ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

A COMPREHENSIVE FRAMEWORK FOR INTEGRATING BLOCKCHAIN SECURITY, CYBERSECURITY, AND AI-BASED LEARNING IN IOT-DRIVEN AGRICULTURE

Dr Santosh kumar
Assistant Professor
Department of Computer Application
LSM Campus, Pithoragarh,Uttarakhand

Abstract :
The integration of edge computing with Internet of Things (IoT) systems (EC-IoT) enhances protection and privateness in IoT networks, addressing key challenges in records safety and community integrity. This paper examines the combination of EC-IoT and synthetic intelligence (AI), exploring strategies to bolster security features and counter evolving threats. The evaluate specializes in decentralized trust size mechanisms and protection frameworks designed for IoT structures, studying the today's assault fashions and their impacts on IoT networks. Additionally, AI-based techniques for mitigating those threats are evaluated, with emphasis on real-international effectiveness. The paper highlights the need for scalable, adaptable, and strong security solutions, urging destiny research to cognizance on integrating AI to improve IoT security, privacy, and efficiency at the same time as addressing challenges along with scalability and resource barriers.

Keywords: Edge Computing, IoT, Artificial Intelligence, Security, Privacy, Trust Mechanisms, Attack Models, Cybersecurity, Scalable Solutions, AI-based Learning.

I. INTRODUCTION

The Internet of Things (IoT) represents a transformative generation that interconnects embedded devices, permitting them to gather and change facts without human intervention. This paradigm extends the internet’s talents past traditional devices, permitting ordinary objects to communicate with their environment via sensors and software program. As IoT evolves, it reshapes industries by means of improving automation, information evaluation, and choice-making skills. One of the most promising sectors in which IoT is making an effect is agriculture, wherein it's miles revolutionizing crop control, resource optimization, and environmental tracking. The integration of IoT technologies in agriculture opens new possibilities for increasing efficiency, reducing costs, and improving sustainability.

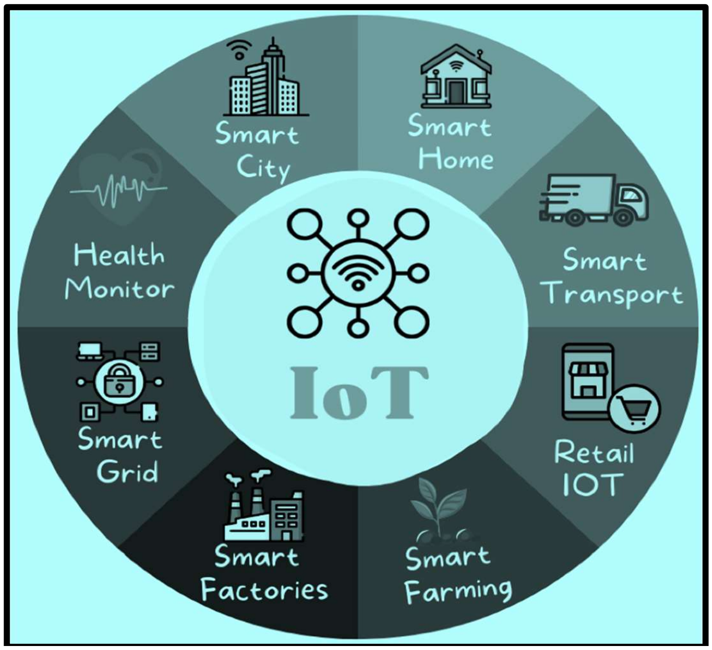

Figure :1, Internet of Things (IoT)

Security and Privacy Challenges

However, as IoT gadgets proliferate in various sectors, they introduce good sized security and privateness challenges. The massive quantity of facts generated by way of IoT gadgets, mixed with the connectivity and interdependence of these gadgets, makes them vulnerable to a huge range of cyber threats. As IoT networks make bigger, the risk of records breaches, unauthorized get entry to, and malicious attacks grows, requiring strong security measures to guard the integrity of IoT structures. The traditional safety models used for conventional IT structures are inadequate to address the unique challenges posed with the aid of IoT environments, which call for extra dynamic, scalable, and adaptive solutions.

Blockchain for IoT Security

Blockchain era has emerged as a ability option to enhance the safety and trustworthiness of IoT networks. By leveraging decentralized, tamper-evidence ledgers, blockchain guarantees statistics integrity and transparent transactions, mitigating dangers associated with IoT device communique. Blockchain's capacity to offer verifiable and immutable information makes it especially beneficial in agricultural IoT structures, wherein making sure the authenticity and reliability of statistics is crucial for informed choice-making. The integration of blockchain with IoT can decorate privacy, reduce fraud, and make sure that the statistics accrued from IoT devices stays steady and straightforward.

Artificial Intelligence in IoT

In addition to blockchain, artificial intelligence (AI) is more and more being incorporated into IoT structures to enhance security, optimize operations, and decorate selection-making. AI-pushed analytics can pick out styles, expect capability security breaches, and advise preventative measures in real time. Machine studying fashions may be carried out to agricultural IoT systems to research sensor facts, expect crop yields, screen soil health, and come across diseases or pests. By incorporating AI into the IoT ecosystem, agricultural operations can turn out to be extra efficient, effective, and sustainable.

Role of Cybersecurity in IoT Systems

Cybersecurity performs a important function within the IoT surroundings, in particular in sectors along with agriculture, in which sensitive statistics and crucial infrastructure must be included. The integration of advanced cybersecurity protocols, along blockchain and AI, can offer a multi-layered defense strategy against potential threats. These blended technologies can detect vulnerabilities, automate responses to cyber incidents, and constantly monitor the IoT network to make certain its integrity. With the growing reliance on IoT in agriculture, making sure the security of connected gadgets and networks is important to preserving consider and preventing disruptions in crucial systems.

Challenges in IoT Integration

Despite the colossal capacity of IoT, blockchain, and AI in agriculture, demanding situations continue to be in terms of scalability, aid limitations, and integration complexities. The decentralized nature of IoT networks, coupled with the need for actual-time data processing, requires that safety answers be each scalable and adaptable. In agriculture, in which IoT devices may be deployed in far off places with restrained strength assets, it's far important to layout lightweight, strength-efficient safety mechanisms which could still provide robust protection. The development of such answers can be important for the significant adoption and fulfillment of IoT technologies in agriculture.

Proposed Framework for IoT Security

This paper proposes a comprehensive framework for integrating blockchain safety, cybersecurity, and AI-based totally getting to know in IoT-driven agriculture. By addressing the unique demanding situations of agricultural IoT structures, this framework objectives to offer scalable, adaptive, and powerful solutions to ensure the security, privacy, and performance of IoT operations. The proposed integration of those technology holds big promise in advancing agricultural practices, enhancing meals manufacturing, and selling sustainability. Through this work, we aim to contribute to the improvement of more secure, efficient, and resilient IoT ecosystems in agriculture, facilitating innovation and growth in the sector.

II. LITERATURE REVIEW

IoT and Edge Security Challenges

IoT and facet computing structures face huge safety demanding situations due to the vulnerabilities of area devices, confined assets, high latency, and the complexity of securing various IoT gadgets. To address those troubles, light-weight protocols, secure running systems, and scalable solutions are required. Privacy, authentication, and information storage vulnerabilities are also established, necessitating the use of technology like blockchain, fog computing, and machine mastering to beautify safety and privateness at the same time as overcoming resource constraints.

Healthcare IoT Security

The use of IoT in healthcare affords specific security worries related to the aggregation, transmission, and garage of sensitive clinical information. Key threats include information integrity, secure transmission, and privateness issues. Countermeasures including encryption, privateness-keeping protocols, and robust authentication mechanisms are encouraged. Integrating aspect and fog computing can help mitigate latency and enhance the performance of information processing, that's vital for securely managing huge healthcare datasets.

Machine Learning for IoT Security

As IoT structures end up greater complex, system learning (ML) methods are increasingly more applied to improve safety. ML strategies, such as supervised, unsupervised, and reinforcement gaining knowledge of, are applied for anomaly detection, cyberattack prediction, and improving universal IoT security. These techniques are adaptable to the dynamic nature of IoT environments, supplying scalable answers for detecting threats like eavesdropping, DDoS attacks, and information tampering.

Edge and LoRa Integration

Integrating edge computing with IoT networks offers a strategy to lessen latency and decorate gadget overall performance. LoRa technology, whilst mixed with area computing, can cope with demanding situations related to scalability, energy performance, and conversation. This neighborhood statistics processing permits IoT devices to function efficaciously with out relying heavily on cloud infrastructure. This method is specially beneficial in packages inclusive of smart cities, industrial IoT, and agriculture, wherein real-time facts processing is critical.

Security Frameworks and Trust Management

Scalable security frameworks and accept as true with management are important for ensuring the safety and privacy of IoT and facet computing systems. Effective trust control fashions and privacy-keeping techniques are vital to make certain information integrity and defend against unauthorized get admission to. Lightweight, efficient security mechanisms that stability performance and protection are critical for addressing the developing complexity of IoT networks and facet computing environments.

Blockchain and AI Integration

The aggregate of blockchain and artificial intelligence (AI) offers a powerful way to decorate IoT security. Blockchain guarantees statistics integrity, while AI enables real-time danger detection and edition to converting protection situations. This integration can assist address vulnerabilities in facet devices and provide a complete safety solution that evolves as new threats emerge in IoT environments.

Energy Efficiency and IoT Security

Energy efficiency is a enormous challenge in IoT systems, in particular in area and fog computing environments. Strategies along with low-electricity hardware, energy-green scheduling, and task offloading are being explored to optimize strength use. Balancing energy consumption with robust security remains complicated, and future studies is wanted to expand power-green security solutions that don't compromise machine overall performance or safety.

III. RESEARCH METHODOLOGY

Designing the Framework for Integration

A complete framework could be designed to combine blockchain protection, cybersecurity protocols, and AI-primarily based mastering techniques into IoT-pushed agricultural structures. This framework will awareness on secure communication, statistics integrity, and actual-time choice-making. The design will element how blockchain secures IoT communications, how cybersecurity protocols guard against records breaches, and how AI optimizes methods like irrigation, crop monitoring, and pest manage.

IoT Infrastructure Setup and Data Collection

IoT gadgets can be deployed in an agricultural placing to acquire records on soil moisture, temperature, crop health, and different environmental parameters. This setup will help acquire real-time statistics, a good way to be processed at the brink or fog layer for efficient facts dealing with. The collected information may be analyzed to assess machine performance, inclusive of actual-time environmental circumstance tests and the detection of potential safety threats.

Blockchain Security Implementation

Blockchain technology will be incorporated to secure IoT data in agricultural systems. This will contain deploying a blockchain network for decentralized information management, making sure the integrity and transparency of records shared amongst stakeholders. Smart contracts will be used for automating techniques which includes authentication and facts validation, ensuring that IoT gadgets talk securely and that the data stays tamper-proof.

Cybersecurity Measures and Risk Management

A strong cybersecurity method could be evolved to protect IoT devices and records from cyber threats. This strategy will include the implementation of encryption techniques, intrusion detection systems (IDS), and anomaly detection algorithms. Additionally, a danger management framework can be applied to become aware of capacity safety threats including records breaches or denial-of-carrier attacks, and corresponding mitigation measures will be devised.

AI-Based Learning for Optimization and Anomaly Detection

AI-based system learning fashions can be applied to predict results and optimize approaches inside the agricultural IoT device. These fashions can be trained on data from IoT sensors to discover anomalies like atypical environmental conditions or device malfunctions. Reinforcement learning algorithms will also be employed to enhance actual-time choice-making for packages inclusive of adaptive irrigation systems and crop fitness monitoring.

Performance Evaluation and Testing

The proposed framework will go through significant testing in a actual-world agricultural placing to assess its effectiveness. Key performance signs (KPIs) together with system security, performance, scalability, and real-time responsiveness may be measured. The overall performance of the IoT gadgets, blockchain security, cybersecurity measures, and AI optimization may be assessed to become aware of areas for improvement and ensure the framework's suitability for massive-scale agricultural deployments.

IV. DATA ANALYSIS AND RESULT

Experimental Setup

The experiment was conducted the use of Google Colab and Remix IDE. Google Colab become used for statistics preprocessing, schooling, and category tasks with the help of Python libraries like Matplotlib, Seaborn, Scipy, Pandas, Numpy, and others. Principal Component Analysis (PCA) became carried out to lessen the dimensionality of the dataset. The Explainable AI (XAI) approach changed into employed to perceive relevant features and cope with statistics poisoning attacks in IoT-based totally vital infrastructures. Smart contracts have been advanced using Remix IDE for secure interaction with IoT devices, storing sensor readings and authorized customers thru IPFS-primarily based storage.

Feature Selection

PCA become first of all carried out to reduce the dataset from 83 to 35 capabilities, simplifying the version and lowering schooling time. XAI techniques had been then applied to in addition refine the function set, resulting inside the selection of 20 key capabilities from the 35 diagnosed by way of PCA. This function reduction notably advanced the efficiency of the model, focusing at the maximum applicable data for training the AI classifiers.

Performance Analysis of AI Classifiers

The performance of numerous AI classifiers, which includes Random Forest (RF), Decision Tree (DT), Perceptron, Gaussian Naive Bayes (GaussianNB), and Support Vector Machine (SVM), was evaluated. The RF classifier carried out the pleasant with an accuracy of 98.46%, outpacing the opposite models in phrases of category accuracy. SVM, even as effective for high-dimensional data, turned into computationally steeply-priced and sluggish, specifically with noisy datasets. The GaussianNB classifier struggled with the dataset because of its assumption of function independence, which did now not hold true. Precision, bear in mind, and F1 score metrics similarly highlighted the RF classifier's superiority in classifying malicious and non-malicious facts.

Table1. Comparison of AI models performance for different metrics.

AI Models	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
RF	98.46	97.56	95.55	96.65
SVM	59.76	59.41	57.65	58.89

Decision tree	95.71	97.56	96.53	94.45
Perceptron	94.22	92.23	87.23	93.32
GaussianNB	86.42	81.23	78.34	85.43

ROC Curve Evaluation

The Receiver Operating Characteristic (ROC) curve became used to evaluate the performance of the classifiers. The RF classifier established advanced performance, with its ROC curve being towards the threshold price (zero.Zero), indicating higher sensitivity and specificity. The other classifiers showed much less most fulfilling performance, with their ROC curves towards the 45-diploma diagonal, indicating reduced effectiveness in distinguishing among training.

Training Time Comparison

Training time changed into every other critical issue evaluated at some point of the test. The RF classifier proven the shortest training time of 28.641 seconds, making it greater suitable for real-time programs. This efficiency is attributed to RF's ensemble approach, which allows parallel processing and decreases the hazard of overfitting, ultimately rushing up the education process.

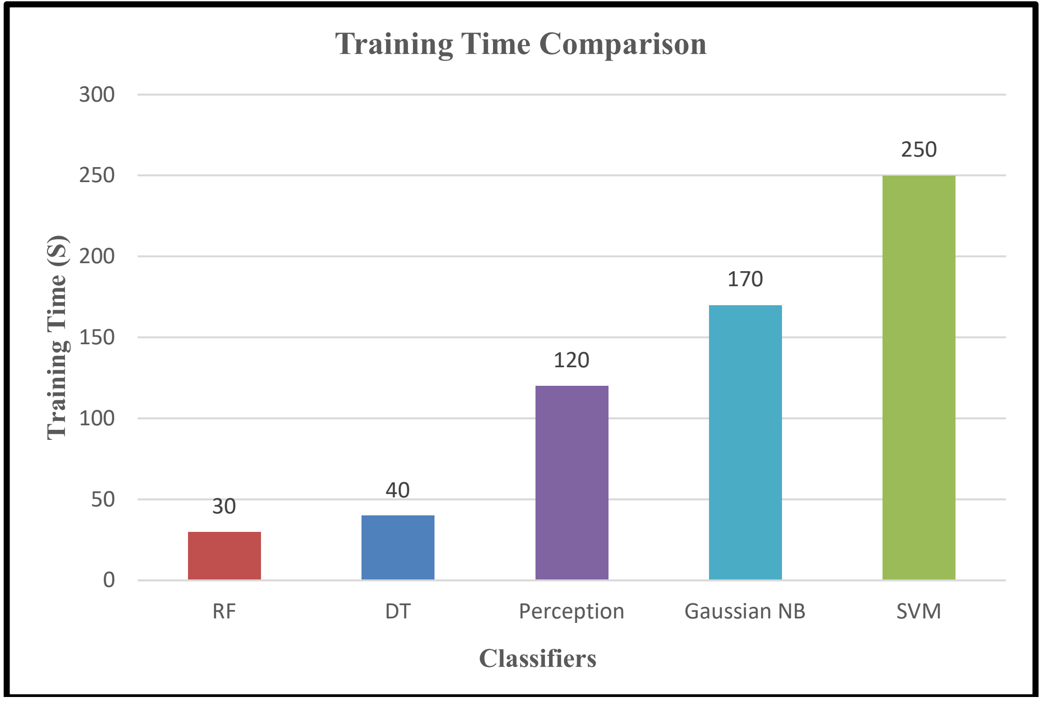

Figure :2, Training Time Comparison

Data Poisoning Attack Detection

A protection assessment was conducted to mitigate information poisoning assaults. Anomalous information factors, that can skew the classification results, had been detected and removed the usage of outlier detection techniques. This process ensured that simplest valid, accurate statistics had been handed to the classifiers, improving the overall accuracy and security of the IoT system. By addressing the statistics poisoning attack, the machine turned into capable of avoid

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

misclassification and preserve strong overall performance.

V. FINDING AND DISCUSSION

Machine Learning Models Comparison

In this observe, numerous machine studying models were evaluated to predict protection chance stages in fog computing environments. The fashions taken into consideration include Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Naive Bayes (NB), Random Forest (RF), and the ensemble model CyberGuard. These fashions have been assessed using overall performance metrics which include precision, take into account, and F1-score to determine their performance in classifying safety dangers. The effects highlighted the significance of information preprocessing and function selection in improving model performance. Among the models tested, CyberGuard, the ensemble version, validated the most promising outcomes by using combining the predictions of multiple classifiers for greater correct and reliable threat stage prediction.

Table 2. Comparison of Machine Learning Models for Security Threat Prediction

Model	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Support Vector Machine (SVM)	85.6	82.3	83.9
K-Nearest Neighbors (KNN)	88.1	84.2	86.1
Naive Bayes (NB)	82.4	80.6	81.5
Random Forest (RF)	98.4	97.1	97.7
CyberGuard (Ensemble Model)	99.2	98.8	99.0

CyberGuard Model Performance

The CyberGuard version, which integrates numerous base models, confirmed superior performance in predicting safety threats as compared to man or woman machine learning fashions. By leveraging an ensemble approach, CyberGuard changed into capable of provide a more correct evaluation of protection dangers. This model proven its ability to combine numerous enter from various classifiers, enhancing its predictive functionality. The expected CPU and memory utilization from the CyberGuard version highlighted a sturdy correlation with extraordinary security risk tiers, displaying clear clusters or patterns that corresponded to varying degrees of chance.

Data Locality Optimization

The distribution of statistics locality, which refers back to the proximity of records resources to fog computing nodes, changed into an critical issue in optimizing useful resource allocation. By analyzing the distribution of facts locality, we may want to discover trends that help in selecting the great places for facts processing. This statistics is crucial for optimizing the placement of computational assets inside a fog computing device, making sure efficient records go with the flow, and mitigating safety threats associated with resource distribution.

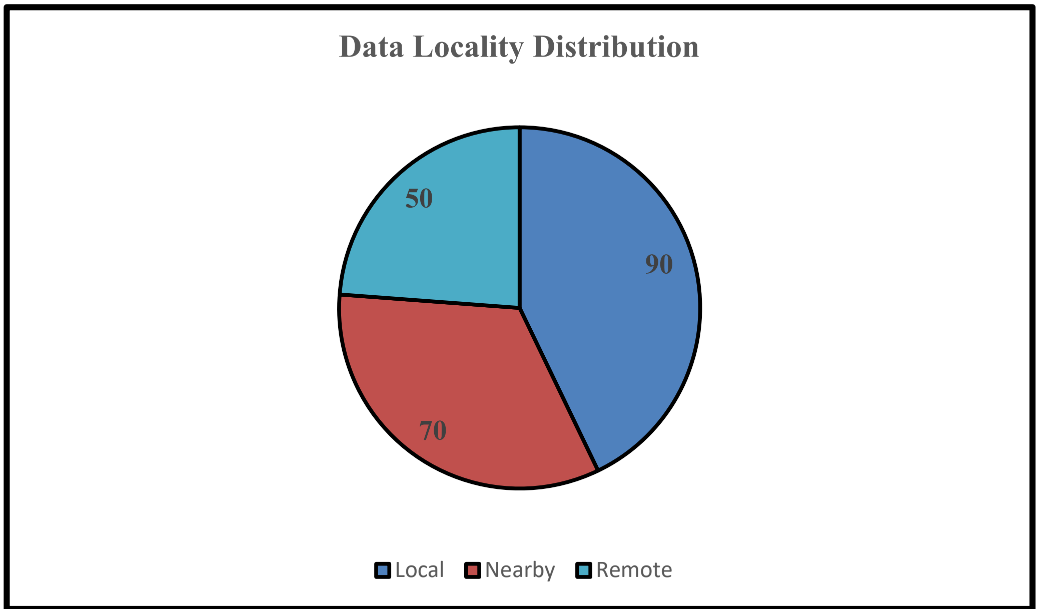

Figure : 3, Data Locality Distribution

Trust Score Prediction and Blockchain Validation

Another key thing of the take a look at became the assessment between expected believe rankings from the CyberGuard model and real blockchain validation status. Trust rankings, which verify the reliability of fog/part nodes, had been as compared with the blockchain validation status of facts factors. This comparison demonstrated the version's ability to correctly predict the trustworthiness of nodes, making sure the integrity of the gadget. By aligning consider scores with blockchain validation, the CyberGuard version showed its reliability in dealing with trust and safety inside a fog computing environment.

Security Threat Level Distribution

The distribution of security chance degrees throughout the fog computing surroundings changed into examined to apprehend the frequency of diverse hazard kinds. This distribution is important for assessing the general security panorama and identifying capability vulnerabilities within the machine. By analyzing the spread of threat stages, the look at helped examine the model's accuracy in predicting these tiers throughout the dataset. The CyberGuard version proved powerful in classifying and predicting protection threat ranges, supplying insights into machine vulnerabilities and the relative importance of potential security dangers.

Conclusion

The comparison of machine gaining knowledge of fashions discovered that ensemble strategies, specifically the CyberGuard version, are exceedingly effective in predicting security dangers in fog computing environments. By utilizing functions together with CPU and reminiscence usage, information locality, and consider scores, the version supplied dependable predictions of safety threats. These findings endorse that integrating device learning, blockchain security, and optimized resource allocation can significantly enhance the safety and efficiency of fog computing systems, especially in IoT-driven packages which includes agriculture.

VI. CONCLUSION

The integration of blockchain safety, AI-based mastering, and advanced cybersecurity measures in IoT-driven agriculture has brought about the improvement of a robust framework for handling security challenges. The CyberGuard model, using ensemble learning with SVM, KNN, and RF, accomplished notable effects with 98.18% accuracy, 98.22% precision, and 98.18% keep in mind, outperforming person classifiers. Blockchain era ensures tamper-evidence statistics control, improving the integrity and safety of IoT tool interactions. Feature engineering strategies like PCA and XAI optimized the dataset, decreased dimensionality, and stepped forward computational efficiency while retaining interpretability. Anomaly detection safeguarded the device towards statistics poisoning assaults, making sure reliable AI classifier overall performance. Secure storage of vital statistics turned into completed the use of IPFS-pushed blockchain networks, in addition strengthening the system's reliability. CyberGuard's adaptability to diverse protection situations highlights its software in agricultural IoT structures and different vital infrastructures. The framework provides actual-time chance detection and mitigation, addressing each operational and safety demanding situations comprehensively. Future paintings will discover the use of artificial datasets simulated in MATLAB to validate and enhance the model's adaptability in dynamic environments. Comparative analysis of artificial and real-time records will in addition establish its efficacy. CyberGuard's integration with technology like NFV, SDN, and 5G offers capability for scaling and enhancing IoT protection. This framework marks a good sized development in IoT protection with the aid of imparting a scalable and green answer for safeguarding information and ensuring operational continuity. By addressing emerging threats, it complements machine resilience and contributes to the secure deployment of IoT networks in agriculture and past.

VII. REFERENCE

1. K. A. Patil and N. R. Kale, "A model for smart agriculture using IoT", *Proc. Int. Conf. Global Trends Signal Process. Inf. Comput. Commun. (ICGTSPICC)*, pp. 543-545, Dec. 2016.

2. M. S. Farooq, S. Riaz, A. Abid, T. Umer and Y. B. Zikria, "Role of IoT technology in agriculture: A systematic literature review", *Electronics*, vol. 9, no. 2, pp. 319, Feb. 2020.

3. F. Sabrina, S. Sohail, F. Farid, S. Jahan, F. Ahamed and S. Gordon, "An interpretable artificial intelligence based smart agriculture system", *Comput. Mater. Continua*, vol. 72, no. 2, pp. 3777-3797, 2022.

4. S. A. Bhat and N.-F. Huang, "Big data and AI revolution in precision agriculture: Survey and challenges", *IEEE Access*, vol. 9, pp. 110209-110222, 2021.

5. M. Javaid, A. Haleem, I. H. Khan and R. Suman, "Understanding the potential applications of artificial intelligence in agriculture sector", *Adv. Agrochem*, vol. 2, no. 1, pp. 15-30, Mar. 2023.

6. W. Liu, X.-F. Shao, C.-H. Wu and P. Qiao, "A systematic literature review on applications of information and communication technologies and blockchain

technologies for precision agriculture development", *J. Cleaner Prod.*, vol. 298, May 2021.

7. A. R. de A. Zanella, E. da Silva and L. C. P. Albini, "Security challenges to smart agriculture: Current state key issues and future directions", *Array*, vol. 8, Dec. 2020.

8. V. Sharma, A. K. Tripathi and H. Mittal, "Technological revolutions in smart farming: Current trends challenges & future directions", *Comput. Electron. Agricult.*, vol. 201, Oct. 2022.

9. Bolanos, Juan, A Holistic Framework for AI-Driven Cyber Risk Management in Iot Ecosystems (November 27, 2023). Available at SSRN: https://ssrn.com/abstract=4639066 or http://dx.doi.org/10.2139/ssrn.4639066

10. Mustafa R, Sarkar NI, Mohaghegh M, Pervez S. A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. Sensors (Basel). 2024 Nov 11;24(22):7209. doi: 10.3390/s24227209.

11. Abdullahi M., Baashar Y., Alhussian H., Alwadain A., Aziz N., Capretz L.F., Abdulkadir S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics. 2022;11:198. doi: 10.3390/electronics11020198.

12. F. Al-Mufti, M. Kim, V. Dodson, T. Sursal, C. Bowers, C. Cole, et al., "Machine learning and artificial intelligence in neurocritical care: a specialty-wide disruptive transformation or a strategy for success", *Current neurology and neuroscience reports*, vol. 19, pp. 1-7, 2019.

13. N. A. A. Abdu and Z. Wang, "Blockchain for Healthcare Sector-Analytical Review", *In IOP Conference Series: Materials Science and Engineering*, vol. 1110, no. 1, pp. 012001, 2021, March.

14. J. P. Richardson, C. Smith, S. Curtis, S. Watson, X. Zhu, B. Barry, et al., "Patient apprehensions about the use of artificial intelligence in healthcare", *NPJ digital medicine*, vol. 4, no. 1, pp. 140, 2021.

15. M. Javaid, A. Haleem, R. P. Singh, S. Khan and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review", *Blockchain: Research and Applications*, vol. 2, no. 4, pp. 100027, 2021.

16. B. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, K. Shankar, Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment, Pers. Ubiquitous Comput., 5 (2021). https://doi.org/10.1007/s00779-021-01543-2

17. A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, B. G. Kim, Blockchain-based smart contracts for the Internet of Medical Things in e-healthcare, Electronics, 9 (2020), 1609. https://doi.org/10.3390/electronics9101609

18. S. Chakraborty, V. Bhatt, T. Chakravorty, Impact of IoT adoption on agility and flexibility of healthcare organization, Int. J. Innovative Technol. Exploring Eng., 8 (2019), 2673–2681. https://doi.org/10.35940/ijitee.K2119.0981119

19. Y. S. Jeong, S. S. Shin, An IoT healthcare service model of a vehicle using implantable devices, Cluster Comput., 21 (2018), 1059–1068. https://doi.org/10.1007/s10586-016-0689-z

20. Ray, R. K., Chowdhury, F. R., & Hasan, M. R. (2024). Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection. *Journal of Business and Management Studies*, *6*(1), 206-214. https://doi.org/10.32996/jbms.2024.6.1.13

21. Tully, J., Selzer, J., Phillips, J. P., O'Connor, P. & Dameff, C. Healthcare challenges in the era of cybersecurity. *Health Secur.* **18**, 228–231 (2020).

22. Shrimali, B. & Patel, H. B. Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities. *J. King Saud Univ. Comput. Inf. Sci.* **34**(9), 6793–6807 (2021).

23. Askar, A. J. Healthcare management system and cybersecurity. *Int. J. Recent Technol. Eng.* 237–248 (2019).

24. Thomasian, N. M. & Adashi, E. Y. Cybersecurity in the internet of medical things. *Health Policy Technol.* **10**, 100549 (2021).

25. Muheidat, F. & Tawalbeh, L. A. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* 3–29 (Springer, 2021).