Towards Unveiling Vulnerabilities and Securing IoT Devices: An Ontology-Based Approach

Mukund Bhole
Institute of Computer Engineering
TU Wien
Vienna, Austria
mukund.bhole@tuwien.ac.at

Wolfgang Kastner
Institute of Computer Engineering
TU Wien
Vienna, Austria
wolfgang.kastner@tuwien.ac.at

Thilo Sauter
Institute of Computer Technology, TU Wien
Dep. of Integrated Sensor Systems
Danube University Krems, Austria
thilo.sauter@tuwien.ac.at

***Abstract*—In the rapidly expanding landscape of Internet of Things (IoT), sensors have emerged as pivotal components, playing a critical role in sensing and data collection. However, this crucial function also renders them susceptible to potential threats such as unauthorized access and security breaches. This paper investigates the vulnerabilities that lead to these threats and offers a comprehensive set of best practices aimed at fortifying the security of IoT devices. We highlight key measures such as secure device design, robust authentication mechanisms, encrypted communication protocols, regular updates, and emphasize the importance of collaborative efforts among stakeholders using an ontological approach. An Ontology provides a structured framework for organizing knowledge, facilitating clearer communication, efficient data management, and enhanced decision-making. Thus, this paper contributes to the development of a more secure and resilient IoT ecosystem.**

***Index Terms*—IoT Security, Vulnerabilities, Industry 4.0, IoT Devices**

I. Introduction

The IoT has revolutionized industries and daily life, facilitating exceptional connectivity through devices that gather and transmit data for various applications, spanning from smart homes to industrial automation. However, the widespread use and significance of these devices in IoT systems render them prime targets for malicious actors seeking unauthorized access or data breaches. Active research is underway to develop security solutions addressing resource constraints and scalability issues, with technologies such as blockchain and software-defined networking bolstering IoT security and efficacy [1], [2].

Furthermore, the IoT has garnered substantial attention for its potential to seamlessly merge physical and digital realms, offering significant business value across sectors like manufacturing, energy, and healthcare. Despite its promise, the nascent nature of IoT technology exposes vulnerabilities in network protocols, resulting in various attacks like flooding, replay, man-in-the-middle, and others, jeopardizing system integrity [3]. Malware-based attacks exploit weaknesses in device and network security, including insecure interfaces and software/firmware, leveraging variants such as Hydra, PsyB0t, and Mirai [4], [5].

Understanding these vulnerabilities is imperative for proactive measures, as the same vulnerability can be exploited across multiple victims, necessitating collaborative efforts and stakeholder involvement. Here, ontological approaches offer insights into complex vulnerabilities, facilitating preemptive security measures [6]. Ontology-based approaches structure these concepts and relationships to reduce ambiguity, communicate knowledge, and improve consistency and accuracy [7], [8]. In this paper, we provide an ontology for IoT security practice, defining the relationships between architectural components and IoT secure practices. We delve into the most common IoT security vulnerabilities, proposing collaborative security practices to ensure ongoing protection. We acknowledge the continuous evolution of security measures as the IoT landscape expands, highlighting the need for state-of-the-art security measures to safeguard sensitive data and privacy while maximizing the benefits of interconnectedness. The paper addresses the following research questions:

- **RQ1:** What are the most common vulnerabilities in the IoT landscape?
- **RQ2:** What are the different security practices in the IoT landscape?
- **RQ3:** How can collaborative efforts aid in maintaining a secure ecosystem?
- **RQ4:** How can ontologies be employed to establish the relationship between best practices and the IoT landscape within a secure ecosystem?

These questions are dealt with in the subsequent sections of this paper: Section III provides an overview of IoT device vulnerabilities, Section IV presents best security practices for IoT devices, Section V discusses proposed secure ecosystems along with best practices in IoT security and collaborative efforts among stakeholders, Section VI presents the implementation of a secure ecosystem using a use case, and Section VII offers concluding remarks and futurework.

II. Related work

Nazir et al. [9] designed a security ontology using the Security Toolbox: Attacks & Countermeasures (STAC) framework. The ontology addresses various parameters, including authentication, access control, authorization, and privacy, using a context-awareness methodology that enables untrained users to make informed security decisions.

Mozzaquatro et al. [10] proposed IoTSec, a reference ontology for M2M communications' security concepts, aimed at securing the IoT environment. IoTSec formalizes IoT security knowledge, supporting the development of new applications and fostering a deeper understanding of key concepts. It improves anomaly detection and introduces novel security approaches. Additionally, IoTSec facilitates quantitative security assessment by identifying risks and assisting managers in integrating security insights.

De Franco et al. [11] introduced SecAOnto, an ontology that formalizes knowledge related to security assessment, emphasizing its various aspects and addressing the correlation between information security and software assessment. Utilizing the STAC framework, SecAOnto aims to support methods grounded in rigorous assessment criteria.

Tao et al. [12] introduced an ontology-based security service framework that supports security and privacy preservation in interactions. Their security ontology defines a common vocabulary for service providers and customers using the Semantic Web Reasoning Language (SWRL). It explicitly describes security elements in device communications, focusing on integrity and confidentiality (Digital Signature, Encryption, SecurityToken), enhancing data protection and access control.

The above existing related work lacks a focus on leveraging the real-time identification of security vulnerabilities using industry resources and stakeholder engagement, which we aim to contribute via this paper.

III. Vulnerabilities in IoT Devices

Based on the studies presented by [13], [14], we have analyzed that among all, the following are the most exploited vulnerabilities by adversaries. Table I shows a few of the vulnerabilities targeted by adversaries in IoT devices. These vulnerabilities are presented in an either/or relation, where they may coincide with each other. However, in a broader context, adversaries might perceive them differently.

A. Limited Resources

A significant trend is the inverse relationship between decreasing security resources and increasing security requirements for IoT end nodes. This has led to extensive research in developing lightweight security technologies for resource-constrained devices. Traditional security mechanisms, like cryptographic solutions intended for more powerful devices, demand greater computational power and energy consumption. Limited resource attacks can disrupt communication channels, leading to unauthorized use of essential IoT resources such as bandwidth, memory, CPU time, and disk space, resulting in battery drain and potentially rendering IoT nodes unable to serve legitimate users [15]. Unfortunately, many companies prioritize rapid product development, often neglecting security considerations [16].

Many IoT devices face processing power and memory constraints due to their compact and cost-effective nature. This renders them susceptible to ransomware attacks as the number of interconnected devices expands [17]. Additionally, inherent limitations such as limited memory capacity expose IoT devices to buffer overflow attacks, where attackers exploit vulnerabilities to execute unauthorized code or crash the device [18]. Moreover, constrained processing power often prevents effective implementation of complex security protocols or encryption algorithms, leaving devices vulnerable to brute force or denial-of-service attacks [19]. Battery-powered IoT devices are particularly at risk due to security measures accelerating battery depletion, leaving them vulnerable to exploitation when offline [20]. Furthermore, reliance on low-bandwidth communication protocols makes IoT devices susceptible to attacks such as jamming or spoofing, where attackers disrupt communication by flooding the network or impersonating legitimate devices [21]. Thus, it is crucial to implement robust security measures tailored to the specific constraints of IoT sensor devices.

B. Constrained Communication Channels

In the realm of the IoT, communication relies heavily on seamless exchanges among interconnected devices, predominantly through wireless protocols. However, this convenience poses a significant challenge due to the vulnerability of constrained communication channels. The wireless nature exposes these channels to potential interception and manipulation by malicious actors. Insufficient encryption or the absence of robust security measures jeopardizes data integrity and confidentiality [22], [23].

Constrained communication channels may lack support for strong encryption or authentication mechanisms, making it easier for attackers to eavesdrop or impersonate devices [21]. Some IoT devices use lightweight or proprietary protocols without built-in security, making them vulnerable to interception or manipulation. Moreover, these channels often lack sufficient error-handling mechanisms, making it hard to detect or recover from malicious activity [24]. Additionally, limited bandwidth increases susceptibility to attacks like jamming or spoofing, where attackers disrupt communication by flooding the network or impersonating legitimate devices.

C. Diverse Application Contexts

The utilization of devices spans a wide array of application contexts, ranging from environmental monitoring to manufacturing, with industrial processes underpinning the foundation of the IoT landscape [25]. In each of these diverse scenarios, the integration of devices introduces specific security considerations and challenges that necessitate customized solutions. For instance, devices collect and transmit data on factors such as air quality, temperature, and pollution levels. The challenge lies in protecting against data manipulation or unauthorized access, which could yield misleading information or disrupt decision-making processes. In the domain of healthcare, where devices play a pivotal role in remote patient monitoring and diagnostics, ensuring the confidentiality of sensitive data becomes paramount.

The security landscape of IoT devices is multifaceted and influenced by various factors. Firstly, differing security needs

TABLE I
SOME VULERABILITIES TARGETED IN IOT DEVICES

Threat	Year	Compromised Entity	Impact
A. Limited Resources			
Mirai Botnet[1]	2016 -Present	IoT devices—such as cameras, routers, and DVRs	Distributed Denial-of-Service (DDoS) attacks that overwhelmed and temporarily shut down the services of major internet platforms, including Twitter, Spotify, and Netflix, among others.
BrickerBot malware[2]	2017 -Present	IoT devices running an outdated version of the Dropbear SSH server with public, geographically dispersed IP addresses.	IoT botnet software that generated record-setting denial-of-service attacks
BlueBorne[3]	2017	Bluetooth	BlueBorne affects ordinary computers, mobile phones, and the expanding realm of IoT devices.
KRACKs attack[4]	2018	WPA2 Wi-Fi networks	The device supports Wi-Fi, it is most likely to be affected KRACK
B. Constrained Communication Channel			
BLE Attack[5]	2019 -Present	Bluetooth IoT Medical devices	Medical devices like insulin pumps and glucose monitors. These weaknesses could empower attackers to intercept sensitive patient data or tamper with the operation of critical devices
Zigbee Attack[6]	2020 -Present	Zigbee-based smart home devices	Smart home devices such as door locks and light bulbs, leveraging encryption and authentication flaws to gain unauthorized access or disrupt device functionality
LoRaWAN Attack[7]	2021- Present	LoRaWAN Networks	LoRaWAN networks applied in sectors like smart agriculture and industrial monitoring, potentially enabling attackers to intercept data or launch denial-of-service attacks
RFID Attack[8]	2018- Present	RFID-based access control systems in office buildings	Intercepting and cloning RFID card signals, effectively bypassing physical security measures and gaining unauthorized entry.
C. Diverse Application Context			
Stuxnet[9]	2010	IoT devices particularly Siemens devices	Sabotaging Iran's nuclear program by causing centrifuges to malfunction. This incident underscored the potential catastrophic impact of IoT vulnerabilities on critical infrastructure
Wannacry ransomware attack[10]	2017 -Present	Medical IoT devices	Impacting healthcare institutions by exploiting vulnerabilities in Windows operating systems, including those present in medical IoT devices. This attack led to significant disruptions in patient care, emphasizing the urgent need for robust security measures in healthcare IoT deployments

[1]http://tinyurl.com/miraibotnet, [2]http://tinyurl.com/brickerbot, [3]http://tinyurl.com/blueborne, [4]http://tinyurl.com/krackattack, [5]http://tinyurl.com/bleattack, [6]http://tinyurl.com/zigbeeattack, [7]http://tinyurl.com/LoRaWANexploit, [8]http://tinyurl.com/rfidattack, [9]http://tinyurl.com/stuxnetvuln, [10]http://tinyurl.com/healthcareiotvuln

across deployment contexts necessitate tailored approaches. Industrial manufacturing devices may require robust security measures to combat physical tampering [26], while healthcare devices prioritize data privacy. Environmental conditions also play a crucial role, as devices operate in diverse settings where factors like temperature variations and electromagnetic interference can compromise reliability [27]. Furthermore, variations in network infrastructure, ranging from wired to wireless protocols, introduce vulnerabilities in data transmission and access control. Compliance with regulations adds another layer of complexity, with different sectors subject to specific standards such as Health Insurance Portability and Accountability Act (HIPAA) (in the US) and General Data Protection Regulation (GDPR) (in Europe) for healthcare, and IEC 27001-02 [28] for IoT security in manufacturing. Integration challenges arise as devices must seamlessly interact with existing systems, posing compatibility and interoperability concerns that, if overlooked, can lead to vulnerabilities. Lastly, user behavior within different contexts introduces additional risks, with IoT devices in smart homes vulnerable to social engineering or phishing attacks targeting human interaction patterns. Thus, a comprehensive understanding of these factors is essential for developing robust security measures to safeguard IoT ecosystems against potential threats.

IV. ENHANCING IOT DEVICE SECURITY: BEST PRACTICES

The process of enhancing IoT device security can be built upon the foundations of four pillars. Proficiency in these pillars may lead to a protected environment and foster a sense of security within the ecosystem. While the presented practices may intersect with one another, they collectively contribute to bolstering security measures in a broader context. The four pillars are as follows:

A. Secure Device Design

In the complex landscape of the IoT, establishing robust security begins with integrating measures into device design. Security considerations must seamlessly integrate into IoT device architecture, utilizing hardware-based features, trusted components, and adherence to industry standards. Hardware-based mechanisms like secure enclaves and cryptographic accelerators effectively mitigate vulnerabilities. Trusted components and secure boot processes enhance device resilience. Adhering to industry standards, such as those by National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), and International Electrotechnical Commission (IEC), provides a structured approach. These proactive steps demonstrate a commitment to safeguarding

IoT devices against cyber threats. Examples include (but not limited):

- Hardware-Based Security: Utilizing Physical Unclonable Functions (PUFs) for device authentication and secret key generation provides a solid foundation for secure IoT device design [29].
- Secure Boot and Firmware Updates: Implementing secure boot mechanisms tailored for IoT devices ensures the integrity and authenticity of firmware during boot-up processes [30].
- Network Security: Addressing security challenges in IoT-based wired/wireless device networks by implementing encryption protocols, authentication mechanisms, and network segmentation strategies [31].
- Data Security: Incorporating security considerations such as data encryption, integrity verification, and access control mechanisms into IoT-based big data architecture and integration [32].
- Secure Software Development Practices: Integrating secure development practices into Agile methodologies ensures security considerations throughout the software development lifecycle [33].
- Continuous Monitoring and Response: Employing continuous monitoring and response mechanisms to detect and mitigate security threats effectively in the IoT ecosystem [19].

B. Robust Authentication Mechanisms

In the realm of IoT security, safeguarding the integrity and confidentiality of device data is of utmost importance. To achieve this, the implementation of robust authentication mechanisms stands as one of the fundamental pillars. Strong authentication mechanisms, such as biometrics or Two-Factor Authentication (2FA), serve as potent safeguards against unauthorized access to sensitive device data. Biometrics, which leverage unique physiological or behavioral traits, offer a level of security that is challenging to replicate, as each individual's biometric markers are distinctive. Technologies like fingerprint recognition and facial scans add an extra layer of authentication, significantly enhancing the difficulty for malicious entities to breach the system. Similarly, employing two-factor authentication requires users or devices to provide two independent forms of verification, such as a password and a temporary code sent to a registered device, before gaining access to the data.

Examples of these authentication mechanisms include (but not limited):

- Hardware-Based Security: An approach involving the implementation of security features directly into the hardware of IoT devices, such as secure elements or Trusted Platform Modules (TPMs), to protect sensitive data and cryptographic keys from physical attacks [34].
- Integrating Blockchain for Authentication: Blockchain technology offers a decentralized and tamper-resistant platform for authentication in IoT device networks. This integration enhances security by providing a transparent and immutable record of transactions, ensuring the integrity and authenticity of device data [35].
- Lightweight Fuzzy Extractor (LFE) for Authentication: A LFE is a cryptographic mechanism used for biometric authentication in IoT device security. It addresses the challenges of securely storing and authenticating biometric data in resource-constrained environments typical of IoT devices [36].
- Improved Elliptic Curve Cryptography (IECC) Authentication: IECC is designed as a malware detection and prevention approach for secure data transmission among IoT devices. The malware detection approach incorporates LSTM deep learning techniques [37].

C. Encrypted Communication Protocols

In the realm of IoT security, implementing encrypted communication protocols is pivotal for safeguarding device-generated data. This involves encoding transmitted data into a form decipherable only by authorized recipients, ensuring confidentiality and integrity throughout transmission. Employing robust encryption algorithms like Advanced Encryption Standard (AES) provides a formidable defense against eavesdropping and unauthorized data interception. Symmetric key encryption, efficient for IoT devices with limited computational resources, employs the same key for both encryption and decryption. Encryption Algorithms [38]:

- ChaCha20: A stream cipher designed for high security with low computational requirements, suitable for resource-constrained IoT devices. It can be implemented in IoT protocols such as TLS/DTLS, SMP, CoAP, MQTT, IPSec, Zigbee, and LoRaWAN.
- Twofish: A symmetric key block cipher known for its security and efficiency, offering strong encryption for IoT communications. It can be implemented in custom security protocols.

Asymmetric key encryption, though computationally intensive, uses a pair of public and private keys for encryption and decryption, enabling secure key exchange mechanisms. Encryption Algorithms [39]:

- ElGamal: Based on the discrete logarithm problem, ElGamal encryption is suitable for secure communication in IoT networks. It is commonly used in Multi-Party Computation (MPC) protocols implemented in IoT devices.
- McEliece Cryptosystem: Resistant to quantum attacks and based on error-correcting codes. It is commonly used in high-security IoT deployments.

Homomorphic encryption enables computations on encrypted data without decryption, preserving data privacy while enabling secure data processing. Encryption Algorithms [40]:

- Brakerski-Fan-Vercauteren (BFV): Suitable for IoT applications requiring secure computation on encrypted data. BFV encryption can be used in protocols where IoT data is outsourced to third-party services or cloud providers for analysis or storage while ensuring data confidentiality.

- Homomorphic Encryption for Arithmetic of Approximate Numbers (HEAAN): Optimized for arithmetic operations on approximate numbers, beneficial for IoT analytics.

Post-quantum cryptography addresses security against quantum computing attacks. Encryption Algorithms [41]:

- NTRU: Resistant to quantum attacks, based on lattice-based encryption, suitable for securing IoT communications. It can be used in IoT protocols such as MQTT, CoAP, HTTP/HTTPS, TLS/DTLS, BLE, LoRaWAN, 6LoWPAN, and Modbus.
- SPHINCS+: Provides secure encryption for IoT devices, resistant to quantum attacks, using a stateless hash-based signature scheme. It can be used in IoT protocols such as MQTT, CoAP, HTTP/HTTPS, TLS, BLE, LoRaWAN, 6LoWPAN, and Modbus.

Authenticated encryption ensures both confidentiality and integrity of the data, protecting against eavesdropping and tampering attacks. Encryption Algorithms [42]:

- Advanced Encryption Standard - Galois/Counter (AES-GCM): Provides both confidentiality and integrity through a combination of symmetric encryption and Message Authentication Codes (MACs). It is used in IoT protocols such as TLS/DTLS, IPsec, MQTT, HTTP/HTTPS, LoRaWAN, 6LoWPAN, and Modbus.
- Synthetic Initialization Vector (SIV): Offers deterministic authenticated encryption, suitable for IoT applications requiring message deduplication. It is used in IoT protocols such as TLS/DTLS, IPsec, MQTT, HTTP/HTTPS, LoRaWAN, 6LoWPAN, Modbus, and SNMP.

D. Regular Software Updates

The practice of regular software updates stands as a crucial pillar in fortifying the security of IoT devices, including devices, against the ever-evolving landscape of cyber threats. These updates play a pivotal role in addressing vulnerabilities, fixing bugs, and incorporating the latest security patches to thwart potential exploits. Despite the embedded software running complex operations in IoT devices, including devices, they are not immune to security flaws. Timely software updates serve as a proactive measure to prevent these vulnerabilities from being exploited by malicious actors.

Examples of update mechanisms include (but not limited):

- Over-the-air (OTA) updates: These allow firmware updates to be delivered remotely over the air, enabling seamless and efficient updates without physical access to the device [43].
- Scheduled update: These allocate specific time slots for software updates to minimize disruption to IoT device operations and network bandwidth [44].
- Rollback mechanisms: These enable IoT devices to revert to a previous firmware version in case of update failures or compatibility issues [45].

V. Building a Secure Ecosystem: Collaborative Efforts and Stakeholder Involvement

Fig. 1 provides an overarching view of building a secure ecosystem for IoT devices. The implemented methods in the ecosystem are: 1) Ontological Representation of Best Security Practices, 2) Stakeholder Engagement and Collaboration, 3) Information Sharing Using Ontology, 4) Establishing Industry-wide Security Standards and Protocols, and 5) Leveraging Vulnerability Databases and Certification Details.

The left part of the diagram presents the best security practices (the four pillars) in a basic ontological form in Protégé[1], with the direct instantiation of the use case (MPS-Distribution Group) and the stakeholders involved in the development of the ontology. This serves as a target for addressing vulnerabilities in devices with limited resources, constrained communication channels, and diverse application contexts. The ontology provides a shared understanding of the concepts and relationships within the domain, guiding the development of the system application.

Conversely, the right part illustrates collaborative efforts and stakeholder engagement in the development of the ontology by suggesting which security measures are feasible for which components or groups of components of the system. It also offers further insights into existing device vulnerabilities via vulnerability databases and IoT device certification details from the IEEE sensors registry.

Collaboration enables stakeholders to leverage the collective expertise of manufacturers, developers, regulators, and end-users in identifying, mitigating, and addressing security gaps across the IoT ecosystem. Manufacturers embed security measures during device design, developers create secure software, regulators establish guidelines, and end-users ensure responsible usage and prompt updates [46].

Central to this collaboration is information sharing using ontology, facilitating the exchange of threat intelligence and best practices in IoT security to foster a collective defense mechanism. Establishing industry-wide security standards and protocols provides a common ecosystem for designing and managing secure IoT systems. The dynamic nature of IoT security requires ongoing collaboration to adapt to emerging threats through regular interactions and joint initiatives.

Securing IoT devices demands a unified front, where collaborative efforts enhance information flow, raise standards, and promote collective vigilance. Leveraging resources like the IEEE sensors registry [2] (which contains details such as Product category, vendor, product series, product name, product model, application vertical, datasheets, and devices certifications), along with vulnerability databases such as OSV [3], MITRE CVE [4], NVD-NIST [5], CN NVD [6], and JVN [7], ensures a

[1]https://protege.stanford.edu/
[2]https://sensorsregistry.ieee.org/
[3]https://osv.dev/
[4]https://cve.mitre.org/
[5]https://nvd.nist.gov/vuln/search
[6]https://www.cnnvd.org.cn/
[7]https://jvn.jp/en/

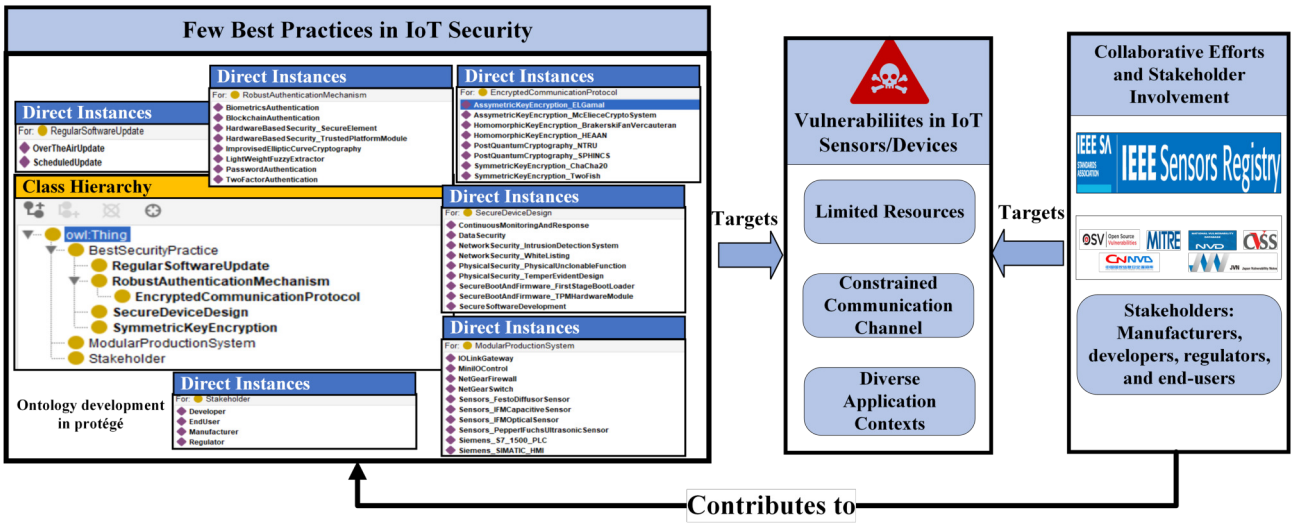

Fig. 1. Building a secure ecosystem for IoT devices

comprehensive investigation of existing vulnerabilities and reinforces security measures for IoT devices.

VI. Implementation

The Distributing Pro Station[8] depicted in Fig. 2 handles the tasks of holding, sorting, and feeding workpieces. It comprises three Stacking modules and a Conveyor module. Each Stacking module includes a double-acting solenoid-controlled cylinder for pushing out workpieces, with proximity sensors at both ends for position detection. Workpieces are stored in vertical magazines, with IO link sensors (optical (IFM), ultrasonic (Pepperl+Fuchs), and capacitive (IFM)) at the top determining the stack height. Light barrier and level sensors monitor magazine emptiness. The stacking module feeds workpieces onto a conveyor belt controlled by a DC motor controller. Diffuser sensors (Festo) track workpiece positions on the conveyor. The system is automated by a PLC (Siemens Simatic S7-1500), with status displayed on an HMI (Siemens Simatic TP 700). Communication is facilitated by a switch (Netgear), IO link gateway, and mini IO links between components. Using the secure ecosystem approach, the implementation is done as follows:

- Using Ontology: We have identified the stakeholders who assigned the property assertions of the implemented security practices for the use case, as depicted in Fig. 4 and Fig. 3 shows the graphical representation of the ontology with arc types.
- Using Vulnerability Databases: We found the vulnerability in Siemens S7-1500 PLC (CVE-2022-38465)[9] and Siemens Simatic HMI panel (CVE-2022-40227)[10].
- In the IEEE Sensors Registry: Unfortunately, there is no available data on the devices used in the use case.
- Stakeholders: By explicitly stating which security practices each system component implements, provide a clear and unambiguous representation of the security measures in place within the system. This makes it easier for stakeholders to understand the security posture of the system and also aids in developing the best practice ontology.

Upon reviewing the aforementioned information for final analysis, CVE-2022-38465 regarding Siemens S7-1500 PLC raises concerns about the built-in global private key, indicating its inadequacy in terms of security. This vulnerability could potentially enable attackers to uncover the private key of a CPU product family through an offline attack targeting a single CPU within that family. However, it's worth noting that the implemented security practice (see Fig. 4) employs symmetric key encryption, which serves as a protective measure against external attacks on the system.

Additionally, considering CVE-2022-40227 regarding Siemens Simatic HMI panel raises concerns about devices not properly validating input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. However, if we consider the communication of HMI through a firewall, it's worth noting that the implemented security practice (see Fig. 4) is whitelisting, which restricts remote connection access to authorized users only. This measure serves as a protective measure against this type of attack.

VII. Conclusion

In this work, we have identified and addressed the most common vulnerabilities in IoT devices, such as limited resources, constrained communication channels, and diverse application contexts. These are the most exploited vulnerabilities in IoT devices and are discussed in response to

[8]https://ip.festo-didactic.com/InfoPortal/MPS/MPS403I4.0/EN/index.html
[9]https://www.cve.org/CVERecord?id=CVE-2022-38465
[10]https://www.cve.org/CVERecord?id=CVE-2022-40227

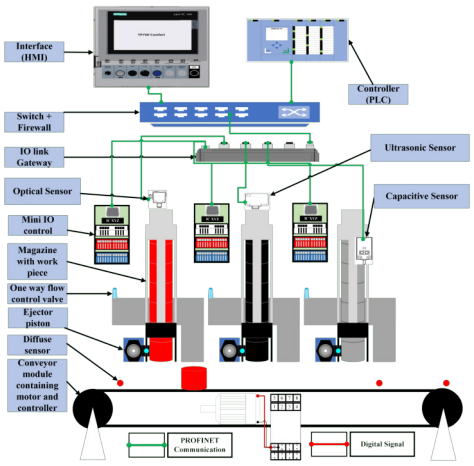

Fig. 2. MPS 403-1 (Distribution Group)

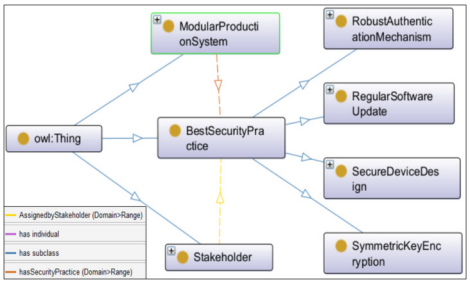

Fig. 3. Graphical representation of ontology with arc types (via OntoGraf)

RQ1 in Section III. We propose a comprehensive set of best practices to mitigate these vulnerabilities and ensure the integrity, confidentiality, and reliability of data. By implementing secure IoT practices, we demonstrate the effectiveness of four key pillars: secure device design, robust authentication mechanisms, encrypted communication protocols, and regular updates. The cited studies also reflect the evolving landscape of technological advancement and suggest how industries should adapt accordingly. This addresses **RQ2** in Section IV.

Additionally, by emphasizing collaborative efforts and stakeholder involvement, we have advocated for the establishment of a secure ecosystem in IoT devices to effectively mitigate the risks posed by cyber threats and vulnerabilities. By utilizing an ontological approach for knowledge sharing of IoT security practices which answers **RQ3** in Section V, we can collectively strive to build a secure and more resilient IoT ecosystem. As a tangible demonstration of use of ontology to demonstrate the relationship between best practices and IoT landscape within our secure ecosystem approach, we have applied our principles to the IoT landscape of MPS (Distribution Pro Station) [11] which answers **RQ4** in Section VI.

In future work, the developed ontology can be reused for different applications based on its system architecture. Furthermore, the ecosystem can also incorporate various safety practices, which could lead to both a safe and secure IoT ecosystem.

[11]https://ip.festo-didactic.com/InfoPortal/MPS/MPS403I4.0/EN/index.html

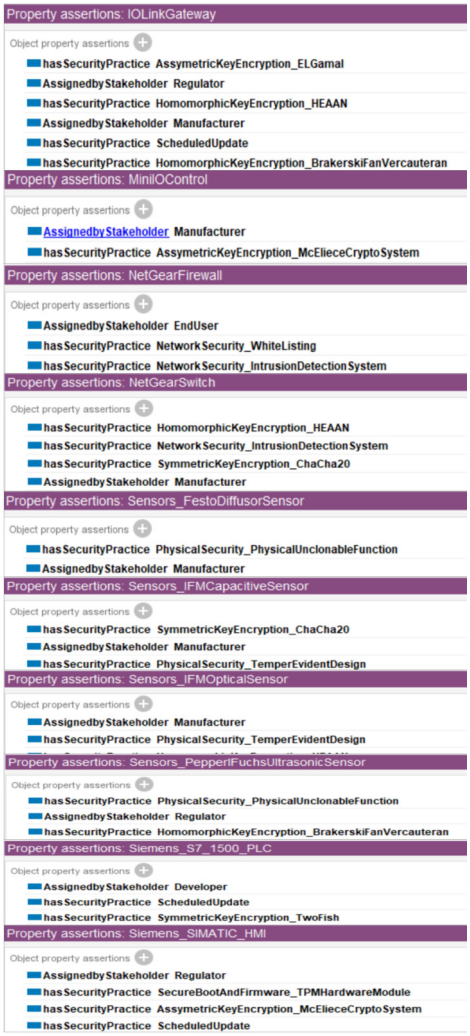

Fig. 4. Instantiation of implemented security practice ontology for MPS 403-1 (Distribution Group)

ACKNOWLEDGMENT

This paper was supported by TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry, a research cooperation between TU Wien and TÜV AUSTRIA.

REFERENCES

[1] S. Sajid Ullah, V. Oleshchuk, and H. S. G. Pussewalage, "A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges," *Computer Networks*, vol. 235, p. 109994, 2023.

[2] T. Sauter and A. Treytl, "Iot-enabled sensors in automation systems and their security challenges," *IEEE Sensors Letters*, vol. 7, no. 12, pp. 1–4, 2023.

[3] B. chander and K. Gopalakrishnan, *Security Vulnerabilities and Issues of Traditional Wireless Sensors Networks in IoT*, 2020, pp. 519–549.

[4] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, "Future iot-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," *International Journal of Communication Systems*, vol. 33, no. 12, 2020.

[5] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van herle, "A review of the security vulnerabilities and countermeasures in the internet of things solutions: A bright future for the blockchain," *Internet of Things*, vol. 23, p. 100888, 2023.

[6] M. Bhole, W. Kastner, and T. Sauter, "Knowledge representation of asset information and performance in ot environments," in *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2023, pp. 1–8.

[7] A. Bunte, A. Diedrich, and O. Niggemann, "Integrating semantics for diagnosis of manufacturing systems," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016, pp. 1–8.

[8] C. Hildebrandt, A. Scholz, A. Fay, T. Schröder, T. Hadlich, C. Diedrich, M. Dubovy, C. Eck, and R. Wiegand, "Semantic modeling for collaboration and cooperation of systems in the production domain," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017, pp. 1–8.

[9] A. Nazir, S. Sholla, and A. Bashir, "An ontology based approach for context-aware security in the internet of things (IoT)," *Int. J. Wirel. Microw. Technol.*, vol. 11, no. 1, pp. 28–46, Feb. 2021.

[10] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the internet of things," in *2015 IEEE International Workshop on Measurements Networking (MN)*, 2015, pp. 1–6.

[11] F. de Franco Rosa, M. Jino, and R. Bonacin, "Towards an ontology of security assessment: A core model proposal," in *Information Technology - New Generations*, 2018, pp. 75–80.

[12] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040–1051, 2018.

[13] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, 2021.

[14] M. P. Bhole, "Data analysis and results of threat groups in ot environment," Nov 2023. [Online]. Available: https://researchdata.tuwien.at/records/ewmb8-3ad52

[15] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "Iot vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168 825–168 853, 2020.

[16] N. Torres, P. Pinto, and S. I. Lopes, "Security vulnerabilities in lpwans—an attack vector analysis for the iot ecosystem," *Applied Sciences*, vol. 11, no. 7, 2021.

[17] T. A. Ahanger, U. Tariq, F. Dahan, S. A. Chaudhry, and Y. Malik, "Securing iot devices running pureos from ransomware attacks: Leveraging hybrid machine learning techniques," *Mathematics*, vol. 11, no. 11, 2023.

[18] J. Foster, V. Osipov, N. Bhalla, N. Heinen, and D. Aitel, *Buffer Overflow Attacks*, 01 2005.

[19] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.

[20] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51 915–51 932, 2019.

[21] L. Huraj, M. Šimon, and T. Horák, "Resistance of IoT sensors against DDoS attack in smart home environment," *Sensors (Basel)*, vol. 20, no. 18, Sep. 2020.

[22] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "Iot vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168 825–168 853, 2020.

[23] T. A. Idriss, H. A. Idriss, and M. A. Bayoumi, "A lightweight puf-based authentication protocol using secret pattern recognition for constrained iot devices," *IEEE Access*, vol. 9, pp. 80 546–80 558, 2021.

[24] A. Goulart, A. Chennamaneni, D. Torre, B. Hur, and F. Y. Al-Aboosi, "On wide-area iot networks, lightweight security and their applications—a practical review," *Electronics*, vol. 11, no. 11, 2022.

[25] U. A. Usmani, A. Happonen, and J. Watada, "Secure integration of iot-enabled sensors and technologies: Engineering applications for humanitarian impact," in *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2023, pp. 1–10.

[26] M. Hammad, R. M. Jillani, S. Ullah, A. Namoun, A. Tufail, K.-H. Kim, and H. Shah, "Security framework for network-based manufacturing systems with personalized customization: An industry 4.0 approach," *Sensors*, vol. 23, no. 17, 2023.

[27] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of iot applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, 2024.

[28] "ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 10 2022.

[29] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (puf)-based security solutions for internet of things," *Computer Networks*, vol. 183, p. 107593, 2020.

[30] A. Marchand, Y. Imine, H. Ouarnoughi, T. Tarridec, and A. Gallais, "Firmware integrity protection: A survey," *IEEE Access*, vol. 11, pp. 77 952–77 979, 2023.

[31] W. Fei, H. Ohno, and S. Sampalli, "A systematic review of iot security: Research potential, challenges, and future directions," *ACM Comput. Surv.*, vol. 56, no. 5, nov 2023.

[32] M. K. Abiodun, J. B. Awotunde, R. O. Ogundokun, E. A. Adeniyi, and M. O. Arowolo, *Security and Information Assurance for IoT-Based Big Data*, 2021, pp. 189–211.

[33] Y. Valdés-Rodríguez, J. Hochstetter-Diez, J. Díaz-Arancibia, and R. Cadena-Martínez, "Towards the integration of security practices in agile software development: A systematic mapping review," *Applied Sciences*, vol. 13, no. 7, 2023.

[34] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[35] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 618–623.

[36] S. Ebrahimi and S. Bayat-Sarmadi, "Lightweight fuzzy extractor based on lpn for device and biometric authentication in iot," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 706–10 713, 2021.

[37] R. Aiyshwariya Devi and A. Arunachalam, "Enhancement of iot device security using an improved elliptic curve cryptography algorithm and malware detection utilizing deep lstm," *High-Confidence Computing*, vol. 3, no. 2, p. 100117, 2023.

[38] J. P. Degabriele, J. Govinden, F. Günther, and K. G. Paterson, "The security of chacha20-poly1305 in the multi-user setting," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 1981–2003.

[39] R. J. McEliece, "A public key cryptosystem based on algebraic coding theory," 1978.

[40] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, jul 2014.

[41] D. J. Bernstein, *Introduction to post-quantum cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 1–14.

[42] P. Rogaway, "Authenticated-encryption with associated-data," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. New York, NY, USA: Association for Computing Machinery, 2002, p. 98–107.

[43] J. Bauwens, P. Ruckebusch, S. Giannoulis, I. Moerman, and E. D. Poorter, "Over-the-air software updates in the internet of things: An overview of key principles," *IEEE Communications Magazine*, vol. 58, no. 2, pp. 35–41, 2020.

[44] N. H. Bui, C. Pham, K. K. Nguyen, and M. Cheriet, "Energy efficient scheduling for networked iot device software update," in *2019 15th International Conference on Network and Service Management (CNSM)*, 2019, pp. 1–5.

[45] B.-C. Choi, S.-H. Lee, J.-C. Na, and J.-H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 39–44, 2016.

[46] "IEC 24748-1: Part 1: Guidelines for life cycle management," 11 2018.