This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ITIKD63574.2025.11005327, 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)

Emergent Intrusion Detection System for Fog enabled Smart Agriculture Using Federated Learning and Blockchain Technology: A Review

Vijayalakshmi Chakravarthy
Department of Computer Science
Brunel University of London
Middlesex, UB8 3PH, UK
2164988@brunel.ac.uk

David Bell
Department of Computer Science
Brunel University of London
Middlesex, UB8 3PH, UK
david.bell@brunel.ac.uk

Subhashini Bhaskaran
Multimedia Science Department
Ahlia University
Manama, Bahrain
sbhaskaran@ahlia.edu.bh

Abstract*— The rapid evolution of smart agriculture has revolutionized traditional farming practices by integrating Internet of Things (IoT), artificial intelligence (AI), and fog computing to enhance productivity, efficiency, and sustainability. However, this increasing interconnectivity also exposes smart agricultural systems to cybersecurity vulnerabilities, necessitating robust and adaptive Intrusion Detection Systems (IDS). This paper presents a comprehensive review of the latest advancements in intrusion detection for fog-enabled smart agriculture, focusing on the synergistic integration of federated learning (FL) and blockchain (BC) technologies. FL enables collaborative privacy-preserving anomaly detection across distributed agricultural IoT nodes, mitigating data exposure risks. Meanwhile, blockchain strengthens security by providing decentralized trust management, immutable logging, and secure model aggregation in FL-based IDS. We analyze existing state-of-the-art approaches, highlight their advantages and limitations, and discuss emerging challenges, such as adversarial attacks, computational overhead, data heterogeneity, and communication constraints in FL-based IDS frameworks. Furthermore, we examine how blockchain enhances the resilience of federated learning against security threats while maintaining system integrity in real-world smart farming applications. This review also proposes a novel system architecture that optimally integrates fog computing, federated learning, and blockchain to enhance intrusion detection accuracy, energy efficiency, and system resilience in smart agriculture. The insights provided in this review aim to guide researchers and practitioners in developing next-generation, secure, and adaptive intrusion detection frameworks for future cyber-resilient smart agriculture.

Keywords*— *Smart Agriculture, Intrusion Detection Systems, Fog Computing, Federated Learning, Blockchain.

I. INTRODUCTION

The incorporation of cutting-edge technologies in agriculture has led to smart farming, utilizing the Internet of Things (IoT), machine learning, and big data analytics to enhance productivity (Deniz & Gülçin, 2024) [1]. Smart farming technologies and precision agriculture [2] are gaining more attraction for their potential to fulfill the increasing demand and meet global food supply needs. However, the increased connectivity of smart agriculture raises concerns about security vulnerabilities and cyber threats. Traditional detection mechanisms face challenges with the scalability, privacy, and adaptability needed for such environments. As systems evolve, the need for intelligent intrusion detection systems (IDS) become essential to safeguard the agricultural infrastructures. Consequently, the emerging concepts like fog computing, federated learning and blockchain technology provide promising solutions through decentralized, privacy-preserving, and tamper-proof security mechanisms in smart agriculture.

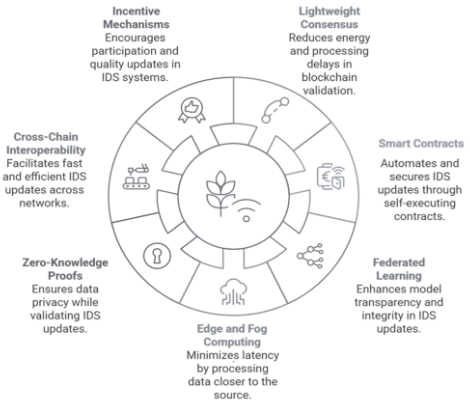

Fig. 1. Optimization of IDS for Smart Agriculture

Intrusion detection systems have been extensively explored to secure IoT environments, with various approaches addressing unique challenges. Hybrid models can achieve rapid detection of known threats through signature-based methods while improving accuracy for unknown threats using machine learning-based anomaly detection [3]. However, challenges remain, including the need for up-to-date datasets, methodologies for zero-day attack detection, and consideration of system usability in on-device detection. Centralized IDS systems aggregate data onto a single server for analysis, providing centralized control and efficient model updates. However, centralized systems are prone to bottlenecks and inefficiencies in geographically distributed networks. In contrast, decentralized IDS, such as peer-to-peer

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ITIKD63574.2025.11005327, 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)

systems, distribute intelligence across devices, improving privacy and reducing reliance on central servers. However, these systems often face challenges related to incomplete information sharing and vulnerabilities to compromised peers. Distributed multi-level IDS, such as fog-cloud hierarchical systems [4] reduce response times and conserve resources by processing data closer to the source. Despite these advantages, such systems often require raw data sharing between layers, raising privacy concerns. To overcome these limitations, federated learning (FL) has emerged as a promising paradigm for intrusion detection [5]. FL enables collaborative model training without transferring raw data, preserving user privacy while leveraging collective knowledge [6]. Despite these advancements, FL faces challenges in heterogeneous IoT environments, including varying device capabilities, communication constraints, and vulnerabilities to malicious model updates. Blockchain technology has gained attention for its ability to enhance security, privacy, and trust in distributed systems, making it a natural complement to IDS and FL [7]. In the context of IDS, blockchain provides a decentralized and immutable ledger to securely record intrusion detection events, improving auditability and trust [8]. Building on these advancements, our work integrates blockchain technology with FL to optimize a robust, privacy-preserving intrusion detection framework for smart architecture as shown in Fig. 1.

This review highlights the integration of state-of-the-art IDS solutions within the context of fog computing and advanced technologies such as federated learning and blockchain to enhance IDS in a decentralized and privacy-preserving manner, which is particularly vital in smart agriculture environments. The paper also proposes a new system architecture that optimizes the integration of fog computing, federated learning, and blockchain offering insights into how security can be tailored to this architecture. This forward-looking approach aims to conceptualize a more efficient and secure framework tailored for the specific needs of smart agriculture.

II. Intrusion Detection for Fog Enabled Smart Agriculture

Fog computing as shown in Fig. 2, is an extension of cloud computing, allowing for decentralized data processing at the edge of the network that significantly benefits agricultural

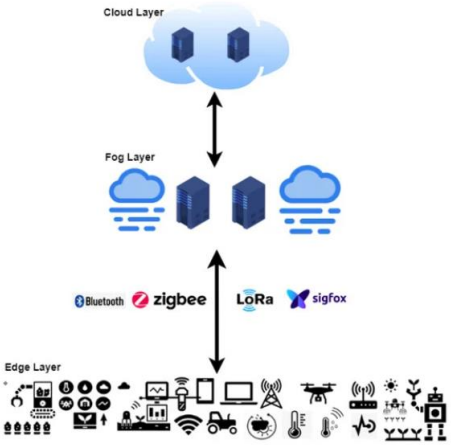

Fig. 2. Three-tier architecture for Smart Agriculture [9]

operations by providing reduced latency, real-time analytics and decision-making capabilities. However, the distributed nature of fog nodes makes them susceptible to security threats such as data breaches, denial-of-service (DoS) attacks, and insider threats [10]. So, the integration of IDS within fog enabled smart agriculture is crucial for enhancing security and ensuring data integrity. However, implementing IDS in fog enabled smart agriculture poses several challenges, including limited computational resources at edge nodes and the dynamic nature of agricultural operations. To mitigate these challenges, lightweight IDS solutions that employ machine learning algorithms can enhance performance without overwhelming the network resources [11]. Table I shows the literature reviewed on the IDS for fog-enabled smart agriculture. It suggests using different datasets and performance metrics to improve model robustness, and proposes incorporating advanced machine learning techniques to improve IDS effectiveness and adaptability. Thus, the table emphasizes energy-efficient, scalable, and real-world deployable IDS solutions, particularly in fog-enabled federated learning environments for smart agriculture.

III. Federated Learning for Intrusion Detection

Federated Learning (FL) allows multiple distributed devices to train machine learning models without sharing raw data, preserving data privacy [12]. Recent research has explored FL for IDS in various domains. Fig. 3 shows the general architecture of federated learning. FL-Based IDS studies demonstrate improved detection accuracy while maintaining privacy [13]. The authors [14] proposed a

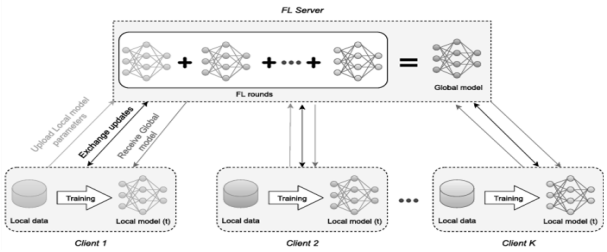

Fig. 3. General architecture of Federated Learning [14]

federated learning-based intrusion detection system (FELIDS) that aims to protect data privacy while enhancing the detection of cyberattacks in Agri-IoT networks. The system employed

TABLE I. Literature on IDS in Fog-Enabled Smart Agriculture

Author	Methodology	Key Findings	Limitations	Future Directions
[15]	Proposes a hybrid deep learning model combining CNN, Bi-GRU and WHO algorithm.	Achieved 99.35%, 99.71% accuracy on DDoS Attack, ToN-IoT Datasets respectively.	Need for extensive computational resources for training the deep learning models, may not cover all possible attack scenarios in smart farming, overfitting.	Integrating more advanced technologies for improvement, different performance metrics and datasets could be explored.

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI: 10.1109/ITIKD63574.2025.11005327, 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)

[16]	Detects malicious UAV behavior through a machine-learning model deployed at the UAVs in a simulated farm.	The proposed IDS using XGBoost achieved 99.77% accuracy.	Scalability, real-world testing, attack variability.	Machine vision integration, real-world deployment, enhanced security measures, energy optimization
[17]	Effectively addresses class imbalance, feature selection and classification using SMOTE, RFE, PSO and CNN	Achieved high performance with an accuracy 99.99% NSL KDD data set.	Limits the generalizability of the findings to other datasets/ real-world scenarios, relies on pre-trained CNN models.	Investigating the integration of other advanced machine learning techniques to further enhance the performance and robustness of the IDS.

three deep learning classifiers—Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs)—to detect intrusions using three recent datasets CSE-CIC-IDS2018, MQTTset, and InSDN, and achieved the accuracy of 93.29%, 94.09%, and 94.15% for DNN, CNN, and RNN respectively. The results showed that FELIDS achieves comparable or better accuracy while preserving data privacy. Challenges in FL for IDS include communication overhead, data heterogeneity, and adversarial attacks [18].

Literature on federated learning for intrusion detection is shown in Table II. The table shows FL presents a promising solution for intrusion detection in smart agriculture but faces critical challenges in data heterogeneity, security vulnerabilities, and communication constraints. It suggests the future work that focus on optimizing FL for non-IID data, enhancing security measures, and reducing communication overhead, particularly in fog-enabled federated learning environments for real-time IDS deployment. Furthermore, the comparative analysis of IDS approaches for IoT Security is shown in Table III. The table presents various intrusion detection system methodologies applied to Industrial IoT (IIoT) and IoT networks, evaluating their effectiveness based on different performance metrics while also highlighting limitations. While the proposed methodologies demonstrate high accuracy, most models lack in real-world validation, testing on modern IIoT datasets, device-specific vulnerability classification and handling encrypted traffic. So, the future research should enhance real-world testbeds, encrypted traffic detection, modern IIoT datasets in fog-enabled federated learning-based IDS for IIoT.

IV. BLOCKCHAIN FOR SECURE FEDERATED LEARNING IN SMART AGRICULTURE

Blockchain technology as shown in Fig. 4 provides a decentralized, immutable ledger to enhance security in federated learning frameworks [18]. It offers some services and benefits for IoT such as smart contracts, peer-to-peer network, secure and transparent exchange of information and assets without the need for a central authority, encrypted data transmission between devices. Blockchain are used in IoT environments for different purposes including positioning, security, privacy, incentives, decentralization, and audit at different IoT layers [19]. The paper [20] presents a decentralized federated learning framework termed Fed-Trust, which integrates a temporal convolutional generative network (TCGAN) for semi-supervised detection of cyberattacks in IIoT environments. The Fed-Trust framework is deployed in a distributed manner leveraging fog computing servers, thus optimizing the resource-constrained edge nodes within the IIoT environment using ToN_IoT and LITNET-2020 datasets, achieving 92.05% and 93.13% respectively. The authors of [7] proposed a Blockchain and FL-based secure architecture for enhanced external intrusion detection in smart farming. Federated Learning is utilized for privacy preservation-based external intrusion detection-based ensemble learning and smart land data authentication as the PoAh consensus algorithm offers aggregated gradient values, which is part of Blockchain technology. The performance of the proposed secured architecture was better than existing works with the average processing time 3.663 secs, and the accuracy 99.56%. Literature on blockchain for secure federated learning in fog enabled smart agriculture is shown in Table IV. The table provides a comparative analysis of blockchain, fog computing, and federated learning integration within IoT and smart agriculture applications. It highlights methodologies, key findings, limitations, and future directions across four studies. The studies provide valuable insights into

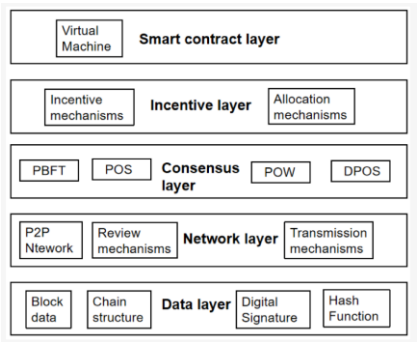

Fig.4. Blockchain architecture [21]

the convergence of blockchain, fog computing, and federated learning in IoT-based smart agriculture. However, challenges remain in scalability, security standardization, computational efficiency, and real-world implementation. Future work should focus on real-world testing, AI-driven intrusion detection, and post-quantum cryptography to enhance privacy, security, and efficiency in decentralized agricultural ecosystems.

TABLE II. LITERATURE STUDY ON FEDERATED LEARNING FOR INTRUSION DETECTION

Category	Description
Methodology	• The methodology involves implementing federated learning frameworks across various edge devices within smart agricultural environments. Key algorithms utilized include Federated Averaging (FedAvg) and secure aggregation techniques to enhance data privacy while facilitating collaborative model training [12]. • Data from IoT devices are used to train intrusion detection models without transferring raw data to a centralized server, ensuring compliance with privacy regulations [22].

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI: 10.1109/ITIKD63574.2025.11005327, 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)

Key Findings	• Research indicates that federated learning is secure and reliable and can significantly contribute to the rapid and efficient detection and prevention of various threat vectors that target IoT ecosystems [23]. • Research analyses federated learning for heterogeneous Anomaly detection systems based on different environments and applications; Various types of IDS, relevant ML approaches and its associated issues with possible solutions to establish the need for FL were also investigated [24].
Limitations	• Despite its advantages, federated learning faces challenges such as heterogeneous data distributions across devices, which can impact model convergence. Additionally, issues related to communication overhead and the requirement for robust device connectivity can hinder real-time performance in deployment settings [25]. • A single malicious participant in federated learning can completely replace the joint model with another one that has the same accuracy but also incorporates backdoor functionality [26].
Future Directions	• Federated neural architecture search (FNAS) is an emerging research direction. Handling non-IID problems in FNAS and applying heuristic optimization algorithms may be an interesting future direction [27]. • Need for more efficient and secure aggregation algorithms and the use of model compression or sparsification techniques to solve the communication bottleneck of the federated learning systems; Need for a well-designed incentive mechanism to encourage data owners to participate in federated Learning systems [28].

TABLE III. COMPARATIVE ANALYSIS OF IDS APPROACHES FOR IOT SECURITY

Reference	**Methodology**	**Performance Metrics**	**Limitation**
[29]	Proposed an IDS for IIoT using the Genetic Algorithm (GA) and RF, LR, NB, DT, ET, XGB using UNSW- NB15.	Acc = 87.61 VAC =95.87 Rc =98.34 Pr =82.51 F1 =89.73 Auc =98	Methodology is not implemented in datasets such as ToN_IoT, UNSW-NB15 and AWID etc. that contain traffic patterns generated by IIoT devices.
[30]	Proposed the federated-learning (FL) -based anomaly detection approach to proactively recognize intrusion in IoT networks using decentralized on-device data.	Acc = 90.255%	A testbed of IoT devices and evaluation with live data from device-specific data sets to classify all known and unknown vulnerabilities of IoT devices are not done.
[31]	proposed an intelligent intrusion detection mechanism- FedACNN, by assisting CNN through the federated learning mechanism.	Acc = 99.76%	Intrusion detection on encrypted traffic data of edge-assisted IoT is not done.

V. PROPOSED SYSTEM ADDRESSING OPEN CHALLENGES AND FUTURE DIRECTIONS

Therefore, from the literature, it is very clear that despite capable advancements, several challenges such as efficient resource utilization, adversarial attacks and interoperability etc. remain in the smart agriculture. As the agricultural sector increasingly adopts IoT devices, the associated cybersecurity risks necessitate robust security solutions to protect sensitive information and ensure data integrity. In consequence, the review has distinctly spotlighted the enhancement of intrusion detection systems within fog enabled smart agriculture, focusing on the integration of federated learning and blockchain technology. Federated learning emerges as a promising framework, allowing for collaborative model training across distributed devices while preserving data privacy. However, challenges such as communication overhead and data heterogeneity remain significant hurdles to its effective implementation. Simultaneously, blockchain technology offers a decentralized approach to enhance security and trust within federated learning frameworks, though issues regarding scalability and resource demands need to be addressed for broader adoption.

Considering these observations, we intend to propose our future system aims to optimize the integration of fog computing, federated learning and blockchain to mitigate computational and storage overhead while developing robust defenses against potential adversarial attacks for smart agriculture as shown in Fig. 5. Fig. 6 shows the flow diagram illustrating the proposed intrusion detection system. The flow diagram provides a systematic, privacy-preserving approach for intrusion detection in IoT environments using federated learning and blockchain. It effectively distributes computation across edge and fog nodes, enhances security through blockchain smart contracts, and reduces data transmission overhead. However, challenges such as computational complexity, communication overhead, and potential

TABLE IV. LITERATURE ON BLOCKCHAIN FOR SECURE FEDERATED LEARNING IN FOG ENABLED SMART AGRICULTURE

Category	**Description**			
Author	[32]	[33]	[34]	[35]
Paper	Exploring the synergy of fog computing, blockchain, and federated learning for IoT applications: a systematic literature review	Blockchain-Enabled Smart Agricultural Knowledge Discovery System using Edge Computing	A systematic review of the purposes of blockchain and fog computing integration: classification and open issues	AgriSecure: a fog computing-based security framework for agriculture 4.0 via Blockchain
Methodology	A SLR methodology following Kitchenham & Charters' guidelines to investigate the integration of fog computing, blockchain, and federated	Proposes integration of IoT, blockchain, and edge computing, use of Hyperledger, ML algorithms to analyze data and generate knowledge patterns	A SLR methodology following Kitchenham & Charters' guidelines and Geographically Distributed Agile Development (GDAD) empirical studies.	Proposes a security framework that includes sensor layer, fog computing layer, distributed network using SDN, and a blockchain-based network and is tested with DDoS attack to evaluate

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/ITIKD63574.2025.11005327, 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)

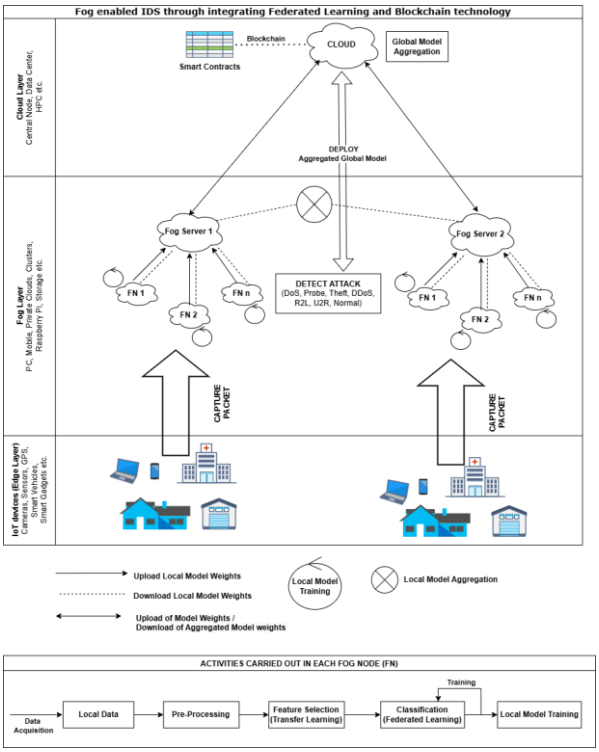

Fig. 5. Proposed Intrusion Detection System Architecture

	learning within IoT applications.			its performance.
Key Findings	The integration of FC, BC, and FL within IoT applications offers security, privacy, and performance standards	Improved Data Management, Enhanced Decision Making, Increased Crop Yield, Security and Privacy	Major advances in terms of security, privacy, data management, and trust management.	Improved performance during a DDoS attack, network management, and security
Limitations	Complexity, Security Concerns, Data Privacy and Regulation, Performance Overhead, Ethical Issues	Complexity, Cost, Scalability	Scalability, Lack of Standards and Regulations, Quantum resilience, Artificial intelligence, and Big data analysis.	Does not address other potential security threats in Agriculture 4.0, limited to a simulated environment, Scalability and performance in large-scale deployments were not tested.

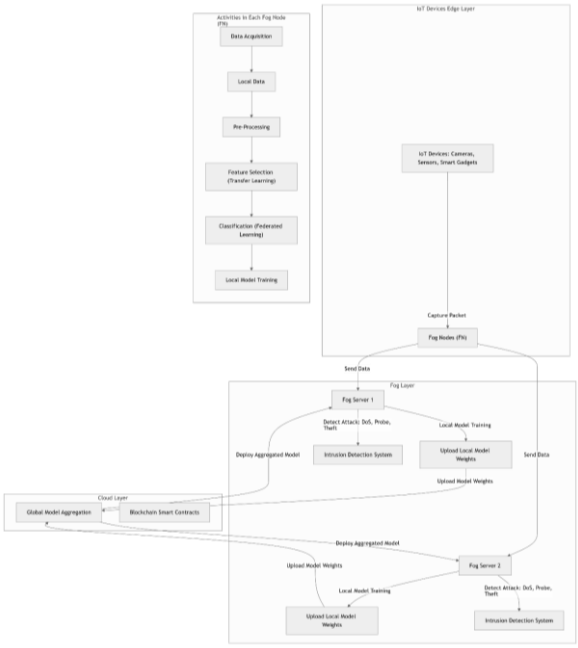

Fig. 6. Flow diagram of the Proposed Intrusion Detection System

Future Directions	Develop guidelines to facilitate existing frameworks, Establish industry standards to ensure interoperability, Extend to diverse network environments like Mobile/RAN Networks (e.g., 5G and 6G).	Extending the system to develop analysis based on personalized recommendations, Enhanced ML models Integration with 5G broader adoption	As a result of network-wide storage transactions, storage needs to be raised, On a worldwide scale competent and uniform rules and regulations are necessary, Evaluation and standardization of post-quantum cryptography primitives are required.	Incorporating ML methods to security framework, Developing an intrusion detection system using various DL algorithms, Expanding the framework to address a broader range of security threats and vulnerabilities in Agriculture 4.0, Conducting real-world deployments and testing scalability in diverse agricultural settings.

bottlenecks at fog servers must be addressed for real-world scalability. By addressing these challenges, stakeholders can foster a more secure and efficient agricultural ecosystem that leverages cutting-edge technological advancements.

VI. CONCLUSION

The agricultural sector is increasingly adopting IoT devices for precision farming, which generate vast amounts of data. Smart farming enhances conventional farming practices by introducing on-field smart sensors and devices. Though the use of heterogeneous, internet-connected devices has exposed potential cyber-attacks and vulnerabilities in the agriculture sector. These attacks introduce the ability to remotely control and exploit on-field sensors and autonomous vehicles

(tractors, aerial vehicles, etc.). Potential agricultural attacks can create an unsafe and unproductive farming environment. This creates a need for robust security mechanisms to protect sensitive information and prevent unauthorized access. Besides, detection mechanisms play a significant role in monitoring network traffic and identifying potential threats, thereby safeguarding agricultural data and systems [36]. This paper reviews state-of-the-art research and acknowledges important work related to security and privacy aspects in precision agriculture. We envisioned a clear shot that federated learning and blockchain technology could offer a transformative approach in enhancing IDS in fog enabled smart agriculture. Our further research work will be proceeded to implement and deploy the proposed intrusion detection system as shown in Fig. 5, using real time data and to evaluate its significant performance on smart agriculture as well as other IoT systems. As the agricultural landscape continues to evolve, future research will be vital in refining these technologies, enhancing their applicability, and ensuring the security of smart agricultural systems.

REFERENCES

[1] D. Uztürk and G. Büyüközkan, “Industry 4.0 technologies in smart agriculture: a review and a technology assessment model proposition,” Technological Forecasting and Social Change, Volume 208, 123640, ISSN 0040-1625. 2024. [Online]. Available: https://doi.org/10.1016/j.techfore.2024.123640.

[2] [Online]. Available: https://www.microsoft.com/en-us/research/project/farmbeats-iot-agriculture/

[3] N. Jeffrey, Q. Tan and J. R. Villar, "A hybrid methodology for anomaly detection in cyber–physical systems," Neurocomputing, Volume 568, 2024, 127068, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2023.127068.

[4] S. Roy, J. Li and Y. Bai, "A two-layer fog-cloud intrusion detection model for IoT networks," Internet of Things, Volume 19, 2022, 100557, ISSN 2542-6605. [Online]. Available: https://doi.org/10.1016/j.iot.2022.100557.

[5] V. T. Nguyena and R. Beuran, “FedMSE: Federated learning for IoT network intrusion detection”. arXiv 2024, [Online]. Available: arXiv:2410.14121.

[6] S. A. Rahman, H. Tout, C. Talhi and A. Mourad, "Internet of things intrusion detection: centralized, on-device, or federated learning?," in IEEE Network, vol. 34, no. 6, pp. 310-317, November/December 2020, doi: 10.1109/MNET.011.2000286.

[7] S. K. Singh, M. Kumar, A. Khanna and B. Virdee, "Blockchain and FL-based secure architecture for enhanced external intrusion detection in smart farming," in IEEE Internet of Things Journal, vol. 12, no. 3, pp. 3297-3304, 1 Feb.1, 2025, DOI: 10.1109/JIOT.2024.3478820.

[8] S. Mohammed, Md. R. Hasan, Y. Bai, and J. Li, "Enhancing smart home security: blockchain-enabled federated learning with knowledge distillation for intrusion detection," Smart Cities 8, no. 1: 35. 2025. [Online]. Available: https://doi.org/10.3390/smartcities8010035

[9] K. Yogeswaranathan, and R. Collier, "A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture," Sensors 21, no. 17: 5922. 2021. [Online]. Available: https://doi.org/10.3390/s21175922.

[10] C. Victor, L. Golightly, P. Modesti, Q.A. Xu, L.M.T. Doan, K. Hall, S. Boddu, and A. Kobusińska, "A survey on intrusion detection systems for fog and cloud computing," Future Internet 14, no. 3: 89. 2022. [Online]. Available: https://doi.org/10.3390/fi14030089

[11] S. Khanam, I.B. Ahmedy, M.Y. Idna Idris, M.H. Jaward and A.Q. Bin Md Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things," in IEEE Access, vol. 8, pp. 219709-219743. 2020, DOI: 10.1109/ACCESS.2020.3037359.

[12] H.B. McMahan, E. Moore, D. Ramage and S. Hampson, “Communication-efficient learning of deep networks from decentralized data,” Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 54, 1273-1282. 2017. [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a.html.

[13] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.C. Liang and Q. Yang, “Federated learning in mobile edge networks: a comprehensive survey,” IEEE Communications Surveys & Tutorials, 22(3), 2031-2063. 2020. DOI:10.1109/COMST.2020.2986024

[14] O. Friha, M.A. Ferrag, L. Shu, L. Maglaras, K.K.R Choo and M. Nafaa, “FELIDS: Federated learning-based intrusion detection system for agricultural internet of things,” Journal of Parallel and Distributed Computing, Volume 165, Pages 17-31, ISSN 0743-7315. 2022. [Online]. Available: https://doi.org/10.1016/j.jpdc.2022.03.003.

[15] K. Kethineni and G. Pradeepini, “Intrusion detection in internet of things-based smart farming using hybrid deep learning framework,” Cluster Comput 27, 1719–1732. 2024. [Online]. Available: https://doi.org/10.1007/s10586-023-04052-4

[16] S. Junaid, K. Hayawi, A.W. Malik, Z. Anwar and Z. Trabelsi, "A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming," Applied Sciences 13, no. 6: 3857. 2023. [Online]. Available: https://doi.org/10.3390/app13063857

[17] A. El-Ghamry, A. Darwish and A.E. Hassanien, “An optimized CNN-based intrusion detection system for reducing risks in smart farming,” Internet of Things, Volume 22, 100709, ISSN 2542-6605. 2023. [Online]. Available: https://doi.org/10.1016/j.iot.2023.1007094

[18] D. C. Nguyen, M. Ding, Q. Pham, P. N. Pathirana, L. B. Le, and A. Seneviratne, "Federated learning meets blockchain in edge computing: opportunities and challenges," in IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12806-12825, 15 August 15, 2021, DOI: 10.1109/JIOT.2021.3072611.

[19] Arshad, QuA., Khan, W.Z., Azam, F., Khan, M. K., Yu, H., and Zikria, Y. B., “Blockchain-based decentralized trust management in IoT: systems, requirements and challenges,” Complex Intell. Syst. 9, 6155–6176. 2023. [Online]. Available: https://doi.org/10.1007/s40747-023-01058-8

[20] M. Abdel-Basset, N. Moustafa and H. Hawash, "Privacy-preserved cyberattack detection in industrial edge of things (IEoT): A blockchain-orchestrated federated learning approach," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7920-7934, Nov. 2022, DOI: 10.1109/TII.2022.3167663.

[21] Ning, Weiguang, Yingjuan Zhu, Caixia Song, Hongxia Li, Lihui Zhu, Jinbao Xie, Tianyu Chen, Tong Xu, Xi Xu, and Jiwei Gao, "Blockchain-based federated learning: a survey and new perspectives," Applied Sciences 14, no. 20: 9459. 2024. [Online]. Available: https://doi.org/10.3390/app14209459

[22] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., & et al., “Advances and open problems in federated learning,” Foundations and Trends in Machine Learning, 14(1-2), 1-210. 2021. [Online]. Available: http://dx.doi.org/10.1561/2200000083).

[23] A. Vyas, P. -C. Lin, R. -H. Hwang and M. Tripathi, "Privacy-preserving federated learning for intrusion detection in IoT environments: a survey," in IEEE Access, vol. 12, pp. 127018-127050, 2024, DOI: 10.1109/ACCESS.2024.3454211.

[24] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta and Thippa Reddy Gadekallu, “Federated learning for intrusion detection system: concepts, challenges and future directions,” Cryptography and Security, 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2106.09527S.M. Kasongo, “An advanced intrusion detection system for IIoT based on GA and tree based algorithms,” IEEE Access 9. 2021. 113199-113212.

[25] Yang, Q., Liu, Y., Chen, T., and Tong, Y., “Federated machine learning: concept and applications,” ACM Transactions on Intelligent Systems and Technology, 10(2), 1-19. 2019. [Online]. Available: https://doi.org/10.1145/3298981

[26] Vitaly Shmatikov, “What are machine learning models hiding?,” CITP Blog - Formerly Freedom to Tinker. 2018. [Online]. Available: https://blog.citp.princeton.edu/2018/07/26/what-are-machine-learning-models-hiding/ (Accessed: 20/Feb/2025).

[27] Hangyu Zhu, Jinjin Xu, Shiqing Liu and Yaochu Jin, “Federated learning on non-IID data: A survey,” Neurocomputing, Volume 465, Pages 371-390, ISSN 0925-2312. 2021. [Online]. Available: https://doi.org/10.1016/j.neucom.2021.07.098.

[28] Žalik, Krista Rizman, and Mitja Žalik, "A review of federated learning in agriculture," Sensors 23, no. 23: 9566. 2023. [Online]. Available: https://doi.org/10.3390/s23239566.

.

[29] S.M. Kasongo, “An advanced intrusion detection system for IIoT based on GA and tree based algorithms,” IEEE Access 9. 2021. 113199-113212

[30] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 15 Feb.15, 2022, DOI: 10.1109/JIOT.2021.3077803.

[31] W. V. Solis, J. Marcelo Parra-Ullauri and A. Kertesz, "Exploring the synergy of fog computing, blockchain, and federated learning for IoT applications: a systematic literature review," in IEEE Access, vol. 12, pp. 68015-68060, 2024, DOI: 10.1109/ACCESS.2024.3398034.

[32] U Sakthi and J DafniRose, “Blockchain-enabled smart agricultural knowledge discovery system using edge computing,” Procedia Computer Science, Volume 202, Pages 73-82, ISSN 1877-0509. 2022. [Online]. Available: https://doi.org/10.1016/j.procs.2022.04.011.

[33] Alzoubi, Y.I., Gill, A. and Mishra, A, “A systematic review of the purposes of blockchain and fog computing integration: classification and open issues,” J Cloud Comp 11, 80. 2022. [Online]. Available: https://doi.org/10.1186/s13677-022-00353-y

[34] Padhy, Sasmita, Majed Alowaidi, Sachikanta Dash, Mohamed Alshehri, Prince Priya Malla, Sidheswar Routray, and Hesham Alhumyani, "AgriSecure: a fog computing-based security framework for agriculture 4.0 via blockchain" Processes 11, no. 3: 757. 2023. [Online]. Available: https://doi.org/10.3390/pr11030757

[35] M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and privacy in smart farming: challenges and opportunities," in IEEE Access, vol. 8, pp. 34564-34584, 2020, DOI: 10.1109/ACCESS.2020.2975142.