Towards Security and Privacy of SCADA Systems through Decentralized Architecture

Abel O. Gomez Rivera, Deepak K. Tosh
Department of Computer Science, University of Texas at El Paso, TX, USA
aogomezrive@miners.utep.edu, dktosh@utep.edu

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems are typically of complex as well as centralized in nature which control and monitor the physical processes through field devices and actuators. SCADA systems are heavily utilized in Critical National Infrastructures, such as electrical power generation plants, water supplies, and gas pipelines. The proper and continuous operation of such systems is crucial for the economic growth of government and our society. The adoption of modern communication technologies in the SCADA system to enable efficient monitoring of human-inaccessible environment potentially introduces several security vulnerabilities including denial of service attacks, data and identity spoofing, and data poisoning etc.. Such security vulnerabilities negatively impact the system's operational capability. In this paper, we first review the security postures of modern SCADA systems by understanding the architectural components. Then, we analyze the security challenges and vulnerabilities associated with these architectures. We also provide a high level decentralized SCADA system architecture that potentially alleviates the above-stated security issues by utilizing the benefit of tamper-resistant ledger.**

***Keywords*—SCADA systems, Fossil Power Plants, Cybyer-Physical Systems, Identity Management, Blockchain.**

I. Introduction

Cyber-physical systems (CPS) are vastly used to monitor and control the physical process [1] of major industrial infrastructures including electric power grids, gas pipelines, and water networks [2]. The security of CPS in Supervisory Control and Data Acquisition (SCADA) systems is critical for the sustainability of society, i.e., prolonged outages of SCADA systems could result in catastrophic consequences to cyber-enabled critical services, such as energy, transportation, health, etc. SCADA systems found in power generation plants monitor the production of 48% of the total electricity produced in the U.S. Due to the significant role of SCADA systems, government, and academic research has started to focus on their cyber-security and security vulnerabilities [3]–[5].

SCADA architectures were initially designed to work isolated using proprietary communication protocols, such as Modbus, to exchange information [6]. The Modbus protocol does not consider cyber-security as significant concerns. It was designed to work in private networks where only trusted components are interconnected. The lack of proper security and authentication measures make Modbus vulnerable to standard cyber-attacks such as data manipulation, identity spoofing, denial of service (DoS), and others [7]. To ensure the security of critical components, modern SCADA systems implement physical access restrictions [8]. However, the adoption of modern communication protocols in the SCADA systems allows remote operators to monitor the state of devices. The restriction of physical access only protects the physical integrity of critical components, but it does not protect them from malicious users that can exploit vulnerabilities in the remote access protocols. Another approach to improve the security of SCADA systems has focused on the development of Intrusion Detection Systems (IDSs) and the implementation of the Distributed Network Protocol (DNP3). IDSs can detect data anomalies and abnormal operations of the overall system. However, state-of-art IDSs cannot precisely differentiate if the anomaly is the result of an attack or a defective device. The DNP3 protocols was designed to address the security gap of Modbus, DNP3 facilitate communications between substations as the collection and processing of data [9].

The modernization of SCADA systems removes the isolation that used to protect proprietary protocols. Legacy devices are now capable of connecting to the Internet through advanced Remote Terminal Units (RTUs) [1], which introduce cyber-security vulnerabilities that can affect data collection by field sensors. Cyber-attacks that target data are mainly categorized into three attack areas (1) Availability, (2) Confidentiality, and (3) Integrity [10]. To address the latest growth of cyber-attacks to critical infrastructures. The National Institute and Technology (NIST) has established a program that has three security objectives: (i) Network Protection, (ii) Authentication and Authorization, and (iii) Secure Communications Protocols [8], [10]–[12].

To address the security objectives outlined by the NIST, modern cyber-security solution that implements complex and costly algorithms such as cryptography, and hashing techniques are required. However, modern SCADA systems cannot adopt state-of-art cyber-security solutions. There are two major roadblocks to enable such adoption. First, standard CPS found at SCADA systems are low-end devices with limited resources, CPS devices in SCADA systems face challenges such as limited physical protection, limited capabilities, and legacy dependencies [13]. Second roadblock, state-of-art SCADA architectures are centralized architectures, i.e., a single central SCADA master controls and monitor a power generation plant. Centralized architectures are vulnerable to a single point of failure attacks [14], i.e., an attacker can compromise the complete system by taking control of a single entity. Ensuring NIST's security objectives (authentication, the integrity of data, and authorization of devices) with such strict limitations calls for lightweight protocols that ensure the security of legacy devices while introducing minimal overhead to the already complex network of SCADA systems. This paper analyzes the security vulnerabilities from the viewpoint of the devices

978-1-7281-5584-5/19/$31.00 ©2019 IEEE
DOI 10.1109/CSCI49370.2019.00230

within the industrial zone of SCADA systems, besides the state-of-art architecture analysis this paper introduces candidate solution that have the capabilities to address the security vulnerabilities of SCADA systems.

In this paper, we examine the following research questions:

1) What are the challenges that SCADA systems face in power generation plants?
2) How can a decentralized architecture address the challenges of SCADA systems and CPS?
3) How an identity management protocol can improve the security, privacy, and data integrity of SCADA systems?

Section II analyzes different approaches to address the security issue of SCADA systems. In Section III, we analyze the state-of-art SCADA architecture and components. We research the security threats associated with SCADA systems in Section IV. In Section V, we describe the challenges and opportunities of decentralized architectures and identity-management protocols. Finally, Section VI describes future work and concludes the paper.

II. Related Works

The literature of SCADA systems mostly focuses on the identification and categorization of security vulnerabilities [10], [15]–[17], by proposing frameworks to develop IDSs and define attack vectors. The assessments of SCADA systems try to identify the security vulnerabilities that can be potentially exploit by malicious users. Outside the vulnerability assessments of SCADA systems, we consider the importance of a consensus-based framework using blockchain to prevent data manipulation in power grids [18] as the closest related work to this paper. The consensus-based framework aims to eliminate data manipulation at the smart meter level commonly found at homes. Although blockchain has been rigorously exercised to achieve data provenance in cloud [19] [20], IoT [21], Internet of Battlefield Things [22] [23], smart city applications [24] etc., its applicability has not been well tested for security of SCADA systems.

Different from previous work, this paper analyzes the security vulnerabilities from the viewpoint of the industrial zone that in general consist of physical devices that capture and process environmental data. Besides the analysis of the security vulnerabilities in state-of-art SCADA architectures we identify candidate solutions that have the capabilities to address the security issues (e.g., authentication, spoofing of devices and data) of modern SCADA systems.

III. SCADA Architecture

State-of-art SCADA architectures consists of three major zones (1) Industrial Zone, (2) Industrial Demilitarized Zone, and (3) Enterprise Zone [25] (illustrate in fig. 1), in which sensor data is disseminate through legacy and proprietary protocols.

A. Industrial Zone

The Purdue Enterprise Reference Architecture (PERA) [25], namely the Purdue model, is a reference model used to describe different levels and zones on which SCADA

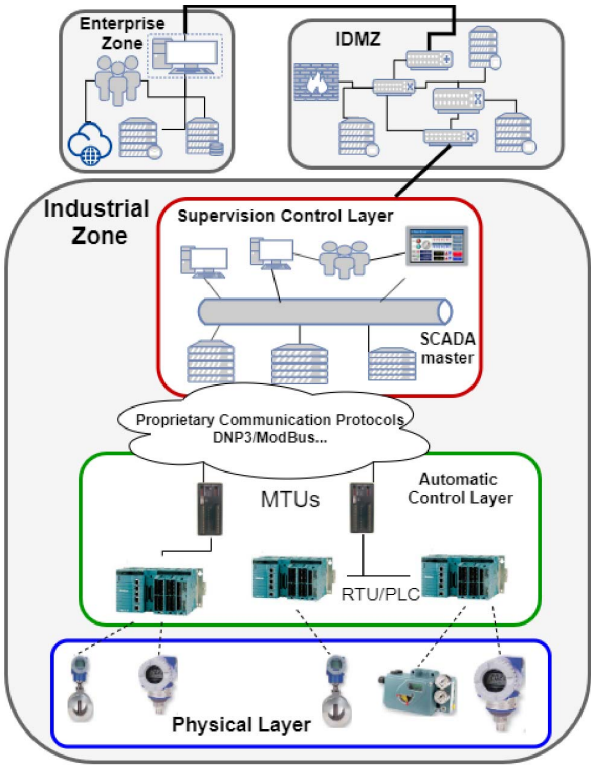

Fig. 1: State-of-art SCADA Architecture.

systems can be described. For the lowest zone (industrial zone) of the Purdue model, we analyze four main layers that describe operational processes and primary operation controls of SCADA systems: (1) Edge Physical Layer, (2) Automatic Control Layer, (3) Supervision Layer, and (4) Communication Protocols Layer [2].

1) Edge Physical Layer: The Edge physical layer consists of field devices, which varied from a wide range of sensors (e.g., temperature sensors), actuators (e.g., pumps, valves), and protection devices (e.g., circuit breakers). Physical devices monitor and collect data from their environment. They are usually low-end devices with limited capabilities and resources. In regular operation, the data gathered by such devices is analyzed and processed by the SCADA master. Data-driven architectures such as SCADA systems, require accurate, trusted, and real-time data.

Incorrect, delayed, or malicious data can affect the proper operation of Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). The SCADA master depends on both previous-mentioned devices to make critical operational decisions. We review two standard attacks that have the most impact in terms of data: (1) hide abnormal behavior by sending false information with normal states, an attacker can hide the impact to the system by sending fake data to monitor devices such as RTUs and SCADA master. This type of attack allows the attacker to disperse and impact a broader set of devices before being detected. (2) Opposite to the first attack, an attacker can trigger emergency shutdown protocols by sending false information with abnormal states, causing an outage in the power grid.

2) Automatic Control Layer: The control layer, as the name implies, controls, and monitors field devices. The layer consists of two major components (1) RTUs or PLCs and (2) Master Terminal Units (MTUs). RTUs/PLCs transform digital signals from the control center to analog signal and vice-versa. MTUs are more involved in the sense that they control the overall performance of the architecture. MTUs have more resources, which are used to implement security protocols to monitor the state and overall behavior of the network.

Modern MTUs can connect to the Internet, and remote users can control them. The deficient application of access control policies and the early adoption of DNP3 introduces security vulnerabilities to SCADA systems (e.g., elevation of privilege). A malicious user can get unauthorized access to one MTUs, and from the compromised device, the attacker can elevate the attack and take control of other critical components such as the SCADA master. MTUs also hold critical and private information regarding the operational state of the system. An attacker can obtain a copy of the data and then perform an offline analysis to design customs attacks like the Stuxnet attack that targeted specific controllers [26].

3) Communication Protocols Layer: DNP3 and Modbus are communication protocols that connect the SCADA master to the automatic control layer [1]. DNP3 was designed to address the security issues of Modbus. However, DNP3 and Modbus are still vulnerable to cyber-attacks, such as DoS attacks, man-in-the-middle attacks, and replay attacks [10]. The proprietary protocols of SCADA systems were designed to operate in a trusted environment, and they lack a robust security mechanism to authenticate the origin of data and devices within the SCADA system.

The evolution of communication protocols removed the isolation and weakened the security through obscurity of SCADA systems. Malicious users can utilize previous-mentioned attacks to disrupt the communication between the SCADA master and the operational components in the physical layer. If such communication is lost, the SCADA master might trigger a system reboot, which can cause an outage in cyber enable critical services.

4) Supervision Layer: The supervision layer is the highest layer of a typical Industrial Zone. It consists of multiple components such as SCADA master, Human-Machine Interface (HMI), and database servers. The supervision layer monitors and controls all physical operations.

The state of physical devices is monitor by the SCADA master through MTUs. MTUs forward the sensor data to the SCADA master through the communication layer. Then data sensor is analyzed by the SCADA master, which makes critical operational decisions, e.g., in a power generation plant, the combustion of coal must maintain a specific temperature to ensure its maximum utilization. The SCADA master regularly monitors the temperature of the boiler by requesting the MTUs the latest data from temperature sensors located at the boiler. If the SCADA master does not receive the information in a certain period or if the information is incorrect (due to a malicious user, or defective sensor), the SCADA master assumes a problem with the combustion. Such problem can trigger an emergency shutdown creating significant disruption in the overall operation of the system.

B. Industrial Demilitarized Zone

The Industrial Demilitarized Zone (IDMZ) delimits the perimeter of the SCADA network, it consists of firewalls and proxy servers that prevent the disclosure of private data. IDMZs are commonly used to enforce access control policies to Enterprise Zones. The implementation of such IDMZs is still in early adoption on SCADA systems.

C. Enterprise Zone

The Enterprise Zone hosts basic administration systems such as access to e-mail and the Internet. This zone usually summarizes data and information gathered from the Industrial Zone. Due to the openness of the Enterprise Zone and its direct connection to physical and operational devices, the Enterprise Zone introduces security vulnerabilities to the architecture such as unpatched systems and open access to the Internet.

IV. Security Threats

The adoption of standard communication protocols to enable efficient monitoring introduces security vulnerabilities to SCADA systems [1]. Authors in [27], through a cyber-security assessment of SCADA systems, identified that data flow is an essential security objective for such systems. Data flow relates to how the data is managed and transmitted. Protecting the data flow answers the following questions: Who is authorized to request information? What type of information is disclosed or requested? When and how information is provided?

Unauthorized access to critical and private data is a primary concern for modern SCADA systems. Malicious users can infiltrate the system and alter sensor data to introduce anomalies, which can also be originated by defective devices. Modern MTUs are equipped with IDSs to detect such data anomalies [28]. However, state-of-art IDSs face two challenges: (1) they may not comply with the standards of SCADA systems, (2) IDSs sometimes unable to differentiate the anomalies whether they were introduced by defective sensors or by malicious users. To develop a robust and more comprehensive IDSs, authors in [29] proposed to implement a custom Anomaly Detection Systems (ADSs), that comply with standard requirements of SCADA systems such as high availability, and real-time detection. The custom ADS can also detect if the anomaly was the result of an attack or a defective device.

State-of-art IDSs are reactive, i.e., the detection of an intrusion is detected after the fact. Reactive measures to detect intrusions are not enough to comply with the high availability requirement of SCADA systems [27]. SCADA systems must implement preventive measures instead of reactive to ensure high availability and a robust security. Such measures can be firewalls and proxy servers that analyze and block unauthorized access. Modern SCADA systems implement firewalls and proxy servers at the supervision control layer and the IDMZ. However, their implementation at lower levels, such as remote access points and MTUs, is not considered. The proper security of all assets is critical for the security of SCADA systems. SCADA systems typically have two types of assets physical and digital, which need to be secured. Physical assets are field sensors and devices (e.g., RTUs/PCLs, MTUs, and sensor devices). Digital assets are the information that field sensors gathered. To ensure the protection of these assets, NIST has

identified 3 primary security objectives for SCADA systems: (1) Availability, (2) Integrity, and (3) Confidentiality [10].

NIST's security objectives introduce a standardized security framework that recommends the most critical security vulnerabilities of SCADA systems. In [3], authors proposed an attack-tree model that assess NIST's security objectives based on password policies and port auditing. Although they provide possible attack vectors, the criteria for choosing them is not well defined. The research in [10] proposed to map and group NIST's security objectives into three attack categories: (1) availability, (2) confidentiality, and (3) integrity. An additional objective to ensure data provenance was proposed in [30]. Data provenance provides a way to track and identify activities since the data origin. To have a more comprehensive classification of the SCADA security threats, we classify them into three categories: (1) Privacy attacks, (2) Data Integrity attacks, and (3) Data Flow attacks. We define data flow as the stream of information that gets from field sensors to the SCADA master. Data integrity refers to the state of the data; for our purpose, we want to ensure that the data has not been altered during transmission. We consider that the data stream is private, and only authorized components in the SCADA system can view and analyze the data.

- Data Flow Attacks: This type of attack targets the capability of a SCADA master to access the information gathered by field sensors. A malicious user can potentially deploy a DoS attack to one MTU, disrupting communication between field sensors and the SCADA master.
- Privacy Attacks: These attacks aim to obtain unauthorized data from field sensors or any other critical information like passwords or configuration from the SCADA master or RTUs.
- Data Integrity Attacks: Field sensors continuously gather data from their environment, which is then sent to the automatic control layer over analog signals to RTUs or PLCs. RTUs transforms the analog signals of a field sensor into digital signals that are then forwarded to the MTUs. Malicious users can intercept the data and modify to represent a false state of the SCADA system, or they can fabricate fake data disrupting the flow of data and operations of the overall system.

In the following section, we analyze the advantages and disadvantages of candidate technologies and protocols that can provide a comprehensive solution to address the previous-mentioned attacks. We focus our analysis in a decentralized SCADA architecture that address the single point of failure vulnerability of centralized architectures.

V. Decentralized Architecture for Secure Data Flow in Power Generation Plants

State-of-art SCADA systems are not suited to address the security vulnerabilities (e.g., identity spoofing) that modern communication protocols introduce. SCADA architectures are centralized platforms in general, where a single controller entity manages the state and overall operation of the system. Previously-mentioned data attacks (described in section IV), can affect the performance of such a single entity, causing detrimental effects to the SCADA system.

In this section, we discuss the components of a decentralized SCADA architecture suitable to address data attacks like data flow, privacy, and data integrity. Furthermore, we analyze the security benefits and implementation challenges of a suitable blockchain-based SCADA architecture that modifies the functionality of critical components such as MTUs, and SCADA master. Figure 2 illustrates the suitable modified SCADA system that implements a blockchain platform to address the security vulnerabilities of the SCADA master, MTUs, and physical devices. The blockchain-based SCADA system will implement a decentralized platform, which replicates sensor data among multiple MTUs, eliminating the single point of failure vulnerability. Besides the decentralized platform, the SCADA architecture will also implement an identity manager device, responsible for the proper identification of each field sensor.

Our analysis focuses on the Industrial Zone, and it consists of four main security objectives: (1) data integrity, (2) confidentiality, (3) availability, and (4) authentication of field sensors. The blockchain-based SCADA assumes the following: there exists a secure local connection between the physical layer and the automatic control layer, and modern MTUs can support a full blockchain implementation. To have a comprehensive analysis of the decentralized SCADA architectures, we group NIST's security objectives in three categories: *(i) Authentication and Authorization, (ii) Accountability and Availability, (iii) Device's Identity*.

A. Device's Identity

The embedded and low-end devices of SCADA systems bring new challenges regarding its authenticity and identification. SCADA systems are private in general, where every device is trusted and known. However, malicious users can still introduce rogue devices, which can transmit fake measures to the SCADA master [31]. The detection and elimination of rogue devices is challenging and in general costly in terms of processing power and time. A suitable decentralized SCADA system must achieve two tasks to eliminate the possibility of rogue devices: (1) device authentication and (2) attestation [32]. State-of-art techniques to authenticate devices are not suitable for the low-end devices commonly found at SCADA systems. The low-end devices often lack the security capabilities necessary to implement proper authentication and attestation protocols. Additionally, the devices are resource-constrained, limiting the functionality and capabilities to perform extra work outside their intended operation [1], [32].

To circumvent the operational constraints of field devices, the decentralized SCADA architecture will introduce a new component called authentication manager. The authentication manager will provide standard authentication and attestation protocols. It will be deployed between RTUs/PLCs and MTUs. Moreover, it will ensure the authenticity of data with minimal disruption to the already deployed operational system. By developing a comprehensive authentication and attestation protocol, the manager will rank field devices based on the sensibility of their data and how possible it is to exploit a vulnerability in the device [17]. The authentication manager

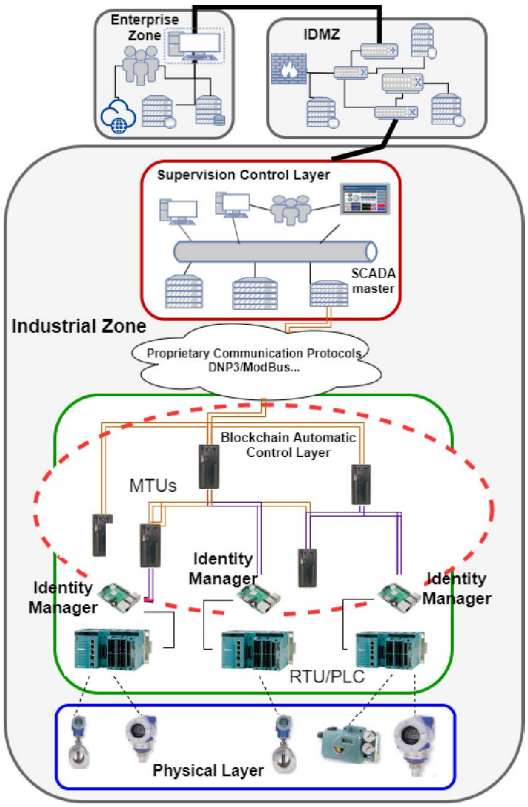

Fig. 2: Blockchain-based SCADA Architecture.

will provide hardware authentication protocols such as physical unclonable functions (PUFs) that will generate unique IDs based on unique physical characteristics [33]. The implementation of PUFs will ensure data origin, which can provide data provenance eliminating malicious data, i.e., MTUs nodes will be capable of validating incoming traffic before storing it. MTUs will have the ability to verified data origin, and unauthorized or abnormal data will be filtered out. PUFs will also be utilized to implement a continuous attestation protocol. The unique ID generated through PUFs will be randomly and continuously checked during the life cycle of the device.

B. Accountability and Availability

The standard requirement of high availability in SCADA systems introduces challenges to the network. A SCADA master needs a constant flow of information from field devices to make operational decisions. In general, SCADA masters have enough resources to monitor and control the overall operations of the system, but they are not resilience to cyber-attacks, (e.g., a single point of failure). The availability of centralized architectures such as SCADA systems can be affected if its central entity gets compromised by malicious users. A suitable decentralized platform such as blockchain could improve the resilience to cyber-attacks and availability of SCADA systems.

The blockchain platform of the decentralized architecture will introduce a peer-to-peer network that will interconnect the SCADA master and MTUs. The common distributed storage of blockchain called distributed ledger will hold all sensor data, and it will be disseminated among all peers of the blockchain [34]. By nature blockchain platforms implement a distributed append-only and immutable ledger, which will provide three essential attributes: (1) non-repudiation where devices will be accountable for their transactions, (2) data integrity that will ensure that the information is valid and accurate, and (3) data provenance that will provide a method to validate data origin. The SCADA master will utilize the distributed ledger to monitor the behavior of field sensors, detecting abnormal data or rouge devices. In general, blockchain platforms provide high availability by distributing responsibility and resources among multiple devices [18].

C. Authentication and Authorization

A blockchain-based SCADA system must adequately monitor and manage the identities of all devices in the system. The correct identification of the devices enables a trusted network where only honest peers can initiate and maintain communications. In general, blockchain platforms are vulnerable to Sybil attacks. In a Sybil attack, a malicious user creates false blockchain peers that can be used to overdrive the network policies by forcing a malicious consensus among false and real peers [35]. To avoid Sybil attacks, a robust implementation of an identity management protocol is needed, which will also be responsible for implementing access control policies of the blockchain-based SCADA system.

The identity management protocol will be deployed on the blockchain peers, and will provide three standard functions: (1) identity provisioning, (2) update, revocation, and (3) lookup of access privileges [36]. Devices of the blockchain-based SCADA system will only be responsible for a set of limited activities, (e.g., send sensor data, request a measure from a sensor). The devices will only have the minimum required privileges to fulfill their assignments. If a device tries to access unauthorized information or if the identity management protocol identifies abnormal behavior, access to such a device will be revoked. With the implementation of the identity management protocol, the blockchain-based SCADA system will eliminate the possibility of a privilege escalation attack.

VI. Concluding Remarks and Future Work

SCADA systems are heavily used in National Critical Infrastructures, such as power generation plants. The proper and continuous operation of the critical infrastructures is of extreme importance for the security of cities and society. Modern SCADA systems have adopted proprietary devices and communication protocols to enable efficient remote monitoring. However, due to legacy constraints, modern SCADA systems still utilize legacy protocols such as Modbus to exchange data among internal devices. Legacy SCADA communication protocols were designed to work in isolated networks, and their design does not consider cyber-security as significant concerns. The adoption of remote monitoring protocols opens SCADA systems to the Internet, due to this, modern SCADA systems are vulnerable to cyber-attacks such as DoS attacks.

In this paper, we analyzed the security challenges and vulnerabilities of modern SCADA systems. Furthermore, we reviewed suitable solutions that have the potential to address its security vulnerabilities: (1) blockchain, and (2) identity management protocols. First, we analyzed the advantages of a

new identity management solution to monitor field sensors' authentication, and access management. Second, we analyzed the impact of introducing a blockchain platform that tightens the security postures of RTUs and SCADA master. In future work, we will implement and evaluate the proposed blockchain-based SCADA platform in a simulated environment.

REFERENCES

[1] A. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2015, pp. 1–6.

[2] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of scada systems against cyberphysical attacks," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 5, pp. 28–45, May 2017.

[3] C. Ten, G. Manimaran, and C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, July 2010.

[4] (2014, Jun.) Energy Sector. [Online]. Available: https://www.dhs.gov/cisa/energy-sector

[5] G. Falco, C. Caldera, and H. Shrobe, "Iiot cybersecurity risk modeling for scada systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4486–4495, Dec 2018.

[6] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[7] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *CoRR*, vol. abs/0909.0576, 2009. [Online]. Available: http://arxiv.org/abs/0909.0576

[8] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," vol. 56, pp. 1–27, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815001388

[9] R. Amoah, S. Camtepe, and E. Foo, "Formal modelling and analysis of dnp3 secure authentication," *Journal of Network and Computer Applications*, vol. 59, pp. 345 – 360, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804515001228

[10] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1–8.

[11] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, December 2017.

[12] E. Madhan, U. Ghosh, D. K. Tosh, K. Mandal, E. Murali, and S. Ghosh, "An improved communications in cyber physical system architecture, protocols and applications," in *16th Annual IEEE Intl. Conference on Sensing, Communication, and Networking (SECON)*, 2019, pp. 1–6.

[13] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyberphysical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.

[14] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for iot," in *Internet of Things – ICIOT 2018*, D. Georgakopoulos and L.-J. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 3–18.

[15] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52 – 80, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548215000207

[16] C. Ten, C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *2007 IEEE Power Engineering Society General Meeting*, pp. 1–8.

[17] H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyberphysical systems," vol. 67, pp. 57–71, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302679

[18] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[19] D. K. Tosh, S. Shetty, P. Foytik, C. Kamhoua, and L. Njilla, "Cloudpos: A proof-of-stake consensus design for blockchain integrated cloud," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 2018, pp. 302–309.

[20] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach," *IEEE Consumer Electronics Magazine*, vol. 8, no. 4, pp. 38–44, 2019.

[21] A. Gomez, D. K. Tosh, and L. Njilla, "Scalable blockchain implementation for edge-based internet of things platform," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019.

[22] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure internet-of-battlefield things (iobt) architecture," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 593–598.

[23] E. Buenrostro, A. Gomez, D. K. Tosh, J. Acosta, and L. Njilla, "Evaluating usability of permissioned blockchain for internet-of-battlefield things security," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019.

[24] A. A. Malik, D. K. Tosh, and U. Ghosh, "Non-intrusive deployment of blockchain in establishing cyber-infrastructure for smart city," in *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2019, pp. 1–6.

[25] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in Industry*, vol. 101, pp. 1 – 12, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166361517307285

[26] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[27] I. Nai Fovino, L. Guidi, M. Masera, and A. Stefanini, "Cyber security assessment of a power plant," vol. 81, no. 2, pp. 518–526, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378779610002452

[28] Q. Zhu, C. Rieger, and T. Baar, "A hierarchical security architecture for cyber-physical systems," in *2011 4th International Symposium on Resilient Control Systems*, pp. 15–20.

[29] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," vol. 99, pp. 45–56, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0142061517328946

[30] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," vol. 67, pp. 469–482, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790617313423

[31] P. Koopman, "Embedded system security," *Computer*, vol. 37, no. 7, pp. 95–97, Jul. 2004. [Online]. Available: http://dx.doi.org/10.1109/MC.2004.52

[32] W. Feng, Y. Qin, S. Zhao, and D. Feng, "Aaot: Lightweight attestation and authentication of low-resource things in iot and cps," *Computer Networks*, vol. 134, pp. 167 – 182, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618300471

[33] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, pp. 9–14.

[34] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, July 2018.

[35] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technology Engineering Management Conference (TEMSCON)*, June 2017, pp. 137–141.

[36] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for internet of things in enterprises," in *Trust, Privacy and Security in Digital Business*, S. Furnell, H. Mouratidis, and G. Pernul, Eds. Cham: Springer International Publishing, 2018, pp. 167–181.