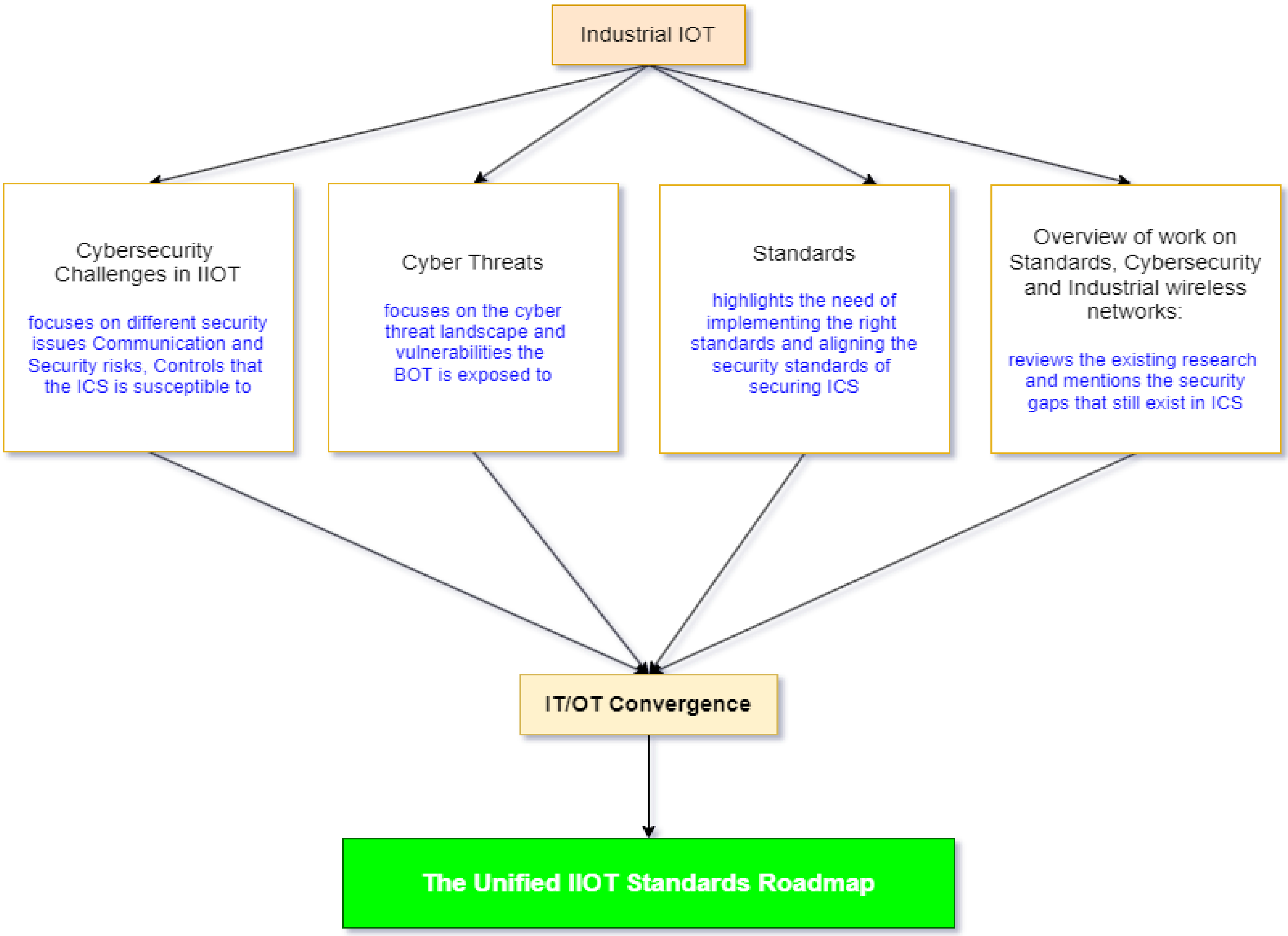
Industrial IOT: Security and Fog Computing

Overview:

Like many other fields, the IoT domain is growing very fast. However, with this growth comes many cybersecurity challenges. Previous research in the IoT domain has mostly focused on finding control measures to address deficiencies in different areas of IoT including security, privacy, vulnerabilities, and resiliency. However, the need for security standards and assessment frameworks that specifically focuses on IoT-based smart environments is also as important as the research itself. As part of the background and existing research work, this section will focus on the security and privacy concerns for IoT-based smart environments as well as existing research on security standards or assessment frameworks.

Security issues:

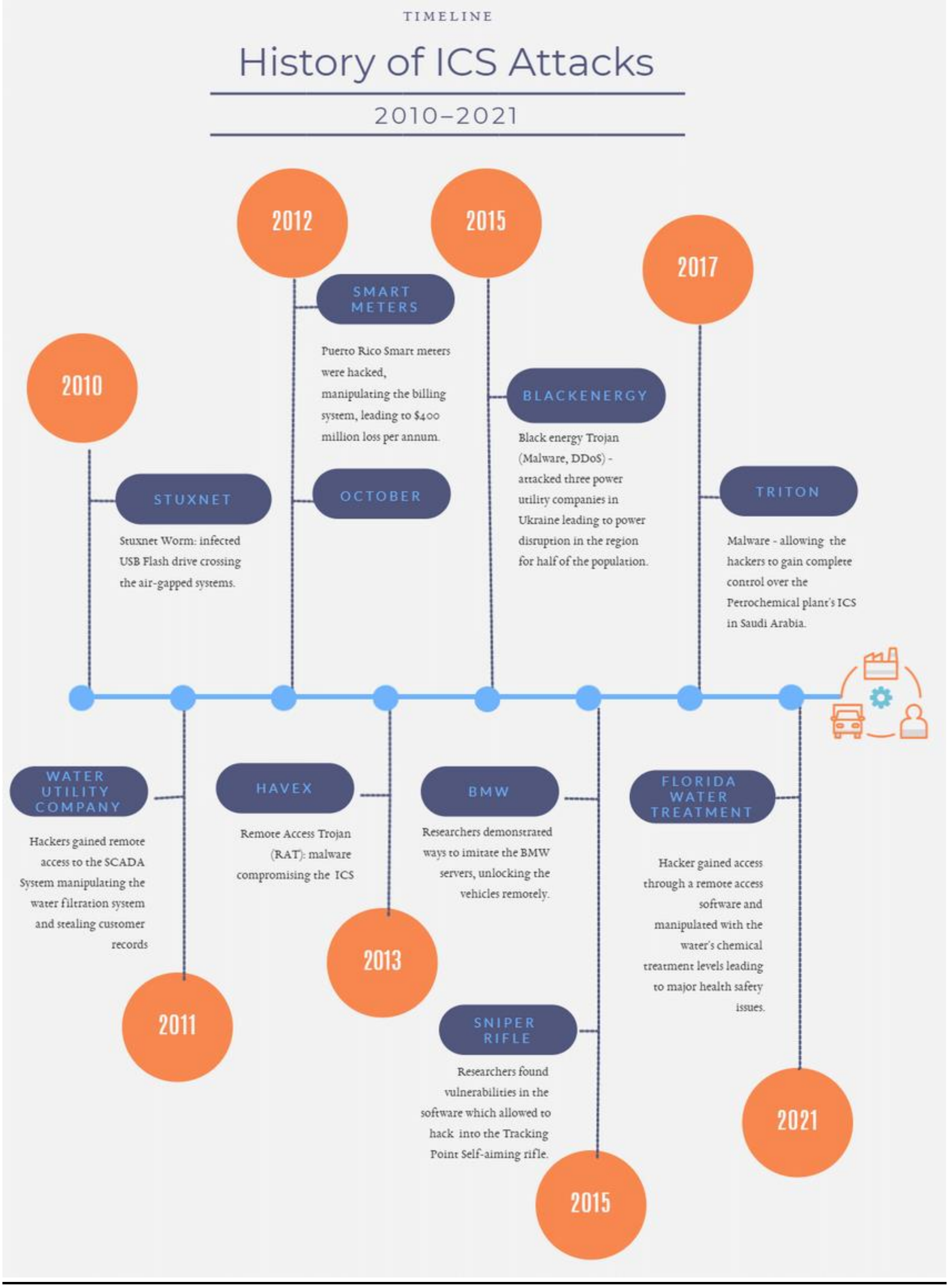
Cyberattacks at the operational technology (OT) level have grown considerably recently, as it involves integrating new interfaces (i.e., IT systems, cloud, etc.) providing flexibility and remote access to both new/old OT (i.e., SCADA, PLCs, etc.) systems. One of the reasons for the increased awareness in this domain is a significant increase in ICS cyberattacks (i.e., the USA's largest fuel-pipeline ransomware attack). Additionally, proprietary production knowledge becomes an IT security problem with Industrial IoT exposed to various types of cyber threats due to its dependency on new communication models and devices. Lack of convergence between IT and OT systems develops knowledge gaps allowing sophisticated and targeted cyberattacks to take place


Industrial IOT
Cybersecurity Challenges in IIOT
focuses on different security issues Communication and Security risks, Controls that the ICS is susceptible to
Cyber Threats
focuses on the cyber threat landscape and vulnerabilities the BOT is exposed to
Standards
highlights the need of implementing the right standards and aligning the security standards of securing ICS
Overview of work on Standards, Cybersecurity and Industrial wireless networks:
reviews the existing research and mentions the security gaps that still exist in ICS
IT/OT Convergence
The Unified IIOT Standards Roadmap

Security Controls and Standardization:

Threat intelligence frameworks provide visibility and classify threats based on predefined metrics. Outdated and legacy systems deployed in the production environment reduce the efficiency and impact of security controls.

A fully connected factory involves different applications, services, communication models, and cloud structures. Service level agreements are of high importance for assessing, aligning, and controlling the security, privacy, and quality of service (QoS) metrics associated with the I4.0 environment. Situations where SLAs are not assessed and monitored properly may lead to unexpected service disruption, downtime, and third-party subcontracting vendor issues.



TIMELINE

History of ICS Attacks

2010–2021

2010

STUXNET

Stuxnet Worm: infected USB Flash drive crossing the air-gapped systems.

2011

WATER UTILITY COMPANY

Hackers gained remote access to the SCADA System manipulating the water filtration system and stealing customer records

2012

SMART METERS

Puerto Rico Smart meters were hacked, manipulating the billing system, leading to $400 million loss per annum.

OCTOBER

2013

HAVEX

Remote Access Trojan (RAT): malware compromising the ICS

2015

BLACKENERGY

Black energy Trojan (Malware, DDoS) - attacked three power utility companies in Ukraine leading to power disruption in the region for half of the population.

2015

BMW

Researchers demonstrated ways to imitate the BMW servers, unlocking the vehicles remotely.

SNIPER RIFLE

Researchers found vulnerabilities in the software which allowed to hack into the Tracking Point Self-aiming rifle.

2017

TRITON

Malware - allowing the hackers to gain complete control over the Petrochemical plant's ICS in Saudi Arabia.

2021

FLORIDA WATER TREATMENT

Hacker gained access through a remote access software and manipulated with the water's chemical treatment levels leading to major health safety issues.

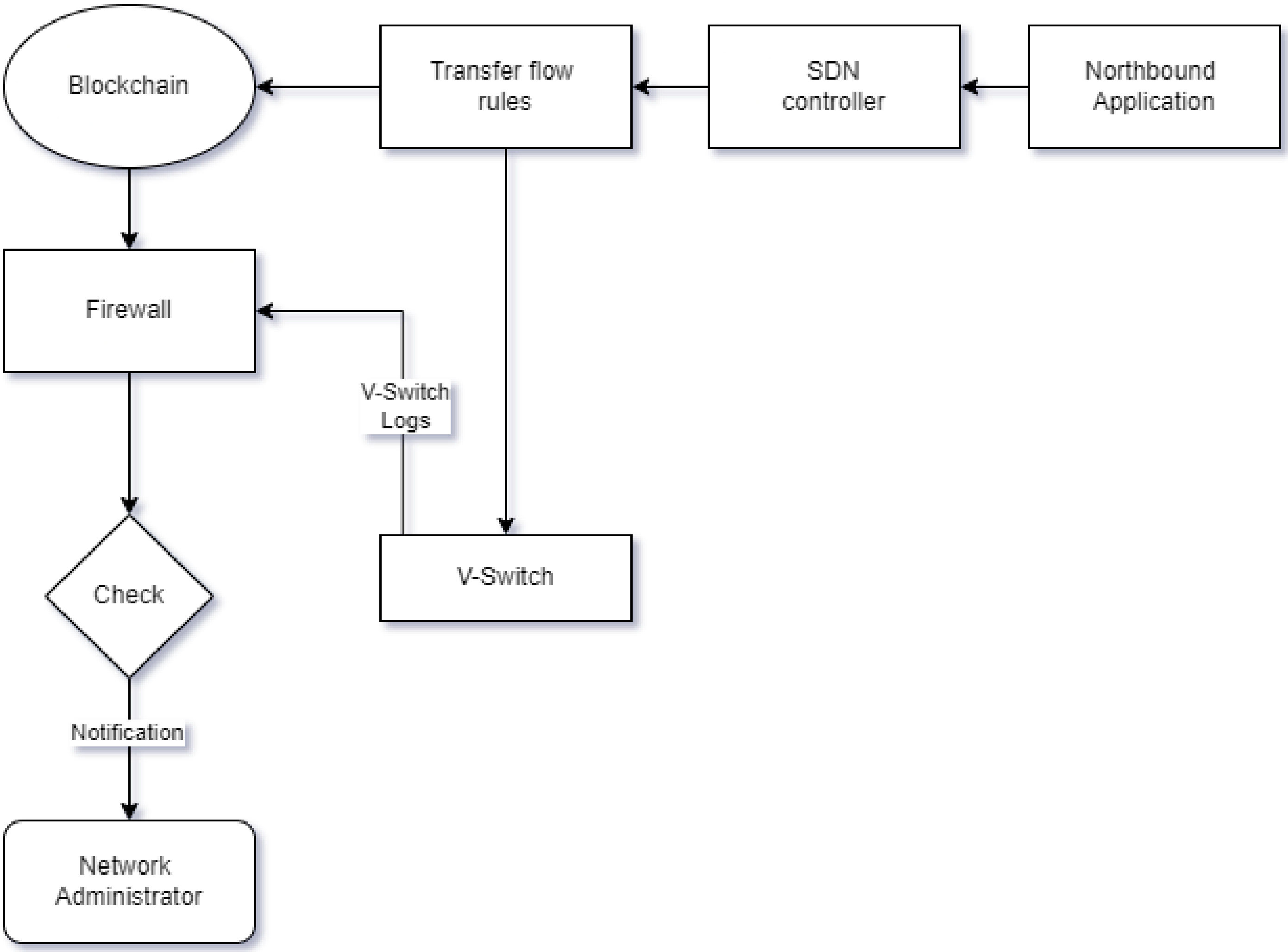
Blockchain-Based Integrity Checking System:

The Blockchain is the key element in the design of our integrity checking systems. The basic idea is to provide a solution where all flow rules that are generated from the controller are stored in a verifiable and immutable database.

Differently from the public blockchains, the private ones determine who is allowed to participate in the network, and defined actions and permissions are assigned to identifiable participants. Hence, consensus mechanisms such as Proof of Work are not required. Our blockchain is composed of only two nodes: SDN controller, and firewall. The SDN controller creates blocks and shares it with the firewall via the blockchain. The first node has all the permissions, i.e., read, write, and send, whereas the firewall can only read and receive.

Performance Evaluation:

BICS performance can be improved by adjusting the number of bogus rules put into the network. To do this test, we disconnect the SDN controller and inject the rules at the switch level. Table 9 illustrates the detection time and rate of BICS. We find that BICS achieves a 100% detection rate with a very short detection time. The complete detection rate is explained by the fact that the blockchain is immutable, which means that data recorded to a blockchain cannot be changed. To ensure immutability, the blockchain is built around two primary concepts: hashes and block chains, both of which are mathematically proven to maintain data integrity.

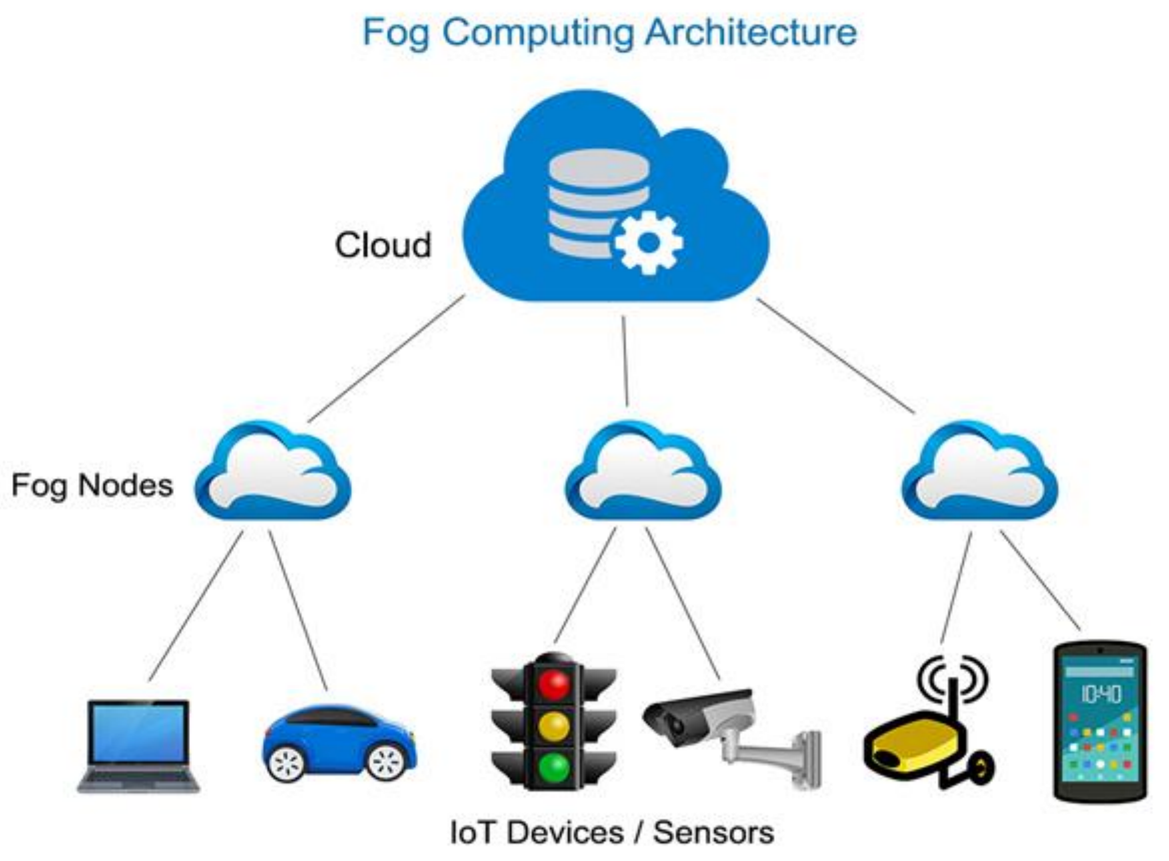


Fog Computing:

Fog is a relatively recent paradigm that presents new challenges for efficient and scalable network architectures. It is planned to expand steadily over the next few years in order to realize Industry 4.0. Energy conservation, real-time communication, efficient spectrum use, cache memory on edge devices, and resource allocation optimization are all unresolved concerns that must be addressed in order to enable future automation. Without such considerations, the guaranteed QoS needs of IoT devices may not be met. In the future, researchers must give solutions to these issues in order to further the industrial revolution. This study aims to provide a summary of existing solutions that use fog computing to enable Industrial IoT applications.

Fog computing provides services and applications similar to those provided by clouds, but with improved QoS parameters and performance that addresses important IIoT requirements. Important benefits of fog computing that impact its adoption for IIoT include:

- Data storage on network edge nodes decreases transmission delays by removing the requirement to obtain data from far clouds.
- Fog computing enables faster data processing and analysis for IIoT applications.
- Data storage on edge nodes will reduce processing and compute delays.
- Cache-enabled nodes prevent irrelevant information from being transmitted over the network.
- Can handle all IoT applications, including smart grids, smart cities, D2D, and vehicular ad hoc networks (VANETS), by utilizing the edge networking concept.
- Provides restricted and necessary contact between end devices and cloud service providers.



Questions:

Short Questions:

Q1) How does fog computing enhance security in Industrial IoT environments compared to conventional cloud-based approaches?

Q2) Discuss about the current issues in Industrial IOT?

Long Questions:

Q1) Explain in detail about fog computing?

Q2) Explain the idea of Block-chain integrity and discuss on its performance evaluation?

References:

- Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. IEEE Trans. Ind. Inform. 2014, 10, 2233–2243.
- Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmapLL Dhirani, E Armstrong, T Newe - Sensors, 2021 - mdpi.com
- Security and privacy in the industrial internet of things: Current standards and future challenges Gebremichael, LPI Ledwaba, MH Eldefrawy… - IEEE …, 2020 - ieeexplore.ieee.org
- Deploying fog computing in industrial internet of things and industry 4.0M Aazam, S Zeadally, KA Harras - … Transactions on Industrial …, 2018 - ieeexplore.ieee.org