based automation [13] of agricultural events can change the agriculture sector from being static and manual to dynamic and smart, leading to enhanced production with reduced human efforts. Precision Agriculture (PA) along with Wireless Sensor Network (WSN) are the main drivers of automation in the agriculture domain [14], [15].Most of the exchanged and generated information is for and about the activities of the farmer. The agricultural IoT process information that is important for the farmers, including their private information. This information, for example, weather information should always be accurate. If there is an attack and modification, it may lead to losses.

*Corresponding author: Martin Otieno

The farmer therefore, requires to be exposed to the techniques of evaluating the trustworthiness of the smart devices such as drones. They expect to verify whether they are working correctly as designed, were correctly designed to meet his expectations and how it ensures that it remains trustworthy [16]. The vulnerabilities and threats may lead to modification of IoT design or functionality, leading to errors in the information the farmers get. This may lead to losses, thereby, necessitating mistrust in these devises [17], [18]. Many studies have focused on countermeasures to mitigate the threats to and by the IoTs to farming efficiency [19], [20], [21] and productivity but very few have focused on how to ensure trust by the farmers on these devices.

Multiple parameters are involved in plants health including water level, temperature, soil statistics, crops' nature, weather conditions, fertilizer types and water requirements. PA enables a farmer to know precisely what parameters are needed for healthy crop, where these parameters are needed and in what amount at a particular instance of time. This involves the use of sensor-based devices [22], [23], [24], [25] that monitor, record and deliver directly to the farmers' laptop or smart devices, this information. This has given rise to precision agriculture, a critical area in smart agriculture as it is one of the most important IoT applications, despite its relative rarity. As our planet is on the verge of a food crisis, these new technological innovations to increase yields could save lives. Predicting natural conditions and reacting to them as quickly as possible is essential for farming's efficiency and profitability [26]. In the past, such forecasts were less precise than they are today, thanks to real-time data availability. The end result is a new direction in farming, with this application driven by the Internet of Things, AI and other smart technologies and it's working out well, except for security challenges. The major contributions of this article are as follows:

- The benefits of Smart Agriculture are outlined
- The various information security challenges of smart agriculture are discussed
- Privacy and trust issues in smart agriculture are expounded in detail
- Some research contributions towards IoT smart agriculture are highlighted

The rest of this article is structured as follows: Section 2 discussed the various benefits of smart agriculture, while Section 3 describes the information security challenges of smart agriculture. However, Section 4 explains some of the privacy and trust issues in smart agriculture, while Section 5 discusses research contributions towards IoT smart agriculture. Towards the end, Section 6 gives the recommendations while Section 7 concludes the paper.

2. Benefits of Smart Agriculture

Smart agriculture involves the use of innovative information technologies such as Internet of Things (IoT), drones, robotics and Artificial Intelligence (AI) in the control and management of farms in order to improve productivity and yield while reducing input, land, and labor requirements [27]-[29]. It seeks to promote efficiency [30] in agricultural production. Like other economic sectors, the rapid development of information technologies has significantly transformed agricultural sector, from initial land preparation to safe and efficient delivery of produce to the market, including many applications for its traceability back to the farm.

The world depends on agriculture as a critical source of food and by 2050, the number of humans is expected to increase by over two billion that requires more food. As explained in [19] reports that the agriculture sector in Malaysia also has been providing a source of food for Malaysian consumption but has been affected by climate change that always have harmful effects on the agriculture sector. Coupled with the challenges, such as doubling food supplies for future consumption, the world agriculture must use agricultural resources in a more accurate and precise method or optimum resource utilization to ensure sustainable food production [21]. This called for smart farming technologies that will bring this vital sector to a higher level of agricultural productivity and profitability. Smart agriculture has integrated information and technologies in communication into sensors and farm equipment [31]-[34]. The agricultural industry has entered a new age when fast and complex decision-making becomes the key to success. Technological developments such as big data [35], IoT, artificial intelligence [36], neural networks, cloud computing, etc., equip farmers with tools and expertise to improve decision-making during their particular phases of production and yielding [22], [37]. The existing facts such as population expansion, climate change, and workforce scarcity have led to developing intelligent farming systems from planting and watering to crop health care and harvests [38]. Environmental and remote automation and surveillance using IoT are expanding fast in agriculture to produce more competent and effective agricultural tools and services [39]-[41]. Smart farming can supply farmers with valuable environmental information obtained from wireless IoT sensors [42] in the growing fields to increase competition and profitability [43].

The smart farming system or infrastructure integrates plant disease diagnosis, fertility ratio analysis, crop monitoring, soil profile monitoring, water spreading, field surveillance, and water stress analysis [44], [45]. Disease diagnosis and crop monitoring can be improved through video and image classification. Water spreading and field monitoring are employed using wireless devices such as drones and UAVs [46]. Soil profile monitoring can be done by collecting the soil profile using sensors. The water stress analysis manages the availability and distribution of the smart farming system. Finally, the fertility rate analysis can aid in effective decision-making in production planning and marketing [38].

3. Information Security Challenges of Smart Agriculture

The researchers in [47] state that while most technologies follow a logistic-growth process, the security development over the lifetime of computer-science technologies [48], surges at a late stage or no relation exists between the technological change and the security development or there exists an inverse relation between security attention and experts' opinion. In development of smart agriculture technologies, where, existing innovative technologies have been modeled to help improve agriculture, security could have been ignored. Authors in [49] observes that smart agriculture is still an emerging technology and therefore, its level of security is still low. On the other hand, the researchers in [50] and [51] state that while smart farming, SF and precision agriculture, PA aim to help farmers use inputs (such as fertilizers and pesticides) more efficiently [52] through using Internet of Things (IoT) devices, they create new security threats that can defeat this purpose in the absence of adequate awareness and proper countermeasures. The researchers in [53] and [54] note that the wide use of data collection and communication technologies has increased concerns about the privacy of farmers and their data. Although some previous studies have reviewed the security aspects of smart farming, the privacy challenges and solutions are not sufficiently explored in the literature. Several other studies have been conducted in data security and privacy in smart agriculture. For example, the researchers in [51] reviewed security and privacy issues and challenges in IoT-based agriculture, while the authors in [4] and [55] discussed the security issues in the smart farming cyber-physical environment. These studies tend to focus on security threats and solutions [56] with a few on privacy such as [4]. The researchers in [57] conducted an extensive literature review on the use of ICT in agriculture, as well as on the associated emerging threats and vulnerabilities. The authors in [22], [58], [59] and [60] report that many aspects of industrial agriculture have not yet fully adapted to the digital world as is evident in the many vulnerabilities [61] currently present within agricultural systems as well as the lack of or the fragmented nature of policy dictating both cyber security and bio-security. These looming oversights create dangers to advanced agricultural systems, which in turn poses risk to businesses, economies, and individuals.

Previous studies have found out that in the heavily mechanized landscape of agriculture, smart technologies and remote administration used in smart farming are quite unfamiliar for its stakeholders with most of the new threats in this specific domain being strongly connected with similar threats that exist in cyber security in other industries [62] and are most frequently related to, data integrity and availability [63], [64], [65], [66], [67]. Since, smart farming involves heavy agricultural machineries getting connected online, there are many emerging vulnerabilities that can potentially lead to disastrous consequences. Agricultural sector, being mostly, an open-field sector is directly influenced by harsh environmental conditions, such as high temperatures, humidity, rain winds and other phenomena to which, electromechanical equipments are susceptible to. These electro-mechanical equipments mostly use sensors to monitor soil, crop and animal environments and are susceptible to malfunction, making it possible to provide false measurements and commands which may lead to severe consequences in agricultural production [68], [69], [70], [71]. In addition to monitoring and controlling sensors, the wireless networks [72], [73] used in the agricultural sector are mainly low power such as LoRaWAN, Zigbee and are affected by the harsh environmental conditions such as temperature, humidity, obstacles and human presence that can lead to communication and data loss [74], [75]. As these devices operate in external environments, the sensors [76] and network devices in many cases are physically accessible, creating a major risk as anyone with malicious intentions can access them either to damage or compromise them in order to make them malfunction [77].

4. Privacy and trust issues in smart agriculture

The key information security principles of confidentiality, integrity and availability along with authentication, accountability and non-repudiation face enormous challenges in the open, insecure environments of smart agriculture [78], [79], [80],[81]. Weather vagaries and even unauthorized, malicious individuals can access the devices and manipulate them, either in the way they work or data they carry leading to losses. Extreme weather can change their working or even cause them to crash [82], [83], [84], [85], [86]. Since they transmit data online, they can suffer man-in-the-middle attacks [87]. Another issue when the data collected from IoT sensors and other machinery is transferred online is data privacy and ownership [88] and [89], as farmers can suffer financial and personal damage due to data breach. The threats to confidentiality are threats to privacy and trust and as such, have a heavy impact on farmers' trust and reliance on smart agricultural technologies. Threats such as the ones identified in [90] include intentional data theft through smart applications and platforms, internal data thefts, illegal sale of data generated from the smart devices and use of foreign equipment such as drones, sensors cameras to access to sensitive and confidential farmer's data [91], [92], [93] have a negative impact on farmers' trust in the technologies. Since smart agricultural technologies mainly focus on automated data collection, analysis and decision-making, it is important to ensure the integrity and availability of data [94], [95], [96], [97], [98], [99], [100], [101].

Any data breach affects the decisions made by artificial intelligence algorithms and have negative impacts on production [102], [103. It could also endanger the eventual consumers of the agricultural products and lead to litigation issues. All these may impact negatively on the trust of farmers on smart agriculture. Trust is enhanced when a smart device works as it was designed to and enables the user to attain his objective. Trust in technology is defined as a willingness to depend on the specific technology in a given situation in which negative consequences are possible [104]. For farmers to adapt to IoT smart farming, they need to trust and believe that the technology is performing to the expected standards, considering that the data/information collected will be critical for decision making. The smart agricultural devices transmit data to mobile phones before it is consumed. They are therefore, expected to collect the data efficiently and automatically in the challenging context of the network connectivity and architecture. The researchers in [105] reports that IoT technologies and applications are intimately associated with people; hence, trust is the major issue. With many research studies such as the research conducted in [106], reporting that more than 70% of the existing IoT systems have severe vulnerabilities due to insecure Web interfaces, lack of encryption for transport, insufficient authorization, and inadequate software protection [107], trust issues arise leading to reluctance by consumers to adopt IoTs and smart agriculture [108], [109], [110], [111], [112], [113], [114].

Users' lack of trust may not just be as a result of lack of understanding of how the device security mechanisms work [115]. The users are more concerned with the privacy of their personal data and how it moves securely in-between these devices [116], [117], [118], [119]. They are more concerned with the safety, usefulness, convenience, efficiency and reliability of the smart devices and most importantly, privacy [120], [121], [122], [123], [124], [125], [126], [127], [128]. All these factors need to be verified by the users themselves, in a simple and efficient way on their own contexts.

5. Research contributions towards IoT smart agriculture

We look at various studies that have attempted to address smart agriculture information security issues and how to mitigate them. We look at the security aspects that they focused on. From Table 1 below, it is evident that most of the research work did not focus on trust, a very key security aspect for implementation of smart agriculture. The few that focus on enhancing trust look at its solutions from the design and functionality perspective, not from developing solutions based on user perspectives. They offer trust management techniques that are widely used to identify untrusted behavior and isolate untrusted objects [129], [130], [131], [132]. However as [115] point out, these techniques still have many limitations like ineffectiveness when dealing with a large amount of data and continuously changing behaviors. Table 1 shows some of the previous works that have been carried out in IoT smart agriculture security.

Table 1 Various research contributions towards IoT smart agriculture

Author	**Contribution**	**Security aspect addressed**
Yazdinejad et al [4]	Categorized the security threats within the SF/PA areas and provided a taxonomy of these threats [133] for SF environments in order to detect the behavior of APT attacks in SF and PA environments.	Threats
Kumar et al. [134]	Proposed a deep privacy-encoding-based FL (PEFL) framework for SA is proposed to achieve the target of data security and privacy.	Deep learning (DL)
Souvik et al. [135]	Designed an Information-Centric IoT-based Smart Farming with Dynamic Data Optimization (ICISF-DDO), that enhances the performance of the smart farming infrastructure with low energy consumption and Improved lifetime.	IoT
Amiri-Zarandi et al. [57].	Presents a holistic review of big data privacy in smart farming using a data lifecycle schema and describes privacy concerns and requirements in smart farming in each of the phases of this lifecycle. They also review the existing solutions and technologies that enhance data privacy in smart farming.	Big data, privacy.

Shadrin et al. [136]	presented an embedded system enriched with the AI for prediction of the growth dynamics of plant leaves, grounded on a low-power embedded sensing system running the neural network-based AI and the long short-term memory network (LSTM) as its core.	AI
Shafi et al. [14]	Demonstrated how wireless sensor network (WSN)-based PA system can be implemented. Further proposed an IoT-based smart solution for crop health monitoring, which is comprised of two modules; a WSN -based system to monitor real-time crop health status and a low altitude remote sensing platform to obtain multi-spectral imagery for crop-health classification.	WSN
Gupta et al. [137]	Provided a multi layered architecture relevant to the precision agriculture domain and discussed the security and privacy issues [138] in this dynamic and distributed cyber physical environment.	Security/Privacy Issues
Torky et al. [139]	Reviewed the types of cyber attacks that can violate the security aspects of SF and PA and presented taxonomy on cyber-threats to SF and PA on the basis of their relations to different stages of Cyber-Kill Chain (CKC) along with their related risk mitigation strategies.	Threats, CKC
Zanella et al. [54]	Reviewed the state of the art smart agriculture security, particularly, in the open field agriculture, its architecture, security issues, challenges and future directions.	SA security architecture, Threats
Al-Fuqaha et al. [140]	Provided an overview of the Internet of Things (IoT) enabling technologies, protocols and application issues along with their key challenges presented in the recent literature and their relation with other emerging technologies.	IoT
Aldhyani et al. [88]	Applied deep learning models, namely long short-term memory and a convolutional neural network combined with long short-term memory (CNN–LSTM), for detecting various types of attacks that threaten Agriculture 4.0	DL, CNN-LSTM.
Stephen et al. [62]	Explored vulnerabilities within the system of advanced agriculture, potential solutions to the risks presented and the future advanced agricultural system that implements CyberBioSecurity.	Threats
Demestichas et al. [22]	Conducts an extensive literature review on the use of ICT in agriculture, the associated emerging threats and vulnerabilities and highlight the mitigation measures.	
Awan et al. [90]	Proposed a novel trust management mechanism to identify malicious and compromised nodes by utilizing trust parameters.	Trust, privacy
Jayashankar et al. [92]	Provide a unique conceptualization of perceived value but also pave the way for a richer conceptualization of IoT core functions that enable farmers to fulfil green and epistemic goals.	Trust, perceived values.
AlHogail [141]	Revealed that McKnight et.al. 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.	Trust, reliability.
Jakku et al. [94]	Explored the socio-technical factors and conditions that influence the development of Smart Farming and Big Data applications, using a multi-level perspective on transitions combined with social practice theory.	Trust, transparency
Sharma et al. [95]	Identified the need and impact of trust determination using the trust model algorithm.	Trust, trust model algorithm.
Ahmed et al. [97]	Presented an overview of technologies in the domains of IoT, Climate-Smart Agriculture (CSA), AI, Machine Learning (ML) and blockchain. They also presented approaches for integrating IoT with CSA data analysis.	IoTs and blockchain technology.
Aldowah et al. [105]	Provided an insight on the challenges of trust in IoT, and recommended solutions from academic, technical and industry aspects.	Trust issues

Vangala et al. [142]	Reviewed smart agriculture security, particularly in open-field agriculture, its architecture, security issues, challenges [143] and future directions.	Security issues
Alghofaili et al. [115]	Propose a model for a trust management model for IoT devices and services that takes leverage from multi-criteria decision-making and deep learning techniques.	Trust management in IoTs

6. Recommendations

The researchers in [115] and [144] offer a trust management solution for IoTs and smart devices based on the simple multi-attribute rating technique (SMART) and long short-term memory (LSTM) algorithm. However, like the other models, it is focused on the developer perspective. This study recommends a solution that can be used by the farmers to evaluate the efficiency and effectiveness of the smart devices without relying on the outputs to determine whether they are working well or not. This should be a form of federated, user-evaluation mechanism, such as recommended in [145], [146], [147] based on the IoTs and whose results are transmitted to the central evaluation server for verification. They propose, for example, in [147] that due to rising privacy concerns [148], federated learning is used to train wearable data with privacy preservation collaboratively. However, under these state-of-the-art (SOTA) schemes suffer fundamental limitations such as users lack convenient channels for providing feedback on wearable devices [147], [149]. The feedback needs to come from the user evaluation schemes on their devices. This should enable them to evaluate if, for example, drones monitoring the farm activities have not deviated from doing what they are supposed to do.

The fear of loss of investment coupled with the expensive implementation of smart agriculture should not be shrouded in any form of uncertainty for the farmer. Loss of market as a result of the produce tracking device erratically giving wrong information to the customer with irreparable damage leads to mistrust in smart farming. As explained in [150]-[152], Federated Learning (FL) is a new machine learning paradigm enhancing the use of local devices, where, at the server level, it aggregates models learned locally on distributed clients to obtain a more general model, ensuring that no private data is sent over the network [153], [154], [155], [156], [157], [158], [159]. This reduces the worry of loss of privacy to users. Such an evaluation technique based on the federation framework enables evaluation strategies for personalization of global models [160], [161][162]. When used by farmers, with their own data as training data locally, and the only transmitted data to external server is the evaluation feedback, then , trust and confidence in the devices will be enhanced [163], [164], [165], [166], [167], [168], [169], [170]. The farmer’s personal data does not leave his own smart-phone or laptop before, during and even after the entire communication process.

7. Conclusion

For people to benefit from smart innovations, it is of utmost importance that the providers are trustworthy. However, observes that their reputation is at an all-time low as incidents such as Cambridge Analytica incident, apps leaking data, discriminating facial recognition applications exposes their untrustworthyness. However, how to measure of trustworthiness remains unclear from the users perspective and therefore, more research needs to be undertaken and mechanisms developed to mitigate this. This is for the reason that grayness in this aspect will continue to pose a threat to people’s personal well-being that is intrinsically intertwined with these technologies. The study proposes that the trust management solutions offered by and others, bundled with federated learning and feedback mechanisms from farmer perspective would assure them of trustworthiness of the smart devices in smart agriculture.

Compliance with ethical standards

Acknowledgments

I would like to thank everyone who provided support during the development of this paper.

References

[1] Kong JL, Fan XM, Jin XB, Su TL, Bai YT, Ma HJ, Zuo M. BMAE-Net: A data-driven weather prediction network for smart agriculture. Agronomy. 2023 Feb 22, 13(3):625.

[2] Roussaki I, Doolin K, Skarmeta A, Routis G, Lopez-Morales JA, Claffey E, Mora M, Martinez JA. Building an interoperable space for smart agriculture. Digital Communications and Networks. 2023 Feb 1, 9(1):183-93.

[3] Li D, Nanseki T, Chomei Y, Kuang J. A review of smart agriculture and production practices in Japanese large-scale rice farming. Journal of the Science of Food and Agriculture. 2023 Mar 15, 103(4):1609-20.

[4] Yazdinejad A, Zolfaghari B, Azmoodeh A, Dehghantanha A, Karimipour H, Fraser E, Green AG, Russell C, Duncan E. A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. Applied Sciences. 2021 Aug 16, 11(16):7518.

[5] Ma L, Long H, Zhang Y, Tu S, Ge D, Tu X. Agricultural labor changes and agricultural economic development in China and their implications for rural vitalization. Journal of Geographical Sciences. 2019 Feb, 29:163-79.

[6] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[7] Süren E, Heiding F, Olegård J, Lagerström R. PatrIoT: practical and agile threat research for IoT. International Journal of Information Security. 2023 Feb, 22(1):213-33.

[8] Yang X, Shu L, Chen J, Ferrag MA, Wu J, Nurellari E, Huang K. A survey on smart agriculture: Development modes, technologies, and security and privacy challenges. IEEE/CAA Journal of Automatica Sinica. 2021, 8(2):273-302.

[9] Prasad R, Rohokale V. Cyber security: the lifeline of information and communication technology. Cham, Switzerland: Springer International Publishing, 2020.

[10] Diya VA, Nandan P, Dhote RR. IoT-based Precision Agriculture: A Review. Proceedings of Emerging Trends and Technologies on Intelligent Systems: ETTIS 2022. 2022 Nov 16:373-86.

[11] Fan J, Li Y, Yu S, Gou W, Guo X, Zhao C. Application of Internet of Things to Agriculture—The LQ-FieldPheno Platform: A High-Throughput Platform for Obtaining Crop Phenotypes in Field. Research. 2023 Mar 20, 6:0059.

[12] Adeleke I, Nwulu N, Adebo OA. Internet of Things (IoT) in the food fermentation process: A bibliometric review. Journal of Food Process Engineering. 2023:e14321.

[13] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[14] Shafi U, Mumtaz R, García-Nieto J, Hassan SA, Zaidi SA, Iqbal N. Precision agriculture techniques and practices: From considerations to applications. Sensors. 2019 Sep 2, 19(17):3796.

[15] Gobezie TB, Biswas A. The need for streamlining precision agriculture data in Africa. Precision Agriculture. 2023 Feb, 24(1):375-83.

[16] Din IU, Guizani M, Kim BS, Hassan S, Khan MK. Trust management techniques for the Internet of Things: A survey. IEEE Access. 2018 Nov 11, 7:29763-87.

[17] El-Ghamry A, Darwish A, Hassanien AE. An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things. 2023 Jul 1, 22:100709.

[18] Lopez ID, Grass JF, Figueroa A, Corrales JC. A proposal for a multi-domain data fusion strategy in a climate-smart agriculture context. International Transactions in Operational Research. 2023 Jul, 30(4):2049-70.

[19] Virk AL, Noor MA, Fiaz S, Hussain S, Hussain HA, Rehman M, Ahsan M, Ma W. Smart farming: an overview. Smart village technology: concepts and developments. 2020:191-201.

[20] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[21] Wheeler T, Von Braun J. Climate change impacts on global food security. Science. 2013 Aug 2, 341(6145):508-13.

[22] Demestichas K, Peppes N, Alexakis T. Survey on security threats in agricultural IoT and smart farming. Sensors. 2020 Nov 12, 20(22):6458.

[23] Yin A, Wang J, Hu S, Sun M, Sun B, Dong M, Zhang T, Feng Z, Zhang H, Shi B, Zhang C. High performance waterproof-breathable fully flexible tactile sensor based on piezotronics coupled OFET. Nano Energy. 2023 Feb 1, 106:108034.

[24] Qin Z, Chen X, Lv Y, Zhao B, Fang X, Pan K. Wearable and high-performance piezoresistive sensor based on nanofiber/sodium alginate synergistically enhanced MXene composite aerogel. Chemical Engineering Journal. 2023 Jan 1, 451:138586.

[25] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[26] Rasel HM, Al Mamun MA, Hasnat A, Alam S, Hossain I, Mondal RK, Good RZ, Alsukaibi AK, Awual MR. Sustainable futures in agricultural heritage: Geospatial exploration and predicting groundwater-level variations in Barind tract of Bangladesh. Science of The Total Environment. 2023 Mar 20, 865:161297.

[27] Javaid M, Haleem A, Khan IH, Suman R. Understanding the potential applications of Artificial Intelligence in Agriculture Sector. Advanced Agrochem. 2023 Mar 1, 2(1):15-30.

[28] Al-Sharafi MA, Al-Emran M, Arpaci I, Iahad NA, AlQudah AA, Iranmanesh M, Al-Qaysi N. Generation Z use of artificial intelligence products and its impact on environmental sustainability: A cross-cultural comparison. Computers in Human Behavior. 2023 Jun 1, 143:107708.

[29] Farrar NO, Ali MH, Dasgupta D. Artificial intelligence and machine learning in grid connected wind turbine control systems: A comprehensive review. Energies. 2023 Feb 3, 16(3):1530.

[30] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17.

[31] Himesh S, Rao EP, Gouda KC, Ramesh KV, Rakesh V, Mohapatra GN, Rao BK, Sahoo SK, Ajilesh P. Digital revolution and Big Data: a new revolution in agriculture. CABI Reviews. 2018 Aug 22(2018):1-7.

[32] Fountas S, Sorensen CG, Tsiropoulos Z, Cavalaris C, Liakos V, Gemtos T. Farm machinery management information system. Computers and electronics in agriculture. 2015 Jan 1, 110:131-8.

[33] Vuran MC, Salam A, Wong R, Irmak S. Internet of underground things: Sensing and communications on the field for precision agriculture. In2018 IEEE 4th World Forum on Internet of Things (WF-IoT) 2018 Feb 5 (pp. 586-591). IEEE.

[34] Nayyar A, Puri V. Smart farming: IoT based smart sensors agriculture stick for live temperature and moisture monitoring using Arduino, cloud computing & solar technology. InProc. of The International Conference on Communication and Computing Systems (ICCCS-2016) 2016 Sep (pp. 9781315364094-121).

[35] Tzounis A, Katsoulas N, Bartzanas T, Kittas C. Internet of Things in agriculture, recent advances and future challenges. Biosystems engineering. 2017 Dec 1, 164:31-48.

[36] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[37] Alfred R, Obit JH, Chin CP, Haviluddin H, Lim Y. Towards paddy rice smart farming: A review on big data, machine learning, and rice production tasks. IEEE Access. 2021 Mar 29, 9:50358-80.

[38] Malik AW, Rahman AU, Qayyum T, Ravana SD. Leveraging fog computing for sustainable smart farming using distributed simulation. IEEE Internet of Things Journal. 2020 Jan 17, 7(4):3300-9.

[39] Adhitya Y, Prakosa SW, Köppen M, Leu JS. Feature extraction for cocoa bean digital image classification prediction for smart farming application. Agronomy. 2020 Oct 25, 10(11):1642.

[40] Talaviya T, Shah D, Patel N, Yagnik H, Shah M. Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides. Artificial Intelligence in Agriculture. 2020 Jan 1, 4:58-73.

[41] Jha K, Doshi A, Patel P, Shah M. A comprehensive review on automation in agriculture using artificial intelligence. Artificial Intelligence in Agriculture. 2019 Jun 1, 2:1-2.

[42] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[43] Khan A, Ilyas T, Umraiz M, Mannan ZI, Kim H. Ced-net: crops and weeds segmentation for smart farming using a small cascaded encoder-decoder architecture. Electronics. 2020 Oct 1, 9(10):1602.

[44] Islam N, Rashid MM, Pasandideh F, Ray B, Moore S, Kadel R. A review of applications and communication technologies for internet of things (Iot) and unmanned aerial vehicle (uav) based sustainable smart farming. Sustainability. 2021 Feb 8, 13(4):1821.

[45] Skotadis E, Kanaris A, Aslanidis E, Michalis P, Kalatzis N, Chatzipapadopoulos F, Marianos N, Tsoukalas D. A sensing approach for automated and real-time pesticide detection in the scope of smart-farming. Computers and Electronics in Agriculture. 2020 Nov 1, 178:105759.

[46] Shamrat FM, Asaduzzaman M, Ghosh P, Sultan MD, Tasnim Z. A web based application for agriculture:"Smart Farming System. International Journal of Emerging Trends in Engineering Research. 2020 Jun, 8(06).

[47] Rehman A, Liu J, Keqiu L, Mateen A, Yasin MQ. Machine learning prediction analysis using IoT for smart farming. Int J. 2020 Sep, 8(9).

[48] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[49] Lieder S, Schröter-Schlaack C. Smart farming technologies in arable farming: towards a holistic assessment of opportunities and risks. Sustainability. 2021 Jun 15, 13(12):6783.

[50] Duangsuwan S, Teekapakvisit C, Maw MM. Development of soil moisture monitoring by using IoT and UAV-SC for smart farming application. Advances in Science, Technology and Engineering Systems Journal. 2020 Jul, 5(4):381-7.

[51] Zamri NN, Mustaffha S. Exposure of Smart Farming Implementation Towards Farmers in Alor Setar: A Case Study. InIOP Conference Series: Earth and Environmental Science 2022 Jul 1 (Vol. 1059, No. 1, p. 012069). IOP Publishing.

[52] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[53] David DP, Maréchal L, Lacube W, Gillard S, Tsesmelis M, Maillart T, Mermoud A. Measuring security development in information technologies: A scientometric framework using arXiv e-prints. Technological Forecasting and Social Change. 2023 Mar 1, 188:122316.

[54] de Araujo Zanella AR, da Silva E, Albini LC. Security challenges to smart agriculture: Current state, key issues, and future directions. Array. 2020 Dec 1, 8:100048.

[55] Bughin J, Hazan E, Ramaswamy S, Chui M, Allas T, Dahlstrom P, Henke N, Trench M. Artificial intelligence: The next digital frontier?.

[56] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[57] Amiri-Zarandi M, Dara RA, Duncan E, Fraser ED. Big data privacy in smart farming: a review. Sustainability. 2022 Jul 25, 14(15):9120.

[58] Misra NN, Dixit Y, Al-Mallahi A, Bhullar MS, Upadhyay R, Martynenko A. IoT, big data, and artificial intelligence in agriculture and food industry. IEEE Internet of things Journal. 2020 May 29, 9(9):6305-24.

[59] Barreto L, Amaral A. Smart farming: Cyber security challenges. In2018 International Conference on Intelligent Systems (IS) 2018 Sep 25 (pp. 870-876). IEEE.

[60] El Arass M, Souissi N. Data lifecycle: From big data to smartdata. In2018 IEEE 5th international congress on information science and technology (CiSt) 2018 Oct 21 (pp. 80-87). IEEE.

[61] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[62] Stephen S, Alexander K, Potter L, Palmer XL. Implications of Cyberbiosecurity in Advanced Agriculture. InInternational Conference on Cyber Warfare and Security 2023 Feb 28 (Vol. 18, No. 1, pp. 387-393).

[63] Murch RS, So WK, Buchholz WG, Raman S, Peccoud J. Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology. 2018:39.

[64] Duncan SE, Zhang B, Thomason W, Ellis M, Meng N, Stamper M, Carneiro R, Drape T. Securing Data in Life Sciences—A Plant Food (Edamame) Systems Case Study. Frontiers in Sustainability. 2020 Dec 14, 1:10.

[65] Mohammadi M, Kavousi-Fard A, Dehghani M, Karimi M, Loia V, Haes Alhelou H, Siano P. Reinforcing data integrity in renewable hybrid AC-DC microgrids from social-economic perspectives. ACM Transactions on Sensor Networks. 2023 Feb 4, 19(2):1-9.

[66] Luo Y, Liu Y, Yang W, Zhou J, Lv T. Distributed filtering algorithm based on local outlier factor under data integrity attacks. Journal of the Franklin Institute. 2023 Jan 10.

[67] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[68] Mohammadpourfazeli S, Arash S, Ansari A, Yang S, Mallick K, Bagherzadeh R. Future prospects and recent developments of polyvinylidene fluoride (PVDF) piezoelectric polymer, fabrication methods, structure, and electro-mechanical properties. RSC Advances. 2023, 13(1):370-87.

[69] Neu J, Croce S, Willian T, Hubertus J, Schultes G, Seelecke S, Rizzello G. Distributed Electro-Mechanical Coupling Effects in a Dielectric Elastomer Membrane Array. Experimental Mechanics. 2023 Jan, 63(1):79-95.

[70] Giap VN, Nguyen QD, Trung NK, Huang SC. Time-varying disturbance observer based on sliding-mode observer and double phases fixed-time sliding mode control for a TS fuzzy micro-electro-mechanical system gyroscope. Journal of Vibration and Control. 2023 Apr, 29(7-8):1927-42.

[71] Campbell W, Galliou S, Tobar ME, Goryachev M. Electro-mechanical tuning of high-Q bulk acoustic phonon modes at cryogenic temperatures. Applied Physics Letters. 2023 Jan 16, 122(3):032202.

[72] Chaitra HV, Manjula G, Shabaz M, Martinez-Valencia AB, Vikhyath KB, Verma S, Arias-Gonzáles JL. Delay optimization and energy balancing algorithm for improving network lifetime in fixed wireless sensor networks. Physical Communication. 2023 Jun 1, 58:102038.

[73] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[74] Window M. Security in precision agriculture: Vulnerabilities and risks of agricultural systems. Luleå: Luleå University of Technology (Doctoral dissertation, Masters' thesis. http://ltu. diva-portal. org/smash/get/diva2: 1322203/FULLTEXT02. pdf).

[75] Champion SL, Mutschler P, Ulicny B, Reuters T, Barrett L, Bethel G, Matson M, Strang T, Ramsdell K, Koehler S. Threats to Precision Agriculture (2018 Public-Private Analytic Exchange Program report)(2020).

[76] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[77] McCartney L, Lefsrud M. Protected agriculture in extreme environments: a review of controlled environment agriculture in tropical, arid, polar, and urban locations. Applied engineering in agriculture. 2018, 34(2):455-73.

[78] Sinha BB, Dhanalakshmi R. Recent advancements and challenges of Internet of Things in smart agriculture: A survey. Future Generation Computer Systems. 2022 Jan 1, 126:169-84.

[79] Bazzana D, Foltz J, Zhang Y. Impact of climate smart agriculture on food security: an agent-based analysis. Food Policy. 2022 Aug 1, 111:102304.

[80] Akhter R, Sofi SA. Precision agriculture using IoT data analytics and machine learning. Journal of King Saud University-Computer and Information Sciences. 2022 Sep 1, 34(8):5602-18.

[81] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[82] Luomala J, Hakala I. Effects of temperature and humidity on radio signal strength in outdoor wireless sensor networks. In2015 Federated Conference on Computer Science and Information Systems (FedCSIS) 2015 Sep 13 (pp. 1247-1255). IEEE.

[83] Boano CA, Tsiftes N, Voigt T, Brown J, Roedig U. The impact of temperature on outdoor industrial sensornet applications. IEEE Transactions on Industrial Informatics. 2009 Dec 4, 6(3):451-9.

[84] Thelen J, Goense D, Langendoen K. Radio wave propagation in potato fields. In1st workshop on wireless network measurement, Riva del Garda, Italy, April 2005 2005 (pp. np-np).

[85] Lopez J, Roman R, Alcaraz C. Analysis of security threats, requirements, technologies and standards in wireless sensor networks. Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. 2009:289-338.

[86] El Bilali H, Allahyari MS. Transition towards sustainability in agriculture and food systems: Role of information and communication technologies. Information Processing in Agriculture. 2018 Dec 1, 5(4):456-64.

[87] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

[88] Aldhyani TH, Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics. 2023 Jan 3, 11(1):233.

[89] Hunt Jr ER, Daughtry CS. What good are unmanned aircraft systems for agricultural remote sensing and precision agriculture?. International journal of remote sensing. 2018 Aug 18, 39(15-16):5345-76.

[90] Awan KA, Ud Din I, Almogren A, Almajed H. AgriTrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things. Sensors. 2020 Oct 29, 20(21):6174.

[91] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[92] Jayashankar P, Nilakanta S, Johnston WJ, Gill P, Burres R. IoT adoption in agriculture: the role of trust, perceived value and risk. Journal of Business & Industrial Marketing. 2018 Sep 21.

[93] Sinha A, Shrivastava G, Kumar P. Architecting user-centric internet of things for smart agriculture. Sustainable Computing: Informatics and Systems. 2019 Sep 1, 23:88-102.

[94] Jakku E, Taylor B, Fleming A, Mason C, Fielke S, Sounness C, Thorburn P. “If they don’t tell us what they do with it, why would we trust them?” Trust, transparency and benefit-sharing in Smart Farming. NJAS-Wageningen Journal of Life Sciences. 2019 Dec 1, 90:100285.

[95] Sharma P, Shukla S, Vasudeva A. Trust-based opportunistic network offloaders for smart agriculture. International Journal of Agricultural and Environmental Information Systems (IJAEIS). 2021 Jan 1, 12(1):37-54.

[96] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[97] Ahmed RA, Hemdan EE, El-Shafai W, Ahmed ZA, El-Rabaie ES, Abd El-Samie FE. Climate-smart agriculture using intelligent techniques, blockchain and Internet of Things: Concepts, challenges, and opportunities. Transactions on Emerging Telecommunications Technologies. 2022 Nov, 33(11):e4607.

[98] West J. A prediction model framework for cyber-attacks to precision agriculture technologies. Journal of Agricultural & Food Information. 2018 Oct 2, 19(4):307-30.

[99] Candiago S, Remondino F, De Giglio M, Dubbini M, Gattelli M. Evaluating multispectral images and vegetation indices for precision farming applications from UAV images. Remote sensing. 2015 Apr 2, 7(4):4026-47.

[100] Ahmed N, De D, Hussain I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. IEEE Internet of Things Journal. 2018 Nov 4, 5(6):4890-9.

[101] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[102] Makridakis S. The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. Futures. 2017 Jun 1, 90:46-60.

[103] Ballell TR. Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review. 2019 Jun 1, 24(2):302-14.

[104] Veith B, Krummacker D, Schotten HD. The Road to Trustworthy 6G: A Survey on Trust Anchor Technologies. IEEE Open Journal of the Communications Society. 2023 Feb 13, 4:581-95.

[105] Aldowah H, Ul Rehman S, Umar I. Trust in IoT systems: a vision on the current issues, challenges, and recommended solutions. Advances on Smart and Soft Computing: Proceedings of ICACIn 2020. 2021:329-39.

[106] Aleisa N, Renaud K. Privacy of the Internet of Things: a systematic literature review (extended discussion). arXiv preprint arXiv:1611.03340. 2016 Sep 13.

[107] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[108] Rehman SU, Manickam S. Denial of service attack in IPv6 duplicate address detection process. International Journal of Advanced Computer Science and Applications. 2016, 7(6).

[109] Leister W, Schulz T. Ideas for a Trust Indicator in the Internet of Things. InThe First International Conference on Smart Systems, Devices and Technologies 2012 May. Oslo: SMART Press.

[110] Fritsch L, Groven AK, Schulz T. On the internet of things, trust is relative. InConstructing Ambient Intelligence: AmI 2011 Workshops, Amsterdam, The Netherlands, November 16-18, 2011. Revised Selected Papers 2 2012 (pp. 267-273). Springer Berlin Heidelberg.

[111] Ion M, Danzi A, Koshutanski H, Telesca L. A peer-to-peer multidimensional trust model for digital ecosystems. In2008 2nd IEEE International Conference on Digital Ecosystems and Technologies 2008 Feb 26 (pp. 461-469). IEEE.

[112] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[113] Daubert J, Wiesmaier A, Kikiras P. A view on privacy & trust in IoT. In2015 IEEE International Conference on Communication Workshop (ICCW) 2015 Jun 8 (pp. 2665-2670). IEEE.

[114] Eder T, Nachtmann D, Schreckling D. Trust and Reputation in the Internet of Things. Universit ̈at Passau, Tech. Rep. 2013 Dec.

[115] Alghofaili Y, Rassam MA. A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. Sensors. 2022 Jan 14, 22(2):634.

[116] Algarni M, Alkhelaiwi M, Karrar A. Internet of things security: A review of enabled application challenges and solutions. International Journal of Advanced Computer Science and Applications. 2021, 12(3).

[117] Zhang F, Pan Z, Lu Y. AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. Information & Management. 2023 Mar 1, 60(2):103736.

[118] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[119] Dhasarathan C, Hasan MK, Islam S, Abdullah S, Mokhtar UA, Javed AR, Goundar S. COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach. Computer Communications. 2023 Feb 1, 199:87-97.

[120] Balasamy K, Krishnaraj N, Ramprasath J, Ramprakash P. A secure framework for protecting clinical data in medical IoT environment. Smart healthcare system design: security and privacy aspects. 2022 Oct 17:203-34.

[121] Page X, Bahirat P, Safi MI, Knijnenburg BP, Wisniewski P. The internet of what? understanding differences in perceptions and adoption for the internet of things. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2018 Dec 27, 2(4):1-22.

[122] Farooq MS, Riaz S, Abid A, Abid K, Naeem MA. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. Ieee Access. 2019 Oct 25, 7:156237-71.

[123] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[124] Bhagat M, Kumar D, Kumar D. Role of Internet of Things (IoT) in smart farming: A brief survey. 2019 Devices for Integrated Circuit (DevIC). 2019 Mar 23:141-5.

[125] Mekala MS, Viswanathan P. A Survey: Smart agriculture IoT with cloud computing. In2017 international conference on microelectronic devices, circuits and systems (ICMDCS) 2017 Aug 10 (pp. 1-7). IEEE.

[126] Preethi A, Reddy PK. Survey on Smart Agriculture a Roadmap for India: Role of IoT, AI. In2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) 2022 Aug 17 (pp. 434-439). IEEE.

[127] Kalyani Y, Collier R. A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture. Sensors. 2021 Sep 3, 21(17):5922.

[128] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[129] Fotia L, Delicato F, Fortino G. Trust in edge-based internet of things architectures: state of the art and research challenges. ACM Computing Surveys. 2023 Jan 13, 55(9):1-34.

[130] Rehman A, Awan KA, Ud Din I, Almogren A, Alabdulkareem M. FogTrust: Fog-Integrated Multi-Leveled Trust Management Mechanism for Internet of Things. Technologies. 2023 Feb 7, 11(1):27.

[131] Korotkova N, Benders J, Mikalef P, Cameron D. Maneuvering between skepticism and optimism about hyped technologies: Building trust in digital twins. Information & Management. 2023 Mar 21:103787.

[132] Lyons JB, aldin Hamdan I, Vo TQ. Explanations and trust: What happens to trust when a robot partner does something unexpected?. Computers in Human Behavior. 2023 Jan 1, 138:107473.

[133] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[134] Kumar P, Gupta GP, Tripathi R. PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture. IEEE Micro. 2021 Sep 16, 42(1):33-40.

[135] Pal S, VijayKumar H, Akila D, Jhanjhi NZ, Darwish OA, Amsaad F. Information-Centric IoT-Based Smart Farming with Dynamic Data Optimization.

[136] Shadrin D, Menshchikov A, Somov A, Bornemann G, Hauslage J, Fedorov M. Enabling precision agriculture through embedded sensing with artificial intelligence. IEEE Transactions on Instrumentation and Measurement. 2019 Oct 14, 69(7):4103-13.

[137] Gupta M, Abdelsalam M, Khorsandroo S, Mittal S. Security and privacy in smart farming: Challenges and opportunities. IEEE Access. 2020 Feb 19, 8:34564-84.

[138] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE

[139] Torky M, Hassanein AE. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Computers and Electronics in Agriculture. 2020 Nov 1, 178:105476.

[140] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials. 2015 Jun 15, 17(4):2347-76.

[141] AlHogail A. Improving IoT technology adoption through improving consumer trust. Technologies. 2018 Jul 7, 6(3):64.

[142] Vangala A, Das AK, Chamola V, Korotaev V, Rodrigues JJ. Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. Cluster Computing. 2022 Apr 18:1-24.

[143] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[144] Aaqib M, Ali A, Chen L, Nibouche O. IoT trust and reputation: a survey and taxonomy. Journal of Cloud Computing. 2023 Dec, 12(1):1-20.

[145] Collarana D, Galkin M, Lange C, Grangel-González I, Vidal ME, Auer S. Fuhsen: A federated hybrid search engine for building a knowledge graph on-demand (short paper). InOn the Move to Meaningful Internet Systems: OTM 2016 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2016, Rhodes, Greece, October 24-28, 2016, Proceedings 2016 (pp. 752-761). Springer International Publishing.

[146] Wang Y, Tian Y, Yin X, Hei X. A trusted recommendation scheme for privacy protection based on federated learning. CCF Transactions on Networking. 2020 Dec, 3:218-28.

[147] Zhou P, Xu H, Lee LH, Fang P, Hui P. Are you left out? an efficient and fair federated learning for personalized profiles on wearable devices of inferior networking conditions. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2022 Jul 7, 6(2):1-25.

[148] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[149] Chen Y, Qin X, Wang J, Yu C, Gao W. Fedhealth: A federated transfer learning framework for wearable healthcare. IEEE Intelligent Systems. 2020 Apr 22, 35(4):83-93.

[150] Xie Y, Wang Z, Gao D, Chen D, Yao L, Kuang W, Li Y, Ding B, Zhou J. Federatedscope: A flexible federated learning platform for heterogeneity. Proceedings of the VLDB Endowment. 2023 Jan 1, 16(5):1059-72.

[151] Long G, Xie M, Shen T, Zhou T, Wang X, Jiang J. Multi-center federated learning: clients clustering for better personalization. World Wide Web. 2023 Jan, 26(1):481-500.

[152] Mu X, Shen Y, Cheng K, Geng X, Fu J, Zhang T, Zhang Z. Fedproc: Prototypical contrastive federated learning on non-iid data. Future Generation Computer Systems. 2023 Jun 1, 143:93-104.

[153] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[154] Zhang M, Huang S, Shen G, Wang Y. PPNNP: A privacy-preserving neural network prediction with separated data providers using multi-client inner-product encryption. Computer Standards & Interfaces. 2023 Mar 1, 84:103678.

[155] Chen J, Xue J, Wang Y, Huang L, Baker T, Zhou Z. Privacy-Preserving and Traceable Federated Learning for data sharing in industrial IoT applications. Expert Systems with Applications. 2023 Mar 1, 213:119036.

[156] Al-Sumaidaee G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. Information Processing & Management. 2023 Mar 1, 60(2):103160.

[157] Pasdar A, Lee YC, Dong Z. Connect api with blockchain: A survey on blockchain oracle implementation. ACM Computing Surveys. 2023 Feb 2, 55(10):1-39.

[158] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[159] Ek S, Portet F, Lalanda P, Vega G. Evaluation and comparison of federated learning algorithms for Human Activity Recognition on smartphones. Pervasive and Mobile Computing. 2022 Dec 1, 87:101714.

[160] Wang K, Mathews R, Kiddon C, Eichner H, Beaufays F, Ramage D. Federated evaluation of on-device personalization. arXiv preprint arXiv:1910.10252. 2019 Oct 22.

[161] Campos EM, Saura PF, González-Vidal A, Hernández-Ramos JL, Bernabé JB, Baldini G, Skarmeta A. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks. 2022 Feb 11, 203:108661.

[162] Ali J, Ali T, Alsaawy Y, Khalid AS, Musa S. Blockchain-based smart-IoT trust zone measurement architecture. InProceedings of the International Conference on Omni-Layer Intelligent Systems 2019 May 5 (pp. 152-157).

[163] Zhang Z, Guo X, Lin Y. Trust management method of D2D communication based on RF fingerprint identification. IEEE Access. 2018 Oct 30, 6:66082-7.

[164] Yang L, Yu K, Yang SX, Chakraborty C, Lu Y, Guo T. An intelligent trust cloud management method for secure clustering in 5G enabled internet of medical things. IEEE Transactions on Industrial Informatics. 2021 Nov 18, 18(12):8864-75.

[165] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[166] Sharma A, Pilli ES, Mazumdar AP, Gera P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. Computer Communications. 2020 Jul 1, 160:475-93.

[167] Kim SK, Park MJ, Rho JJ. Does public service delivery through new channels promote citizen trust in government? The case of smart devices. Information Technology for Development. 2019 Jul 3, 25(3):604-24.

[168] Macedo EL, Delicato FC, de Moraes LF, Fortino G. Assigning Trust to Devices in the Context of Consumer IoT Applications. IEEE Consumer Electronics Magazine. 2022 Feb 24.

[169] Minhas UF, Zhang J, Tran T, Cohen R. A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2010 Nov 22, 41(3):407-20.

[170] Guo J, Ma J, Li X, Zhang T, Liu Z. A situational awareness trust evolution model for mobile devices in D2D communication. IEEE Access. 2017 Sep 22, 6:4375-86.