digital

MDPI

Article

SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture

Panagiotis Radoglou Grammatikis [1], Panagiotis Sarigiannidis [1,*], Christos Dalamagkas [2], Yannis Spyridis [3], Thomas Lagkas [4], Georgios Efstathopoulos [3], Achilleas Sesis [3], Ignacio Labrador Pavon [5], Ruben Trapero Burgos [5], Rodrigo Diaz [5], Antonios Sarigiannidis [6], Dimitris Papamartzivanos [7], Sofia Anna Menesidou [7], Giannis Ledakis [7], Achilleas Pasias [8], Thanasis Kotsiopoulos [8], Anastasios Drosou [8], Orestis Mavropoulos [9], Alba Colet Subirachs [10], Pol Paradell Sola [10], José Luis Domínguez-García [10], Marisa Escalante [11], Molinuevo Martin Alberto [11], Benito Caracuel [12], Francisco Ramos [12], Vasileios Gkioulos [13], Sokratis Katsikas [13], Hans Christian Bolstad [14], Dan-Eric Archer [15], Nikola Paunovic [16], Ramon Gallart [17], Theodoros Rokkas [18] and Alicia Arce [19]

[1] Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece; pradoglou@uowm.gr

[2] Testing Research & Standards Center of Public Power Corporation SA, Leontariou 9, Kantza, 15351 Athens, Greece; c.dalamagkas@dei.gr

[3] Infinity Limited, 2A Heigham Road Imperial Offices, London E6 2JG, UK; yannis@0infinity.net (Y.S.); george@0infinity.net (G.E.); achilleas@0infinity.net (A.S.)

[4] Department of Computer Science, International Hellenic University, 14th km Thessaloniki, 57001 Nea Moudania, Greece; tlagkas@cs.ihu.gr

[5] ATOS Spain SA, Calle De Albarracin 25, 28037 Madrid, Spain; ignacio.labrador@atos.net (I.L.P.); ruben.trapero@atos.net (R.T.B.); Rodrigo.diaz@atos.net (R.D.)

[6] Sidroco Holdings Ltd., Petraki Giallourou 22, Office 11, Nicosia 1077, Cyprus; asarigia@sidroco.com

[7] UBITECH Limited, 26 Nikou & Despinas Pattchi, Limassol 3071, Cyprus; dpapamartz@ubitech.eu (D.P.); smenesidou@ubitech.eu (S.A.M.); gledakis@ubitech.eu (G.L.)

[8] Center for Research and Technology Hellas, Information Technologies Institute, 6th km Charilaou-Thermi Road, 57001 Thessaloniki, Greece; pasiasach@iti.gr (A.P.); kotsiopoulos@iti.gr (T.K.); drosou@iti.gr (A.D.)

[9] Cyberlens Ltd., 10 12 Mulberry Green Old Harlow, Essex CM17 0ET, UK; orestis.mavropoulos@cyberlens.eu

[10] Fundacio Institut De Recerca De L'Energia De Catalunya (IREC), C/ Jardins De Les Dones De Negre 1, 08930 Sant Adria de Besos, Spain; acolet@irec.cat (A.C.S.); pparadell@irec.cat (P.P.S.); jldominguez@irec.cat (J.L.D.-G.)

[11] TECNALIA, Basque Research and Technology Alliance (BRTA), Parque Cientifico Y Tecnologico De Bizkaia, Astondo Bidea, Edificio 700, 48160 Derio Bizkaia, Spain; Marisa.Escalante@tecnalia.com (M.E.); Alberto.Molinuevo@tecnalia.com (M.M.A.)

[12] Schneider Electric, Rue Joseph Monier 35, 92500 Ruel Malmaison, France; benito.caracuel@gmail.com (B.C.); francisco.ramos@se.com (F.R.)

[13] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Hogskoleringen 1, 7491 Trondheim, Norway; vasileios.gkioulos@ntnu.no (V.G.); sokratis.katsikas@ntnu.no (S.K.)

[14] SINTEF, Sem Saelandsveg 11, 7465 Trondheim, Norway; hans.christian.bolstad@sintef.no

[15] CheckWatt AB, Marketenterivagen 1, 41528 Gotebord, Sweden; daneric.archer@checkwatt.se

[16] Realaiz, Mihajla Bogicevica 7, 11000 Beograd, Serbia; nikola.paunovic@realaiz.rs

[17] Estabanell, Calle Rec 26-28, 08400 Granollers, Spain; rgallart@estabanell.cat

[18] INCITES Consulting, 130 Route d'Arlon, L-8008 Strassen, Luxembourg; trokkas@incites.eu

[19] Control Systems Laboratory, Ayesa, 41092 Seville, Spain; aarce@ayesa.com

* Correspondence: psarigiannidis@uowm.gr

check for updates

Citation: Grammatikis, P.R.; Sarigiannidis, P.; Dalamagkas, C.; Spyridis, Y.; Lagkas, T.; Efstathopoulos, G.; Sesis, A.; Pavon, I.L.; Burgos, R.T.; Diaz, R.; et al. SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture. *Digital* **2021**, *1*, 173–187. https://doi.org/10.3390/digital1040013

Academic Editor: Yannis Manolopoulos

Received: 27 April 2021
Accepted: 24 September 2021
Published: 30 September 2021

Abstract: The technological leap of smart technologies and the Internet of Things has advanced the conventional model of the electrical power and energy systems into a new digital era, widely known as the Smart Grid. The advent of Smart Grids provides multiple benefits, such as self-monitoring, self-healing and pervasive control. However, it also raises crucial cybersecurity and privacy concerns that can lead to devastating consequences, including cascading effects with other critical infrastructures or even fatal accidents. This paper introduces a novel architecture, which will increase the Smart Grid resiliency, taking full advantage of the Software-Defined Networking (SDN) technology. The proposed architecture called SDN-microSENSE architecture consists of three main tiers: (a) Risk assessment, (b) intrusion detection and correlation and (c) self-healing. The first tier is responsible for evaluating dynamically the risk level of each Smart Grid asset. The second tier undertakes to detect and correlate security events and, finally, the last tier mitigates the potential threats, ensuring in parallel the normal operation of the Smart Grid. It is noteworthy that all tiers of the SDN-microSENSE architecture interact with the SDN controller either for detecting or mitigating intrusions.

Keywords: anomaly detection; blockchain; cybersecurity; energy management; honeypots; intrusion detection; islanding; privacy; Smart Grid; Software Defined Networking

1. Introduction

The evolution of the Industrial Internet of Things (IIoT) is leading the conventional Electrical Power and Energy Systems (EPES) into a new digital paradigm, widely known as the Smart Grid (SG). Based on S. Tan et al.'s stufy [1], the SG will compose the biggest Internet of Things (IoT) application in the near future. Thus, multiple benefits are provided to both energy consumers and energy utilities, such as many customer choices, pervasive control, self-monitoring and self-healing. However, this progression also creates severe cybersecurity and privacy risks that can lead to devastating consequences or even fatal accidents. It is noteworthy that due to the strict interdependence between the energy sector and the other critical infrastructures, the EPES/SG cybersecurity incidents can severely impact the other critical domains. A characteristic cyberattack against the energy sector was an Advanced Persistent Threat (APT) [2], resulting in a blackout for more than 225,000 people in Ukraine. Similarly, multiple APTs have targeted EPES, such as `DragonFly` [3], `TRITON` [4] and `Crashoverride` [3].

The vulnerable nature of EPES/SG is mainly related to the legacy Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Such systems utilise insecure communication protocols, such as Modbus [5], Distributed Network Protocol 3 (DNP3) [6] and IEC 60870-5-104 [7], that have not been designed with the essential authentication and authorisation mechanisms. While both academia and industry have already provided useful security solutions, such as the IEC 62351 standard, unfortunately, many vendors and manufacturers cannot adopt them, especially in real-time. Moreover, it is worth mentioning that many challenges arise from the IoT area [8]. In particular, the IoT inherits the vulnerabilities of the conventional Internet model. Secondly, the vast amount of the IoT data is an attractive goal for potential cyberattackers.

Therefore, based on the aforementioned remarks, this paper presents the SDN-microSENSE architecture, which aims to strengthen the EPES/SG resiliency. To this end, SDN-microSENSE focuses on three tiers: (a) Risk assessment, (b) intrusion detection and correlation and (c) self-healing. The proposed architecture takes full advantage of the Software-Defined Networking (SDN) technology in order to recognise, mitigate or even prevent the potential cyberattacks and anomalies. It should be noted that SDN-microSENSE is a research Horizon 2020 programme co-founded by the European Union.

The rest of this paper is organised as follows. Section 2 discusses similar works. Section 3 presented the proposed architecture, detailing the role of each component. Finally, Section 5 concludes this paper.

2. Related Work

Many papers have examined the cybersecurity and privacy issues of the energy sector. Some of them are listed in [9–17]. In particular, in our previous work in [14], we provide a detailed survey of the Intrusion Detection Systems (IDS) in SG. In [9], P. Kumar et al. present a comprehensive study, detailing the SG cyberattacks and relevant cybersecurity incidents. Moreover, they introduce a threat model and taxonomy, discussing cyberattacks, privacy concerns and appropriate solutions. In [10], I. Stellios et al. provide a methodology, which is utilised in order to evaluate IoT cyberattacks for Critical Infrastructures. Based on this methodology, they also identify relevant security controls. M. Hassan et al. in [11] discuss differential privacy techniques for Cyber-Physical Systems (CPS). In [12], H. Karimipour et al. present a deep and scalable Machine Learning (ML) system in order to recognise cyberattacks against large-scale SG environments. T. Nguyen et al. in [13] study various countermeasures to increase the electrical power grid's resiliency. In a similar manner, the authors in [15] analyse and review various works concerning how the SDN technology can improve the SG security. In [16], A. Musleh et al. provide a survey regarding the detection of false data injection attacks in the SG. Finally, in [17], the authors provide a survey about the firewall systems for SG/EPES. Next, we emphasise on similar works regarding (a) threat modelling in SG, (b) intrusion detection in SG environments and (c) mitigating or even preventing cyberattacks through SDN. Each paragraph focuses on a dedicated case. Finally, based on this brief literature review, we identify how the proposed architecture is differentiated.

In [18], E. Li et al. introduce a combined method for identifying and evaluating the potential threats against a Distribution Automation System (DAS). In particular, the proposed method relies on attack trees and the Common Vulnerability Scoring System (CVSS) [19] in order to specify the possible threats and then to assess them quantitatively. First, the authors introduce the DAS architecture by identifying the functional characteristics and the security requirements. Next, the authors explain how the CVSS is applied to the attack tree by calculating the CVSS score for each leaf node and path, thereby calculating the most threatening path. Next, based on the DAS architecture defined earlier, the authors specify an attack tree, which considers both the network and physical attacks. Moreover, the leaf nodes correspond to specific Common Vulnerabilities and Exposures (CVEs) whose CVSS score is calculated by the US National Vulnerability Database. Therefore, the CVSS is applied in the entire attack tree, and the most threatening tree is computed. Finally, it is worth mentioning that the authors evaluate their method with a similar one, which relies on the Bayes method and CVSS. Based on this evaluation, first, the proposed method is verified since both methods compute similar results. Secondly, the proposed method calculates higher attack probabilities than that using the Bayes methods and CVSS.

In [20], E. Rios et al. present a continuous quantitative risk management methodology for SG environments. While the paper is focused on SG, the proposed method can be applied in any Information Technology (IT) and IoT ecosystem. In particular, after discussing relevant works, the authors explain the proposed methodology, which consists of five phases, namely (a) system Attack Defence Tree (ADT) modelling, (b) risk assessment over ADT, (c) risk sensitivity analysis over ADT, (d) risk optimisation of defences and (e) continuous refinement of risk evaluation. In the first phase, the ADT is formed, by enumerating and structuring the various underlying threats as well as the respective countermeasures. Next, the second phase calculates (a) the probability, (b) the impact, (c) the cost and finally (d) the risk of each ADT node. Next, the risk sensitivity analysis examines the sensitivity of each ADT node by investigating possible fluctuations in their values. Subsequently, the risk optimisation of defences intends to optimise the countermeasures, taking into account possible technical or administrative constraints, such as the security budget. Finally, the last phase monitors and evaluates continuously the risk-related values (probability, impact, cost and risk) during the system operation, thus providing the appropriate feedback. The authors validate the proposed method by carrying out each phase in a real smart home environment.

The authors in [21] provide an anomaly-based IDS for the IEC 60870-5-104 protocol, which relies on essential access control and outlier detection. The proposed IDS consists of two main components: (a) Sensor and (b) server. The sensor is composed of three modules: (a) Network Traffic Monitoring Module, (b) Network Packet Access Control Module, and (c) IEC-104 Flow Extraction Module. The Network Traffic Monitoring Module undertakes to capture the IEC 60870-5-104 network traffic, using a switched port analyser. The Network Packet Access Control Module adopts a whitelist, which defines the legitimate Medium Access Control (MAC), the IP addresses and the 2404 port, which is the default Transmission Control Protocol (TCP) port for the IEC 60870-5-104 protocol. If the details of an IEC 60870-5-104 packet (i.e., source/destination addresses and source/destination ports) do not agree with the whitelist, then an alert is raised. It is worth mentioning that the alerts are stored in an Elasticsearch database on the server-side. Next, the IEC-104 Flow Extraction Module extracts the TCP/IP network flow statistics used by the outlier detection mechanism for detecting possible anomalies. On the other hand, the server consists of (a) the Anomaly Detection Module and (b) the Response Module. The Anomaly Detection Module applies the outlier detection algorithm, which will distinguish whether an IEC 60870-5-104 is anomalous or not. To this end, three outlier detection algorithms were tested: (a) One-Class Support Vector Machine (SVM), Local Outlier Factor (LOF) and Isolation Forest under different flow timeout thresholds: 15 s, 30 s, 60 s and 120 s. Finally, the Response Module informs the security administrator via Kibana. Based on the evaluation results, Isolation Forest achieves the best performance when the flow timeout is defined at 120 s.

In our previous work [22], we developed DIDEROT. DIDEROT is an Intrusion Detection and Prevention System (IDPS) capable of detecting and mitigating cyberattacks against the DNP3. The architectural model of DIDEROT consists of three modules, namely (a) Data Monitoring Module, (b) DIDEROT Analysis Engine and (c) Response Module. The Data Monitoring Module undertakes to capture the DNP3 network traffic and generate bidirectional network flow statistics. To this end, `Tshark` [23] and `CICFlowMeter` [24] were utilised respectively. Moreover, the Data Monitoring Module is responsible for normalising these statistics by applying the min-max scaling function. Next, the DIDEROT Analysis Engine is composed of two ML classifiers that operate complimentarily. The first classifier detects particular DNP3 cyberattacks (i.e., multiclass classification), including (a) DNP3 injection, (b) DNP3 Flooding, (c) DNP3 reconnaissance, (d) DNP3 replay attacks and (e) DNP3 masquerading. If the first classifier classifies a network flow as normal, then the second classifier is activated to distinguish a possible anomaly (i.e., binary classification). The functionality of the first classifier relies on a decision tree, while the second adopts the DIDEROT autoencoder. Finally, based on the outcome of the DIDEROT Analysis Engine, the Response Module generates security events and informs the `Ryu` SDN controller in order to corrupt the malicious network flow. The evaluation results demonstrate the efficacy of DIDEROT to detect DNP3 cyberattacks.

In [25], P. Manso et al. provide an SDN-based IDPS, which combines the `Ryu` SDN controller and Snort in order to mitigate DoS attacks. The architectural model consists of three virtual machines representing (a) the internal network simulated by `Mininet`, (b) the SDN-based IDPS and (c) online services. It is noteworthy that the second virtual machine (i.e., that hosting the SDN-based IDPS) hosts both `Ryu` and `Snort`. First, Snort receives the overall network traffic through a port mirroring capability provided by `Open vSwitch (OVS)` [26] of the first virtual machine (i.e., Mininet). If Snort detects a potential cyberattack, it informs `Ryu` based on a UNIX domain socket. Next, `Ryu` transmits the appropriate OpenFlow commands to `OVS` of the first virtual machine (i.e., `Mininet`), thus isolating the malicious nodes. The authors evaluate their IDPS with three distributed denial-of-service (DDoS) scenarios, measuring (a) DDoS mitigation time, (b) average Round Trip Time and (c) packet loss. The experimental results demonstrate the efficiency of the proposed IDPS.

The authors in [27] present the SPEAR Security Information and Event Management (SIEM) system. SPEAR SIEM focuses mainly on EPES/SG environments by detecting and correlating relevant security events. In particular, SPEAR SIEM is composed of three architectural layers: (a) Data Capturing layer, (b) Detection Layer and (c) Correlation Layer. In the first layer, SPEAR sensors and the Data Acquisition and Parsing System are responsible for gathering and pre-processing a variety of data, including (a) network flow statistics, (b) packet payload information and (c) operational data (i.e., time-series electricity measurements). Next, the detection layer undertakes to recognise potential anomalies and cyberattacks. To this end, two components are utilised: (a) Big Data Analytics Component and (b) Visual-based Intrusion Detection System (VIDS). The first is capable of detecting a plethora of threats by adopting three detection kinds: (a) Network flow-based detection, (b) packet-based detection and (c) operational data-based detection. On the other side, VIDS utilises advanced visualisation techniques through which the security administrator can recognise additional anomalies not detected previously by the first component. Moreover, VIDS operates as the main dashboard of the SPEAR SIEM. Finally, the last layer is responsible for correlating the security events produced by the previous layer, thus composing security alerts and updating the trust values of the involved EPES/SG assets.

The authors in [28] present an anomaly-based IDS for EPES/SG. The proposed IDS uses operational data (i.e., time-series electricity measurements), and its architecture consists of four modules, namely: (a) Data Collection Module, (b) Pre-Processing Module, (c) Anomaly Detection Module and (d) Response Module. The first module is responsible for collecting the various operational data. The second module isolates and normalises the necessary features. Next, the anomaly detection module uses an outlier detection model, thus recognising possible outliers/anomalies. In particular, six outlier detection methods are tested: (a) Principal Component Analysis (PCA), (b) OneClassSVM, (c) Isolation Forest, (d) Angle-Based Outlier Detection (ABOD), (e) Stochastic Outlier Selection (SOS) and (f) autoencoder. Finally, based on the detection outcome, the Response Module informs the user about the presence of potential security events. The main innovation of this work is the complex data representation during the pre-processing step. The evaluation results demonstrate the efficiency of the proposed IDS.

Admittedly, the previous works present useful methodologies and tools. They focus mainly on detecting and mitigating potential threats. However, none of them provides an integrated solution, combining the functional cybersecurity tiers illustrated by Figure 1. In particular, the proposed solutions do not consider the unique characteristics of EPES/SG in order to mitigate efficiently the various cyberattacks and anomalies. Before the application of a mitigation strategy, the corresponding countermeasures should consider the sensitive nature of EPES/SG. For instance, the isolation of some malicious network flows corresponding to not critical disturbances can cause more disastrous consequences. In addition, the above works do not consider emergencies where appropriate measures should take place in near real-time in order to avoid cascading effects. Finally, the various solutions have to take into account the quality of the energy grid. Therefore, appropriate energy-related optimisation methods should take place when a cyberattack or anomaly is carried out. Based on the aforementioned remarks, SDN-microSENSE aims to provide an integrated solution that will incorporate detection, mitigation and optimisation systems into a common platform. This paper focuses on the architecture behind SDN-microSENSE, detailing the technical specifications of each component and their interfaces. It is noteworthy that due to the complexity of the overall SDN-microSENSE solution and the presence of multiple components, this paper is devoted only to the SDN-microSENSE architecture without discussing in detail the technical details for each component and the corresponding evaluation results. To the best of our knowledge, SDN-microSENSE constitutes the first solution, which integrates and harmonises (a) collaborative risk assessment, (b) intrusion detection and correlation and (c) self-healing into a common platform. Some individual works that demonstrate the efficiency of the corresponding SDN-microSENSE components are given in [29–32].

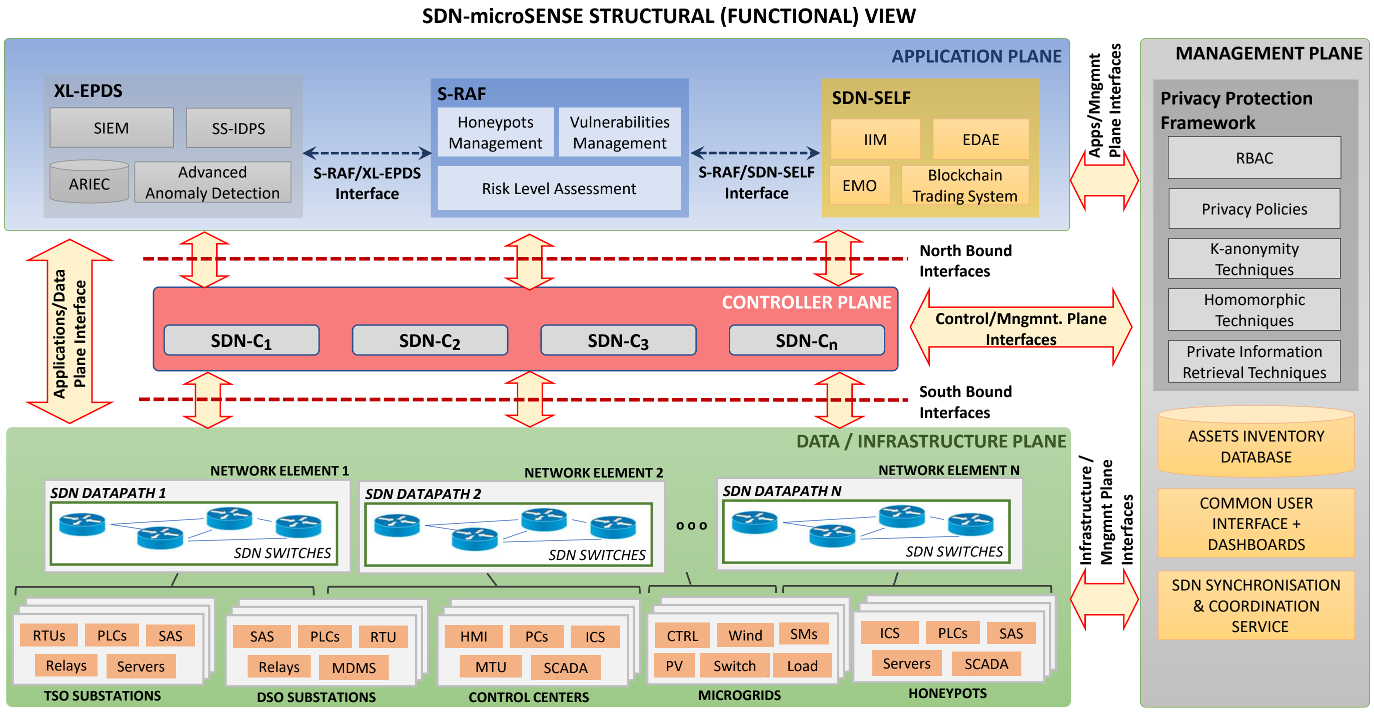

Figure 1. SDN-microSENSE Architecture—Structural View.

3. SDN-microSENSE Architecture

Figure 2 depicts the SDN-microSENSE business logic based on the SDN architectural model. It comprises three main conceptual frameworks [33], namely (a) SDN-microSENSE Risk Assessment Framework (S-RAF), (b) Cross-Layer Energy Prevention and Detection System (XL-EPDS) and (c) SDN-enabled Self-healing Framework (SDN-SELF) that are deployed throughout the four SDN planes: (a) Data Plane, (b) Control Plane, (c) Application Plane and (d) Management Plane. The term *conceptual framework* refers to a set of functions and relationships within a research area [33]. Therefore, the SDN-microSENSE frameworks mentioned earlier focus on the following cybersecurity-related research areas: (a) Risk assessment, (b) intrusion detection and correlation and (d) self healing and recovery. Each of the SDN-microSENSE frameworks takes full advantage of the SDN technology in order to detect, mitigate or even prevent possible intrusions. In particular, S-RAF instructs the SDN Controller (SDN-C) to redirect the potential cyberattackers to the EPES/SG honeypots. The EPES/SG honeypots constitute a security control of S-RAF. Next, XL-EPDS uses statistics originating from the SDN-C to detect possible anomalies or cyberattacks related to the entire SDN network. Finally, SDN-SELF communicates with the SDN-C in order to mitigate possible intrusions and anomalies. The following subsections analyse the components and the interfaces of each SDN-microSENSE framework.

A more detailed view of the SDN-microSENSE architecture, along with the interfaces between the various planes, is depicted in Figure 1. The structural view is based on the SDN architecture, as defined by the Open Networking Foundation (ONF) [34] and Request for Comments (RFC) 7426 [35], and follows the rationale of decoupling the network control with the forwarding functions. Therefore, according to the above specifications, the conceptual frameworks are placed within the Data, Controller, Application, and Management Planes. In particular, the Data Plane contains the EPES/SG infrastructure, the honeypots and the SDN switches. The Controller Plane consists of multiple SDN controllers that receive guidance from the Application and Management Planes and configure the Data Plane accordingly. The conceptual frameworks and their components are placed within the Application Plane. In this plane, the most important operational decisions take place, such as the detection of a cyberattack or the decision to isolate a malicious network flow. Finally, the Management Plane provides all complementary functionalities related to the system usability, including dashboard, databases, and privacy preserving mechanisms to ensure the privacy of data subjects affected by the SDN-microSENSE operation. It is worth mentioning that the Management Plane is placed vertically since it provides complementary services to all planes. Indicatively, the Asset Inventory database is used by all components of the Application Plane in order to access information related to the underlying EPES/SG components. Concurrently, the SDN Synchronisation and Coordination Service (SCS) is accessed by both the Application Plane and the Controller Plane to retrieve the master SDN-C for a particular switch and carry out the master SDN-C election process, respectively.

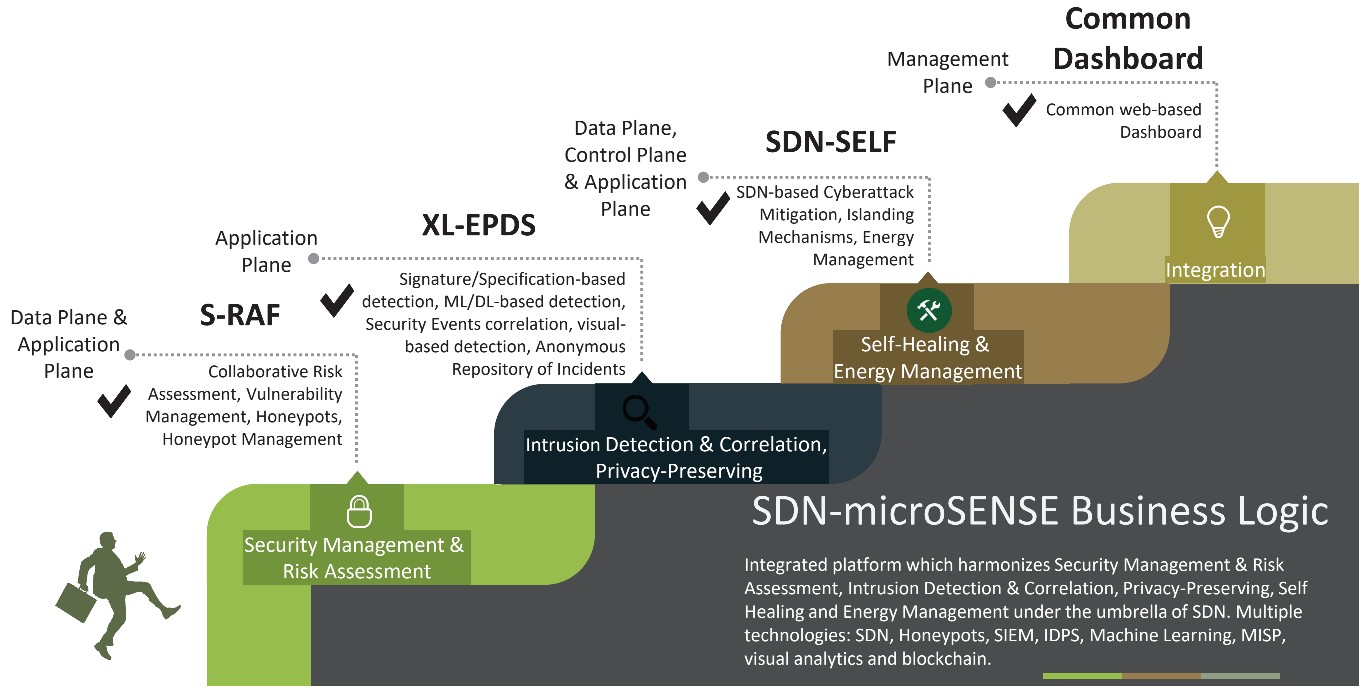
Common Dashboard
Management Plane
✓ Common web-based Dashboard
SDN-SELF
Data Plane, Control Plane & Application Plane
✓ SDN-based Cyberattack Mitigation, Islanding Mechanisms, Energy Management
XL-EPDS
Application Plane
✓ Signature/Specification-based detection, ML/DL-based detection, Security Events correlation, visual-based detection, Anonymous Repository of Incidents
S-RAF
Data Plane & Application Plane
✓ Collaborative Risk Assessment, Vulnerability Management, Honeypots, Honeypot Management
Integration
Self-Healing & Energy Management
Intrusion Detection & Correlation, Privacy-Preserving
Security Management & Risk Assessment
SDN-microSENSE Business Logic
Integrated platform which harmonizes Security Management & Risk Assessment, Intrusion Detection & Correlation, Privacy-Preserving, Self Healing and Energy Management under the umbrella of SDN. Multiple technologies: SDN, Honeypots, SIEM, IDPS, Machine Learning, MISP, visual analytics and blockchain.

Figure 2. SDN-microSENSE Business Logic.

3.1. *S-RAF: SDN-microSENSE Risk Assessment Framework*

S-RAF is a framework that undertakes to implement collaborative and dynamic risk management. Moreover, apart from this role, S-RAF includes a set of EPES/SG honeypots that hide and protect the real EPES/SG assets. The following subsections analyse both the collaborative risk assessment and the EPES/SG honeypots of the SDN-microSENSE architecture.

3.1.1. Security Management and Risk Assessment

An essential function of the SDN-microSENSE architecture is the collaborative and dynamic risk assessment. To this end, S-RAF follows a methodology consisting of seven steps: (a) determining the goal of the EPES risk assessment, (b) analysis of the EPES organisations, (c) EPES cyberthreat analysis, (d) vulnerability analysis, (e) impact analysis (f) risk assessment and (g) risk mitigation. Thus, following this methodology, S-RAF receives the security events and alerts coming from XL-EPDS and incorporates into this information a cumulative risk value for each involved asset and the corresponding connections.

3.1.2. EPES/SG Honeypots and Honeypot Manager

According to [36], a honeypot is "an information system whose value lies in unauthorised or illicit use of the resource". In other words, honeypots are commonly used as an extra security layer in order to act as a decoy, which lures the cyberattackers and captures useful information about their identity and activities [37]. SDN-microSENSE provides a variety of EPES/SG honeypots that implement realistic emulations for three EPES/SG communication protocols: (a) IEC-61850, (b) IEC-60870-5-104, and (c) Modbus/TCP. In more detail, the IEC-61850 honeypot emulates real intelligent electronic devices usually located in circuit breakers of the substations by parsing the Intelligent Capability Description (ICD) files. On the other side, the IEC-60870-5-104 and Modbus/TCP honeypots rely on Conpot. Furthermore, it is noteworthy that the Modbus/TCP honeypot can imitate the responses of the real EPES/SG assets by integrating a generative adversarial network.

The deployment and the lifecycle management of the aforementioned EPES/SG honeypots are provided by the Honeypot Manager (HM). The HM constitutes a web-based interface, which allows the security administrator to inspect the security events and alerts received by XL-EPDS and decides regarding the deployment of an EPES/SG honeypot. In addition, the HM leverages the northbound interface of the SDN-C by dynamically redirecting the malicious network traffic towards the EPES/SG honeypots. The redirection can be activated manually by the HM operator based on the security events and alerts received by XL-EPDS. This mechanism aims to enforce the cyberattackers to react with the EPES/SG honeypots, thus collecting useful information about their activities.

3.2. XL-EPDS: Cross Layer Energy Prevention and Detection System

The XL-EPDS framework utilises various kinds of data in order to detect timely and reliably potential EPES/SG intrusions and anomalies. To this end, the framework integrates a SIEM system especially designed for the energy sector. The proposed SIEM system called XL-SIEM includes a plethora of intrusion and anomaly detectors related to the EPES/SG communication protocols. Moreover, it ensures the privacy of the involved entities through the Overlay Privacy Framework (OPF). Finally, XL-EPDS incorporates an anonymous repository of incidents called ARIEC, which allows the EPES organisations to share with each other the cybersecurity incidents. Each XL-EPDS component is further analysed below.

3.2.1. XL-SIEM and Detectors

XL-SIEM composes a SIEM system capable of detecting multiple EPES cyberattacks by allowing the interconnection with a myriad of security detectors. In particular, the XL-SIEM consists of (a) XL-SIEM agents for processing information received from security detectors and distributed across the EPES infrastructure and (b) the XL-SIEM core, which integrates an event correlation engine, a database and a management dashboard. The security detectors are deployed throughout the EPES infrastructure and undertake to recognise various EPES cyberattacks and anomalies, generating the respective security logs. To this end, both signature/specification-based techniques and ML/DL-based methods are applied. First, `Suricata` is used with the `Quickdraw ICS` signatures and specification rules developed during the project. Next, a set of ML/DL-based detectors [38] are responsible for discriminating cyberattacks and anomalies against a plethora of EPES protocols, such as Modbus/TCP, DNP3, IEC 61850 (Generic Object Oriented Substation Event (GOOSE)), IEC 60870-5-104, Message Queuing Telemetry Transport (MQTT) and Network Time Protocol (NTP). Moreover, there is a detector called `Nightwatch`, which is able to discriminate potential anomalies related to the entire SDN network based on the statistics given by the SDN-C. OPF constitutes another detector of XL-SIEM, ensuring the privacy of EPES/SG entities and transferring relevant security logs to XL-SIEM whether they are relevant violations. Finally, the Discovery tool constitutes a visual-based anomaly detector, which provides the appropriate visual interfaces through which the security administrator can distinguish the presence of an anomaly that possibly cannot be detected by the aforementioned detectors. Next, the XL-SIEM agents are responsible for collecting and normalising the various security logs generated by the XL-SIEM detectors with a standardised format. The normalised events are called security events and are transmitted by the XL-SIEM agents to the XL-SIEM engine or external components. Subsequently, the XL-SIEM engine receives the security events and correlates them, thus producing security alerts. A security alert is defined as a set of security events related to each other through the correlation rules defined by security experts. Finally, the XL-SIEM database and XL-SIEM dashboard store and visualise the security events and alerts generated by XL-SIEM, respectively.

3.2.2. ARIEC: Cloud-Based Anonymous Repository of Incidents

To be aligned with the Directive on security of Network and Information Systems (NIS) [39], which requires mandatory reporting of the cybersecurity incidents by the EPES organisations, the SDN-microSENSE architecture introduces ARIEC, which is a repository of anonymised security events and alerts originating from XL-SIEM. In the context of ARIEC, both security events and alerts are called cybersecurity incidents. They are also accompanied by the risk information calculated by S-RAF. Therefore, ARIEC allows storing and sharing technical details of the cybersecurity incidents among different EPES organisations belonging to a trusted network without identifying the victim identity or other sensitive information that can affect the reputation of the EPES organisation. ARIEC follows a centralised architecture, which relies on the Malware Information Sharing Platform (MISP) and anonymisation procedures based on the differential privacy and Natural Language Processing (NLP) techniques.

3.3. SDN-SELF: SDN-enabled Self-hEaLing Framework

The goal of the SDN-SELF framework is twofold. First, it mitigates the possible anomalies and intrusions detected by XL-EPDS. Secondly, SDN-SELF is responsible for the energy management and optimisation required after the mitigation processes. In particular, SDN-SELF comprises five components: (a) Electric Data Analysis Engine (EDAE), (b) the Islanding and optImisation fraMework (IIM), (c) the rEstoration Machine-learning framewOrk (EMO) and (d) the Blockchain-based Energy Trading System. Each component of the SDN-SELF framework is further analysed in the following subsections, respectively.

3.3.1. EDAE: Electric Data Analysis Engine

Leveraging the SDN programming capabilities, EDAE undertakes to maximise the grid observability and protect the EPES/SG infrastructure in case of cyberattacks or failures. In particular, EDAE continuously monitors the underlying network against Quality of Service (QoS) constraints (e.g., latency and available bandwidth) provided by the EPES/SG operator and the cybersecurity incidents delivered by S-RAF. In comparison to existing state of the art, refs. [40–44] EDAE aims to combine the satisfaction of QoS, security and observability requirements in a single optimisation scheme. Three main scenarios are distinguished, namely:

- *Scenario A: QoS constraints are not satisfied*. Supposing the communication quality is degraded in a manner that criteria of minimum latency cannot be satisfied. In that case, EDAE employs the PaDe [45] genetic algorithm in order to decompose the multi-objective problem of path reconstruction to multiple single-objective ones that are resolved using the asynchronous generalised island model to distribute the solution process [46]. The final solution (i.e., the optimal path that maximises the grid QoS and observability) is obtained as the set of the best individual solution in each single-objective island.
- *Scenario B: An EPES/SG device is disconnected from the network*. In a more specific scenario that a Phase Data Concentrator (PDC) is disconnected from the network, the Phasor Measurement Units (PMUs) connected to that PDC should be reallocated to the next available PDC so that the security and QoS constraints are not validated for any of the existing PMUs. In this case, a Mixed-Integer Linear Programming algorithm chooses and applies the best PMU reallocation scheme to minimise the overall network latency. This problem is also studied by [40]; however, authors are limited to maximising observability, while EDAE also addresses QoS and security requirements.
- *Scenario C: Change of security risk*. Supposing that the security risk of an intermediate switch changes dramatically, EDAE finds alternative paths so that the risk level of

the rest infrastructure will be maintained while the QoS requirements of the rest applications are intact.

3.3.2. IIM: Islanding and optImisation fraMework

The purpose of IIM is to preserve the stability of the EPES infrastructure by offering intentional islanding schemes in case of severe disturbances (e.g., disruptions caused by cyberattacks, extreme natural phenomena or human errors), thus avoiding cascading failures that can potentially lead to a blackout. Activated as a response to specific security incidents received from S-RAF, IIM collects information regarding the triggering event, as well as the current status of the grid, and delivers appropriate islanding recommendations, which are evaluated and applied by the system operator. More specifically, the islanding solutions aim to partition the grid into several segments, creating islands that isolate the affected assets and at the same time minimise the power imbalance while maintaining supply to the maximum number of consumers. IIM employs two different methods for calculating the islanding schemes, namely: (1) a genetic algorithm, which provides the optimal solution at the cost of increased time-complexity and (2) a deep learning architecture [31] which addresses the islanding problem by utilising graph convolutional neural networks, able to provide the solution in real-time.

3.3.3. EMO: rEstoration Machine-learning framewOrk

EMO acts as a modern energy restoration and management framework, incorporating procedures for restoring the electrical grid when there are failures, thus avoiding further damage to the EPES/SG infrastructure. Towards this goal, EMO continuously observes the grid status, aiming to identify islanding cases and automatically commences the required restoration and management processes, ensuring the real-time operation through the optimal allocation of the network capacity. In more detail, the key functionalities of this component are the following:

- Regulating the local variables of Distributed Energy Resources (DERs) (i.e., voltage and frequency), to achieve high power quality that leads to less losses and results in more robust islands in terms of load-balancing capabilities.
- Maintaining the stability of the electrical grid and balancing the available energy of the islands.
- Managing load shedding, including decisions on when, where, and how much load should be shed according to the priorities at each island, in order to mitigate the impact to the end-users.
- Computing the energy exchange feasibility within the islands, after receiving the trading requests from the Blockchain-based Energy Trading System.

At its core, EMO consists of two modules, the first responsible for the economic management of the power flow between the DERs and the second undertaking to control the voltage-reactive and the frequency-active power, based on a hybrid multi-agent system that optimally allocates the requested energy between the units.

3.3.4. Blockchain-Based Energy Trading System

The Blockchain-based Energy Trading System is placed on top of SDN-SELF and aims to secure transactions taking place among the islanded parts of the EPES/SG. In more detail, it consists of two modules, namely the e-auction module and the Blockchain-based Intrusion and Anomaly Detection (BIAD) module. The e-auction module establishes secure and trustworthy networks among the parties involved in energy transactions, including consumers and prosumers and Energy Service Company Organisations that manage the financial transactions. The Vickrey-Clarke-Groves (VCG) [47] mechanism is adopted by e-auction with the aim to reveal the actual valuations of the user's bids by concealing the bids submitted by other users. The communication among the participants is performed through a fabric blockchain network based on the Hyperledger Fabric. Finally, the status of each participating device (e.g., smart meters) is monitored by BIAD. In particular, BIAD constitutes an XL-SIEM detector, which monitors the integrity of the various logs, transmitting the corresponding security logs to XL-SIEM.

3.4. SDN Controller

The SDN-C undertakes to program the underlying intermediary network devices (i.e., SDN switches) according to the instructions from the Application Plane, using OpenFlow v1.3. Based on the `Ryu` SDN controller [48], the SDN-C is a multi-modular application that deploys multiple modules that extend the `Ryu` functionalities. In particular, SDN-C integrates the following new modules: (a) `simpleswitch_enhanced`, and (b) the `ZooClient` module. In more detail, the `simpleswitch_enhanced` module undertakes to re-actively fill the OpenFlow tables of the underlying SDN switches. In comparison to the original `Ryu` implementation, the enhanced reactive application of SDN-microSENSE keeps a record of source MAC addresses and ingress ports of Ethernet frames; therefore, the SDN-C can detect cases of broadcast storms and inserts the corresponding OpenFlow rules to prevent them. The loop-free topology relies on EDAE in order to apply optimisations and enable redundant paths. The SDN-C undertakes to program the underlying intermediary network devices (i.e., SDN switches) according to the instructions from the Application Plane, using OpenFlow v1.3. Based on the `Ryu` SDN controller [48], the SDN-C is a multi-modular application that deploys multiple modules that extend the `Ryu` functionalities. In particular, SDN-C integrates the following new modules: (a) `simpleswitch_enhanced`, and (b) the `ZooClient` module. In more detail, the `simpleswitch_enhanced` module undertakes to re-actively fill the OpenFlow tables of the underlying SDN switches. In comparison to the original `Ryu` implementation, the enhanced reactive application of SDN-microSENSE keeps a record of source MAC addresses and the ingress ports of Ethernet frames; therefore, the SDN-C can detect cases of broadcast storms and inserts the corresponding OpenFlow rules to prevent them. The loop-free topology relies on EDAE in order to apply optimisations and enable redundant paths.

4. SDN-microSENSE Use Cases and Implementation Considerations

SDN-microSENSE intends to address security and privacy requirements that cover the whole energy value chain, involving traditional electricity generators, Transmission System Operators (TSOs), Distribution System Operators (DSOs), DER operators and prosumers. The full potential of the proposed architecture is demonstrated and validated through six use cases/pilots that address various cybersecurity requirements in the area of EPES/SG:

- *Use Case 1 - Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES*: This use case deals with a variety of cybersecurity threats against substations, including station and process buses.
- *Use Case 2 - Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control*: This use case focuses on false-data injection attacks against the whole energy value chain, including generation (power plants), TSO and DSO substation architectures as well as smart metering infrastructures.
- *Use Case 3 - Large-scale Islanding Scenario Using Real-life Infrastructure*: The third use case treats the aftermath of a cyberattack or critical failure that results in an unbalanced grid. The SDN-microSENSE platform acts as a decision support system for the TSO in order to decide on intentionally islanding segments of the affected grid or to shed redundant load in order to balance energy demand and supply [49].
- *Use Case 4 - EPES Cyber-defence against Coordinated Attacks*: This use case aims to evaluate the SDN-microSENSE platform against the detection and mitigation of coordinated cyberattacks, taking place in substations.
- *Use Case 5 - Distribution Grid Restoration in Real-world PV Microgrids*: This use case deals with the detection and mitigation of cyberthreats occurring in the industrial network of a real photovoltaic station.

- *Use Case 6 - Realising Private and Efficient Energy Trading among PV Prosumers*: This use case realises the decentralized energy trading environment that SDN-microSENSE proposes, by involving PV prosumers.

Unarguably, the SDN technology is one of the main enablers that pave the way to a holistic cybersecurity solution that addresses detection and mitigation of cyberthreats. However, it should be noted that SDN introduces new organisational and technical challenges for potential end-users.

First of all, the required technologies (e.g., OpenFlow) require replacement or upgrade of the intermediary network equipment. On top of that, compatibility and vendor integration issues may arise due to vendor-specific implementations that deviate from the standards. Moreover, the IT personnel needs to have specialized knowledge on SDN in order to troubleshoot network issues caused by the SDN control. To sum up, despite its benefits on network management, SDN may introduce unforeseen technical and managerial complications, increase financial costs during adoption, and possibly be rejected by the management if the drawbacks outweigh the benefits [50].

Understanding the concerns of EPES/SG operators on ensuring business continuity, SDN-microSENSE intends to alleviate the drawbacks of SDN by providing unique optimisation and network security options (e.g., detection and isolation of cyberthreats at the access layer [51]), which would be unavailable without the SDN technology. Moreover, business continuity is ensured since the coordination of multiple SDN-Cs employed by SDN-microSENSE prevents the single point of failure caused by software failures or cyberattacks against the Controller Plane.

5. Conclusions

The rise of the IIoT transforms the typical EPES model into a new digital era, thus introducing multiple benefits. However, this progression creates severe cybersecurity and privacy issues. This paper presents the SDN-microSENSE architecture, which introduces a set of cybersecurity and privacy mechanisms based on the umbrella of the SDN technology. SDN-microSENSE defines three main frameworks: S-RAF, XL-EPDS and SDN-SELF. S-RAF applies a collaborative and dynamic risk assessment, thus determining the risk related to each security event and alert. The security events and alerts are generated by XL-EPDS via advanced intrusion detection and correlation mechanisms. Finally. SDN-SELF introduces a set of mitigation and energy management actions that can ensure the normal operation of the EPES/SG organisations.

Author Contributions: Conceptualization, P.R.G., P.S., C.D., T.L.; Methodology. I.L.P., R.T.B., R.D.; Software, P.R.G., P.S., C.D., Y.S., G.E., T.L., A.S. (Achilleas Sesis), A.S. (Antonios Sarigiannidis), R.T.B., D.P., S.A.M., G.L., A.P., T.K., A.D., O.M., A.C.S., P.P.S., J.L.D.-G., M.E., M.M.A., B.C., F.R.; Investigation, P.R.G., P.S., C.D., Y.S., G.E., T.L., A.S. (Achilleas Sesis), A.S. (Antonios Sarigiannidis), R.T.B., D.P., S.A.M., G.L., A.P., T.K., A.D., O.M., A.C.S., P.P.S., J.L.D.-G., M.E., M.M.A., B.C., F.R.; Validation, V.G., S.K., H.C.B., D.-E.A., R.G.; Resources, N.P.; Writing—Original Draft Preparation, P.R.G., C.D., Y.S.; Writing—Review & Editing, P.R.G., C.D., Y.S., T.R.; Supervision, P.S., T.L.; Project Administration, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833955.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833955.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ABOD	Angle-Based Outlier Detection
ADT	Attack Defence Tree
APT	Advanced Persistent Threat
BIAD	Blockchain-based Intrusion and Anomaly Detection
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAS	Distribution Automation System
DDoS	Distributed Denial-of-Service
DERs	Distributed Energy Resources
DNP3	Distributed Network Protocol 3
DSO	Distribution System Operator
EDAE	Electric Data Analysis Engine
EMO	rEstoration Machine-learning framewOrk
EPES	Electrical Power and Energy Systems
GOOSE	Generic Object Oriented Substation Event
HM	Honeypot Manager
ICD	Intelligent Capability Description
ICS	Industrial Control System
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IIM	Islanding and optImisation fraMework
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LOF	Local Outlier Factor
MAC	Medium Access Control
MISP	Malware Information Sharing Platform
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NIS	Network and Information System
NLP	Natural Language Processing
NTP	Network Time Protocol
ONF	Open Networking Foundation
OPF	Overlay Privacy Framework
OVS	Open vSwitch
PCA	Principal Component Analysis
PDC	Phase Data Concentrator
PMU	Phasor Measurement Unit
QoS	Quality of Service
RFC	Request for Comments
SCADA	Supervisory Control and Data Acquisition
SCS	Synchronisation and Coordination Service
SDN	Software-Defined Networking
SDN-C	SDN Controller
SDN-SELF	SDN-enabled Self-healing Framework
SG	Smart Grid
SIEM	Security Information and Event Management
SOS	Stochastic Outlier Selection
S-RAF	SDN-microSENSE Risk Assessment Framework
SVM	Support Vector Machine
TCP	Transmission Control Protocol
TSO	Transmission System Operator
VCG	Vickrey-Clarke-Groves
XL-EPDS	Cross-Layer Energy Prevention and Detection System

References

1. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of security advances in smart grid: A data driven approach. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 397–422. [CrossRef]
2. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1851–1877. [CrossRef]
3. Stellios, I.; Kotzanikolaou, P.; Psarakis, M. Advanced persistent threats and zero-day exploits in industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 47–68.
4. Di Pinto, A.; Dragoni, Y.; Carcano, A. TRITON: The First ICS Cyber Attack on Safety Instrument Systems. In Proceedings of the Black Hat USA, Mandalay, LV, USA, 4–9 August 2018; Volume 2018, pp. 1–26.
5. Radoglou-Grammatikis, P.; Siniosoglou, I.; Liatifis, T.; Kourouniadis, A.; Rompolos, K.; Sarigiannidis, P. Implementation and Detection of Modbus Cyberattacks. In Proceedings of the 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 7–9 September 2020; pp. 1–4.
6. Darwish, I.; Igbe, O.; Saadawi, T. Vulnerability Assessment and Experimentation of Smart Grid DNP3. *J. Cyber Secur. Mobil.* **2016**, *5*, 23–54. [CrossRef]
7. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Giannoulakis, I.; Kafetzakis, E.; Panaousis, E. Attacking IEC-60870-5-104 SCADA Systems. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; Volume 2642, pp. 41–46.
8. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
9. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
10. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
11. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 746–789. [CrossRef]
12. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R.; Leung, H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* **2019**, *7*, 80778–80788. [CrossRef]
13. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
14. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
15. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2637–2670. [CrossRef]
16. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
17. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Liatifis, T.; Apostolakos, T.; Oikonomou, S. An overview of the firewall systems in the smart grid paradigm. In Proceedings of the 2018 Global information infrastructure and networking symposium (GIIS), Thessaloniki, Greece, 23–25 October 2018; pp. 1–4.
18. Li, E.; Kang, C.; Huang, D.; Hu, M.; Chang, F.; He, L.; Li, X. Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees. *Information* **2019**, *10*, 251. [CrossRef]
19. Johnson, P.; Lagerström, R.; Ekstedt, M.; Franke, U. Can the common vulnerability scoring system be trusted? a bayesian analysis. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 1002–1015. [CrossRef]
20. Rios, E.; Rego, A.; Iturbe, E.; Higuero, M.; Larrucea, X. Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees. *Sensors* **2020**, *20*, 4404. [CrossRef] [PubMed]
21. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Sarigiannidis, A.; Margounakis, D.; Tsiakalos, A.; Efstathopoulos, G. An Anomaly Detection Mechanism for IEC 60870-5-104. In Proceedings of the 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 7–9 September 2020; pp. 1–4.
22. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Karypidis, P.A.; Sarigiannidis, A. DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, 25–28 August 2020; pp. 1–8.
23. Tsoukalos, M. Using tshark to watch and inspect network traffic. *Linux J.* **2015**, *2015*, 1.
24. Habibi Lashkari, A.; Draper Gil, G.; Mamun, M.S.I.; Ghorbani, A.A. Characterization of Tor Traffic using Time based Features. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 19–21 February 2017; SCITEPRESS—Science and Technology Publications: Porto, Portugal, 2017; pp. 253–262. [CrossRef]
25. Manso, P.; Moura, J.; Serrão, C. SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. *Information* **2019**, *10*, 106. [CrossRef]
26. Pfaff, B.; Pettit, J.; Koponen, T.; Jackson, E.; Zhou, A.; Rajahalme, J.; Gross, J.; Wang, A.; Stringer, J.; Shelar, P.; et al. The Design and Implementation of Open vSwitch. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*; USENIX Association: Oakland, CA, USA, 2015; pp. 117–130.

27. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Iturbe, E.; Rios, E.; Martinez, S.; Sarigiannidis, A.; Eftathopoulos, G.; Spyridis, I.; Sesis, A.; Vakakis, N.; et al. SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Comput. Netw.* **2021**, *193*, 108008. [CrossRef]
28. Efstathopoulos, G.; Grammatikis, P.R.; Sarigiannidis, P.; Argyriou, V.; Sarigiannidis, A.; Stamatakis, K.; Angelopoulos, M.K.; Athanasopoulos, S.K. Operational data based intrusion detection system for smart grid. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; pp. 1–6.
29. Lazaridis, G.; Papachristou, K.; Drosou, A.; Ioannidis, D.; Chatzimisios, P.; Tzovaras, D. On the Potential of SDN Enabled Network Deployment in Tactical Environments. In *IFIP Advances in Information and Communication Technology*; Springer: Berlin/Heidelberg, Germany, 2021, pp. 252–263.
30. Charalampos-Rafail, M.; Thanasis, K.; Vasileios, V.; Dimosthenis, I.; Dimitrios, T.; Panagiotis, S. Cyber Attack Detection and Trust Management Toolkit for Defence-Related Microgrids. In *IFIP Advances in Information and Communication Technology*; Springer: Springer: Berlin/Heidelberg, Germany, 2021; pp. 240–251.
31. Sun, Z.; Spyridis, Y.; Lagkas, T.; Sesis, A.; Efstathopoulos, G.; Sarigiannidis, P. End-to-End Deep Graph Convolutional Neural Network Approach for Intentional Islanding in Power Systems Considering Load-Generation Balance. *Sensors* **2021**, *21*, 1650. [CrossRef]
32. Ivanova, A.; Paradell, P.; Domínguez-García, J.L.; Colet, A. Intentional Islanding of Electricity Grids Using Binary Genetic Algorithm. In Proceedings of the 2020 2nd Global Power, Energy and Communication Conference (GPECOM), Izmir, Turkey, 20–23 October 2020; pp. 297–301.
33. Leshem, S.; Trafford, V. Overlooking the conceptual framework. *Innov. Educ. Teach. Int.* **2007**, *44*, 93–105. [CrossRef]
34. *SDN Architecture*; Technical Report for SDN ARCH 1.0 06062014; Open Networking Foundation: Palo Alto, CA, USA, 2014.
35. Overview of RFC7426: SDN Layers and Architecture Terminology–IEEE Software Defined Networks. Available online: https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology (accessed on 27 April 2021).
36. Holz, T.; Raynal, F. Detecting honeypots and other suspicious environments. In Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 15–17 June 2005; pp. 29–36.
37. Diamantoulakis, P.; Dalamagkas, C.; Radoglou-Grammatikis, P.; Sarigiannidis, P.; Karagiannidis, G. Game Theoretic Honeypot Deployment in Smart Grid. *Sensors* **2020**, *20*, 4199. [CrossRef] [PubMed]
38. Kotsiopoulos, T.; Sarigiannidis, P.; Ioannidis, D.; Tzovaras, D. Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm. *Comput. Sci. Rev.* **2021**, *40*, 100341. [CrossRef]
39. Markopoulou, D.; Papakonstantinou, V.; de Hert, P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Comput. Law Secur. Rev.* **2019**, *35*, 105336. [CrossRef]
40. Qu, Y.; Liu, X.; Jin, D.; Hong, Y.; Chen, C. Enabling a Resilient and Self-healing PMU Infrastructure Using Centralized Network Control. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Tempe, AZ, USA, 21 March 2018; ACM: Tempe, AZ, USA, 2018; pp. 13–18. [CrossRef]
41. Pham, T.A.Q.; Hadjadj-Aoul, Y.; Outtagarts, A. Deep reinforcement learning based qos-aware routing in knowledge-defined networking. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 14–26.
42. Rezaee, M.; Yaghmaee Moghaddam, M.H. SDN-Based Quality of Service Networking for Wide Area Measurement System. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3018–3028. [CrossRef]
43. Hong, J.B.; Yoon, S.; Lim, H.; Kim, D.S. Optimal Network Reconfiguration for Software Defined Networks Using Shuffle-Based Online MTD. In Proceedings of the 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26–29 September 2017; pp. 234–243. [CrossRef]
44. Wang, M.; Liu, J.; Mao, J.; Cheng, H.; Chen, J.; Qi, C. RouteGuardian: Constructing secure routing paths in software-defined networking. *Tsinghua Sci. Technol.* **2017**, *22*, 400–412. [CrossRef]
45. Mambrini, A.; Izzo, D. PaDe: A Parallel Algorithm Based on the MOEA/D Framework and the Island Model. In *Parallel Problem Solving from Nature – PPSN XIII*; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 711–720. [CrossRef]
46. Izzo, D.; Ruciński, M.; Biscani, F. The Generalized Island Model. In *Parallel Architectures and Bioinspired Algorithms*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 151–169. [CrossRef]
47. Sessa, P.G.; Walton, N.; Kamgarpour, M. Exploring the Vickrey-Clarke-Groves Mechanism for Electricity Markets. *IFAC-PapersOnLine* **2017**, *50*, 189–194. [CrossRef]
48. Ryu SDN Framework. Available online: https://ryu-sdn.org/ (accessed on 6 July 2021).
49. Towards Securing Large-Scale Grid Interconnection Infrastructures—SDN microSENSE. Available online: https://www.sdnmicrosense.eu/ (accessed on 7 July 2021).
50. Sokappadu, B.; Hardin, A.; Mungur, A.; Armoogum, S. Software Defined Networks: Issues and Challenges. In Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp), Mauritius, 19–21 September 2019; pp. 1–5. [CrossRef]
51. Campus Network for High Availability Design Guide. Available online: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html (accessed on 7 July 2021).