Industrial and Consumer Internet of Things: Cyber Security Considerations, Threat Landscape, and Countermeasure Opportunities

Stephen Ugwuanyi
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—The requirements of industrial, consumer or generic Internet of Things (IoT) networks are evolving due to advances in sensor and wireless networks, embedded systems, edge and cloud computing. IoT is becoming increasingly pervasive in the industrial domain, and these networks face the additional challenge of evolving network architecture towards integrating Information Technology (IT) and Operational Technology (OT) networks. This paper analyses the underpinning cybersecurity risks and attack landscape in Industrial IoT (IIoT) and suggests potential countermeasure opportunities for future hybrid IoT applications based on lessons from IIoT projects.**

Keywords—Internet of Things, Consumer Internet of Things, Industrial Internet of Things, Cyber Security, Countermeasure Opportunities.

I. INTRODUCTION

Industrial Internet of Things (IIoT) is a network of machine type IoT devices that finds applications in many fields [1] to facilitate industrial system's efficiency, drive real-time automation, and reduce operational and maintenance costs [2]. Traditional IIoT is a network of industrial control systems termed Operational Technology (OT) with unique communication protocols. General Electric (GE) described it as "an internet of things, machines, computers and people, enabling intelligent operations using advanced data analytics to transform business outcomes" [3]. However, we are concerned with resource-constrained industrial IoT devices that would require additional resources to implement new cybersecurity features. Given the nature of the use cases and the sensitivity of the data generated, serious concerns are warranted: what industrial IoT device should be connected to the internet and for what purpose?. The reasons have extended beyond a typical example of remotely turning ON or OFF of electronic devices or for process automation [4]. Current requirements include making IoT devices smarter, interconnected, and sharing data seamlessly over secure internet platforms to improve system efficiency and productivity levels [5]. Other benefits and future research areas include reconfigurability, remote access, scalability, interoperability, power utilisation, standardisation, and low latency communication [5].

The convergence of Information Technology (IT) and OT networks brings many control, monitoring, operational, and cost-saving benefits as well as exposes OT network boundaries to new types of cybersecurity threats. The convergences are occasioned by emerging technologies shown in Figure 1. IT and OT networks have the same Confidentiality, Integrity, and Availability (CIA) priority in the network/information security model but ranked in different priority order, IT – (CIA) and OT - (AIC) [6]. This implies that certain compromises have to be reached in some legacy OT use cases in prioritising safety and availability against security. An IT system may trade availability with security by shutting down systems in the event of cyber-attacks. In contrast, OT may trade availability with security when not connected to the internet.

Industrial cybersecurity is the process of protecting Industrial Control Systems (ICS) from cyber-attacks. Industrial cyber threats could come from the inside or outside of an organisation and relate to industrial safety concerns for protecting critical infrastructure. Privacy and security are some of the most significant challenges for applying IoT in the industries. The types of security vulnerabilities recorded in generic IoT networks are increasingly seen in the industrial domains [5]. Notable examples include the Stuxnet discovered in 2010 by the VirusBlockAda that affected the Iranian uranium facility in 2014 [7], the Mirai botnet that affected millions of network routers and IP cameras in 2016 [8], the Distributed Denial of Service (DDoS) attack that took down the Finland heating system in 2016 [9], Brickerbot that leveraged the default password and user names on IoT devices in 2017 [10], and the 2021 Colonial Pipeline ransomware and data breach cyberattack that impacted computerised devices [11]. The security systems developed for consumer IoT networks cannot be directly deployed to industrial networks because of the differences in communication requirements. The communication requirements of Cyber-Physical Systems (CPS) and generic IoT is different and not clearly defined [1] but they are expected to handle data processing with higher levels of CIA. Similarly, emerging IoT innovations are enabling the successful convergence of IT and OT networks with no formal boundary [12].

This research is funded by the Nigerian Petroleum Technology Development Fund (PTDF) award number PTDF/ED/PHD/USO/1092/17

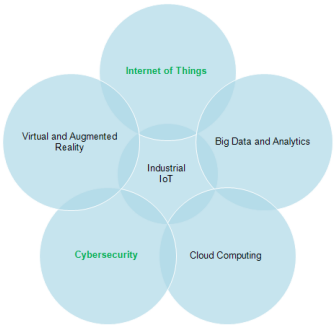

Figure 1. Drivers of Industrial Internet of Things

Threats issues of industrial IoT devices have not been well investigated compared to the security and privacy issues of consumer IoT devices. In this paper, our contributions include:

- Analyse the current research directions in the generic IoT security practices, which allowed us to identify and compare with the OT world.
- Discuss the different challenges and opportunities of industrial IoT networks due to IT and OT convergence.
- Present the security considerations of industrial IoT based on lessons from different industrial IoT projects.

The remaining part of the paper is structured as follows: Section II presents the current research direction in industrial and consumer IoT security; Section III discusses the security protocols for IIoT applications; Section IV presents the security-based architecture of IoT network; Section V compared the security requirements and countermeasures opportunities of both domains; and Section VII concludes the paper with a summary of cybersecurity considerations for IIoT.

II. Related Work

Security is one of the existent gaps in industrial IoT systems. Industrial networks comprise legacy technologies such as Control and Data Acquisition (SCADA) systems, Human Machine Interface (HMI), Distributed Control System (DCS), ICS, and Intelligent Electronic Devices (IEDs). The legacy devices have common security issues such as implementing lightweight authentication and encryption systems, updating security patches, enhancing interoperability, etc. They do not meet the cybersecurity requirements of new IT threats permeating OT environments by using new IoT devices for different purposes. IoT products are implemented based on market competitiveness to get hold of the market and increase return on investments rather than building secured systems [13]-[14]. Software and hardware are often seen deployed straight from research laboratory to real-life situation without proper testbed investigations. The testings, when carried out, is on a small scale [15]-[16]-[17] and cannot be extrapolated to the actual world scenario in capacity and performance.

The publications by the Industrial Internet Consortium (IIC) shows a great deal of effort in ensuring that features such as "interoperability, security, connectivity, business models, and standards architecture are firmly rooted in reality" in the approved industrial IoT testbeds [18]. The report also indicates that most designs initially lack edge security implementation for Device-2-Device (D2D) and Device-2-Cloud (D2C) communications. According to the Internet Security Framework (IISF), most IoT security solutions claimed were not substantiated but are the same as the existing network and firewall security approaches in IT systems. However, the current research effort is towards developing common security frameworks for cyber-security in IIoT systems that will smoothly realise industrial 4.0. IIoT refers to applications in manufacturing, healthcare, energy, smart city, transportation, while Industrial 4.0 refers to the manufacturing sector [3] – we use the terms interchangeably in this paper.

There are many approaches to tackling industrial IoT security. One approach is through modelling and validation of network designs. A Model-Based Design (MDB) has been proposed to handle cyber-attacks on CPS [19]. However, the methods have limitations on modelling and analysing capabilities both for the physical and cyber domains as observed in the Extended Data Flow Diagram (xDFD) approach and Attack Tree-Based Model. For instance, the study of power networks could be modelled in MATLAB/Simulink to investigate fuzzy, interruption, man-in-the-middle, replay, overflow, and down-sampling security attacks (cybersecurity functions) scenarios and countermeasures opportunities before the method is implemented. Another approach is the use of nanoscale electronic technology primitives such as memristors, carbon nanotubes and graphene [20]. Integrating nanoscale technology into IoT design adds good authentication and secret key generation mechanisms with bits response rate error as the potential downside. Such errors are known to be resolved by error correction cryptographic systems such as syndrome-based schemes and code offset schemes, especially in Physical Unclonable Functions (PUFs) [21]. PUF security by design approach allows security to be introduced at the circuit level of IoT devices during the manufacturing process. More studies have been conducted on security key generation using PUF [22], in which some were found to be vulnerable to modelling attacks and are affected by other factors such as thermal noise, electrical properties, and ageing [23]-[24]-[25]-[26].

Securing IoT nodes in [27] used a Traffic-Aware Detection and Patching Scheme to strengthen the wireless networks of IoT by resolving the critical sections of intermediate nodes using traffic information. The intermediate nodes here refer to gateways, computer systems, access points that must be intelligent enough to detect the links where malware emanate. However, the end nodes in industrial IoT are difficult to patch because of their limited processing capabilities, which stops them from recovery from attacks. Software-based security at the IoT devices seems impracticable as problems of resources constraints, software update capabilities, and power consumption remains open research areas. However,

Software Defined Networking (SDN) has been proposed to improve access security and defend industrial IoT from DDoS attacks [28]. Most known IIoT attacks are usually launched through servers, memory units, I/O bandwidth, socket, Internet Control Message Protocol (ICMP), Domain Name System (DNS), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP).

The risks associated with IoT devices can be evaluated using a graphical approach. Gemini et al. used a three-phased model to pre-process network vulnerabilities, graphically analyse their dependencies, and visualise security parameters [29]. Cost modelling is the framework for improving the risks mitigation strategy for industrial IoT networks' overall security and operational efficiency. To introduce secure IoT systems with zero human intervention that can reduce time and human cost compared to the user-dependent provisioning common in Amazon Web Service, Microsoft Azure, and OneNet, we recommend IoT network security measures presented in section VI. [30] implemented a Remote Authentication Dial-In User Service and one-time password authentication system to perform the provisioning process (discover and connect to IoT network) using a state machine. The method offers far better performance than the legacy ICS and could complete the provisioning process within 4 seconds.

III. Industrial IoT Security Protocols

The number of standardised security protocols for industrial IoT may be difficult to itemise. However, we classify the security protocol of generic IoT networks that are increasingly used in the industrial domains into Asymmetric Key Scheme (AKS) and Symmetric Key Pre-Distribution Scheme (SPKDS) [31]. The AKS is based on Public Key Cryptography (PKC) with a high computational cost and energy consumption profile as the trade-off while SPKDS is based on secret-key cryptography, probabilistic and deterministic key distribution. Elliptical Curve Cryptography (ECC) and Nth Degree-Truncated Polynomial Ring Units (NTRU) primitives are two security enhancements to further increase cryptosystem deployment in IoT constrained environments.

Recent studies have looked at using Authentication and Key Agreement (AKA) protocols to maintain the security of device-to-device communication [32]-[33]-[34]-[35]. While some have increased data overhead, others were vulnerable to network attacks. There are many ways of overcoming these challenges. One example is implementing Proxy Mobile IPV6 (PMIPv6) over the 6LoWPAN mobile network to support group communication if latency and signalling overhead are to be reduced. In Machine Type Communication (MTC), enhanced group-based AKA protocol has been proposed to solve the issues of signaling congestion and bandwidth overhead [32]. However, group communication security in network-assisted and non-network assisted scenarios is a concern to IoT's growing applications. The increased communication overhead and cyber-attacks were observed as the issues of introducing Internet Protocol (IP) into constrained sensor networks [36]. Integrated IP-based IoT networks exhibit problems of IP translation between IPv6 and IPv4, which is against the adaptability to new incompatible technology design goals for IPv6 by the Internet Engineering Task Force (IETF). [37] used a Hash Function (HF) algorithm to match an internal IPv6 address to external IPv4 address in a home IoT network scenario. With the dynamic address protocols and a port-mapping models, the issues of constant network topology changes due to geographical displacement of the sensors could be addressed. In the context of industrial IoT, Next Generation Firewall and Gateways (NGFW-G) will play the role of ensuring security of incompatible network protocol through decrypting and re-encrypting of data or message across communication channels. For the security requirements of future virtualisation oriented industrial IoT networks, [38] explored the IP management and security strategies of Docker and Kubernetes based orchestration platforms for multi-tenant industrial IoT networks.

IV. The Architecture of Industrial and Consumer IoT

IoT architecture is a question of hardware and protocol types, application and deployment requirements summed up to what Alasdair outlined as components an IoT project must take into account whether the deployment environment is greenfield or brownfield [12]. The fundamental principle of industrial IoT architecture is the extension of machine-to-machine design to the internet, making it more intelligent and open to the interconnectivity of other things or industries considering how many devices the architecture will be designed for, Proof of Concepts (PoC), and time to market. The core architecture of industrial IoT systems has specific security layers, with each having specific security risks identified to originate from users, things to be connected, and the connection method [4]. In a comparative perspective, Bhattarai and Wang believed that object-driven security is more important than user-driven security [39]. While others think that Industrial IoT deployment will be dependent on security, Sadeghi et al. [40]; data integrity and compatibility, Suresh et al. [4]; and policy concerns, Martonosi [41].

The security issues of industrial IoT could be classified into the forms of technology and security [12]. From the technology perspective, digital certification through an authoritarian security approach used to provide a closed system and sandbox environment in Apple and Microsoft smart devices may be considered a good security approach for industrial applications with closed boundaries. However, the tremendous market value of Google as soon as they introduced Android Technology which is an open-source solution, shows that security was not considered a priority by generic IoT consumers even with the high cases of cyber-attacks. On the contrary, the industries have seen the potential benefits of the technology. Still, they are not willing to compromise security at either the device, network, software, or reference architecture levels. The threats landscape of both IoT devices falls within the remit of Open System Interconnection (OSI) reference architecture. However, we will adopt a mix of the three and four-layer IoT threats actors architecture evidenced in recent studies [42].

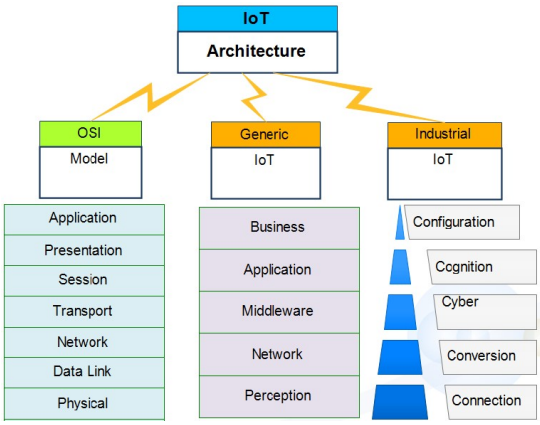

Figure 2 Unified Security-Based IoT Architecture

The architecture of consumer and industrial IoT shown in Figure 2 has different levels of control processes and adopts a unified intelligent five-level architecture [43] - [44] as applicable in most recent designs. It is the reference tool for connecting critical facilities (physical devices) within the field network to the internet. The connection process creates inter-operational and security challenges as a result of the vertical and horizontal communication structures. Data transmission in industrial IoT consumes a reasonable amount of bandwidth, and the inadequacy of the required bandwidth causes packets retransmission, processing delay and noise. For economic and technical reasons, edge computing is one of the ways of saving bandwidth and supporting short-latency applications.

- **The connection level** is composed of heterogeneous devices for data acquisition. The introduction of new IoT devices will improve the existing data acquisition systems in terms of security and reliability. Protocols such as NB-IoT, LTE-M, DASH7, NB-Fi, SigFox, and LoRa are innovative sensor data collection protocols enabling industrial IoT.

- **Conversion Level** is the machine component layer. Before the sensor data is processed, context-awareness is carried out to ascertain the nature of data expected from the various edge devices.

- **Cyber Level** is described as the central point for sensor data processing. IoT device performance is evaluated using visible benchmarked info-graphs designed using cyber level algorithms.

- **Cognition Level** aggregates the information obtained using big data analytics and deep machine learning techniques for system optimisation, task scheduling and intelligent decision making.

- **Configuration Level** is the decision state for self-configuration, network adjustment, and optimisation for resilience, variations, and disturbances.

According to Gilchrist [12], telematics (unidirectional), inquiries (bidirectional), commands (prioritised bidirectional) and notifications (single directional) are the conventional IoT communication patterns. Specific design requirements for industrial IoT include device capability, data storage, the scale of deployment, connectivity, and IP address which leaves every device identifiable in a network as a traffic source. IPv6 offers the best solution for IoT deployment at a massive scale with a seamless connection to the internet [45].

V. Industrial vs Consumer Internet of Things

Industrial IoT emerged from the generic/consumer-based IoT, and each technology is an enabler of disruptive innovations using similar hardware, software, and network technologies. As surveyed in [46], the industrial readiness for IoT adoption shows that IoT is permeating from the consumers to industry, creating technological gaps between the legacy industrial systems and the new IoT solutions. The recent botnet, dyne, and other cyber-attacks are due to new IoT technologies being developed without sufficient security. The definition of security in the two categories of IoT applications differs slightly. Security in consumer-based IoT means the privacy of the user data and confidentiality of the data generated contrary to safety and availability of services as additional features in industrial IoT. They are usually off the shelf solutions and are mostly designed with interest in functionality and time to market [47], giving rise to their wide range of deployment globally [30].

In a bid to analyse the current security challenges of both network domains and the potential impact associated with such permeation, we present the summary of findings of recent studies that acknowledges that such risks exist. The security of smart home controllers, as conducted in [47], showed high vulnerabilities when exposed to brute force, password, network-based remote, man-in-the-middle, and Address Resolution Protocol (ARP) attacks. Both have security limitations based on the platforms and networks level analysis of industrial and consumer-based IoT solutions [48]. A similar study that analysed the vulnerabilities of inter-connected ICS protocols and IoT devices using Shodan and Rapid7 showed increased use of outdated protocols without sufficient online security protection [49]. Many industrial IoT devices and protocols currently connected to the internet are not secured. Making CPS smart is to assist in failure prediction, proactive maintenance, physical process monitoring, and activity learning to improve overall system efficiency and effectiveness. An example could be the implementation of a smart grid with edge computing capabilities. Edge computing has been considered useful in improving data transfer for remote visualisation of condition monitoring, machine-to-machine communication and edge aggregation of data [50].

A. Consumer IoT Devices

Generic IoT involves internet-connected devices aimed at consumers. Such devices are connected to the internet mainly for the convenience that comes from remote access capabilities. Issues of privacy and confidentiality need to be addressed to prevent sensitive information from leaking, as was found in four smart medical IoT patient monitoring devices implemented using Secure Sockets Layer (SSL) and

Transport Layer Security (TLS) encryption [51]. Data encryption is not a complete solution as the network's user data traffic flow correlational analysis could reveal user behavioural patterns even when encrypted.

B. *Industrial IoT devices*

Industrial IoT is categorised into manufacturing, oil and gas, transportation, agriculture, health care, smart city and utilities. Legacy IIoT devices like IEDs still run on vulnerable operating systems, making them susceptible to malware infections. They are used to monitor and control industrial production lines and carry out real-time industrial processing locally or remotely. The devices are physically secured and installed in a restricted area but are vulnerable to network-related attacks. On-device edge-oriented security provides privacy preservation but has limited hardware capabilities for training data samples. Cloud intelligence security is suitable for scalable networks with access to larger training datasets but offers low privacy preservation and challenging network capacity unsuitable for latency-sensitive use cases.

VI. COUNTERMEASURE OPPORTUNITIES

There are opportunities as well as challenges of interconnecting IoT devices of both IT and OT settings. Integrating IT and OT networks introduce security risks across each domain's interfaces. Existing OT legacy firewalls and gateways lack the security capabilities to protect the OT domain from IT-related threats, given the trends of changing network architecture and the emergence of new security risks. IoT deployment can be inhibited by various deployment requirements classified into the node, link, path, and global problems [52]. Deployment requirements can also be based on the hardware, networking and software perspective. Nodes have issues of energy depletion, which at a certain level causes random behaviour. Such poor performance affects the functionality of other sensors within the system. The networking problems are mainly due to link type (symmetric or asymmetric), scheduling mechanism and energy utilisation. This is a big challenge in networks where the different sensor data rate is occasionally sent to a lower data-carrying communication link. Link failure means that a more significant part of the network will be cut off, and data sets will be lost. This creates a network congestion problem within the MAC protocol layer. The software errors such as watchdog timers, buffer overflow, incorrect patch download often result in node reboot, wrong readings, and non-packet forwarding. The countermeasure opportunities for managing these risks include:

A. *Next-Generation Firewall and Gateway*

Next-Generation Firewalls and Gateways (NGFW-Gs) enables the protection of both legacy OT and emerging IT networks from advanced cybersecurity attacks based on premediated rules in implementing the security capabilities. NGFW-G are intermediate hardware, software, and data-driven security approach for logical and physical, IT and OT network segmentation with a higher level of intelligence. Its consideration in future hybrid IoT networks will enforce access control, data encryption and management, system whitelisting, malware protection, patch update and management, and authorising communication from shielded IoT devices.

B. *Next-Generation Virtual Private Network*

Virtual Private Network Networks (VPNs) provide encrypted connection tunnels for IoT devices in separate locations as a layer of security for data exchanged. A VPN connection for IT and OT networks can be encrypted using

Table 1 IoT Attack Mechanisms, Impact and Countermeasure Opportunities

ATTACKS MECHANISMS	P	N	A	IMPACT	COUNTERMEASURES
Ransomware	✓		✓	Network and database access denial, Loss of device control and data (authenticity)	Root access implementation, code verification, and strong encryption system.
Data Leakage			✓	Loss of sensitive data (confidentiality)	Data leakage prevention system to prevent certain network operations, monitor the traffics.
Cloning	✓			Cloned IoT devices not identified could compromise the network, impersonation	Lightweight and strong authentication algorithms
DDoS	✓	✓	✓	Bandwidth-bursting, node energy depletion, reduced network performance due to network outages	Proactive boarder gateway protocols, intrusion protection and detection systems
Physical Attack	✓			Hardware and code modification that could lead to permanent damage, tampering, and destruction	Tamper proof packaging and physical security
Man-in-the-middle		✓		Loss of data	Implementation of lightweight and strong cryptographic methods
Routing, Sinkhole		✓		Compromised communication links (availability)	Geo-routing protocols
Jamming	✓			Service outage	Jamming traffic detection and re-routing
Eavesdropping	✓			Private data interception that could lead to future network attack	Access network security, node, and network segmentation
Replay		✓		Traffic flooding due to data retransmissions	Timestamp and session key implementation
Sybil		✓		Presence of pseudo-identities and node deception.	Social or behavioural based Sybil node detection algorithms.
Note: P – Perception, **N –** Network, **A -** Application					

industrial-grade security protocols such as OpenVPN, Transport layer Security (TLS), WireGuared, Internet Protocol Security (IPSec), and strong cryptographic primitives. The disadvantage of applying VPN in the OT network is the need for other software and support infrastructure not part of OT operating systems.

C. *Defense-in-Depth Security Architecture*

Implementing Defense-in-Depth (DiD) security approach with NGFW-G and Demilitarised Zone (DMZ) overcomes many security failures common in OT networks by providing multiple security layers. The many security layers introduce resilience for increased threats vectors detection. However, unified security models have the advantage of centralising network management roles and reducing the security hardware footprints across the network boundaries. DMZ will allow hybrid IT and OT networks to be decomposed into smaller network segments, each having NGFW-G. This offers more security visibility and effectively differentiates between cyber threats and system error as IT network security is limited in threat detection in OT networks.

D. *Encryption Techniques*

Various cryptographic algorithms have been proposed to solve the emerging cases of attacks on critical infrastructure. Cryptography security algorithms in the form of a private key (symmetric) and public-key (asymmetric) are the most commonly used security techniques [53]. Cryptography in this context is the method of protecting user/device data from unauthorised access. It is realised using the original data generated by the device, encrypted to protect the data readability/decrypted to recover the original data and cipher text which is the recovered data [54]. The security levels of the encryption algorithm are dependent on the size of the cypher key used. From the review of various crypto combinations, One-Time Password (OTP) and RSA, AES and RSA, AES and Fully Homomorphic Encryption (FHE), AES and Secure Hash Algorithm (SHA-2), OTP and Transposition Technique, Columnar cipher and vigenere cipher, and RSA and Triple DES have been implemented. Comparing the security requirement of AES, ARC4, Hash Message Authentication Code (HMAC), RNG, RSA, ECC security schemes at the code level in the SensorTile module (STEVAL-STLCX01V1) for industrial application, a stronger security system with increased speed of encryption and decryption and digitally signed keys were the observed advantages.

E. *Key Management System*

Certificate Authority (CA) based Key Management System (KMS) functions on the principles of cryptographic schemes in distributed automation networks [55]. KMS is responsible for registering and certifying Access Points (APs) and smart sensors and also manage their connection within trusted networks, as shown in Figure 3. The AP confirms the identity of smart sensors and issues them with a group key. The sensors termed smart should have the capabilities of aggregating datasets, manage power by switching between different power saving modes, and advertises routing information periodically. The roles of system initialisation, issuance of certification to initialised sensors, sensor's pseudonyms and private key generation, mutual authentication, secure group key distribution and key update resides at CA.

The problem of industrial IoT devices engaging in group communication is the management of key agreement protocols. Diffie-Hellman based security establishment protocols are useful in two-node active attack protection systems [46]. Studies requiring multiple nodes of active sensors message exchange invalidates the use of only Diffie-Hellman protocol as an attack protection protocol. The use of a pre-distribution key will also fail as more than two sensors will likely choose the same number of keys as the number of devices in the network grows due to an inextricable interconnectedness of the IoT devices [56]. In end-to-end encryption, asymmetric cryptography can be employed. The problem associated with encryption in a multi-tenant network environment is multiple encryptions that lead to increased data retransmission between the interconnected IoT devices, data traffic congestion, and increased power consumption [57]. It makes the encryption security methods not suitable for constrained industrial IoT. Where the IoT devices can withstand the key computing requirements due to the availability of a constant power source or increased memory and computational resources, the key management system, as illustrated in Figure 3, allows secure communication between IoT devices A and B with signed public and private keys.

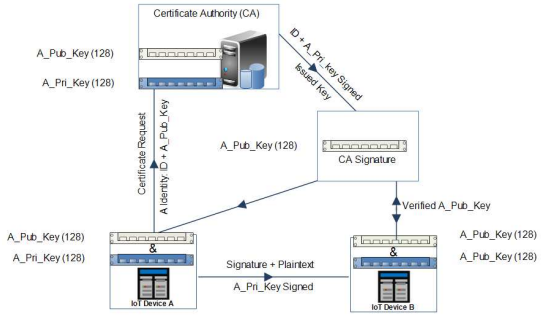

Figure 3 Certificate Authority Based Key Management System

F. *Cybersecurity Considerations and Recommendations*

- Categorising access authorisation and restriction for a certain group of IT devices to access OT networks by incorporating active directory-based policy, whitelisting, and blacklisting. This will reduce the extra complexity in implementing deep packet inspection.
- One layer of security protection is inadequate in hybrid IT and OT networks. NGFW-G functionalities should be enriched with system-wide threat and vulnerability detection, anomaly detection, process and zones classification, asset discovery, and data collection. To perform malware protection, intrusion prevention, and application intelligence and control in OT networks, unidirectional NGFW-G is most suitable.
- A hybrid IT and OT network should never be administered from less secured IoT devices and networks. All external and non-authenticated internal access should be classified as unsecured since they are the easiest path to compromising networks.

- OT and IT network should incorporate security by design, lightweight encryption, and zero trust architecture.

VII. Conclusion

Industrial and generic IoT networks have existed in separate spheres with different network and security requirements, but modern OT systems incorporate IT systems' capabilities. This implies that certain IT devices may be used in OT networks in such network scenarios while still connected to the IT network. Through detailed security analysis of industrial and consumer IoT networks and results from our previous projects, we have demonstrated that new security considerations such as NGFW-G are required to provide fine-grained security and application policies across organisational boundaries. Implementing defence-in-depth strategies will also help detect and respond to intrusions for internal and external security risks.

References

[1] Y. Uygun and E. B. Reynolds, *Advanced Manufacturing Innovation Ecosystems: The Case of Massachusetts*. 2017.

[2] S. Ugwuanyi and J. Irvine, "Intelligent internet of things (IoT) node demonstrator for device monitoring and control in the oil and gas sector," *arXiv*. 2019.

[3] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, 2018.

[4] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," *2014 Int. Conf. Sci. Eng. Manag. Res.*, pp. 1–8, 2014.

[5] T. Lennvall, M. Gidlund, and J. Akerberg, "Challenges when bringing IoT into Industrial Automation," pp. 932–937, 2017.

[6] Z. Anshu, Mittal; Andrew, Slaughter; and Paul, "Protecting the connected barrels Cybersecurity for upstream oil and gas A report by Deloitte Center for Energy Solutions," 2017.

[7] A. Nourian and S. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 1, pp. 2–13, Jan. 2018.

[8] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018, pp. 1–8.

[9] Lee Mathews, "Hackers Use DDoS Attack To Cut Heat To Apartments," 2016. [Online]. Available: https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#4e13f6f71a09. [Accessed: 06-Nov-2018].

[10] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, 2017.

[11] MARISA PEÑALOZA, "Ransomware Attack Shuts Down Colonial Pipeline : NPR," May-2021. [Online]. Available: https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline?t=1621954536124. [Accessed: 25-May-2021].

[12] Alasdair Gilchrist, "IoT Security Issues," *De|G Press*, 2017. [Online]. Available: https://ebookcentral.proquest.com/lib/strath/reader.action?docID=4810138&query=. [Accessed: 23-Jan-2018].

[13] U. S. Clusters, "Cyber security," p. 60, 2010.

[14] I. S. Issues and P. E. Central, "Alasdair Gilchrist IoT Security Issues," 2017.

[15] M. Hemmatpour, M. Ghazivakili, B. Montrucchio, and M. Rebaudengo, "DIIG: A Distributed Industrial IoT Gateway," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, pp. 755–759, 2017.

[16] S. Raza, *Lightweight Security Solutions for The Internet of Things*, vol. 2013, no. 139. 2013.

[17] P. D. Candidate and A. Paolo, "Design, implementation and experimentation of a protocol stack for the Internet of Things," no. July, 2012.

[18] T. Industrial, I. Consortium, and T. I. Internet, "Why We Build Testbeds : First Results," no. September, pp. 1–10, 2017.

[19] J. Wan, A. Canedo, and M. A. Al Faruque, "Security-aware functional modeling of Cyber-Physical Systems," in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2015, vol. 2015-October.

[20] G. S. Rose and G. S., "Security Meets Nanoelectronics for Internet of Things Applications," in *Proceedings of the 26th edition on Great Lakes Symposium on VLSI - GLSVLSI '16*, 2016, pp. 181–183.

[21] K. Sun, Y. Shen, Y. Lao, Z. Zhang, X. You, and C. Zhang, "A New Error Correction Scheme for Physical Unclonable Function," in *2018 IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2018*, 2019, pp. 374–377.

[22] Y. Ikezaki, Y. Nozaki, and M. Yoshikawa, "IoT device oriented security module using PUF," *IMFEDK 2016 - 2016 Int. Meet. Futur. Electron Devices, Kansai*, 2016.

[23] T. Idriss, H. Idriss, and M. Bayoumi, "A PUF-based paradigm for IoT security," *2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016*, pp. 700–705, 2017.

[24] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," *Dig. Tech. Pap. - IEEE Int. Solid-State Circuits Conf.*, vol. 59, pp. 158–160, 2016.

[25] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu, "A Novel Security Key Generation Method for SRAM PUF Based on Fourier Analysis," *IEEE Access*, vol. 6, pp. 49576–49587, 2018.

[26] H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura, "Cryptographie key generation from PUF data using efficient fuzzy extractors," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 23–26, 2014.

[27] "Traffic-Aware Patching for IoT Device Cyber Security," 2018. [Online]. Available: http://ieeexplore-spotlight.ieee.org/article/traffic-aware-patching-intermediate-nodes-cyber-security-iot-devices/. [Accessed: 19-Jan-2018].

[28] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of

Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, 2018.

[29] G. George, S. M. Thampi, and S. Member, "A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations," *IEEE Access*, vol. PP, no. c, p. 1, 2017.

[30] D. Wang, S. Lee, Y. Zhu, and Y. Li, "A zero human-intervention provisioning for industrial IoT devices," *Proc. IEEE Int. Conf. Ind. Technol.*, no. MiM, pp. 1271–1276, 2017.

[31] A. H. Raheem, "An Integrated Security Protocol Communication Scheme for Internet of Things using the Locator / ID Separation Protocol Network," 2017.

[32] B. L. Parne, S. Gupta, and N. S. Chaudhari, "SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network," *IEEE Access*, vol. 6, pp. 3668–3684, 2018.

[33] F. Liu, J. Xu, F. Hu, C. Wang, and J. Wu, "Lightweight Trusted Security for Emergency Communication Networks of Small Groups," vol. 23, no. 2, pp. 195–202, 2018.

[34] E. Abd-Elrahman, H. Ibn-Khedher, and H. Afifi, "D2D group communications security," *Int. Conf. Protoc. Eng. ICPE 2015 Int. Conf. New Technol. Distrib. Syst. NTDS 2015 - Proc.*, 2015.

[35] C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed Group Key Management for Event Notification Confidentiality among Sensors," *IEEE Trans. Dependable Secur. Comput.*, vol. X, no. c, pp. 1–15, 2018.

[36] Y. Qiu and M. Ma, "Secure Group Mobility Support for 6LoWPAN Networks," *IEEE Internet Things J.*, pp. 1–1, 2018.

[37] Y. Xu, R. Tan, S. Wu, and Q. Tang, "Connect internet with sensors by 6LoWPAN," *J. Networks*, vol. 8, no. 7, pp. 1480–1487, 2013.

[38] S. Ugwuanyi, R. Asif, and J. Irvine, "Network Virtualization: Proof of Concept for Remote Management of Multi-Tenant Infrastructure," in *Proceedings - 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application, DependSys 2020*, 2020.

[39] S. Bhattarai and Y. Wang, "Internet of Things Security and Challenges," *IEEE Computer*, no. to be published. 2018.

[40] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, pp. 1–6, 2015.

[41] M. Martonosi, "Keynotes: Internet of Things: History and hype, technology and policy," *2016 49th Annu. IEEE/ACM Int. Symp. Microarchitecture*, pp. 1–2, 2016.

[42] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[43] J.-Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1504–1526, 2017.

[44] W. Jin, Z. Liu, Z. Shi, C. Jin, and J. Lee, "CPS-enabled worry-free industrial applications," *2017 Progn. Syst. Heal. Manag. Conf. PHM-Harbin 2017 - Proc.*, 2017.

[45] S. Ugwuanyi, F. Attaran, S. Hussaini, and A. Merehil, "The State of IPv6 Deployment: A global Review," vol. 8, no. 4, pp. 1026–1035, 2017.

[46] X. Wang, H. Qiu, and F. Xie, "A survey on the industrial readiness for internet of things," *2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017*, vol. 2018-Janua, pp. 591–596, 2018.

[47] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," *2016 21st Asia South Pacific Des. Autom. Conf.*, pp. 519–524, 2016.

[48] S. Ugwuanyi and J. Irvine, "Security Analysis of IoT Networks and Platforms," in *2020 International Symposium on Networks, Computers and Communications, ISNCC 2020*, 2020.

[49] A. Hansson and A. Gurtov, "Analyzing Internet-Connected Industrial Equipment," pp. 29–35, 2018.

[50] S. Dol, "SMART motor for industry 4.0," *2018 IEEMA Eng. Infin. Conf.*, pp. 1–6, 2018.

[51] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext Data Transmissions in Consumer IoT Medical Devices," 2018.

[52] G. Ferrari, *Sensor networks : where theory meets practice*. Springer, 2009.

[53] M. Shankar and P. Akshaya, "Hybrid Cryptographic Technique U Sing Rsa," vol. 6, no. 6, pp. 39–48, 2014.

[54] K. Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing," 2017.

[55] Z. Sun, Q. Guo, and F. Sun, "Key Management for Feeder Automation Systems with Centralized Mode," in *2009 International Conference on Information Management, Innovation Management and Industrial Engineering*, 2009, pp. 456–459.

[56] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[57] K. Ghanem, R. Asif, S. Ugwuanyi, and J. Irvine, "Bandwidth and security requirements for smart grid," in *IEEE PES Innovative Smart Grid Technologies Conference Europe*, 2020, vol. 2020-October, pp. 36–40.