FedTIU: Securing Virtualized PLCs Against DDoS Attacks Using a Federated Learning Enabled Threat Intelligence Unit

Priyanka Verma[1], Miguel Ponce De Leon[2], John G. Breslin[1], Donna O'Shea[3]
[1]Data Science Institute, University of Galway, Ireland, {firstname.lastname}@universityofgalway.ie
[2]VMware Research, VMware, Cork, Ireland, mponcedeleon@vmware.com
[3]Department of Computer Science, Munster Technological University, Cork, Ireland, donna.oshea@mtu.ie

***Abstract*—Conventional Programmable Logic Controller (PLC) systems are becoming increasingly challenging to manage due to hardware and software dependencies. Moreover, the number and size of conventional PLCs on factory floors continue to increase, and virtualized PLC (vPLC) offers a solution to address these challenges. The utilization of vPLC offers the advantages of streamlining communication between high-level applications and low-level machine operations, enhancing programming ability in process control systems by abstracting control functions from I/O modules, and increasing automation in industrial control networks. Nevertheless, the connection of vPLC to the internet and cloud services presents a considerable cybersecurity risk, and the crucial aspect of information security for vPLCs is ensuring their availability. Distributed Denial of Service (DDoS) attacks can be particularly devastating for vPLCs, as they rely on internet connectivity to function. DDoS attacks on vPLC overwhelm it and causing it to become unavailable. vPLCs manages control systems and if targeted by a DDoS attack, these systems could become unresponsive, leading to significant disruption to industrial processes. Thus, implementing effective DDoS protection measures is crucial for ensuring the availability and reliability of vPLCs in industrial settings. Therefore, this work proposes a Federated learning enabled Threat Intelligence Unit (FedTIU) for detecting DDoS attacks on vPLCs on an Edge Compute Stack near to vPLC. The proposed approach involves collaborative model training using federated learning techniques to gain knowledge of new attack patterns from other industrial sites while maintaining data privacy.**

***Index Terms*—IIoT, Industry 4.0, Federated Learning, DDoS Detection, vPLC**

I. Introduction

Industry 4.0 aims to break away from the conventional automation pyramid by closely integrating production and business levels through cyber-physical systems (CPSs), which connect physical and virtual worlds. This integration will enable automation systems to become more flexible and intelligent [1]. However, the current industrial landscape is characterized by specialized hardware and software components designed for specific purposes, resulting in a mix of communication technologies within industrial automation. An instance of this would be Programmable Logic Controllers (PLCs), which have the task of regulating tangible procedures by utilizing sensors and actuators to interact with the physical realm. These devices are customized and commissioned for specific applications and use cases, and also employ proprietary hardware and software, often specific to the manufacturer, which makes it challenging to integrate different systems and can lead to vendor lock-in [2].

Virtual Programmable Logic Controllers (vPLCs) address the limitations of traditional PLCs by utilizing virtualization technology [3]. With vPLCs, deterministic real-time control is executed on virtualized edge servers, and the cloud provides the comprehensive vPLC management interface. This means that vPLCs are not limited to specific hardware and can be easily scaled and modified based on changing requirements. Thus, vPLCs offer increased flexibility, scalability, and cost-effectiveness compared to traditional PLCs.

As the vPLC solution is cloud-based, it supports the integration of production and business levels and offers increased resilience. The VMware Edge Compute Stack (ECS) efficiently manages resources located at the edge according to each vPLC's requirements. Furthermore, the complete virtualization of PLC controls utilizing the VMware ECS, which facilitates the operation of Virtual Machines (VM) and containers on standard IT servers at the edge, plays a crucial role in enhancing industrial automation. In summary, vPLCs offer increased flexibility, scalability, and cost-effectiveness compared to traditional PLCs.

However, Industrial control systems (ICS), including vPLCs are vulnerable to cyberattacks that can have severe consequences for critical infrastructure [4]. Attackers aim to compromise vPLC systems by exploiting vulnerabilities in the communication protocols or gaining unauthorized access to one of the systems in the industrial networks. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks [5] are the major threat to the availability of vPLCs, as they can exhaust system resources and cause downtime. Furthermore, the ModBus/TCP, Profinet/IP, DNP3 communication protocol used by vPLCs lacks built-in security features, making it susceptible to attacks that flood the system with TCP SYN requests.

Conventional security solutions, such as anti-virus software and intrusion detection systems, are not suitable for safeguarding vPLCs as a result of their constrained resources.

The project is funded by Science Foundation of Ireland (SFI) under the Grant 16/RC/3918 and EU's MSCA with agreement Number 847577

Furthermore, the effectiveness of existing Machine Learning (ML) and Deep Learning (DL) models for detecting such attacks is limited due to the lack of data available for training the model within the industrial site. Additionally, these isolated models are not equipped to recognize new attack types or variants encountered by other industries, which is critical information as it could potentially affect their industry in the future.

Therefore this research work proposes a solution to address DDoS attacks on vPLCs in industrial settings by utilizing Federated Learning (FL). The solution involves a Federated Learning enabled Threat Intelligence Unit (FedTIU) located along with vPLC at the VMware ECS. FedTIU at ECS acts as a gateway for all requests to the vPLC. The FedTIU uses a trained model to classify the request as either an attack or normal, and with FL, the classification result can be shared with other clients by utilizing a global model.

The rest of the paper is organized as follows: Section 2 describes the background and information related to vPLC and an overview of the existing state-of-the-art techniques. Section 3 presents the attack scenario and section 4 describes the proposed approach against DDoS attack to secure vPLC. Section 5 concludes this work and also discuss about the work in progress for further research.

II. Background and Related Work

This section presents the introduction about vPLC and also discusses the existing state of art techniques present in the literature to handle cyber attacks in ICS.

A. About vPLC

Since the 1970s, PLCs have been ubiquitous in ICS, offering control to autonomously regulate industrial processes. The manufacturing sector commonly employs various PLCs to precisely perform I/O controls. However, every PLC has been a specialized single-purpose hardware component that requires a controller unit, making it a bulky and costly element to host on-site. Moreover, it is also quite costly if needs to be updated once deployed [6].

In recent years, there has been a drive to separate the logic and control functionalities (software) of the PLC from the I/O element (hardware) [3]. This enables the separation of discrete PLCs from the industrial floor and allows the hosting of control functions at the edge (ex. ECS) in the form of vPLCs [7].

Moreover modernization of the industrial automation components is happening at pace because it is reducing hardware costs by moving to common Information Technology (IT) infrastructure and commodity hardware. It is also improving operational efficiency and reducing cost by allowing the PLC to be remotely programmed and upgraded, eliminating on-site visits of the PLC programmer. A virtualization approach to the PLC and the ability to remotely program the PLC is enabling agility and operational efficiency not possible with the current approach.

For example, Software Defined Automation is hosting an industrial Control-as-a-Service offering, leveraging IEC 61131-3 automation software that is allowing for the virtualizing of the PLC software logic within a real-time hypervisor [8].

The IT architecture of Control-as-a-Service builds on the cloud computing paradigm, using an on-premise edge compute stack along with network connectivity to the public cloud [9]. Nevertheless, conventional SCADA and the protocols used, such as Modbus/TCP, Profinet/IP, DNP3, etc., play an indispensable role in communication with most PLC devices. Regrettably, most of these protocols do not have security features nor authentication required to execute remote commands on a control device. Consequently, the vPLC environment is susceptible to cyber-physical attacks.

B. State of Art Techniques in ICS

In the current state of research, the development of solutions to counter DDoS attacks and other cyber threats against vPLCs is lacking. The relative novelty of vPLCs has not yet drawn significant attention from researchers in this area. Nevertheless, there are some existing solutions that have been proposed by researchers to address cyber threats in traditional ICS.

DDoS attacks targeting ICS systems have been a topic of research from years back. Teixeira et al. [10] have examined various types of attacks on control systems that concentrate on disrupting communication between sensors/actuators and a PLC.

The protection of PLCs from attacks is challenging due to their limited computing power, resulting in limited research on this topic. In a study by Xiao et al. [11], introduced an approach for detecting anomalies in PLCs using power consumption data. However, these existing solutions against attack detection for PLC are not applicable for providing defense against vPLC. Because vPLCs are software-based emulations of physical PLCs, and as such, they have different security concerns and limitations than physical PLCs.

Therefore, new defense mechanisms and security solutions specifically designed for vPLCs are needed to address the unique security challenges posed by virtualization.

III. Attack Scenario

ICS domain faces various attack vectors, but vPLCs are particularly vulnerable due to their integration with cloud computing. Attacks on vPLCs fall into three primary categories: attacks that target availability, confidentiality, and integrity.

The present work focuses on the scenario depicted in Figure 1 where an attacker, located outside the industrial facility, exploits a vulnerability of the system (existing within the industry periphery) from the public network to gain access to the industrial system. The attacker can gain access through any public website opened by a worker within the industrial site. Once access is gained, the attacker performs a DDoS attack by sending Modbus/TCP packets to the vPLC at a higher rate in comparison to that it was designed to handle. This slows down the supporting supervisory functions of the vPLC,

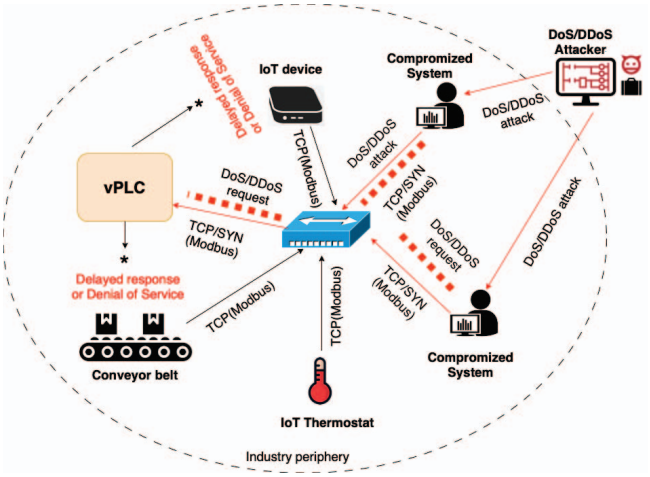

Fig. 1. Attack scenario considered

including sharing alarms, collecting management records, and re-configuring the I/O hardware element connected to the vPLC.

The attacker executes an ARP spoofing attack after getting the internal system access by transmitting fraudulent ARP messages that link the attacker's MAC to the IP addresses of both the vPLC and Human Machine Interface (HMI). This enables the attacker to intercept and manipulate network traffic or stop all communication, causing a DoS attack. By executing a DoS attack, the attacker aims to place the system in an unsafe state, hindering the administrative user's ability to supervise or regulate the industrial system. This type of attack is influenced by the approach outlined in [6].

IV. FL Enabled Threat Intelligence Unit

This section presents federated learning enabled Threat Intelligence Unit to detect the DDoS attack request against vPLC hosted on the edge compute stack in the manufacturing industry. The system model architecture considered is shown in Figure 2 and consists of different sites of manufacturing industries. Instead of hardware PLC, each industry is using a vPLC hosted at ECS. The vPLC processes the request made by the components of an industrial site. However, DDoS attacks can affect the availability of vPLC for serving the benign request as mentioned in section III.

The proposed FedTIU sits along the vPLC at ECS and consists of three major components; Threat Analysis Unit (TAU), the Screening and filtering Unit (SFU), and the aggregator associated with the ARIA cloud. In more detail, the SFU contains a Traffic Policy Database (TPD) and Filtering Sub-Unit (FISU). TAU includes an Espy Sub-Unit (ESU), Local Training Sub-Unit (LTSU), and the Database (DB) to train the local model. LTSU is responsible for training the local model on the local dataset collected through the ESU.

Figure 3 presents the architecture details of the proposed FedTIU. For all the incoming traffic, it will be forwarded to SFU (1). In SFU the TPD forwards it to FISU (2) or sends it to TAU for analysis purposes (3) when no policy is available. ESU classifies the traffic using edge data analysis, responding to the query (4). Meanwhile, ESU notifies LTSU of the suspicious flow (5) and stores the traces in DB. LTSU uses the informed flow to retrain the global model and sends training results to ESU (6). LTSU then distributes policies to TPD (7) and FISU (8). Finally, FISU rejects (9) or sends (10) the flow to access vPLC.

A. Threat Analysis Unit

The Threat Analysis Unit is responsible for training the local model and predicting new threats. The TAU coordinates with the SFU to respond to new threats and provide policies for them to the TPD and the FISU for future detection. The TAU consists of two major components; (i) an ESU and associated Database which is responsible for classifying the request as per edge data analysis and responding to TDP for the requested query, but does not update the policy. (ii) The LTSU, another TAU unit responsible for performing the local training on the local data. Here we used the hybrid CNN+GRU+MLP based DL model for training the local model. Whenever ESU detects a new treat, it notifies it to the LTSU then the LTSU retrains the model and shares it to the aggregator for global model aggregation. The training results are then sent to TPD and FISU to update and store the policies for the future.

B. Screening and Filtering Unit

SFU is responsible for monitoring and filtering incoming requests as per the defined policies. SFU consists of two major components; (i) TPD which is used to store the policies, whenever a request arrives for vPLC it will be first checked with TPD. If policies exist for such requests they will be forwarded to FISU for filtering. (ii) FISU, filters the traffic as per the traffic policy, i.e. forwards it to vPLC or rejects the flow.

C. Aggregator

The aggregation process is a crucial step in federated learning, where the model gradients from different LTSUs are combined to update the global model. In our proposed approach, a scheduler selects participants, send the global model to them, participants retrain the model, and send the updated models back for aggregation to update the global model.

V. Conclusion

There are a number of attack vectors against industrial control systems, but for vPLCs they will now inherit attacks with a heritage in the Internet world, with the adoption of the cloud computing paradigm. Additionally, the communication protocols employed by vPLC lack built-in security measures and do not usually mandate any authentication for executing commands remotely on control devices. Thus the vPLC environment is open to cyber-physical attacks. In this study, our focus is on the DDoS attack which can affect the availability of vPLC services for its intended users.

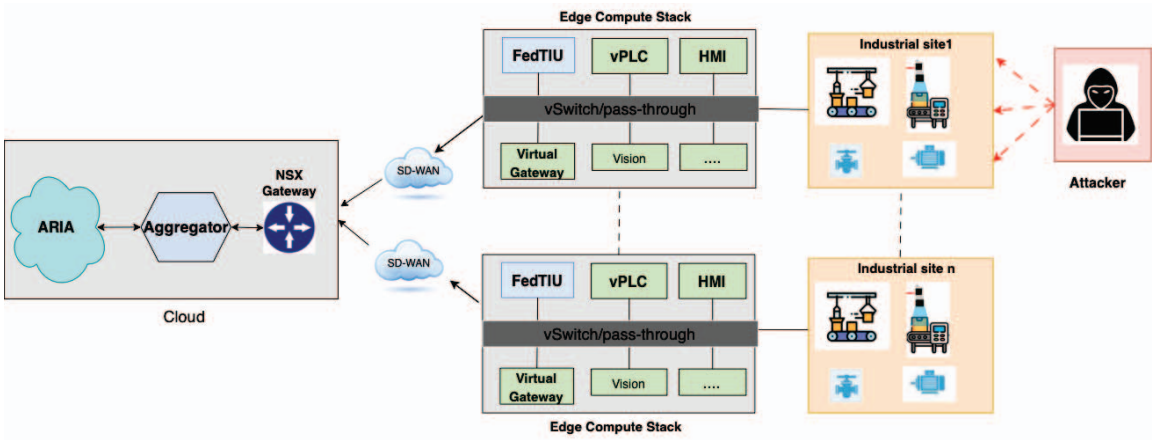

Fig. 2. System model architecture

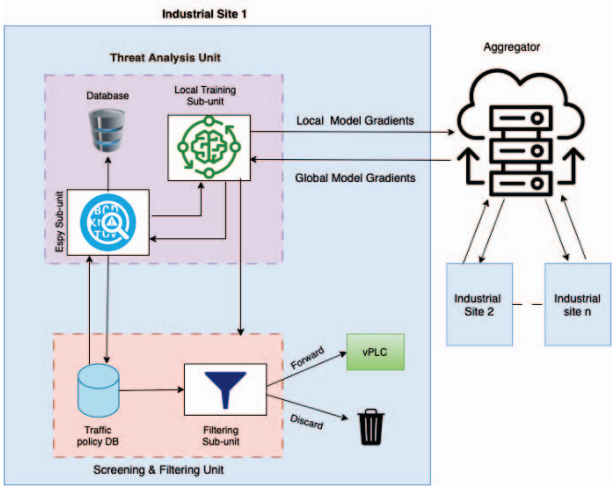

Fig. 3. Architecture of proposed FedTIU approach

Therefore, this work proposed a Federated learning enabled Threat Intelligence Unit to detect DDoS attacks against vPLCs hosted on the ECS in the manufacturing industry. The proposed approach consists of three major components: Threat Analysis Unit, Screening and Filtering Unit, and Aggregator. The system model architecture is designed to enable other industrial sites to get their local DL model to learn about the attack in case if it happens on one site, improving the overall security of the industrial ecosystem. Moreover, proposed model also leverages collaborative learning using FL along with ensuring the data privacy of the individual industrial sites.

However, we are working on to simulate the similar environment to test the proposed approach and include the results in our future research.

ACKNOWLEDGMENT

The project is funded by Science Foundation of Ireland (SFI) under the Grant 16/RC/3918 and EU's MSCA with agreement Number 847577. This work has also received support from the VMware Academic Program. In order to promote open access, the author has chosen to apply a CC BY public copyright license to any version of the Author Accepted Manuscript that results from this submission.

REFERENCES

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE industrial electronics magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[2] E. R. Alphonsus and M. O. Abdullah, "A review on the applications of programmable logic controllers (plcs)," *Renewable and Sustainable Energy Reviews*, vol. 60, pp. 1185–1205, 2016.

[3] T. Cruz, P. Simoes, and E. Monteiro, "Virtualizing programmable logic controllers: Toward a convergent approach," *IEEE Embedded Systems Letters*, vol. 8, no. 4, pp. 69–72, 2016.

[4] P. Verma, J. G. Breslin, and D. O'Shea, "Fldid: Federated learning enabled deep intrusion detection in smart manufacturing industries," *Sensors*, vol. 22, no. 22, p. 8974, 2022.

[5] P. Verma, S. Tapaswi, and W. W. Godfrey, "A request aware module using cs-idr to reduce vm level collateral damages caused by ddos attack in cloud environment," *Cluster Computing*, pp. 1–17, 2021.

[6] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of scada testbeds for cybersecurity research: A modular approach," *Computers & Security*, vol. 77, pp. 531–546, 2018.

[7] "Virtualized programmable logic controllers a paradigm shift toward industrial edge and cloud computing, an industrial internet consortium tech brief 20210907." https://www.iiconsortium.org/pdf/IIC-Edge-vPLC-Tech-Brief-20210907.pdf. Accessed: 2023-03-02.

[8] O. Givehchi, J. Imtiaz, H. Trsek, and J. Jasperneite, "Control-as-a-service from the cloud: A case study for using virtualized plcs," in *2014 10th IEEE Workshop on Factory Communication Systems (WFCS 2014)*, pp. 1–4, IEEE, 2014.

[9] A. Willner and V. Gowtham, "Toward a reference architecture model for industrial edge computing," *IEEE Communications Standards Magazine*, vol. 4, no. 4, pp. 42–48, 2020.

[10] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*, pp. 55–64, 2012.

[11] Y.-j. Xiao, W.-y. Xu, Z.-h. Jia, Z.-r. Ma, and D.-l. Qi, "Nipad: a non-invasive power-based anomaly detection scheme for programmable logic controllers," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, pp. 519–534, 2017.