Trust-based decentralized blockchain system with machine learning using Internet of agriculture things

Tanzila Saba[1], Amjad Rehman[1], Khalid Haseeb[1,2], Saeed Ali Bahaj[3], Jaime Lloret[4,5*]

[1]Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University Riyadh11586, Saudi Arabia; email: tsaba@psu.edu.sa, arkhan@psu.edu.sa
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; email: khalid.haseeb@icp.edu.pk
[3] MIS Department College of Business Administration, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; email: s.bahaj@psau.edu.sa
[4] Universitat Politenica de Valencia, Spain; email: jlloret@dcom.upv.es
[5] Staffordshire University, Stoke, UK

*Correspondence: jlloret@dcom.upv.es

Abstract: The growth of Internet of Agriculture Things (IoAT) with wireless technologies has resulted in significant advances for smart farming systems. However, various techniques have been presented to predict the soil and crop conditions. Nonetheless providing a quality-enabled autonomous system is one of the important research challenges. Furthermore, in the event of network overloading, most existing work needs help to handle trustworthy communication. As a result, this paper proposes a smart optimization model to develop reliable and quality-aware sustainable agriculture using machine learning. Firstly, the proposed model utilizes intelligent devices to automate the data collection and transmission. It analyzes the independent performance variables to support the consistent decision-making process for the forwarding scheme. Secondly, the proposed model investigated blockchain-based security principles for integrating the trusted system to reduce communication interference. The proposed model has been validated through simulations, and numerous experiments have demonstrated its efficacy regarding network parameters.

Keywords: machine learning; network trust; computing resources; agriculture; economic growth

1. Introduction

In recent years, wireless systems based on the Internet of Things (IoT) have seen significant growth in various industries. IoT is a network that allows physical devices, equipment, sensors, and other items to communicate without human intervention [1, 2]. Modern technologies are being implemented in the agriculture sector using wireless devices to increase farming productivity and management of costs. Precision agriculture uses smart IoT devices for remote sensing and monitoring crop conditions at various growth stages [3, 4]. One of the most significant economic sectors in many nations is agriculture, which emphasizes the significance of effectively managing the water resources for plants, crops and maintaining the survival of agricultural land. Sensor systems are one of the most frequently used technologies in deploying precision agriculture. Remote sensing techniques have started interacting with IoT devices for autonomous functions using sensors' communication and data aggregation functionalities. Several real-time situations exploring machine learning techniques with sensors enable technologies such as transportation, medical, military, mobile phones, and household appliances [5, 6]. In modern times, several environmental changes affect crop and field conditions, and IoT-based systems aid farmers in increasing production and lowering yield costs. Current wireless communications solutions are integrated with cloud platforms to support smart agriculture development and may increase production productivity and product quality [7, 8]. However, agriculture related operations may be correctly accomplished using a reliable and more sustainable manner regarding sensing, identification, transmission, monitoring, and feedback capabilities [8, 9]. Secured technologies significantly perform authentic functionalities in a distributed manner and attain network integrity [10, 11]. However, agriculture systems with robust functionalities of machine learning models are required for efficient and lightweight communication paradigms. The private agriculture data must be trustworthy and protected from unauthorised access until it is received on valid storage and processing devices. The security methods for the IoAT systems not only offer reliable information on farmer devices but also decrease the risks against sustainable communication. In this work, we aim to provide a model for the agricultural network using machine learning and eliminate the additional overhead on the devices. Moreover, the proposed model supports a security system with various techniques and protects IoT information from critical situations.

The following is a summary of the research's significant contributions.

i. Examines the available resources for the nodes to transmit the agricultural data at minimal cost using network edges.
ii. Using machine learning, the route performance is computed regarding reliable decision-making and transmission consistency.
iii. Proposed a a trusted IoT system to maintain data authentication and security from unauthorized disclosure.
iv. The proposed model is validated by extensive tests and outperforms earlier research studies.

The research paper is organized into the following sub-sections. Section 2 contains a discussion of the literature review. Section 3 provides a detailed description and design of the proposed model. Section 4 contains the experimental results, while Section 5 presents the conclusion.

2. Related work

Developing numerous smart technologies using IoT networks has made intelligent farming systems possible. Based on intelligent algorithms, optimal decision-making systems are developed to efficiently perform complex operations for data management [12, 13]. Currently, global population growth needs smart agriculture to fulfill its needs. In addition, food security is a serious challenge among most nations due to decreasing environmental capital, restricted agricultural land supply, and more climate changes. Clustering-based approaches have proved an energy-efficient environment and increased the performance of wireless devices in the farm system. However, due to the significant delay and inefficient energy utilization , most existing studies can only be used for some smart farming applications. Therefore, a cost-effective and scalable protocol for remote monitoring and decision-making of farms in rural areas was presented to concentrate on smart farming applications [14, 15].

Furthermore, sensing nodes should be enabled to support robust services and observe environment management with energy-efficient and improved data delivery ratio. In this regard, cluster heads perform extraordinary responsibilities to transmit the crops' information to connected farmers using sink nodes. Authors [16] presented a system in which blockchain serves as the backbone, IoT devices collect data on the ground, and smart contracts control interactions among these stakeholders. The implementation of the system has been documented in diagrams and extensive descriptions. The ultimate goal of this research was to show how blockchain can be immutable, available, transparent, and safe in agriculture, as well as the robust mechanism that integrates blockchain, smart contracts, and IoT networks.

In [17], the use of WSN technology in smart agriculture applications was investigated. The proposed research looked at the physical and functional power consumption of several WSN components. On the physical, data connection, and network layers, the analysis includes comparing the most commonly used protocols and discussing their energy efficiency. The research's findings precisely identify the primary power consumers, the amount of power they consume, and a full understanding of the critical mechanisms that should be used to improve a WSN's energy efficiency. In [18], the authors explain how to efficiently aggregate and collect data in a smart agricultural system while maintaining privacy protection measures. It presents a framework that is both effective and scalable. The agricultural system employs the genetic algorithm to find the best data collection route. Introducing an unmanned aerial vehicle improves the communication efficiency of resource-constrained sensors in the system, allowing the complete agricultural system to be used for longer periods. According to the experimental investigation, the proposed framework offers good efficiency and scalability. Authors [19] introduced an agricultural IoT security architecture combining blockchain, fog computing, and software-defined networking. Their recommended security model consisted of three major components: an agricultural IoT data management system, a blockchain-based integrity monitoring scheme, and a virtual switch software supporting software-defined networking technologies to improve network management. It is also tested against DDoS assaults using an open-source IoT platform integrating Hyperledger Sawtooth blockchain and software-defined networking technologies.

In [20], the authors investigated the design of wireless sensor nodes and networks for complicated agricultural environments. Moreover, their study also built a novel form of intelligent sensor network equipment to withstand the hard environment of agricultural manufacturing locations. It utilizeddecreases routing tasks, maintains data accuracy in a vast agrarian base region, and assures network data performance and consistency. They also executed experiments to test the system's performance to establish an intelligent agricultural platform based on IoT and machine learning. However, accuracy was not reported. Different ways to provide security are discussed in the literature, including trust management, intrusion detection, firewalls, and key management. When compared to other security solutions, trust management is one of them that can provide enhanced security. In [21], the authors presented a new secure routing algorithm called the energy-aware trust-based secured routing algorithm (EATSRA). The trust score evaluation is used to detect malicious users in WSN. Spatial-temporal constraints effectively are used with a decision tree algorithm to select the best route. The proposed trust-based routing algorithm outperforms existing systems by performance metrics based on the experiments.

Robust Cluster Based Routing Protocol (RCBRP) is presented by [22] to find the routing paths that consume the least energy and hence extend the network lifetime. To investigate it, the proposed strategy is given in six phases. First, the proposed solution is presented in two algorithms: i) an energy-efficient clustering and routing method and ii) an algorithm for calculating distance and energy consumption. By grouping the smart devices, the strategy uses less energy and balances the load. Extensive simulations in Matlab are used to validate the proposed solution. Next, the authors [23] introduced the information scheduling and optimization framework (ISOF). This framework optimizes information scheduling and classification to lower process delay and stagnancy. The delay and stagnancy towards the end of yields are used to calculate the control flexibility of a smart farm. The classification component separates information based on processing and completion times to eliminate backlogs through offloading. This framework inherits the benefits of edge computing and IoT with interoperable features to help with information processing, classification, offloading, and periodic updates.

The contribution and significance are summarized based on the discussed work. Smart agriculture can boost farm productivity and efficiency while keeping costs down. IoT provides a diverse platform for automating things, and smart agriculture is one of the most promising concepts for providing smart services. Most IoT-based solutions have provided energy-efficient strategies to ensure the agriculture sector's long-term feasibility. However, a more reliable and long-term communication mechanism is still required due to the limits of sensors. Furthermore, agricultural devices must incorporate lightweight, trustworthy, and secure solutions to protect farmers' data. The proposed model should be able to securely and promptly provide agricultural data to farmers' mobile devices.

3. Trust-based decentralized multi-regression model

This section describes the details of the proposed model. The developed components are illustrated in Figure 1. Devices initialization, fitness computational using machine learning, digital hashing, and blockchain-enabling security are the main components of the proposed model. The proposed model initially uses multi-regression analysis to identify the next hop for agricultural data transferring. Multi-regression is a statistical technique and it is used by many machine learning applications to identify the relation between dependent and independent variables. The objective function in the proposed model offers a statistical approach for analyzing the optimal result and is based on various network attributes.

Moreover, IoT-based privacy-preserving for data collection and aggregation is also critical for reducing the data risk in agricultural growth. Our security mechanism is divided into three stages: sensors, edges, and data centers. First, agricultural data is protected while transferring from the sensors to edge devices. Second, the intermediate level, comprised of various edges, is protected from suspicious behavior. The incorporation of blockchain technology provides secured functionalities using distributed manner. In such a scheme, nodes perform authentication and integrity functions collaboratively without excessive overheads. Finally, the edged data is securely sent to data centers.

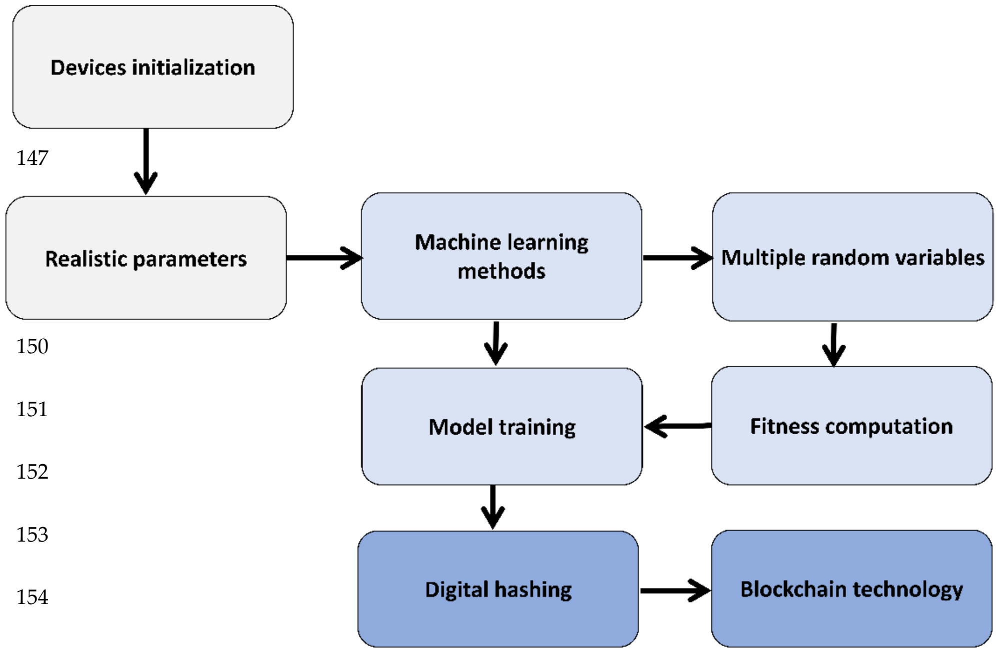


Figure. 1 Block diagram illustrating the proposed agriculture model

3.1 Network registration with machine learning-based IoT system

Initially, all the nodes register their information in the neighboring tables, so network data can be interchanged. All the nodes have unique identities with predefined energy, processing, and transmission constraints. No data transmission is allowed directly from sensor nodes to end-users. It only can be performed using the services of gateway devices. The gateways also perform aggregation and verification functionalities on the nodes' data. Each IoT sensor initially looked up its local table for the transmission of agricultural data. Direct data is transmitted if an entry point to the edge device is detected. Otherwise, the source node investigates the route discovery strategy using multi-regression analysis. The proposed model uses many independent criteria to estimate the weighted score and achieve a more efficient decision-making system. Multiple regression analysis is explored during route discovery to predict the behavior of adjacent nodes and support a trustworthy optimal strategy [23, 24]. On the other side, the edges in the proposed model are mobile, which decreases the transmission distance toward data centers and lowers the overhead for the sensors' tier. The proposed model formulates a numeric score for identifying neighboring nodes by defining the mathematical relationship between various random variables. Let us consider the set of neighbors of the node N_i, which can be defined as given in Equation 1.

$$N_i = (n_i, n_{i+1}, \dots, n_k) \tag{1}$$

The list of neighbors is updated in the local table of N_i, and if any node no longer exists in its vicinity for any reason, its record is eliminated.

The objective of the fitness function is to compute the least cost value C_i for the source node. Later, based on the multiple regressional analysis, the agriculture data is forwarded to mobile edges. By exploring the neighbor's list, the source node computes the cost function using multiple independent factors, as defined in Equation 2.

$$X = \beta_0 + \sum_{i=0}^{k} \beta_i y_i + \alpha \tag{2}$$

where X is the dependent variable, y_i are random variables, and $\beta_0 \dots \beta_i$ denote constant terms. The constant terms denote the impact of each independent variable on the cost function. In the proposed model, the y_i value is the aggregation of composite parameters i.e. link behavior l_b and nodes trust n_t, as given in Equation 3.

$$y_i = l_b + n_t \ , \ i \in N \tag{3}$$

To compute the l_b, along with residual energy e_i, the source node also explicitly keeps track of the packet buffering, as defined in Equation 4.

$$l_b = e_i + (aw_{pkt} / b_{size}) \quad (4)$$

where aw_p is awaiting packets in the queue and b_{size} is the buffer size. That means that a node with a high number of awaiting packets reflects the behavior of a congested link and has a low priority when choosing the next hop. On the other hand, n_t is the composition of direct D_r and indirect D_{ir} trust, by exploring the link behavior as defined in Equation 5.

$$n_t = D_r + D_{ir} \quad (5)$$

3.2 Agricultural security for unreliable IoT environment

This section provides the detail of the security algorithm for the proposed model. Data security is one of the most important criteria for smart communication over the Internet connections. In the proposed model, , the network data is first properly verified, and later forwarded using trust-oriented intermediate devices. The security system utilizes blockchain methods to assure data verification and denies interruptions from unauthorized nodes. Furthermore, it utilizes the functions of hashing and digital signatures to achieve authentication and data protection. Firstly, the security system uses hashing techniques on the sensors' messages d_i with secret key k and generates the fixed-length blockchain hashes P_i, as given in Equation 6.

$$H(P_i) = D(d_i, k), \; k \in Ki \quad (6)$$

The private keys of the nodes are used to encrypt the digital hashes further and provide data authentication. Afterward, all the generated hashes P_i, $P_{i+1}, \ldots, P_n$ are integrated as given in Equation 7.

$$Z = H(P_i) + H(P_{i+1}) + \cdots + H(P_{i+n}) \quad (7)$$

The security system verified the data authentication by utilizing the nodes' public keys. Once the authentication process is completed, the proposed model decrypts the encrypted data using appropriate secret keys. Figure 2 shows the phases of the security system comprised of node verification, data blocks, digital hashes, and node authentication. Nodes must be connected and registered to a network's infrastructure to communicate with end users. Through the mutual authentication process, nodes' identities are first verified. If they are supposed to be hostile, they are marked as malicious and recorded such information in the routing tables. However, if nodes are reliables and their identities are verified, unique codes are created and combined into blocks to preserve data secrecy and integrity. Later, data is appropriately checked before being sent to smart devices.

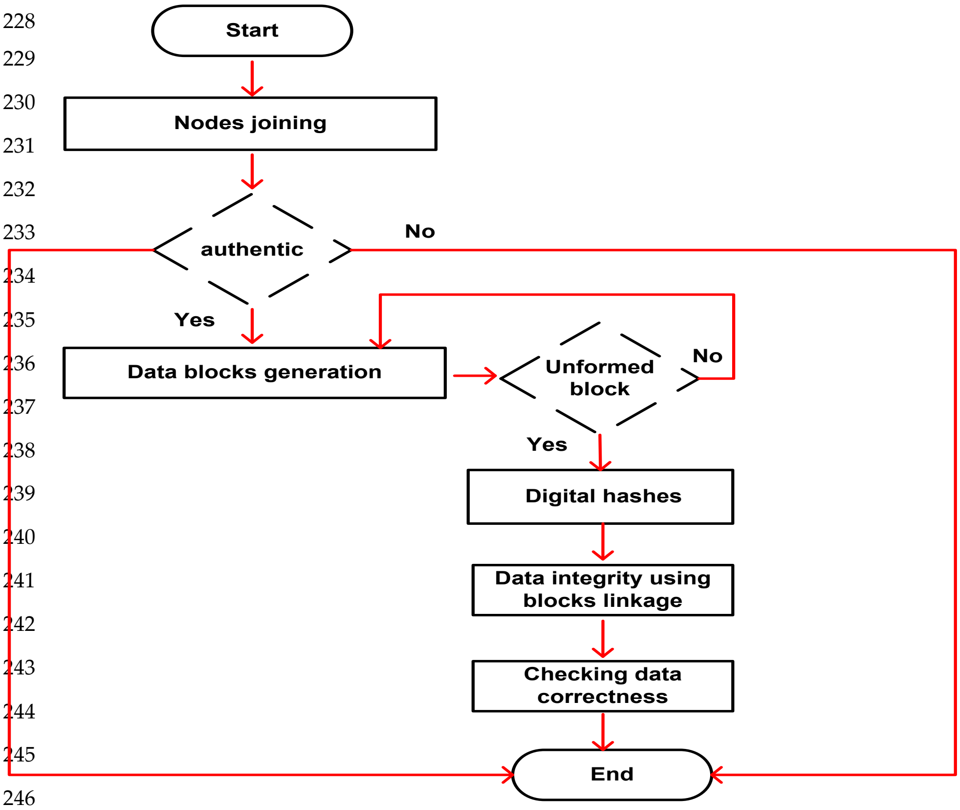
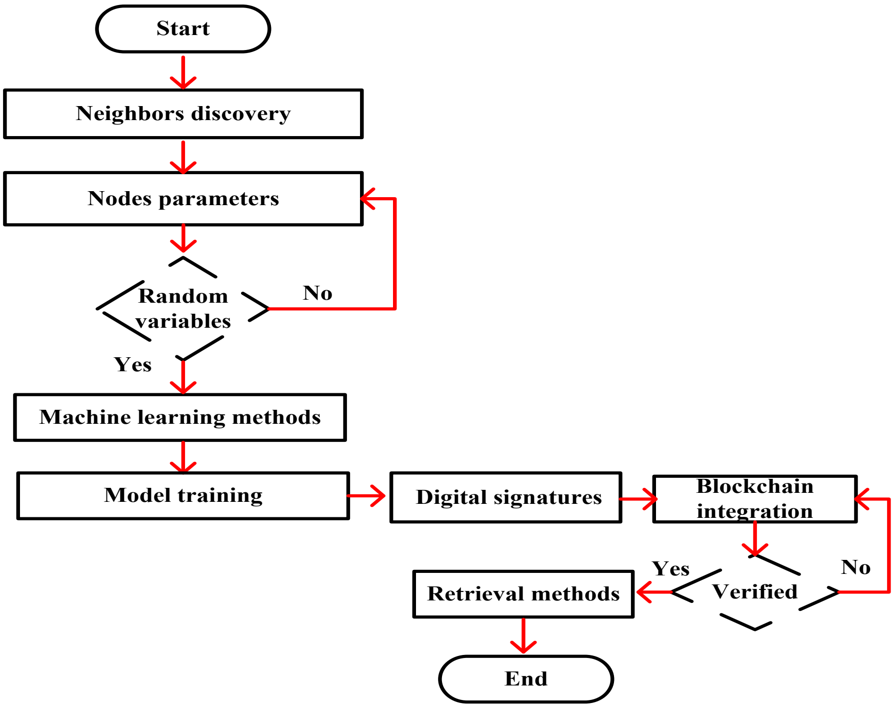


Figure 2. Algorithm for data authentication and security

The flowchart for the route discovery with trusted communication is shown in Figure 3. The main procedures involve network initialization, evaluation of independent parameters, fitness computation, and digital hashing. Beginning with the identification of neighboring nodes, the machine learning technique is exploited to compute the fitness value. The fitness value explores the network data to provide a prediction value. In terms of energy effectiveness and reliability, the chosen nodes produce optimal results for the transmission of agricultural data. Moreover, the proposed model offers integrity and authentication functionalities for IoT devices through digital hashing. Furthermore, data is protected by the implementation of block-wise encryption and decryption techniques.



258

Figure 3. Flowchart of the route discovery with trusted collaboration 259

4. Simulation environment 260

In this section, the simulation environment and an explanation of the experiments are provided. We compare our proposed model with earlier research studies. We used the Cooja simulator for creating the agricultural-based simulation environment with the support of wireless and IoT devices. Temperature, air pressure, and moisture sensors capture the data. The simulation settings for the set of experiments are listed in Table 1. A 300m x 300m space was used for the simulation tests. All the sensors are homogeneous in terms of communication resources. In experiments, edge devices act as mobile gateways and are rotated at 5m/s to 25 m/s. The packet size is set to 64 bytes. We run the 25 simulations for the verification of experimental results. Initially, some stages of simulations are recorded in log files to get real-time data. Later, the proposed model utilizes such log files to extract the needful data in decision-making criteria. The simulations are executed with two scenarios i.e. varying sensors and the varying speed of edge devices. Finally, the proposed model is compared to ISOF, RCBRP regarding energy consumption, packet delivery ratio, network overhead, and data delay.

Table 1: Simulation parameters 272

Parameters	Values
IoT Devices	30, 60, 90, 120, 150
Initial energy	2j
Nodes and Sink deployment	Random
Packet size	64 bytes
Transmission range	5m
Simulation time	2000s
Network diameter	300m x 300m
Malicious devices	10
Sensors	Temperature, air pressure, moisture

273

4.1 Results analysis and discussion 274

In this section, we present the discussion regarding performance metrics for the proposed model and other related studies. Also, the security analysis is provided for the proposed model in terms of proposed processes. The uniqueness of each IoT device is identified by its identity. No two nodes can have the same identities. However, both are marked as malicious and block the incoming request or data. To initiate the network connection, the registration stage needs to execute and map the tables table information. To attain the privacy of the data, the proposed model executes lightweight encryption methods and generates different hashes using the cryptographic algorithm to achieve integrity as well. All the authentication errors are stored inside log files. All the blocks are inter-link in the form of blockchain technology, so it gives a very hard time for intruders to change the entire chain of data blocks. The verification is performed using digital signatures using private keys of data-originating nodes.

Finally, we compared the proposed model to existing solutions regarding energy consumption. The contrast is shown in Figures 4(a) and 4(b), which show that the proposed model increased energy usage efficiency by 13% and 16%, respectively. It has been noticed that as the number of IoT sensors grows, so does the amount of energy consumed. On the other hand, the proposed model employs a fitness function to provide an intelligent energy solution and uses multi-variable regression analysis to provide updated routes smoothly. By utilizing fewer control messages and retransmissions, the proposed model balances the energy consumption of the smart communication system and extends the total lifetime.

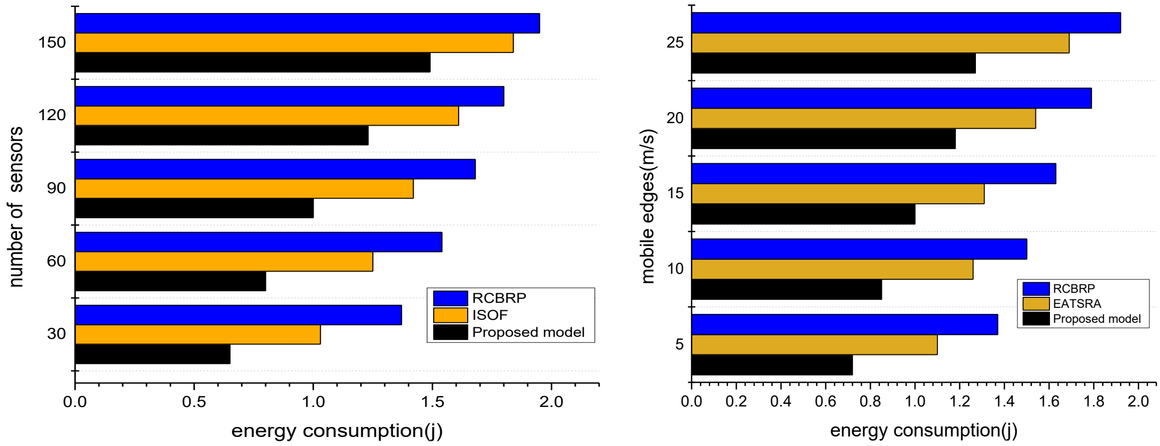
Moreover, with the supply of updated routes based on realistic data, the IoAT system incurs the least communication cost. In addition, updating routes based on realistic parameters reduces the communication load for the IoAT system, resulting in an efficient system. We compared the proposed model's performance with related strategies in terms of data latency. Figures 5(a) and 5(b) show the performance of the proposed model compared to existing solutions, revealing that the proposed model reduces end-to-end latency by 16% and 19%, respectively. It's because of the IoAT system's realistic parameters and the acquired data integration with regression analysis. The results ensure a fair distribution of node resources and accelerate the packet transmission process to smart devices. The mobile edges not only improve the efficiency of node bandwidth usage but also provide a minimal delay in evaluating and delivering the farmers' data to the cloud network.

Furthermore, the security solution reduces unnecessary traffic by preventing hostile devices from flooding the green space interaction connection with fake route request packets. As a result, the suggested model improves the response time between the data requested and the deliverable system while maintaining a tolerable delay rate. Figures 6(a) and 6(b) show the proposed model's performance in terms of packet delivery ratio for various IoT sensors and the speed of mobile edges. Even in malfunctioning nodes, the proposed model dramatically boosts the delivery rate of data packets by 18% and 21%, respectively. It is because the devices' are trusted mutually based on the composite factors. Moreover, appropriate security methods are explored to achieve data privacy and authentication for sharing agricultural data. Digital hashing provides the rapid detection of rogue devices and increases the data integrity of the communication system.

Furthermore, the edge devices are more durable and serve as a supervisor for sensor data received from the IoAT; after proper authentication, the data is supplied to the application user with significant rights. Figures 6(a) and 6(b) show the proposed model's performance in terms of packet delivery ratio for various IoT sensors and the speed of mobile edges. Even in the presence of malfunctioning nodes, the proposed model dramatically boosts the delivery rate of data packets by 16% and 17%, respectively. It is because the devices' are trusted mutually based on the composite factors.

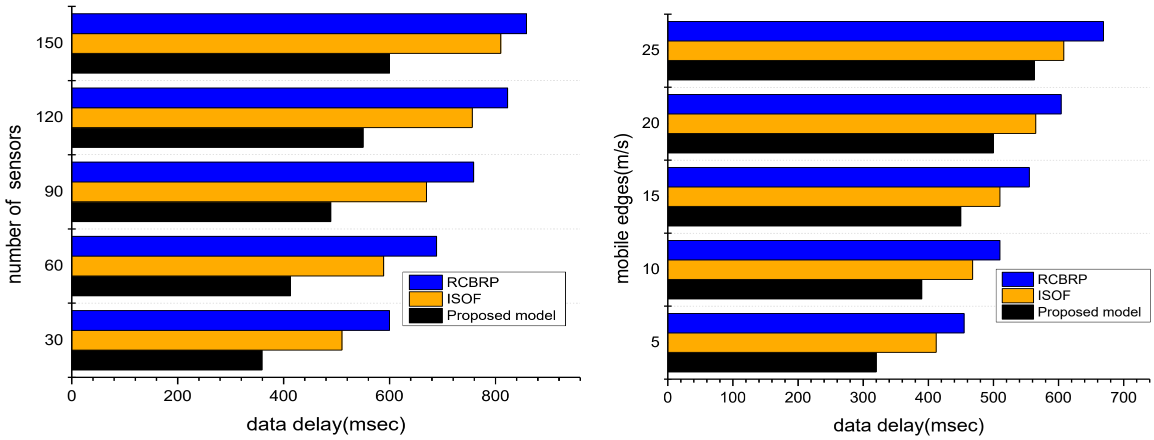
Additionally, appropriate security methods are explored to achieve data privacy and authentication for sharing agricultural data. Digital hashing provides the rapid detection of rogue devices and increases the data integrity of the communication system. Furthermore, the edge devices are more durable and serve as a supervisor for sensor data received from the IoAT; after proper authentication, the data is supplied to the application user with significant rights. Figures 7(a) and 7(b) show the comparison of the proposed model to the existing solutions regarding network overhead. Using different numbers of devices and speeds of mobile edges, it can be seen that the proposed model reduces overheads by 18% and 21%, respectively. This is due to the proposed model's machine learning method to learn routing decisions and track the IoAT system effectively by investigating mobile edges. In the proposed model, multi-parameters re-evaluate forwarding states whenever any unreliable links are found in transmitting the farmer data. Furthermore, packet information increases the decision to predict the links' performance in the presence of unknown devices. Moreover, blockchain technologies create chain-oriented encryption and authentication phases to offer a trust-based security solution.

4.2 Simulation graphs



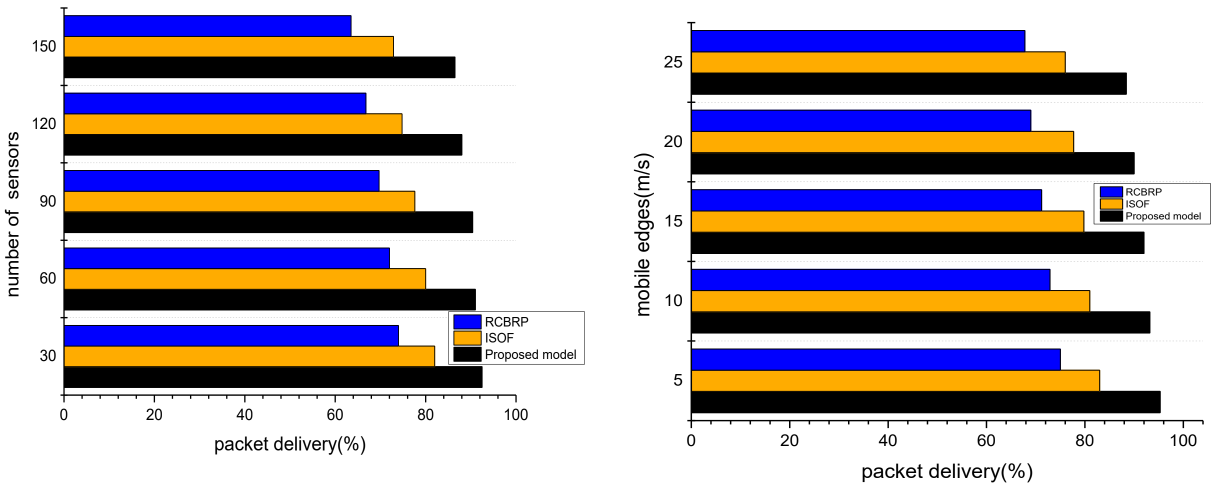
(a) **(b)**

Figure 4. energy consumption with varying sensors and mobile edges scenarios



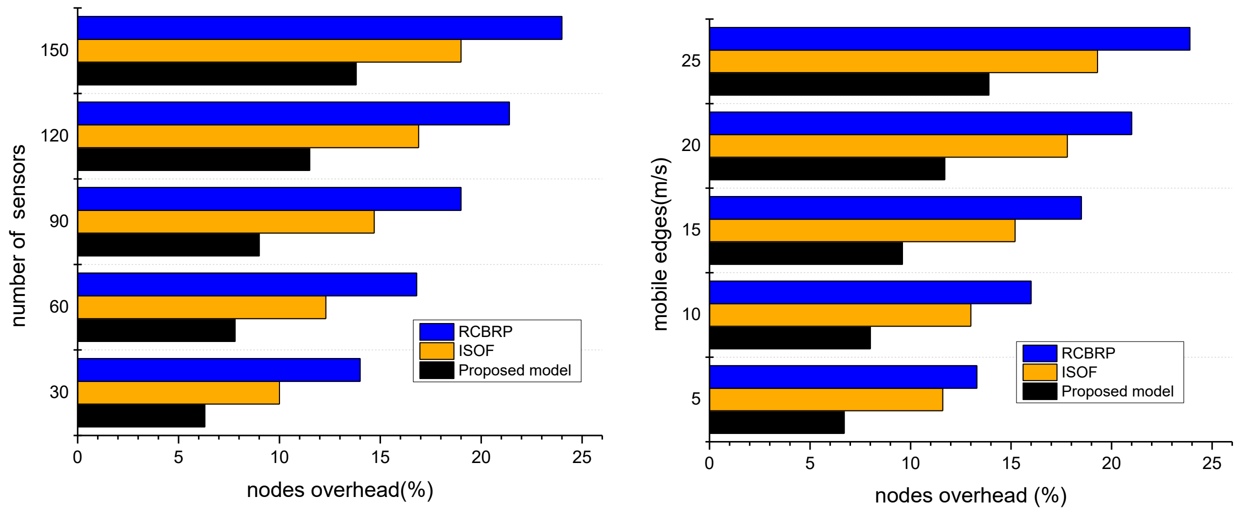
(a) **(b)**

Figure 5. data delay with varying sensors and mobile edges scenarios



(a) **(b)**

Figure 6. packet delivery ratio with varying sensors and mobile edges scenarios



(a) **(b)**

Figure 7. nodes overhead with varying sensors and mobile edges scenarios

5. Conclusion

Agriculture systems are made up of many autonomous devices that collect, process, and transmit real-time data. These devices come with a variety of IoAT sensors to help with the development of smart communication and increase agricultural productivity. There have been numerous proposals for improving the performance of smart systems. Despite this, most of them need help to transfer massive amounts of data from farmers to wireless equipment with minimal latency and high-quality assurance. Security with trusted routing is also essential to protect sensitive data from unauthorized nodes. In intelligence, a technique for computing communication trust and routing strategies in farming systems using machine learning is required. The proposed model analyzed environmental factors and verifies the reliability of the forwarding system by exploiting a multi-variable linear regression technique. Furthermore, trust-based security methods have been used to improve the efficacy of routing decisions. According to simulations, the proposed model delivers significant performance by lowering communication costs and improving data security by eliminating link disruption. In the future, we will evaluate the performance of the proposed model against intrusion detection with the support of a large-size dataset. Moreover, the mobile cloud communication paradigm needs to be included to further improve the proposed model.

Acknowledgements: This work has been funded by the “Ministerio de Ciencia e Innovación” through the Project PID2020-114467RR-C33, by the "Ministerio de Economía y Competitividad" through the Project TED2021-131040B-C31, and by "Proyectos de innovación de interés general por grupos operativos de la Asociación Europea para la Innovación en materia de productividad y sostenibilidad agrícolas (AEI-Agri)” in the framework “Programa Nacional de Desarrollo Rural 2014-2020”, for the grant GO TECNOGAR, in cofuding EU 80% by the "Fondo Europeo Agrícola de de Desarrollo Rural-FEADER" and 20% by the "Ministerio de Agricultura, Pesca y Alimentación" with a total fund of 432.329,05 €. Being the "Dirección general de desarrollo Rural, innovación y Formación Agroalimentaria" (DGDRIFA) the national managing authority entrusted with the application of the FEADER grant.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Goel, S.S., A. Goel, M. Kumar, and G. Moltó, *A review of Internet of Things: qualifying technologies and boundless horizon.* Journal of Reliable Intelligent Environments, 2021. **7**(1): p. 23-33.
2. Wan, R. and N. Xiong, *An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks.* Human-centric Computing and Information Sciences, 2018. **8**(1): p. 1-22.

3. Shafi, U., R. Mumtaz, J. García-Nieto, S.A. Hassan, S.A.R. Zaidi, and N. Iqbal, *Precision agriculture techniques and practices: From considerations to applications.* Sensors, 2019. **19**(17): p. 3796.
4. García, L., L. Parra, J.M. Jimenez, M. Parra, J. Lloret, P.V. Mauri, and P. Lorenz, *Deployment strategies of soil monitoring WSN for precision agriculture irrigation scheduling in rural areas.* Sensors, 2021. **21**(5): p. 1693.
5. Ji, B., Y. Wang, K. Song, C. Li, H. Wen, V.G. Menon, and S. Mumtaz, *A survey of computational intelligence for 6G: Key technologies, applications and trends.* IEEE Transactions on Industrial Informatics, 2021. **17**(10): p. 7145-7154.
6. Al-Garadi, M.A., A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, and M. Guizani, *A survey of machine and deep learning methods for internet of things (IoT) security.* IEEE Communications Surveys & Tutorials, 2020. **22**(3): p. 1646-1685.
7. Quy, V.K., N.V. Hau, D.V. Anh, N.M. Quy, N.T. Ban, S. Lanza, G. Randazzo, and A. Muzirafuti, *IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges.* Applied Sciences, 2022. **12**(7): p. 3396.
8. Ayaz, M., 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, 2019. **7**: p. 129551-129583.
9. Haseeb, K., I. Ud Din, A. Almogren, and N. Islam, *An energy efficient and secure IoT-based WSN framework: An application to smart agriculture.* Sensors, 2020. **20**(7): p. 2081.
10. Khalaf, O.I. and G.M. Abdulsahib, *Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks.* Peer-to-Peer Networking and Applications, 2021. **14**(5): p. 2858-2873.
11. Abbas, G., A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, *Safety, Security and Privacy in Machine Learning Based Internet of Things.* Journal of Sensor and Actuator Networks, 2022. **11**(3): p. 38.
12. Jiang, Y., G. Tong, H. Yin, and N. Xiong, *A pedestrian detection method based on genetic algorithm for optimize XGBoost training parameters.* IEEE Access, 2019. **7**: p. 118310-118321.
13. Haseeb, K., A. Rehman, T. Saba, S.A. Bahaj, and J. Lloret, *Device-to-device (D2D) multi-criteria learning algorithm using secured sensors.* Sensors, 2022. **22**(6): p. 2115.
14. Mahajan, H.B., A. Badarla, and A.A. Junnarkar, *CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming.* Journal of Ambient Intelligence and Humanized Computing, 2021. **12**(7): p. 7777-7791.
15. Faid, A., M. Sadik, and E. Sabir, *An Agile AI and IoT-Augmented Smart Farming: A Cost-Effective Cognitive Weather Station.* Agriculture, 2021. **12**(1): p. 35.
16. Pranto, T.H., A.A. Noman, A. Mahmud, and A.B. Haque, *Blockchain and smart contract for IoT enabled smart agriculture.* PeerJ Computer Science, 2021. **7**: p. e407.
17. Banđur, Đ., B. Jakšić, M. Banđur, and S. Jović, *An analysis of energy efficiency in Wireless Sensor Networks (WSNs) applied in smart agriculture.* Computers and Electronics in Agriculture, 2019. **156**: p. 500-507.
18. Yuan, J., W. Liu, J. Wang, J. Shi, and L. Miao, *An efficient framework for data aggregation in smart agriculture.* Concurrency and Computation: Practice and Experience, 2021. **33**(10): p. e6160.
19. Friha, O., M.A. Ferrag, L. Shu, and M. Nafa. *A robust security framework based on blockchain and SDN for fog computing enabled agricultural internet of things*. in *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*. 2020. IEEE.
20. Liu, Y., *Intelligent analysis platform of agricultural sustainable development based on the Internet of Things and machine learning.* Acta Agriculturae Scandinavica, Section B—Soil & Plant Science, 2021. **71**(8): p. 718-731.
21. Selvi, M., K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, and A. Kannan, *An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks.* Wireless Personal Communications, 2019. **105**(4): p. 1475-1490.
22. Shafiq, M., H. Ashraf, A. Ullah, M. Masud, M. Azeem, N. Jhanjhi, and M. Humayun, *Robust cluster-based routing protocol for IoT-assisted smart devices in WSN.* Computers, Materials & Continua, 2021. **67**(3): p. 3505-3521.
23. Kumar, D.P., T. Amgoth, and C.S.R. Annavarapu, *Machine learning algorithms for wireless sensor networks: A survey.* Information Fusion, 2019. **49**: p. 1-25.

24. Gambhir, E., R. Jain, A. Gupta, and U. Tomer. *Regression analysis of COVID-19 using machine learning algorithms*. in *2020 International conference on smart electronics and communication (ICOSEC)*. 2020. IEEE.

Tanzila Saba earned her Ph.D. in document information security and management from Faculty of Computing, Universiti Teknologi Malaysia, Malaysia in 2012. Currently, she is Prof and Associate Chair of Information Systems Department in the College of Computer and Information Sciences Prince Sultan University Riyadh KSA. She is also leader of the AIDA Research Lab at PSU.

Amjad Rehman is a senior researcher in the Artificial Intelligence & Data Analytics Lab CCIS Prince Sultan University Riyadh Saudi Arabia. He received his Ph.D. & Postdoc from the Faculty of Computing Universiti Teknologi Malaysia with a specialization in Forensic Documents Analysis and Security. His keen interests are in Data Mining, Health Informatics and security.

Khalid Haseeb received his Ph.D. in Computer Science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia in 2016. He is working as an Assistant Professor in the Department of Computer Science at Islamia College Peshawar, Pakistan. His research areas include wireless sensor networks, ad-hoc networks, network security, Machine learning, Internet of Things, Software Define Networks and cloud computing.

Saeed Ali Bahaj is an Associate Professor at MIS Department COBA Prince Sattam bin Abdulaziz University Al-kharj Saudi Arabia. He earned his doctorate at Pune University India in 2006. His main research interests include Artificial Intelligence, information management, forecasting, information engineering, big data mining and information security.

Jaime Lloret received his Ph.D. in telecommunication in 2006. He is Full Professor at the Polytechnic University of Valencia, Spain. He is the Chair of the Integrated Management Coastal Research Institute. Since 2016 he is the Spanish researcher with highest h-index in the TELECOMMUNICATIONS. He is included in the world’s top 2% scientists according to the Stanford University List.