Towards Intrusion Detection Systems Dedicated to Agriculture Based on Federated Learning

Usman Rabiu ISAH, Pascal BERTHOME, and Laurent BOBELIN
Laboratoire d'Informatique Fondamentale d'Orléans, INSA Centre Val de Loire, France,
e-mail: firstname.lastname@insa-cvl.fr

***Abstract*—The recent advancements in technologies such as Artificial Intelligence, Internet of Things (IoT), drones, and embedded systems have led to significant changes in industrial systems architectures. This shift from simple systems to complex systems with hundreds of devices has made securing these systems difficult.**

Intrusion Detection Systems (IDS) are mandatory tools to secure them. IDS is an area where AI is used to detect malicious traffic on heterogeneous systems involving IoT, embedded systems, and more classic LAN. Machine learning (ML)and deep learning(DL) have been extensively explored as a means to automate IDS giving them an edge to detect new forms of attacks. In this research, we will focus on IDS for networks dedicated to agriculture.

***Index Terms*—Intrusion Detection System, IoT, Precision Agriculture, Machine Learning**

I. Introduction

The rise of IoT has led to significant changes in our day-to-day life. Industrial systems now consist of sensors and actuators, local gateways, and servers that are coupled together in a common architecture. The industrial system architecture can include various types of networks, such as ad-hoc vehicle networks, low-energy sensor and actuator networks, traditional computer networks, and networks composed of these elements. In this architecture the part of IoT devices is growing at a fast pace: by 2023 IoT devices will account for 50% of all networked devices. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018 [1].

In the field of Agriculture, this rapid development leads to the integration of IoT devices such as flying drones to detect diseases, tractors guided by tracking/positioning systems, temperature and hydrometry sensors, and watering actuators, all of which gather data to feed decision analysis systems for farmers [2]. IoT technology is revolutionizing agriculture by providing fast and reliable information, helping the sector to address the challenge of feeding a projected 9.8 billion people by 2050 [3]. IoT-powered automation and optimization of agricultural processes are leading to a fundamental change in traditional farming methods, helping to overcome age-old challenges in agriculture[4]. Significant research has been conducted on the uses and acceptance of IoT technologies in the field of smart agriculture [5], [6], [7], [8].

As the number of connected devices keeps increasing fast, IoT devices will carry insights worth 11 trillion dollars [9]: this has made those devices a target for cybercriminals. IoT devices are increasingly targeted due to their little to no security updates as well as weak credential usage [10]. IDS are means offered to monitor networks and detect potential intrusions. ML/DL has been used in several research to detect anomalies in IoT networks [11][12][13]. Training a machine learning model requires data that might be sensitive from the industrial perspective, federated learning (FL) allows decentralized training thus not sharing sensitive data. This research aims to develop an ML/FL based IDS specific to IoT networks dedicated to agriculture. The rest of the paper is organized as follows: Section II describes the devices, architecture, threats, and specificity of IoT networks in agricultural environments. Then Section III enumerates the application of ML and DL in IDS. Finally section IV presents our roadmap to develop FL-based IDS targeting networks dedicated to agriculture.

II. IoT in Agriculture

A. Devices

Sensors are the most common IoT devices used in agriculture today. They can monitor various parameters such as rain, moisture, humidity, temperature, and wind to help farmers forecast necessary actions to maintain high production levels. Other common

devices include actuators like automatic sprinklers, antifreeze towers, and farmbots, as well as flying drones used for monitoring and detecting problems on plots. (Autonomous) tractors are also connected devices that are often guided by GPS systems.

B. Architecture

Figure 1 gives an overview on how devices are usually coordinated using edge/fog architecture.

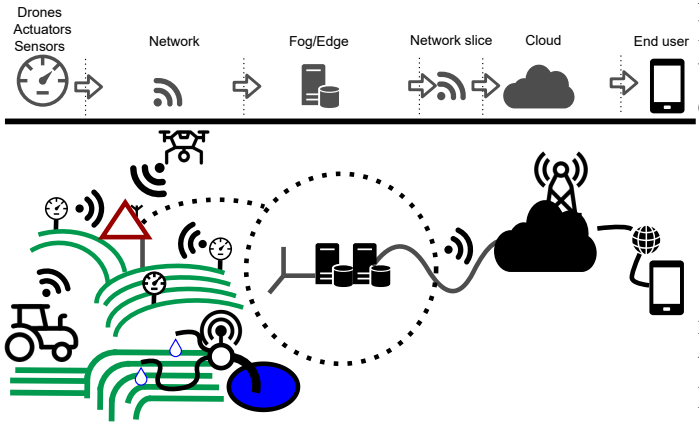

Fig. 1. A fully equipped agricultural exploitation

IoT devices in agricultural premises usually communicate with a gateway or with each other. Some devices may use LPWAN protocols and gateways antennas like LoRaWAN, while others may use wired communications or Bluetooth/WiFi to exchange with base stations[14]. Gateways communicate with each other using WAN or VLAN, to gather and analyze data.

C. Threats and specificity

War in Ukraine showed how food production is highly critical in case of conflicts: any part of the production chain, from fields to storage, is a potential target of cyber or physical attacks [15].

According to [1], there has been a 776% growth in attacks between 2018 to 2019 and the total number of DDOS attacks will double from 7.9 million in 2018 to 15.4 million by 2023. The threat volume is constantly growing. The Hacker News reported that there were about 134 million attempts to hack IoT devices by exploiting a common vulnerability as of December 2022 [16]. IoT devices in agriculture are connected to local and remote networks, making them vulnerable to network-based attacks such as denial-of-service (DoS) attacks and man-in-the-middle (MITM) attacks. These devices can be infected with malware, which can compromise the security of the device and the network it is connected to. Sensitive information such as farm layout, crop information, and weather data can be a target for data breaches.

One of the main challenges of in-field deployed devices is the lack of qualified personnel to repair or mitigate risks in case of an attack or failure. Additionally, most on-field deployed devices have low energy consumption requirements and it is usually not feasible to remotely stop an intrusion on a local system.

III. Intrusion Detection Systems and Machine Learning

IDS is a software or hardware system that monitors all activities within a given network and tries to detect malicious activity or data. IDS can be Host-based IDS (HIDS) deployed on the host system to detect any anomaly, or Network-based IDS (NIDS) deployed at the network edge. Anomaly-based IDS scans for activities and network data that deviate from specific patterns or baselines of usage. Signature-based IDS scans network packets and usage activity to detect similarities to known attacks. Both have limitations against unknown attacks and can generate false positives [17].

For decades, research are been conducted to improve the efficiency of IDS. The advances in artificial intelligence (AI) and machine learning (ML) have opened a new niche for research by incorporating ML into an IDS, for example, [12], [18], [13], [11], [2]. ML is able to deal with huge amounts of data produced by the boom in smart devices and high-speed networks. According to [1], 5G networks will generate traffic 3x compared to 4G networks. ML allows computer algorithms to learn from a large set of data and make predictions on unknown data. By integrating this feature, the efficiency of IDS has been improved to be able to detect an attack that is unknown to the system with high accuracy. FL is a new field in ML that allows decentralized training of models. With FL, the models(client) are trained individually using local data, after which the client model will update a global model maintained by an aggregator(server). The client does not send its training data to the server thus, the data will

remain where it is generated, thereby maintaining its privacy [19].

Various fields benefit from AI, but until recently only a few works focused on the possible application of AI to IDS [12], [18], [13], [11], [2]. IoT devices have limited processing capabilities coupled with weak security [10]. A significant number of research focus on IDS in IoT, but due to the nature of their deployment, IoT devices gather high volume sensitive data that need consideration. Some works proposed an FL approach to IDS [20], even some proposed an FL-based IDS for IoT [21].

IV. Road-map

INSA Centre Val de Loire is already involved in European MERIAVINO project [22], AGreen Tech Valley network [23], and uses a farmbot [24] as a research platform; working on those projects has helped us to identify challenges related to the security of such systems. Moreover, those projects give us access to IoT devices dedicated to agriculture, real platforms where those devices are deployed, and datasets. As a first step, we intend to setup simulation/emulation environments to reproduce the behavior we observed on the real platforms.

Then we will use these environments to develop and validate new solutions and algorithms to detect attacks on IoT devices in an agricultural setting. once validated in those environments, the solution will be deployed on real-life platforms to evaluate the performance in real conditions.

We hope to show that it is possible to secure IoT devices in agriculture and provide a safer, more secure environment for farmers and their crops.

References

[1] Cisco annual internet report (2018-2023)[white paper]. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

[2] Manishkumar Dholu and K.A. Ghodinde. Internet of things (iot) for precision agriculture application. In *2018 2nd (ICOEI)*, pages 339–342, 2018.

[3] UN DESA. World population projected to reach 9.8 billion in 2050. https://www.un.org/development/desa/en/news/population/world-population-prospects-2017.html.

[4] Muhammad Ayaz, Mohammad Ammad-Uddin, Zubair Sharif, Ali Mansour, and El-Hadi M. Aggoune. Internet-of-things (iot)-based smart agriculture: Toward making the fields talk. *IEEE Access*, 7:129551–129583, 2019.

[5] Sameer Qazi and et al. Iot-equipped and ai-enabled next generation smart agriculture: A critical review, current challenges and future trends. *IEEE Access*, 10:21219–21235, 2022.

[6] Mohamed Rawidean Mohd Kassim. Iot applications in smart agriculture: Issues and challenges. In *2020 IEEE(ICOS)*, pages 19–24, 2020.

[7] Vaishali Puranik, Sharmila, Ankit Ranjan, and Anamika Kumari. Automation in agriculture and iot. In *2019 4th(IoT-SIU)*, pages 1–6, 2019.

[8] Olakunle Elijah and et al. An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, 5(5):3758–3773, 2018.

[9] Abdul Salam and Syed Shah. Internet of things in smart agriculture: Enabling technologies. In *2019 IEEE 5th (WF-IoT)*, pages 692–695, 2019.

[10] Ayush Kumar, Mrinalini Shridhar, Sahithya Swaminathan, and Teng Joon Lim. Machine learning-based early detection of iot botnets using network-edge traffic. *Computers and Security*, 117, 6 2022.

[11] S. Shinly Swarna Sugi and S. Raja Ratna. Investigation of machine learning techniques in intrusion detection system for iot network. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pages 1164–1167, 2020.

[12] Ng Yee Jien, Mohammad Tahir, Mohammad Dabbagh, Yap Kian Meng, and Ali Farooq. Performance evaluation of machine learning algorithms for intrusion detection in iot applications. In *2022 IEEE (IICAIET)*, pages 1–6, 2022.

[13] Mehul Kapoor and Puneet Jai Kaur. Hybridization of deep learning & machine learning for iot based intrusion classification. In *2022 BHARAT conference*, pages 138–143, 2022.

[14] Shadi Al-Sarawi and et al. Internet of things (iot) communication protocols: Review. In *2017 8th ICIT conference*, pages 685–690, 2017.

[15] Russia is targeting wheat stocks in ukraine, worsening global food crisis, eu says. https://www.euronews.com/my-europe/2022/04/11/russia-is-targeting-wheat-stocks-in-ukraine-worsening-global-food-crisis-

[16] Ravie Lakshmanan. Realtek vulnerability under attack Over 134 million attempts to hack iot devices. https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.html?m=1,.

[17] Liu Hua Yeo, Xiangdong Che, and Shalini Lakkaraju. Understanding modern intrusion detection systems: A survey. *arXiv: Cryptography and Security*, 2017.

[18] Eddy Prasetyo Nugroho and et al. A review of intrusion detection system in iot with machine learning approach: Current and future research. In *2020 6th(ICSITech)*, pages 138–143, 2020.

[19] Brendan McMahan and et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, volume 54, pages 1273–1282, 20–22 Apr 2017.

[20] Ons Aouedi, Kandaraj Piamrat, Guillaume Muller, and Kamal Singh. Intrusion detection for Softwarized Networks with Semi-supervised Federated Learning. In *ICC 2022 - IEEE International Conference on Communications*, Seoul, South Korea, June 2022. IEEE.

[21] Enrique Mármol Campos and et al. Evaluating federated learning for intrusion detection in internet of things: Review and challenges. *Computer Networks*, 203:108661, 2022.

[22] Meriavino. https://ictagrifood.eu/sites/default/files/MERIAVINO%20Leaflet.pdf.

[23] Agreen tech valley. https://www.agreentechvalley.fr/en/.

[24] Farmbot. https://farm.bot/.